energies

Article

Intelligent Energy Management Systems in Industry 5.0: Cybersecurity Applications in Examples

Barbara Wyrzykowska [1,*], Hubert Szczepaniuk [1], Edyta Karolina Szczepaniuk [2], Anna Rytko [3] and Marzena Kacprzak [3]

[1] Institute of Management, Warsaw University of Life Sciences—SGGW, Nowoursynowska 166 St., 02-787 Warsaw, Poland; hubert_szczepaniuk@sggw.edu.pl
[2] Polish Air Force University, Dywizjonu 303 Street No. 35, 08-521 Dęblin, Poland; e.szczepaniuk@law.mil.pl
[3] Institute of Economics and Finance, Warsaw University of Life Sciences—SGGW, Nowoursynowska 166 St., 02-787 Warsaw, Poland; anna_rytko@sggw.edu.pl (A.R.); marzena_kacprzak@sggw.edu.pl (M.K.)
* Correspondence: barbara_wyrzykowska@sggw.edu.pl

Abstract: The article examines modern approaches to energy management in the context of the development of Industry 5.0 with a particular focus on cybersecurity. Key tenets of Industry 5.0 are discussed, including the integration of advanced technologies with intelligent energy management systems (IEMSs) and the growing need to protect data in the face of increasing cyber threats. The challenges faced by small and medium-sized enterprises (SMEs) using solutions based on renewable energy sources, such as photovoltaic farms, are also analyzed. The article presents examples of IEMS applications and discusses methods for securing these systems, offering an overview of cyber threat protection tools in the context of modern energy management. The analysis carried out provided information that will help businesses make rational decisions and contribute to shaping the state's macroeconomic policy on cybersecurity and energy savings. The results of this research can also help develop more effective strategies for managing technology and IT infrastructure, which is crucial in the digital age of Industry 5.0.

Keywords: intelligent energy management systems; Industry 5.0; cybersecurity; attack vectors; artificial intelligence algorithms

check for updates

Citation: Wyrzykowska, B.; Szczepaniuk, H.; Szczepaniuk, E.K.; Rytko, A.; Kacprzak, M. Intelligent Energy Management Systems in Industry 5.0: Cybersecurity Applications in Examples. *Energies* **2024**, *17*, 5871. https://doi.org/10.3390/en17235871

Academic Editor: Brian D. Fath

Received: 8 October 2024
Revised: 11 November 2024
Accepted: 20 November 2024
Published: 22 November 2024

1. Introduction

The energy transition and rising energy prices are driving up operating costs for companies, which are responding by trying to reduce them through the use of in-house energy production and the implementation of intelligent energy management systems (IEMSs). These systems in Industry 5.0 are a key element of modern manufacturing strategies that combine advanced technologies with the idea of sustainability [1,2]. Unlike previous stages of industrial revolutions, Industry 5.0 focuses on the harmonious interaction between humans and machines, with an emphasis on personalizing production, optimizing processes and minimizing environmental impact [3,4]. Energy management systems, based on artificial intelligence, data analysis and automation, allow the real-time monitoring and control of energy consumption. This not only reduces operating costs but also increases energy efficiency and reduces carbon emissions, which is important for meeting environmental goals. In Industry 5.0, these systems are becoming smarter and more integrated, enabling businesses to adapt their energy strategies to dynamically changing market and technological conditions [5]. With the implementation of new technologies and energy management systems, the issue of cybersecurity has emerged, and the protection of data and computer systems has become a key part of any company's operations. In particular, the Industry 5.0 paradigm has specific features and conditions that have a significant impact on cybersecurity.

It should be emphasized that cybersecurity is a key aspect in ensuring business continuity and the integrity of modern energy systems. This is especially important in the context of the developing smart grid paradigm, which cannot function properly without ensuring cybersecurity. One of the components of the smart grid is IEMSs, which dynamically control the energy flow and implement digital data exchange between stakeholders involved in energy exchange processes. For this reason, ensuring the cybersecurity of energy systems is essential to maintaining operational continuity, reliability, and the stability of energy flow. This article theoretically analyzes selected conditions of cybersecurity of IEMSs starting from the concept of cyber-physical systems (CPSs). The analyses took into account threats to information security attributes for modern energy systems, such as malware attacks, ransomware attacks, DDoS attacks and vulnerabilities of SCADA, IoT and CPSs. In the next research step, methods of ensuring cybersecurity of energy systems were analyzed with particular emphasis on IDS/IPS intrusion detection systems, blockchain technology and artificial intelligence algorithms.

Energy transformation and the provision of cybersecurity present significant challenges for small and medium-sized enterprises [6–9]. In order to identify the main issues related to energy management systems, cybersecurity and methods to protect against cyber threats, the article presents a case study of two companies in the food distribution industry. Moreover, interviews were conducted with the management of 17 companies, including two that were subjected to in-depth analysis. The exploration of these aspects was relevant in the context of technological and energy changes in the era of Industry 5.0.

There were two main objectives of the article: to assess the determinants and challenges of energy management and cybersecurity in the context of Industry 5.0 with a focus on energy management systems (EMSs) in small and medium-sized enterprises (SMEs) using photovoltaic farms and to identify methods of protection against cyber threats.

In the context of energy management and cybersecurity in Industry 5.0, key considerations include access to modern technologies, regulations, as well as the level of awareness among enterprises about cyber threats and the benefits of energy efficiency. Enterprises face challenges in integrating new solutions, such as EMSs that enable the monitoring and optimization of energy consumption. For SMEs, these considerations are often more complex due to limited financial, technological and human resources, which can make it difficult to implement innovative solutions and cyber protection. The identification of methods to protect against cyber threats in the surveyed companies included risk analysis and the implementation of appropriate security tools such as intrusion detection systems, data encryption and regular employee training. Effective energy management, especially with the use of photovoltaic farms, involved the implementation of technologies to regulate energy consumption and minimize energy losses.

The remainder of the article is structured as follows. Section Two presents the research methodology, and then Section Three presents Industry 5.0 as a new era of industrial transformation, highlighting the benefits of a human-centric approach in optimizing energy management. The following fourth point focuses on the challenges of cybersecurity in EMSs and methods to protect against threats. The fifth section presents examples of the practical application of EMSs and methods of protection against cyber threats in SMEs. The next section of the paper concerns the discussion in which we compare our research findings with the results of other studies. The article concludes with a summary and conclusions of the research. Recommendations for companies are also offered, and potential directions for future research on cybersecurity in smart energy systems are indicated.

2. Materials and Methods

The main research objective defined in the Introduction was divided into the following specific objectives:

1. Outlining the key concepts, features and assumptions of a new phase of industrial development called Industry 5.0 in the context of energy management.

2. Theoretical recognition of cybersecurity issues for IEMSs, including threats and protection methods.
3. An assessment of the advantages and disadvantages of EMSs used in small and medium-sized enterprises using photovoltaic farms.
4. Practical identification of key cybersecurity issues in SMEs.
5. Identification of EMS protection methods in the companies surveyed.

The above-defined specific research objectives directly determine the structure of the article. This means that subsequent sections of the paper correspond to the specific objectives.

The research presented in the paper is of a theoretical and empirical nature. Such a research framework favors a holistic and synergistic approach to the cybersecurity of intelligent energy systems. In the theoretical section, the research method regarding the analysis and synthesis of the subject literature as well as the deductive and inductive methods used is described. The aim of the theoretical research was to build a conceptual framework for the empirical section. The research background is Industry 5.0 with particular emphasis on its paradigms and key IT technologies in the context of energy management. In turn, the cybersecurity of smart energy systems required theoretical analysis in terms of threats and countermeasures. In particular, multi-factor analysis of information security attributes for key components of modern energy systems such as SCADA, IoT and CPSs was crucial.

The empirical research had both a quantitative and qualitative dimension. The diagnostic survey method was used in this part of the research. The primary research technique was interviews, while the research tool was interview questionnaires. The empirical research comprised 17 interviews with executives of companies that have undertaken energy transition activities and encountered cybersecurity issues.

The study was divided into two stages. In order to identify the main issues related to energy measures in SMEs, the first stage involved an analysis of two representative food distribution companies that had chosen to use renewable energy to reduce rising energy costs. In the second stage, interviews were conducted with executives in a total of 17 companies (including the two previously surveyed). The interviews focused on the energy management systems used, cybersecurity threats and methods to protect data and IT systems. To avoid publicity, the article does not mention the names of the PV panels installed in the companies analyzed and the names of the monitoring applications offered by PV module manufacturers. Interviews lasted between 15 min and 1 h, during which the following questions were asked:

1. Why was it decided to install photovoltaic systems?
2. Have intelligent energy management systems been used?
3. What data on energy consumption were monitored?
4. What were the indicators analyzed in relation to this?
5. Have attempts at unauthorized access to computer network resources been detected and prevented in the recent period?
6. Were any techniques used to counter cyberattacks?
7. How important is cybersecurity to the functioning of a company?
8. What are the opinions and suggestions on energy management systems and cybersecurity?

Figure 1 shows the adopted research algorithm.

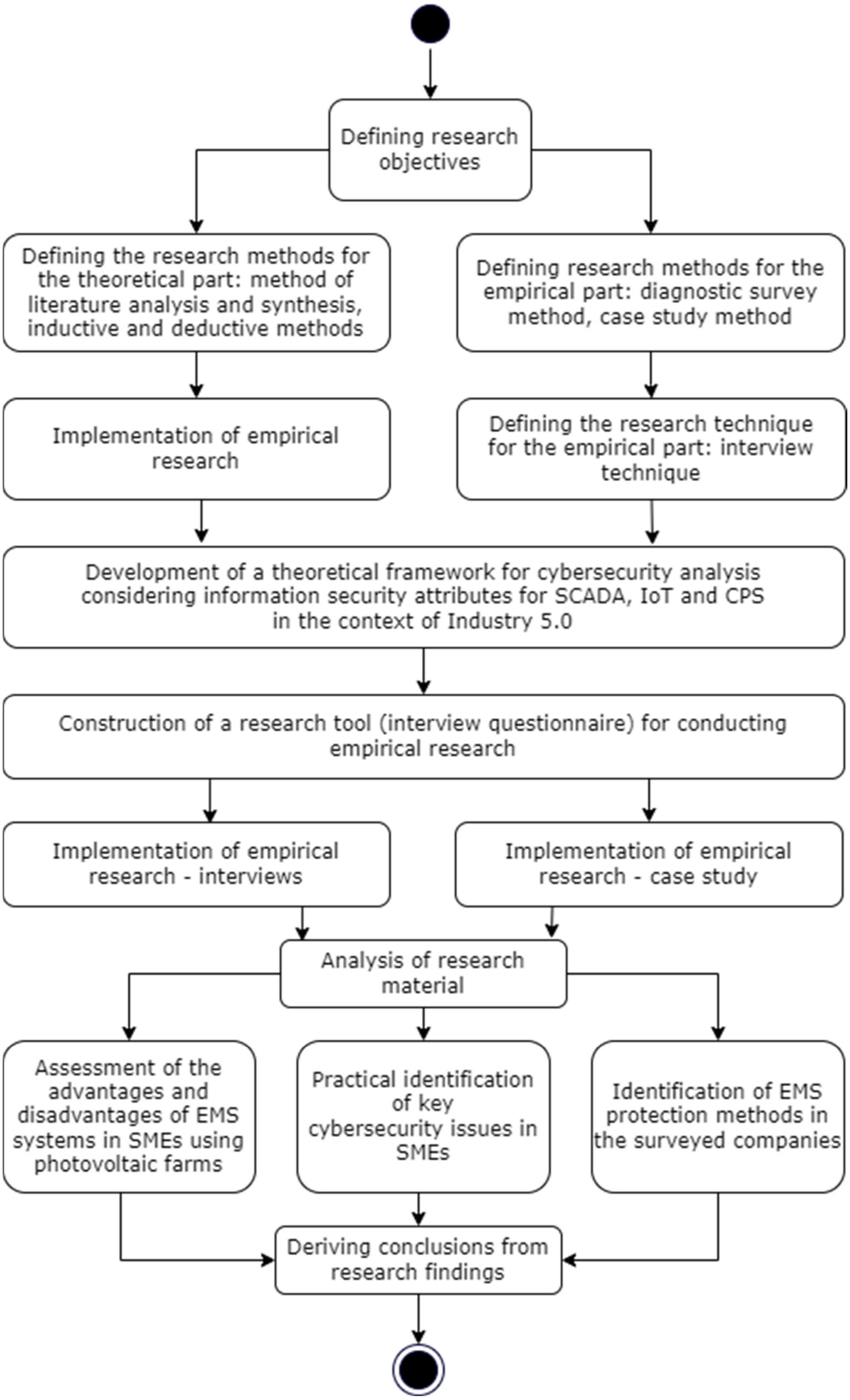
Defining research objectives
Defining the research methods for the theoretical part: method of literature analysis and synthesis, inductive and deductive methods
Defining research methods for the empirical part: diagnostic survey method, case study method
Implementation of empirical research
Defining the research technique for the empirical part: interview technique
Development of a theoretical framework for cybersecurity analysis considering information security attributes for SCADA, IoT and CPS in the context of Industry 5.0
Construction of a research tool (interview questionnaire) for conducting empirical research
Implementation of empirical research - interviews
Implementation of empirical research - case study
Analysis of research material
Assessment of the advantages and disadvantages of EMS systems in SMEs using photovoltaic farms
Practical identification of key cybersecurity issues in SMEs
Identification of EMS protection methods in the surveyed companies
Deriving conclusions from research findings

Figure 1. Research algorithm. Source: own work.

3. Industry 5.0: A New Era of Industrial Transformation in The Energy Sector

3.1. Definitions and Assumptions

The term Industry 5.0 emerged at the beginning of 2015, but it has been called the fifth industrial revolution because of the speed of introduction of new industrial technologies, technical improvements and the change in the integration of human processes. Industry 5.0 is intended to respond to the changing reality and its challenges [10–12]. Unlike Industry 4.0, which prioritizes automation and digitization to increase productivity, Industry 5.0 places a strong emphasis on human involvement. Focusing on sustainability and flexibility, it seeks to strike a balance between technology and human labor [13,14]. Industry 5.0 is developing in various fields such as healthcare, manufacturing, textiles, education, food, energy and others [15,16].

Industry 5.0 is a construct that fits well with the political agenda pursued by the European Union. It combines new technologies and digitalization with a pro-environmental approach, a circular economy and the creation of an 'ecosystem' of companies and partners [17]. The basic assumptions of Industry 5.0 are included in the report Industry 5.0—Towards a sustainable, human centric and resilient European industry, which is the fruit of two debates held during a virtual workshop in 2020 organized by the Prosperity Directorate of the Directorate-General for Research and Innovation. The meetings were attended by representatives of R&D institutes and funding agencies from across Europe. In 2021, the European Commission formally called for a fifth industrial revolution (Industry 5.0) [18].

The core principles of Industry 5.0 are human-centered, sustainability and resilience [12,19]. The human-centered approach puts basic human needs and interests at the center of the production process, moving from a technology-driven progression to an approach that is entirely focused on people and society. This concept assumes the ability of industry to achieve social goals [20–22].

Industry 5.0 sustainability is an approach that involves the use of modern technologies to minimize negative environmental impacts. The development of production systems based on renewable energy sources is one of the postulates of Industry 5.0. The European Commission indicates in its report that reducing carbon emissions by 55% by 2030 requires a sustainable industry [17]. For this reason, it recommends the development of processes that enable the reuse and recycling of natural resources, reduce waste and reduce environmental impact [12,18]. Other sustainability developments include reducing energy consumption, greenhouse gas emissions and waste, and avoiding the depletion and degradation of natural resources [23–25].

Moving toward a green and resilient industry—including the need to pay particular attention to resilience and sustainability, in addition to profitability, is part of the European Commission's work on the Industry 5.0 concept [17,18]. In its report, the European Commission points out that industry is vulnerable to various geopolitical turbulences and natural disasters. It is therefore imperative that it be made resilient to them. Resilience is one of the factors playing a key role in tackling climate change. It is linked to the operation of businesses in a turbulent technological, economic and geopolitical environment. Resilient industries are those that are able to cope with uncertainty, economic downturns, technological change and other challenges, continually innovating and driving the economy forward. This pillar became crucial after the outbreak of the COVID-19 pandemic.

The concept promoted by the European Commission is, in a way, complementary to the philosophy of Industry 4.0. This new approach implies the development of industry toward a production model focused not only on technological innovation and economic growth but also on responsible ecological practices. The premise of Industry 5.0 is also to promote collaboration between businesses, scientific institutions and governments to jointly create innovative solutions for the future. This shift also implies a greater role for humans in production processes rather than seeking to replace them with machines, which emphasizes the human dimension and value in modern production and energy systems [17].

3.2. Industry 5.0 Without Energy Loss

Technological progress is accelerating with new carbon-neutral technologies emerging. Examples of promising new technologies and solutions that can help to achieve fossil fuel free energy are electrification, closed loop, industrial symbiosis, renewable energy solutions, batteries, hydrogen, carbon capture, utilization and storage, energy storage, power-to-x technologies, electro-fuels, smart manufacturing using sensors, connected machines, AI and data analytics [1,12,15,26]. What differentiates Industry 5.0 from Industry 4.0 is the particular emphasis on energy efficiency of enterprises. The fifth industrial revolution emphasizes sustainable production, focusing on energy efficiency, the use of renewable energy and self-sufficiency [12,18,20]. This is a particularly important aspect at a time when energy is becoming a critical resource and the costs associated with it are successively increasing. Better energy management is needed to optimize energy consumption during production. Industry 5.0 uses advanced tools (for example, the Internet of Things (IoT), artificial intelligence (AI) and data analytics) to control energy consumption at every stage of production. The implementation of modern digital technologies in integration with internal and external systems for ESG or CO_2 reporting and data sources (internal and external) brings, among other benefits, the following [1,20,21]:

- Reducing energy waste: IoT sensors enable the real-time monitoring and analysis of energy consumption, allowing energy waste to be quickly identified and eliminated.
- Cost optimization: Solutions based on artificial intelligence make it possible to predict energy needs and automate processes, increasing efficiency and reducing costs.
- Increased operational efficiency: The cloud model, in which modern business management systems operate, is perfectly equipped to handle the sudden increase in computing power needed by companies during higher production or sales demands. Scaling up in the cloud is a matter of just a few clicks.
- Better insight into the operation of the business: By using IoT technology, it is possible to monitor production parameters in real time and act immediately if alarm thresholds are exceeded. This enables more informed decision making when unplanned events occur, leading to savings in production costs, energy and time.

Industrial Internet of Things (IIoT) solutions that are revolutionizing the way energy is monitored and the cost of energy utilities are IEMSs. As energy management software, they provide control over the consumption of energy and other utilities in production. With measurements and calculations available in real time, it is easy to pinpoint deviations from the norm, losses and areas where energy consumption can be optimized.

3.3. Challenges for Industry 5.0

Key technologies such as robotization, artificial intelligence (AI) and big data are opening up new opportunities for businesses, but they also present numerous challenges [12,16,20,27]:

1. People are required to develop competency skills because, when working with advanced robots, employees need to gain knowledge about working with an intelligent machine and a robot manufacturer. In addition to the required soft skills, acquiring technical skills is also an issue for employees. Programming an industrial robot and managing translation in new workplaces are challenging tasks that require a high level of technical skills. In the era of Industry 5.0, employees must not only have technical skills but also adaptability and the ability to work in a dynamically changing environment. Companies need to invest not only in technology but also in the development of employee competencies.
2. Adopting advanced technology requires more time and effort from workers. Adapted smart factories connected by software, collaborative robotics, artificial intelligence, real-time information and the Internet of Things must be adopted in Industry 5.0.
3. Advanced technologies require investment. Training employees for new positions entails additional costs. Companies find it difficult to upgrade production lines for

Industry 5.0. Adopting Industry 5.0 is costly because it requires smart machines and highly skilled workers to increase productivity and efficiency.

4. Security is a challenge for Industry 5.0, as establishing trust in ecosystems is key. Authentication is used in the industry to interact with various devices to counter future quantum computing applications to deploy IoT nodes. The use of artificial intelligence and automation in Industry 5.0 poses a threat to business, so trusted security is required. Industry 5.0 applications focus on ICT systems and therefore lead to strict security requirements to prevent security challenges.

As Industry 5.0 increases the connectivity and proliferation of devices, the need for robust data protection is growing. The interconnectivity inherent in Industry 5.0 requires collaboration between cybersecurity and IT teams to meet security requirements and operational constraints. Manufacturers need to proactively incorporate cybersecurity as a core component of modern devices, increasing the operational resilience of Industry 5.0 against potential cyberattacks [27,28].

3.4. Cybersecurity in the Face of New Challenges—EMS in Industry 4.0 and 5.0

The guidelines for cybersecurity in Industry 5.0 focus on minimizing the risks associated with an expanded number of connected devices and a new approach to human-machine collaboration. Key aspects include the following:

1. Increased attack surface: In Industry 5.0, EMSs have to operate in an even more complex ecosystem where technologies are not only integrated within the factory floor but also with the social environment, employees and energy and raw material suppliers. There is therefore an increased need to protect employees' personal data and privacy, which creates new risks for EMSs. The expanded focus on sustainability and collaboration with large-scale energy management systems, e.g., through integration with smart grid networks, expands the area of exposure to attacks [29].
2. Data security and privacy: With the increasing amount of data generated and processed by complex production systems, maintaining data privacy and integrity is a priority. Introducing strong authentication and data encryption mechanisms, as well as network segmentation, is key [30].
3. Human–machine integration: Due to the increase in human–machine interaction, safeguards against social engineering attacks and training employees to recognize threats are important. Employees need to be aware of potential threats and able to react quickly to anomalies [31].
4. Resilience to attacks: An additional challenge is to ensure that ESMs in Industry 5.0 are resilient not only to traditional hacking attacks but also to energy disruption attacks that can affect production continuity and critical industrial processes. In Industry 5.0, the integration of EMSs with autonomous systems and artificial intelligence also requires protection against threats arising from the possible manipulation of algorithms, which can result in erroneous decisions related to energy distribution and storage [32].
5. Regulatory compliance: The European Union is introducing regulations, such as the Cyber Resilience Act and the NIS2 Directive, which aim to establish cybersecurity standards in organizations, particularly in critical infrastructure sectors [33].

For manufacturers aiming to meet Industry 5.0 cybersecurity standards, the guidelines suggest a two-pronged approach: integrating cybersecurity directly into new hardware and upgrading legacy systems with modern security features such as firewalls, advanced authentication and data management with encryption. Industry 5.0 therefore relies on a more comprehensive approach to cybersecurity [29,34]. Table 1 shows the cybersecurity guidelines for energy management systems (EMSs) in Industry 4.0 and 5.0.

Table 1. Cybersecurity guidelines for energy management systems in Industry 4.0 and 5.0.

Security Aspects	Industry 4.0	Industry 5.0
Integration of technologies	Integration of EMSs into automation and control systems	Extended integration with external technologies, the community, employees and energy suppliers
Key challenges of cybersecurity	Securing IoT and industrial control systems (ICSs)	Protection of privacy and personal data, securing EMSs against disruptive attacks
Scope of protection	Protection inside the production facility	Protection across a broad ecosystem, including integration with smart grid systems
Resilience requirements	Basic protection against external attacks	Requirement to be resilient to power outages and manipulation by autonomous systems and AI algorithms
Security technologies	Standard encryption, network and remote access security	Advanced encryption, network segmentation, anomaly detection systems, AI-dedicated protection
Approach to security	Focus on digitization and process automation	Holistic approach, combining human–machine collaboration and resilience to a wide spectrum of disruptions

Source: Own elaboration based on research.

These guidelines show how cybersecurity requirements are changing in the context of the evolution from Industry 4.0 to 5.0 with a focus on greater integration, the protection of personal data and the complexity of the industrial ecosystem [34,35]. It is worth noting that Industry 5.0 places greater emphasis on collaboration with the environment and resilience to threats, requiring more advanced protection strategies. The digital transformation of businesses requires an innovative approach to data and infrastructure protection. In the face of threats, companies need to take a holistic approach to data protection. Thus, regular risk assessments, clear security policies and advanced technologies will allow for effective risk management and rapid response to threats [36].

4. Cybersecurity Issues of Intelligent Energy Management Systems

The cybersecurity guidelines for energy management systems in Industry 5.0 highlighted in Table 1 require technical analysis in relation to computer science and security science. It should be emphasized that technical and engineering issues of cybersecurity are determinants of the integrity and continuity of modern energy systems embedded in the computer network environment. It is also crucial that security sciences postulate a holistic approach to the issue of cybersecurity, which is consistent with the requirements of Industry 5.0. Table 1 shows that the key issues include, among others, the extended integration of external technologies in energy ecosystems, data privacy protection, resilience to power outages, protection based on anomaly detection using AI algorithms, and applications of the distributed ledger in the cybersecurity of IEMSs.

It is therefore indisputable that next-generation digital threats and the crucial importance of energy systems as elements of critical infrastructure pose new challenges to IEMSs. In particular, the implementation of IoT technologies and CPSs in the energy sector generates a number of new vulnerabilities. Intelligent energy systems process large amounts of data on many characteristics, including system performance, load profiles, and user behavior [37]. Security breaches and the interception of confidential information may lead to disruptions in energy supplies, damage to infrastructure, or even a complete failure of the energy system [37].

It is crucial to emphasize that cybersecurity is an interdisciplinary issue, requiring coordinated actions at many levels, including technological, legal, organizational, procedural and social [38]. Energy systems include a physical layer, which is the carrier of electrical energy, and a cyber layer, which is understood as the carrier of data and information [39].

Based on these assumptions, the cybersecurity of modern energy systems can be considered from the perspective of CPS. This section focuses exclusively on the analysis of selected types of cyber threats. In the literature, cybersecurity is often considered in terms of three key attributes of information security: confidentiality, availability and integrity, e.g., [40–45]. For the purposes of this paper, confidentiality is understood as ensuring access to protected information sets processed in IEMSs only for authorized users and stakeholders. The availability attribute addresses the services of IEMSs and concerns the possibility of using them at the requested time. Integrity will be understood in two ways: broadly, as the functioning of IEMSs in accordance with their intended purposes, and more specifically, as the protection of information sets processed in IEMSs against unauthorized modifications. Among the many key areas of cybersecurity of IEMSs, the following issues were selected for theoretical analysis:

- Cybersecurity threats to intelligent energy management systems;
- Methods of protecting intelligent energy management systems;
- New technologies in the cybersecurity of intelligent energy management systems.

Concentrating theoretical research on the above-mentioned areas allows for the identification of contemporary challenges and threats to the cybersecurity of IEMSs as well as classic and new technology-oriented protection methods.

4.1. Cybersecurity Threats to Intelligent Energy Management Systems

Since IEMSs include a cyber layer in addition to the physical layer, they are exposed to a number of threats that may have a direct impact on the indicated information security attributes. Critical cybersecurity threats to IEMSs include the following:

- Malware and ransomware attacks;
- DDoS attacks;
- Security vulnerabilities in SCADA, IoT and CPS systems.

Technically, malware and ransomware are types of computer software that contain malicious code that can infect IEMSs. Typically, the term malware is commonly used in a general context to describe a broad set of malicious software that is directed against an IT system or a user. The term ransomware is often used in the narrower context of software aimed at blocking access to a computer system often by encrypting files in order to extort a ransom from the user. Incidents related to malware and ransomware attacks on IEMSs can have critical consequences and directly translate into violations of confidentiality, availability and integrity attributes. Malware attacks on smart grids involve infecting the control system, the human–machine interface, compromising data integrity, disrupting system operations and, as a result, potentially gaining unauthorized control over critical infrastructure [46]. The attack vectors can be diverse. In particular, malware can enter the energy system via email, by a website, or through being intentionally or unknowingly installed by end users. Cen et al. [47] describe four phases of a ransomware attack: delivery and reconnaissance, attack instruction, destruction, and extortion demand. One of the key components of a smart grid is the advanced metering infrastructure (AMI), which allows operators to remotely manage devices in customers' homes [48]. AMI is responsible for collecting and analyzing data received from smart meters and manages energy-related applications and services based on the collected data [49]. Ghosal and Conti [49] pointed out that malicious adversaries have many opportunities to attack the AMI infrastructure because it consists of components that are highly vulnerable to such attacks.

In turn, DDoS attacks operating in the Internet domain are aimed at violating the availability attribute by blocking the operation of the IT system or its selected services. A characteristic feature of DDoS attacks is their distributed nature, in which the target server is attacked from a large number of remote computers by sending massive service requests. As a result, resources (CPU time, RAM, I/O operations) are exhausted, the server stops working and thus the service becomes unavailable. It should be noted that DDoS attacks do not require access to technical details such as read–write permissions, operational parameters or knowledge of the power grid topology [50]. As a result, a DDoS attack can lead to power outages, damage to infrastructure, and significant financial losses as well as a number of other threats. There are many different types of DDoS attacks on energy systems. In the environment of cyber-physical energy systems, it is possible to distinguish, among others, attacks aimed at causing the loss of observability of the power system and those aimed at preventing the controllability of devices through lack of response or delayed response [50]. It is also worth noting that DDoS attacks may be a preliminary stage followed by a proper network attack of another type, e.g., man-in-the-middle (MiTM).

Another category analyzed is cybersecurity threats to SCADA, IoT and CPSs, which are often an integral component of intelligent energy systems. Attacks on SCADA, IoT and CPS systems can in particular lead to a violation of the integrity attribute. An example of CPS applications in the smart grid could be phasor measurement units [51]. SCADA (Supervisory Control and Data Acquisition) systems are also key components of modern power networks. The general idea of SCADA systems is to use a central computer to store information on local or remote devices in order to control industrial processes and facilities [52]. SCADA systems are vulnerable to cyberattacks such as False Data Injection (FDI) of the measurement signal, which can bypass conventional detection methods and disrupt power grid operations [53]. Furthermore, SCADA systems are often based on the industrial Modbus communication protocol, which is focused on local area network applications [54]. The literature on the subject indicates that due to the current migration of SCADA systems from a strictly isolated network to the highly connected Internet, the Modbus protocol may present security risks in modern application scenarios [54]. Cyberattacks targeting SCADA systems aim to manipulate network operational control [55]. In particular, this may lead to damage to the power system by taking control of individual components controlled by SCADA systems, such as switches, isolators and relays [55]. It is emphasized that secure key exchange and management systems are crucial to ensuring the security of SCADA-based industrial control systems [56].

The theoretical analyses carried out constitute only a selected set of the cybersecurity threats faced by modern IEMSs. In connection with the analysis of cyber threats to IEMSs, adequate protection methods will be presented.

4.2. Methods of Protecting Intelligent Energy Management Systems in Cyberspace

Ensuring an acceptable level of cybersecurity of IEMSs requires a holistic strategy and coordinated actions. Modern computer science and security sciences have developed a variety of methods for countering cyber threats with the protection of the information security attributes analyzed in the paper. The basics of network security used to protect IEMSs include, among others, access control mechanisms, data encryption, firewalls and antivirus software. However, the key importance of IEMSs to society, the economy and national security requires the implementation of advanced cybersecurity mechanisms. The latest research findings in the field of cybersecurity of smart energy systems available in the literature on the subject focus, among others, on the applications of IDS/IPS systems, blockchain technology and artificial intelligence algorithms. The theoretical analysis of the indicated solutions in terms of the cybersecurity of IEMSs is presented below.

4.2.1. Intrusion Detection Systems

IDSs (intrusion detection systems) and IPSs (intrusion prevention systems) are key tools for the cybersecurity of computer networks. Their main purpose is to detect and prevent unauthorized access to computer network resources. The special feature of intrusion detection systems is the early detection of network attacks and the reduction in false alarms [57]. The general principle of intrusion detection systems is to monitor and analyze network traffic across various protocols and ports, identifying potential attack attempts on network resources. Upon detecting an attack, the system notifies network administrators. The available tools include signature-based intrusion detection systems. Signatures are a predefined database of patterns that contain sequences of bits typical of known network attacks. This allows the intrusion detection system to compare the traffic of monitored packets with the signature database and, on this basis, detect a potential attack. The limitation of such a solution may be the ability to detect only known types of attacks and limited effectiveness against new, unknown threats. The second type of intrusion detection system relies on anomalies to detect unusual activity or behavior in a computer network. Initially, the system establishes typical scenarios of activity and behavior in a computer network, taking into account a number of characteristics and parameters of network traffic. In a further step, the system monitors and analyzes network traffic to detect activity and behavior that deviates from established norms. The advantage of this type of system is the ability to detect new and unusual network attacks. A limitation may be a higher risk of false alarms.

The literature indicates that a conventional IDS may exhibit certain limitations due to the dynamic nature of communication networks in smart grids when the network generates highly dynamic traffic patterns in real time [58]. It is also pointed out that due to system security reasons and economic consequences, the implementation of an intrusion detection system in a smart grid environment is significantly difficult [58]. For this reason, researchers have sought to develop intrusion detection systems in such a way that they can be implemented in the IEMS environment to effectively defend against cyberattacks. For example, there are scientific studies that concern the application of machine learning in intrusion detection systems for the energy sector, e.g., [59–62]. The research results indicate that intrusion detection systems extended with machine learning mechanisms may have significant applications in ensuring the cybersecurity of modern energy systems.

It should also be noted that an intrusion detection system can be part of a broader cybersecurity strategy and act as a second line of defense in a communications network, reinforcing the performance of other protection mechanisms such as encryption and authentication [63].

4.2.2. Blockchain Technology

An innovative technology that has significant cybersecurity potential for IEMSs is blockchain (BC). From the point of view of computer science, BC is a distributed database that is built from blocks linked into a chain using cryptographic algorithms. The blockchain network is secured primarily through consensus algorithms, the main types of which are Proof-of-Work and Proof-of-Stake. The first type of algorithm is based on the computational power involved in securing the network by individual nodes. In turn, the second type of algorithm is based on evidence that individual nodes have a share in the network, which can be expressed by various characteristics depending on the implementation details of a given blockchain and algorithm. Individual types of algorithms are characterized by specific advantages and limitations in terms of energy efficiency or democratic partitioning of nodes in block mining.

Cao et al. [64] emphasized that BC has several specific properties, such as decentralization, immutability, and traceability, which can help to solve the security, integration, and coordination problems faced by centralized smart grids. In particular, the cited researchers in the context of cybersecurity addressed the issues of privacy protection, identity authentication, and data aggregation [64].

Hasan et al. [65] conducted a review of blockchain technology implementations with regard to cybersecurity and energy data protection in smart grids. The results of the review suggest the significant potential of BC in smart grid security. In the detailed research published by Kim and Huh [66], a security plan for a smart grid using BC technology has been proposed. The research findings indicate high efficiency and security through the use of BC technology using Rainbowchain, which induces symmetric compensation through double chains on the consensus algorithm [66].

The latest research findings published by Zhang et al. [67] define a smart grid security architecture based on BC technology, which addresses the issue of conflict between distributed smart grid components and centralized management. The results of the analyzed studies indicate that it is possible to improve the BC data structure to include the characteristics of the smart grid, including thorough multi-layer smart contracts, which addresses the problems of security and insufficient automation [67].

It is worth noting, however, that the literature indicates that blockchain technology cannot solve all security issues, such as those related to external physical devices like smart meters, whose computational power and storage capacity are too limited to handle complex cryptographic calculations [64].

As the results of the analyzed studies indicate, BC technology can be a key component of a holistic cybersecurity strategy for modern energy systems. The decentralized and transparent nature of the blockchain can significantly support the attribute of integrity in IEMS.

4.2.3. Artificial Intelligence Algorithms

Artificial intelligence algorithms are continuously being developed by computer science, increasing their utility and leading to their growing application across various domains. Recent research findings indicate that AI algorithms can effectively support the specific cybersecurity requirements of EMSs. It should be noted that the concept of AI encompasses a wide range of concepts, models, methods, techniques, and tools. There are various concepts and some difficulties in clearly classifying AI solutions. This is due to the fact that some solutions interpenetrate each other or constitute a hybrid of different AI techniques. Nevertheless, the leading concepts in the field of AI include, among others, machine learning, deep learning, fuzzy logic, artificial neural networks, natural language processing, and metaheuristic algorithms.

In this article, machine learning and metaheuristic algorithms are selected from a broad set of artificial intelligence methods and techniques to be analyzed for cybersecurity applications in the energy sector. Machine learning is a field of computer science that concerns automating solutions to complex problems using algorithms and techniques that are difficult to solve using traditional programming methods [68]. Metaheuristic algorithms, on the other hand, are used to solve difficult optimization problems in an approximate way without the need for deep adaptation to each problem [69]. Metaheuristics are often inspired by optimization mechanisms found in nature, e.g., evolutionary algorithms, swarm intelligence, or the gray wolf algorithm.

Berghout et al. [70] published a review study on the application of machine learning in smart grid cybersecurity with the attributes of confidentiality, availability and integrity taken into account [70]. The conclusions of the review emphasized, among others, that deep learning models showed high effectiveness in terms of protection of the attribute of availability [70]. Importantly, the conducted research led to the conclusion that deep learning is more effective than conventional machine learning techniques for confidentiality, availability and integrity attributes [70].

In another study, Diaba et al. [71] demonstrated the effectiveness of a synergistic combination of machine learning with metaheuristic algorithms in supporting cybersecurity in energy systems. The analyzed article presents a metaheuristic artificial root feeding optimization algorithm based on a Boltzmann machine for detecting and classifying types of attacks in smart grids [71]. Experimental comparative studies indicate that the proposed solution is more effective than other neural network algorithms in terms of binary, three-class and multi-class classification [71]. The cited study is also crucial because it indicates that synergistically combining AI methods may be more effective for cybersecurity than using individual methods.

Another relevant study synergistically combined quantum computing and machine learning to detect DDoS attacks on a smart micro-grid [72]. Quantum computers are attracting attention in the area of cybersecurity, especially from the perspective of the speed of solving selected mathematical problems much faster than classical computers. Importantly, the security of some cryptographic methods is based on the mathematical difficulty of the algorithms, which are difficult to solve in a reasonable time by classical computers, even with significant computing power. In the analyzed studies, a quantum model of the support vector machine was presented [72]. The results of the studies indicate that the proposed solution outperforms the classical SVM models in detecting and classifying DDoS attacks on a smart micro-grid and also shows higher efficiency in terms of execution time [72].

5. Examples of Monitoring Applications and Protection Against Cyberthreats

5.1. Electricity Prices for Businesses in Poland

Energy prices for businesses in Poland are highly variable and have increased significantly following the outbreak of war in Ukraine as a result of the global turmoil. Companies, which before the crisis were paying between 480 and 830 PLN/MWh for electricity, were faced with costs in the order of 1600–1800 PLN/MWh after the increases. Energy prices also depended on the type of tariff under which energy was purchased. Pre-enterprises could benefit from the following tariffs: Tariff A (e.g., for the PGE distributor, it amounted to PLN 1769.97 gross) dedicated to large factories, Tariff B (e.g., for distributor PGE, it was PLN 1784.73 gross) for large companies and farms, Tariff C (e.g., for distributor PGE, it was 1826.6) dedicated to SMEs. Small and medium-sized enterprises paid much more for energy than large enterprises, which was not only due to the tariff but mainly due to the price that large enterprises obtain due to their negotiating position; they could obtain lower rates or buy energy at market prices on power exchanges. When the supply of energy was high, e.g., from photovoltaics or wind farms, it was profitable. Such solutions meant that energy charges were much lower than when buying energy from energy operators. In the face of soaring energy prices, investments in RES, especially photovoltaics, have become more profitable, so many companies have started installing them.

5.2. Investment in Renewable Energy Sources—Photovoltaic Farms

This section of the article presents detailed research on two companies from the food distribution industry, which are representative of the other 17 companies analyzed. The companies surveyed before the outbreak of war in Ukraine had average monthly energy costs of PLN 12,000 (Company A) and PLN 16,000 (Company B). After the increases, these costs increased to PLN 17,000 and PLN 25,000 per month, respectively. Due to the drastic increase in energy prices, the surveyed enterprises installed photovoltaic systems that differed in the number of modules, power and energy production. Table 2 shows the detailed parameters of the PV installations:

Table 2. Parameters of photovoltaic installations in the surveyed companies.

Parameters	Company (A)	Company (B)
Number of PV modules	83	104
PV generator power	40 kWp	50 kWp
Surface area required	180 m^2	230 m^2
Energy produced	34,079 kWh/year	44,487 kWh/year
CO$_2$ emissions, that could have been avoided	20,447 kg/year	26,692 kg/year

Source: Own elaboration based on research.

The investment cost for the photovoltaic systems was PLN 120,000 (company A) and PLN 155,000 (company B), respectively. This investment included the purchase of PV modules, inverters and instrumentation to manage the installation. Although the investment reduced energy consumption costs, it did not completely solve their problems, as energy production from PV panels only accounted for 10–15% of the companies' total energy needs. In most cases, the energy produced was consumed for day-to-day needs, and only in the summer months, during peak hours, was there a minimal surplus of energy. Figures 2 and 3 show the monthly energy production (kWh) of the surveyed enterprises by PV modules.

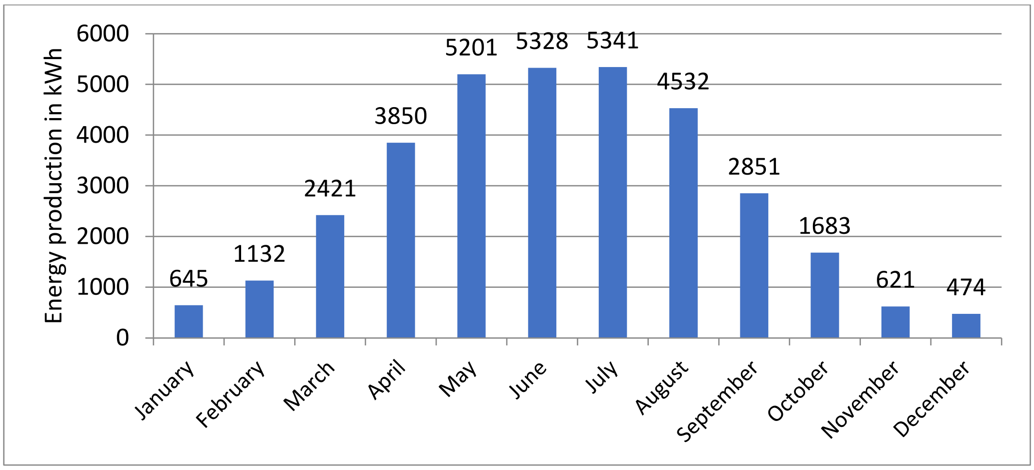

Figure 2. Energy production from photovoltaic panels at company (A) in 2023. Source: own compilation based on research.

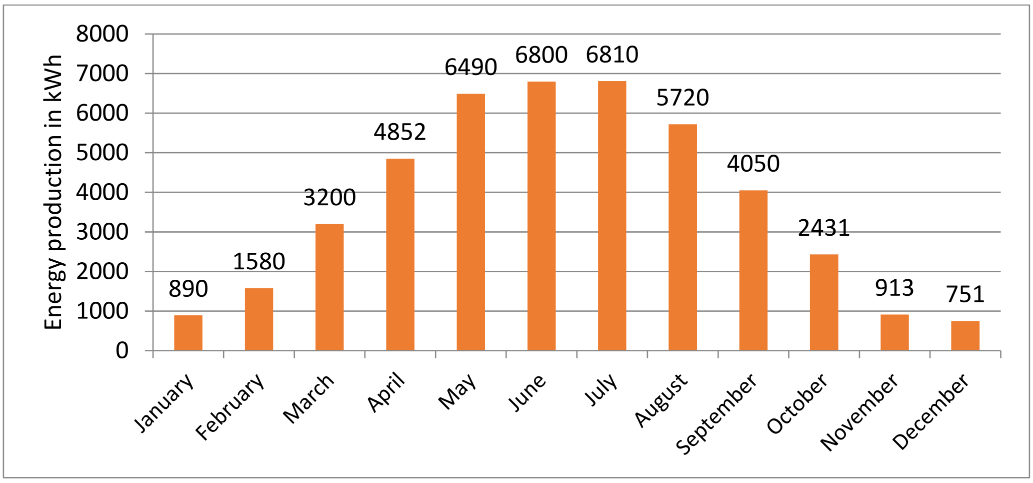

Figure 3. Energy production from photovoltaic panels at company (B) in 2023. Source: own compilation based on research.

Restrictions for the production of more energy in the companies surveyed were the available space and legal regulations that require additional permits for panel installations exceeding 50 kW and the lack of subsidies from the state. These legal restrictions can significantly delay further projects and generate additional administrative costs.

By investing in panels, the surveyed companies not only reduced their energy consumption costs but also reduced their carbon emissions, which had a positive impact on the environment. The data from the analysis confirms the Eaton report [73] conducted on a 1001 sample of industrial, construction and data center companies, noting a growing interest in energy transition and the use of RESs. As many as 77% of companies are preparing to change their energy sources, and 29% have already started the process. More and more companies are seeing the benefits of RESs, which is driven mainly by rising energy prices and pressure to reduce carbon emissions. The report found that one in four companies use RESs as their main source of power. One in three companies have implemented EMSs, which allows for the more efficient monitoring and optimization of energy consumption. Energy transformation, along with digitalization, has become a key factor in the development of companies. As many as 44% of enterprises have identified energy transformation as a top priority, enabling more efficient power consumption and better energy management. Another important aspect is the reporting of environmental and social (ESG) indicators, which is becoming increasingly mandatory for businesses, with 43% paying particular attention to these issues. Basic parameters such as total energy consumption are tracked by half of the businesses. In contrast, 24% monitor CO_2 emissions and 34% analyze energy efficiency. The report's findings indicate that energy transformation is becoming a global trend with companies increasingly looking for ways to manage energy efficiently and reduce their environmental impact.

As a result of the case study and the analysis of the interview responses, the following conclusions can be drawn. The impact of energy prices on business was significant, prompting companies to seek cost optimization solutions. Companies decided to support electricity consumption through their own production and the introduction of smart meter devices (monitoring applications) in order to reduce costs and become partially independent from the price fluctuations of external energy sources (17 respondents answered).

Changing energy sources and reducing energy consumption will require more sophisticated monitoring of power consumption rates and tracking of energy prices to be able to react accordingly and decide whether to buy or sell the energy produced (65% of those asked). Investment in operational infrastructure and intelligent energy management systems, such as a smart meter device based on artificial intelligence and machine learning, is essential to gain real-time data insights (13 respondents answered).

However, innovative measures entail a change in staffing structure and generate additional costs related to cybersecurity. Every element of the energy system represents a potential entry point for cyber criminals, and humans remain the weakest link in the chain. It is therefore essential to continuously improve the organization's resilience to cyber incidents not only through the implementation of modern technologies but also through the systematic training of all employees (16 respondents answered).

The high cost of investment and maintenance of management systems means that companies are often limited to basic protection methods (15 respondents answered). Security administrators must therefore constantly maintain readiness to respond, quickly detect attempted attacks and effectively neutralize them. For SMEs, it is particularly difficult to perform these tasks without state support. Financial constraints are a key barrier to further cybersecurity efforts (14 respondents answered), indicating the need for support programs and appropriate cybersecurity policies aimed at this group of companies.

5.3. Energy Monitoring Applications

Both company (A) and company (B) used simple EMSs to monitor the production and consumption of photovoltaic energy. These systems provided insight into key data such as monthly and hourly energy production, which was particularly important in cases where energy was fed back into the grid. Where all energy produced was consumed for own use, as was the case in the companies surveyed, the ability to track exact hours of production was less important. In the companies surveyed, the monitoring applications had limited capabilities, monitoring only basic parameters related to production and energy consumption. As a result, there was a need for more advanced applications that could monitor more parameters, such as, for example, optimizing energy consumption or automatically adjusting power to the available energy.

5.4. Cybersecurity

The in-depth research in the two companies (A and B) that had installed photovoltaic panels allowed for the creation of a database of questions that were used in subsequent interviews with executives from 15 companies (a total of 17 interviews were conducted). A number of questions were asked, but the article presents the most important ones related to the topic of cybersecurity. The rise of connected devices as part of the IoT is making power grids more vulnerable to hacking attacks. According to Allianz Commercial, ransomware attacks, data security breaches and business disruption were identified as the top global business threats from 2022 to 2023. Cybersecurity outpaced other threats, but this was mainly the case for large and medium-sized companies with annual revenues of more than USD 100 million. Despite this, year on year, more and more attacks are targeting smaller companies, which are easier targets due to the lack of adequate, costly security measures [74]. The interviews found that the companies surveyed had experienced cybersecurity issues mainly in the form of breaches in the availability of IT systems. In some cases, IT systems were blocked or some of their services stopped working. Importantly, there were no cases of direct attacks on energy management systems.

The companies surveyed considered methods of securing and protecting data and countering cyber threats, taking into account the key attributes of information security. A variety of IT measures were used to protect systems, such as smart meter devices including alarms, CCTV readers, sensors and energy detectors, which secured both hardware (hardware) and software (software). The solutions used included the following:

1. Redundancy of computer system components—included duplication of power sources, installation of an emergency power supply automatically activated in the event of a failure, and duplication of storage devices.
2. File encryption—used by half of the companies surveyed.
3. User identification and authentication—used to verify the identity of users by providing valid credentials assigned by the hardware administrator.
4. Software protection—included security solutions for both hardware and software, used in all analyzed companies.
5. Data archiving—creating additional copies of the system and the information stored on it, which is implemented by the majority of companies.
6. Antivirus protection—widely used in all surveyed companies.

The number of companies with these solutions is indicated in Figure 4.

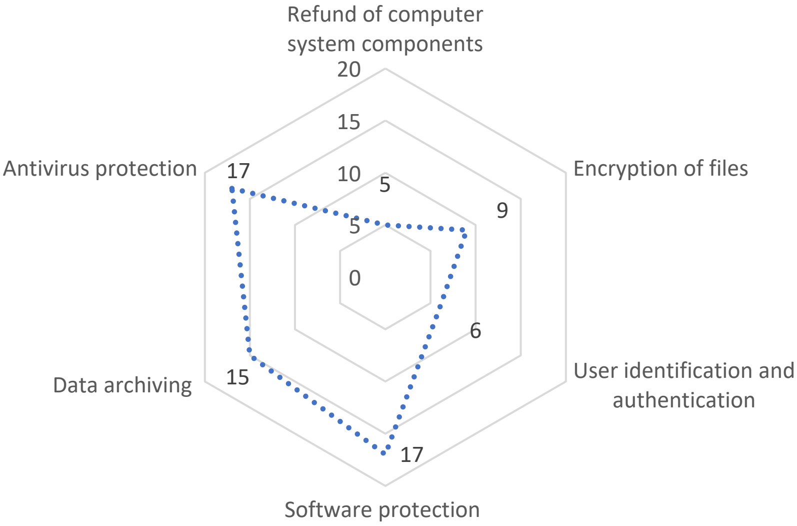

Figure 4. Data protection and cybersecurity methods used in surveyed companies. Source: own compilation, based on research.

These solutions were aimed at increasing the operational security of systems and protecting against potential cyber threats.

The interviews found that in the companies surveyed, basic IT safeguards were used to protect systems, including smart meter devices to protect both hardware (hardware) and software (software). However, with the growing threat of cyberattacks, companies are beginning to recognize the need for more advanced security measures. The companies surveyed were aware of the new challenges that have arisen with the development of technology. All respondents indicated the need for further investment in more advanced security systems that can not only monitor and manage energy but also effectively protect against cyber threats.

6. Discussion of Research Results

The discussion section was aimed at critically evaluating the study's findings and pointing out how important EMSs are in the face of growing cyber threats.

The theoretical analyses conducted lead to the conclusion that cybersecurity is a key determinant of the effectiveness of modern IEMSs. IEMSs are exposed to a number of threats resulting from their functioning in cyberspace. Furthermore, cybersecurity incidents can have serious consequences due to the fact that energy systems are part of critical infrastructure. Ensuring cybersecurity in the modern energy sector should include holistic and synergistic initiatives at the organizational and technical levels. IMES protection methods should include, in particular, a planned and synergistic combination of the latest technologies in the field of intrusion detection systems, blockchain and artificial intelligence algorithms. Our research findings are consistent with other research results. In particular, Agung and Handayani [75] demonstrated the benefits of using blockchain technology as a transaction management tool in smart grids. In other studies, Naeem et al. [76] proposed an intrusion classification scheme for smart grid systems that combines deep learning with metaheuristic optimization. In another important study, Du et al. [77] demonstrated the effectiveness of deep learning in detecting anomalies in industrial control systems. In particular, in the cited study, a marking-based classification method for unknown industrial control protocols was developed [77]. The results of comparative studies indicate that the accuracy and precision of the proposed method are better than benchmark methods [77].

Faced with rapidly rising energy prices, the companies surveyed have opted for an energy transition, in particular investing in RESs such as photovoltaics. The introduction of these technologies helped to reduce energy costs, although photovoltaic energy production only covered 10–15% of their needs. Dziaduszyński et al. [78], in their report on the development of RESs, pointed out that the cost of energy is a significant item in the budgets of many businesses. Entrepreneurs who regularly invest their resources are more likely to optimize this expenditure. They can achieve this in various ways: by switching to a cheaper or more flexible energy supplier, choosing a more favorable tariff tailored to the needs of the business or investing in RES. These actions contribute to lower operating costs, increase competitiveness and reduce environmental impact by reducing harmful emissions [78].

The development of RESs in SMEs is mainly based on the prosumer philosophy, which implies that the company's current energy needs are partly covered by its own renewable sources. The best results are obtained when energy is generated and consumed directly on site. In the 21st century, in the era of smart grids, small and micro-sources of renewable energy are becoming an essential part of the energy mix, supporting traditional sources, mitigating peak energy demand and minimizing transmission losses [78].

In both cases, companies used EMSs to monitor production and consumption, but they had limited functionality. Barriers to greater investment in RESs were a lack of available space, regulations requiring permits and a lack of subsidies for businesses. Globally, the Eaton report indicated a growing interest among companies in energy transformation and an increasing share of energy management systems. At the same time, the digitalization of energy systems brings with it new cybersecurity challenges. Small and medium-sized companies are becoming increasingly vulnerable to cyberattacks, and protecting data and energy systems is becoming a priority. Companies were using basic IT security, but the need for further investment in more advanced protection systems was identified [73].

With the growing threat of cyberattacks, companies increasingly recognize the need for advanced security measures. The companies surveyed were aware of the new challenges that have arisen with the development of technology.

7. Summary and Conclusions

The energy transition is turning small and mid-size businesses into energy producers that need to be managed accordingly. However, changing energy supply and reducing energy consumption will require accurate tracking, advanced power consumption indicators and energy prices in order to buy or sell produced energy at the right time. Therefore, investments are needed in infrastructure and IEMSs based on artificial intelligence and machine learning. These innovative developments lead to cybersecurity challenges. It therefore becomes essential to continuously improve the resilience of companies against cyberattacks not only through the implementation of advanced protection systems but also through the continuous education of employees.

The theoretical study showed the specific requirements of Industry 5.0 in the context of cybersecurity. The technical analysis of threats to IMESs showed that malware and ransomware attacks, DDoS attacks and security vulnerabilities in SCADA, IoT and CPS systems are of critical importance. In turn, security measures based on anomaly detection systems, AI algorithms and distributed ledger technology provide a chance to meet the requirements of modern IMESs operating in the Industry 5.0 environment. Empirical research has shown that basic IT security measures, including monitoring applications, were used in the surveyed organizations. Companies are beginning to recognize the need for more advanced security measures. It identified the need for further investment in more advanced security systems that can monitor and manage energy and effectively protect against cyber threats.

The presented research is not without limitations: namely, the empirical analyses were conducted in a limited number of small and medium-sized enterprises, which limits the possibility of generalizing conclusions to other sectors of the economy or larger enterprises. A larger research sample could have provided more representative results. The research focused on simple EMSs that only monitor basic parameters. An analysis of more advanced systems that optimize energy consumption and support flexible resource management could provide a broader picture of energy management efficiency. Efficiency results for PV installations are strongly dependent on local weather conditions, the area available for installations and applicable legislation. In other countries or regions, results may vary. The research focused on basic IT security systems, which does not reflect the full picture of potential risks and needs for advanced cybersecurity, especially in more complex energy management systems.

The investment costs of smart energy systems result in the simplest data protection methods being used in SMEs. Therefore, there is a need for the state to create support programs and appropriate cybersecurity policies so that they can compete effectively with larger players in the market. There is a need for further research into energy management applications, programs and systems for SMEs to make them more widespread and cheaper. The authors suggest the following future research directions:

1. Future research should cover different industry sectors and different types of businesses (including larger companies) to better understand the impact of energy transition and cybersecurity on business and the environment.
2. Future research should address more advanced EMSs that not only monitor but also optimize energy consumption in real time. Research could also cover the integration of these systems with smart solutions such as artificial intelligence or IoT interoperability.
3. With the growing threat of cyberattacks, future research should focus on more complex cybersecurity strategies, especially in the context of real-time energy management and the development of renewable energy infrastructure.
4. Future research may also focus on the role of public policy and financial support in facilitating the energy transition in the SME sector, examining the impact of subsidies, tax breaks and regulations to support RESs development and increased cybersecurity.

Author Contributions: Conceptualization, B.W., H.S., E.K.S., A.R. and M.K.; methodology, B.W., H.S., E.K.S., A.R. and M.K.; validation, B.W., H.S., E.K.S., A.R. and M.K.; formal analysis, B.W., H.S., E.K.S., A.R. and M.K.; investigation, B.W., H.S., E.K.S., A.R. and M.K.; resources, B.W., H.S., E.K.S., A.R. and M.K.; data curation, B.W., H.S., E.K.S., A.R. and M.K.; writing—original draft preparation, B.W., H.S., E.K.S., A.R. and M.K.; writing—review and editing, B.W., H.S., E.K.S., A.R. and M.K.; visualization, B.W., H.S., E.K.S., A.R. and M.K. All authors have read and agreed to the published version of the manuscript.

Funding: The publication was (co) financed by Science development fund of the Warsaw University of Life Sciences—SGGW.

Data Availability Statement: Data are contained within the article.

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

References

1. Sun, W.; Wang, Q.; Zhou, Y.; Wu, J. Material and energy flows of the iron and steel industry: Status quo, challenges, and perspectives. *Appl. Energy* **2020**, *268*, 114946. [CrossRef]
2. Bednar, P.M.; Welch, C. Socio-technical perspectives on smart working: Creating meaningful and sustainable systems. *Inf. Syst. Front.* **2020**, *22*, 281–298. [CrossRef]
3. Demir, K.A.; Döven, G.; Sezen, B. Industry 5.0 and human-robot co-working. *Procedia Comput. Sci.* **2019**, *158*, 688–695. [CrossRef]
4. Longo, F.; Padovano, A.; Umbrello, S. Value-oriented and ethical technology engineering in Industry 5.0: A human-centric perspective for the design of the factory of the future. *Appl. Sci.* **2020**, *10*, 4182. [CrossRef]
5. Przekota, G.; Katarzyński, D. Wpływ cen nośników energii na ceny produktów i usług [The impact of energy carrier prices on product and service prices]. *Kwartalnik Nauk o Przed-siębiorstwie [Bus. Sci. Q.]* **2024**, *71*, 71–92. [CrossRef]
6. Leng, J.; Sha, W.; Wang, B.; Zheng, P.; Zhuang, C.; Liu, Q.; Wuest, T.; Mourtzis, D.; Wang, L. Industry 5.0: Prospect and retrospect. *J. Manuf. Syst.* **2022**, *65*, 279–295. [CrossRef]
7. Maddikunta, P.K.R.; Pham, Q.-V.; Prabadevi, B.; Deepa, N.; Dev, K.; Gadekallu, T.R.; Ruby, R.; Liyanage, M. Industry 5.0: A survey on enabling technologies and potential applications. *J. Ind. Inf. Integr.* **2021**, *26*, 100257. [CrossRef]
8. Martos, V.; Ahmad, A.; Cartujo, P.; Ordoñez, J. Ensuring agricultural sustainability through remote sensing in the era of agriculture 5.0. *Appl. Sci.* **2021**, *11*, 5911. [CrossRef]
9. Masood, T.; Sonntag, P. Industry 4.0: Adoption challenges and benefits for SMEs. *Comput. Ind.* **2020**, *121*, 103261. [CrossRef]
10. Sharma, I.; Garg, I.; Kiran, D. Industry 5.0 and smart cities: A futuristic approach. *Eur. J. Mol. Clin. Med.* **2020**, *7*, 2515–8260.
11. Aslam, F.; Aimin, W.; Li, M.; Rehman, K.U. Innovation in the era of IoT and Industry 5.0: Absolute Innovation Management (AIM) framework. *Information* **2020**, *11*, 124. [CrossRef]
12. Nahavandi, S. Industry 5.0—A human-centric solution. *Sustainability* **2020**, *11*, 4371. [CrossRef]
13. Adel, A. Future of industry 5.0 in society: Human-centric solutions, challenges and prospective research areas. *J. Cloud Comput. Adv. Syst. Appl.* **2022**, *11*, 40. [CrossRef]
14. Adamczyk, J. Rola cyfryzacji w realizacji zrównoważonego rozwoju w kontekście interesariuszy [The role of digitization in realizing sustainable development in the context of stakeholders]. *Krakowskie Studia Małopolskie [Crac. Malop. Stud.]* **2023**, *4*, 9–13. [CrossRef]
15. Slavic, D.; Marjanovic, U.; Medic, N.; Simeunovic, N.; Rakic, S. The Evaluation of Industry 5.0 Concepts: Social Network Analysis Approach. *Appl. Sci.* **2024**, *14*, 1291. [CrossRef]
16. European Commission. *Industry 5.0: A Transformative Vision for Europe Governing Systemic Transformations Towards a Sustainable Industry*; ESIR Policy Brief No. 3. Independent Expert Report; European Commission: Brussels, Belgium, 2022; pp. 6–13. Available online: https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/38a2fa08-728e-11ec-9136-01aa75ed71a1 (accessed on 5 September 2024).
17. Breque, M.; De Nul, L.; Petridis, A. *Industry 5.0 Towards a sustainable, Human-Centric and Resilient European Industry*; R&I Paper Series Policy Brief; European Commission: Brussels, Belgium, 2021; pp. 8–23. Available online: https://op.europa.eu/en/publication-detail/-/publication/468a892a-5097-11eb-b59f-01aa75ed71a1/ (accessed on 5 September 2024).
18. Xu, X.; Lu, Y.; Vogel-Heuser, B.; Wang, L. Industry 4.0 and Industry 5.0—Inception, conception and perception. *J. Manuf. Syst.* **2021**, *61*, 530–535. [CrossRef]
19. Müller, J. *Enabling Technologies for Industry 5.0 Results of a Workshop with Europe's Technology Leaders. European Commission Directorate-General for Research and Innovation Directorate F—Prosperity Unit F5 Industry 5*; Independent Expert Report; European Commission: Brussels, Belgium, 2020; pp. 3–8. Available online: https://alessandra-flammini.unibs.it/SEAI/approfondimenti/enabling%20technologies%20for%20industry%205%200-KI0420494ENN.pdf (accessed on 5 September 2024).
20. Vacchi, M.; Siligardi, C.; Settembre-Blundo, D. Driving Manufacturing Companies toward Industry 5.0: A Strategic Framework for Process Technological Sustainability Assessment (P-TSA). *Sustainability* **2024**, *16*, 695. [CrossRef]
21. Jin, Q.; Chen, H.; Hu, F. Proposal of Industry 5.0-Enabled Sustainability of Product–Service Systems and Its Quantitative Multi-Criteria Decision-Making Method. *Processes* **2024**, *12*, 473. [CrossRef]
22. Grabowska, S.; Saniuk, S.; Gajdzik, B. Industry 5.0: Improving humanization and sustainability of Industry 4.0. *Scientometrics* **2022**, *127*, 3117–3144. [CrossRef]
23. Wan, P.K.; Leirmo, T.L. Human-centric zero-defect manufacturing: State-of-the-art review, perspectives, and challenges. *Comput. Ind.* **2023**, *144*, 103792. [CrossRef]
24. Ghobakhloo, M.; Iranmanesh, M.; Tseng, M.-L.; Grybauskas, A.; Stefanini, A.; Amran, A. Behind the definition of Industry 5.0: A systematic review of technologies, principles, components, and values. *J. Ind. Prod. Eng.* **2023**, *40*, 432–447. [CrossRef]
25. Piccarozzi, M.; Silvestri, L.; Silvestri, C.; Ruggieri, A. Roadmap to Industry 5.0: Enabling technologies, challenges, and opportunities towards a holistic definition in management studies. *Technol. Forecast. Soc. Chang.* **2024**, *205*, 123467. [CrossRef]

26. Chander, B.; Pal, S.; De, D.; Buyya, R. Artificial Intelligence-based Internet of Things for Industry 5.0. In *Artificial Intelligence-Based Internet of Things Systems*; Springer International Publishing: Berlin/Heidelberg, Germany, 2022; pp. 3–45. [CrossRef]
27. Huang, G.Q.; Vogel-Heuser, B.; Zhou, M.; Dario, P. Digital technologies and automation: The human and eco-centered foundations for the factory of the future [TC Spotlight]. *IEEE Robot. Autom. Mag.* **2021**, *28*, 174–179. [CrossRef]
28. Chander, B.; Kumaravelan, G. Cyberbezpieczeństwo ze sztuczną inteligencją—Część I. In *The "Essence" of Network Security: An End-to-End Panorama*; Springer: Singapore, 2021; pp. 147–171.
29. Santos, B.; Costa, R.L.C.; Santos, L. Cybersecurity in Industry 5.0: Open challenges and future directions. *arXiv* **2024**, arXiv:2410.09538.
30. Mourtzis, D.; Angelopoulos, J.; Panopoulos, N. A literature review of the challenges and opportunities of the transition from Industry 4.0 to Society 5.0. *Energies* **2022**, *15*, 6276. [CrossRef]
31. Anand, P.; Kanike, U.K.; Paramasivan, P.; Rajest, S.S.; Regina, R.; Pryscyl, Ś.S. Embracing Industry 5.0: Pioneering Next-Generation Technology for a Flourishing Human Experience and Societal Advancement. *J. Innov. Soc. Adv.* **2023**, *7*, 1–15.
32. Avdibasic, E.; Toksanovna, A.S.; Durakovic, B. Cybersecurity challenges in Industry 4.0: A state of the art review. *Digit. Sci. Solut.* **2022**, *3*, 32–49. [CrossRef]
33. Fetting, C. *The European Green Deal*; ESDN Report, December 2020; ESDN Office: Vienna, Austria, 2020. Available online: https://www.esdn.eu/fileadmin/ESDN_Reports/ESDN_Report_2_2020.pdf (accessed on 5 November 2024).
34. Kagermann, H.; Wahlster, W.; Helbig, J. *Securing the Future of German Manufacturing Industry: Recommendations for Implementing the Strategic Initiative Industrie 4.0. Final Report of the Industrie 4.0 Working Group*; Acatech—National Academy of Science and Engineering: Munich, Germany, 2013; 678p.
35. Sujatha, R.; Prakash, G. *CyberSecurity Applications for Industry 4.0*; Jhanjhi, N.Z., Ed.; CRC Press: Boca Raton, FL, USA, 2022.
36. AlSalem, T.S.; Almaiah, M.A.; Lutfi, A. Cybersecurity Risk Analysis in the IoT: A Systematic Review. *Electronics* **2023**, *12*, 3958. [CrossRef]
37. Hu, J.-L.; Bui, N.H.B. The Future Design of Smart Energy Systems with Energy Flexumers: A Constructive Literature Review. *Energies* **2024**, *17*, 2039. [CrossRef]
38. Szczepaniuk, E.K.; Szczepaniuk, H. Analysis of Cybersecurity Competencies: Recommendations for Telecommunications Policy. *Telecommun. Policy* **2021**, *46*, 102282. [CrossRef]
39. Wang, P.; Govindarasu, M. Cyber-Physical Anomaly Detection for Power Grid with Machine Learning. In *Advances in Information Security*; Springer International Publishing: Cham, Switzerland, 2019; pp. 31–49, ISBN 9783030182137.
40. Demertzis, K.; Iliadis, L.S.; Anezakis, V.-D. An Innovative Soft Computing System for Smart Energy Grids Cybersecurity. *Adv. Build. Energy Res.* **2018**, *12*, 3–24. [CrossRef]
41. Boeding, M.; Boswell, K.; Hempel, M.; Sharif, H.; Lopez, J., Jr.; Perumalla, K. Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid. *Energies* **2022**, *15*, 8692. [CrossRef]
42. Demertzi, V.; Demertzis, S.; Demertzis, K. An Overview of Privacy Dimensions on the Industrial Internet of Things (IIoT). *Algorithms* **2023**, *16*, 378. [CrossRef]
43. Marchang, J.; McDonald, J.; Keishing, S.; Zoughalian, K.; Mawanda, R.; Delhon-Bugard, C.; Bouillet, N.; Sanders, B. Secure-by-Design Real-Time Internet of Medical Things Architecture: E-Health Population Monitoring (RTPM). *Telecom* **2024**, *5*, 609–631. [CrossRef]
44. Alqahtani, F.; Almutairi, M.; Sheldon, F.T. Cloud Security Using Fine-Grained Efficient Information Flow Tracking. *Future Internet* **2024**, *16*, 110. [CrossRef]
45. Butcher, D.S.; Brigham, C.J.; Berhalter, J.; Centers, A.L.; Hunkapiller, W.M.; Murphy, T.P.; Palm, E.C.; Smith, J.H. Cybersecurity in a Large-Scale Research Facility—One Institution's Approach. *J. Cybersecur. Priv.* **2023**, *3*, 191–208. [CrossRef]
46. Bouramdane, A.-A. Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process. *J. Cybersecur. Priv.* **2023**, *3*, 662–705. [CrossRef]
47. Cen, M.; Jiang, F.; Qin, X.; Jiang, Q.; Doss, R. Ransomware Early Detection: A Survey. *Comput. Netw.* **2024**, *239*, 110138. [CrossRef]
48. Al-Hawawreh, M.; Alazab, M.; Ferrag, M.A.; Hossain, M.S. Securing the Industrial Internet of Things against Ransomware Attacks: A Comprehensive Analysis of the Emerging Threat Landscape and Detection Mechanisms. *J. Netw. Comput. Appl.* **2024**, *223*, 103809. [CrossRef]
49. Ghosal, A.; Conti, M. Key Management Systems for Smart Grid Advanced Metering Infrastructure: A Survey. *IEEE Commun. Surv. Tutor. Thirdquarter* **2019**, *21*, 2831–2848. [CrossRef]
50. Wang, Q.; Tai, W.; Tang, Y.; Zhu, H.; Zhang, M.; Zhou, D. Coordinated Defense of Distributed Denial of Service Attacks against the Multi-Area Load Frequency Control Services. *Energies* **2019**, *12*, 2493. [CrossRef]
51. Diaba, S.Y.; Shafie-khah, M.; Elmusrati, M. Cyber-Physical Attack and the Future Energy Systems: A Review. *Energy Rep.* **2024**, *12*, 2914–2932. [CrossRef]
52. Alanazi, M.; Mahmood, A.; Chowdhury, M.J.M. SCADA Vulnerabilities and Attacks: A Review of the State-of-the-art and Open Issues. *Comput. Secur.* **2023**, *125*, 103028. [CrossRef]
53. Mahi-al-rashid, A.; Hossain, F.; Anwar, A.; Azam, S. False Data Injection Attack Detection in Smart Grid Using Energy Consumption Forecasting. *Energies* **2022**, *15*, 4877. [CrossRef]

54. Yang, Y.-S.; Lee, S.-H.; Chen, W.-C.; Yang, C.-S.; Huang, Y.-M.; Hou, T.-W. Securing SCADA Energy Management System under DDos Attacks Using Token Verification Approach. *Appl. Sci.* **2022**, *12*, 530. [CrossRef]
55. Diaba, S.Y.; Anafo, T.; Tetteh, L.A.; Oyibo, M.A.; Alola, A.A.; Shafie-khah, M.; Elmusrati, M. SCADA Securing System Using Deep Learning to Prevent Cyber Infiltration. *Neural Netw.* **2023**, *165*, 321–332. [CrossRef]
56. Upadhyay, D.; Ghosh, S.; Ohno, H.; Zaman, M.; Sampalli, S. Securing Industrial Control Systems: Developing a SCADA/IoT Test Bench and Evaluating Lightweight Cipher Performance on Hardware Simulator. *Int. J. Crit. Infrastruct. Prot.* **2024**, *47*, 100705. [CrossRef]
57. Yi, L.; Yin, M.; Darbandi, M. A Deep and Systematic Review of the Intrusion Detection Systems in the Fog Environment. *Trans. Emerg. Telecommun. Technol.* **2023**, *34*, e4632. [CrossRef]
58. Sahani, N.; Zhu, R.; Cho, J.-H.; Liu, C.-C. Machine Learning-Based Intrusion Detection for Smart Grid Computing: A Survey. ACM Trans. *Cyber-Phys. Syst.* **2023**, *7*, 1–31. [CrossRef]
59. Murugesan, N.; Velu, A.N.; Palaniappan, B.S.; Sukumar, B.; Hossain, M.J. Mitigating Missing Rate and Early Cyberattack Discrimination Using Optimal Statistical Approach with Machine Learning Techniques in a Smart Grid. *Energies* **2024**, *17*, 1965. [CrossRef]
60. Khan, S.; Kifayat, K.; Kashif Bashir, A.; Gurtov, A.; Hassan, M. Intelligent Intrusion Detection System in Smart Grid Using Computational Intelligence and Machine Learning. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4062. [CrossRef]
61. AlHaddad, U.; Basuhail, A.; Khemakhem, M.; Eassa, F.E.; Jambi, K. Ensemble Model Based on Hybrid Deep Learning for Intrusion Detection in Smart Grid Networks. *Sensors* **2023**, *23*, 7464. [CrossRef] [PubMed]
62. Li, X.J.; Ma, M.; Sun, Y. An Adaptive Deep Learning Neural Network Model to Enhance Machine-Learning-Based Classifiers for Intrusion Detection in Smart Grids. *Algorithms* **2023**, *16*, 288. [CrossRef]
63. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems. *IEEE Access* **2019**, *7*, 46595–46620. [CrossRef]
64. Cao, Y.-N.; Wang, Y.; Ding, Y.; Guo, Z.; Wu, Q.; Liang, H. Blockchain-Empowered Security and Privacy Protection Technologies for Smart Grid. *Comput. Stand. Interfaces* **2023**, *85*, 103708. [CrossRef]
65. Hasan, M.K.; Alkhalifah, A.; Islam, S.; Babiker, N.B.M.; Habib, A.K.M.A.; Aman, A.H.M.; Hossain, M.A. Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1–26. [CrossRef]
66. Kim, S.-K.; Huh, J.-H. A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective. *Energies* **2018**, *11*, 1973. [CrossRef]
67. Zhang, M.; Liu, Y.; Cheng, Q.; Li, H.; Liao, D.; Li, H. Smart Grid Security Based on Blockchain and Smart Contract. *Peer-to-Peer Netw. Appl.* **2024**, *17*, 2167–2184. [CrossRef]
68. Rebala, G.; Ravi, A.; Churiwala, S. Machine Learning Definition and Basics. In *An Introduction to Machine Learning*; Springer International Publishing: Cham, Switzerland, 2019; pp. 1–17, ISBN 9783030157289.
69. Boussaïd, I.; Lepagnot, J.; Siarry, P. A Survey on Optimization Metaheuristics. *Inf. Sci.* **2013**, *237*, 82–117. [CrossRef]
70. Berghout, T.; Benbouzid, M.; Muyeen, S.M. Machine Learning for Cybersecurity in Smart Grids: A Comprehensive Review-Based Study on Methods, Solutions, and Prospects. *Int. J. Crit. Infrastruct. Prot.* **2022**, *38*, 100547. [CrossRef]
71. Diaba, S.Y.; Shafie-Khah, M.; Elmusrati, M. Cyber Security in Power Systems Using Meta-Heuristic and Deep Learning Algorithms. *IEEE Access* **2023**, *11*, 18660–18672. [CrossRef]
72. Said, D. Quantum Computing and Machine Learning for Cybersecurity: Distributed Denial of Service (DDoS) Attack Detection on Smart Micro-Grid. *Energies* **2023**, *16*, 3572. [CrossRef]
73. Eaton. Eaton Report. 2024. Available online: https://www.kierunekenergetyka.pl/konferencje.html (accessed on 20 May 2024).
74. Allianz Commercial. Allianz Risk Barometer. 2024. Available online: https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html (accessed on 28 August 2024).
75. Agung, A.A.G.; Handayani, R. Blockchain for Smart Grid. *J. King Saud Univ.—Comput. Inf. Sci.* **2022**, *34*, 666–675. [CrossRef]
76. Naeem, H.; Ullah, F.; Srivastava, G. Classification of Intrusion Cyber-attacks in Smart Power Grids Using Deep Ensemble Learning with Metaheuristic-based Optimization. *Expert Syst.* **2024**, e13556. [CrossRef]
77. Du, X.; Xu, C.; Li, L.; Li, X. Multigranularity Feature Automatic Marking-Based Deep Learning for Anomaly Detection of Industrial Control Systems. *IEEE Open J. Instrum. Meas.* **2024**, *3*, 1–10. [CrossRef]
78. Dziaduszyński, K.; Tarka, M.; Trupkiewicz, M.; Szydłowski, K. Rozwój Odnawialnych Źródeł energii w Sektorze Mikro, Małych i Średnich Przedsiębiorstw, w tym Możliwość Zastosowania Rozwiązań Prosumenckich. Stan Obecny i Perspektywy Rozwoju [Development of Renewable Energy Sources in the Micro, Small and Medium Enterprises Sector, Including the Possibility of Using Prosumer Solutions. Current State and Development Perspectives]. Raport. 2018. Available online: https://www.teraz-srodowisko.pl/media/pdf/aktualnosci/6284-analiza-rozwoj-OZE-w-sektorze-MSP.pdf (accessed on 20 October 2024).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.