IoT

Article

Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures

Konstantinos Tsiknas [1], Dimitrios Taketzis [2], Konstantinos Demertzis [3,*] and Charalabos Skianis [4]

[1] Department of Electrical and Computer Engineering, Democritus University of Thrace, 67100 Xanthi, Greece; ktsiknas@ee.duth.gr
[2] Hellenic National Defence General Staff, Stratopedo Papagou, 15561 Athens, Greece; d.taketzis@hndgs.mil.gr
[3] Laboratory of Complex Systems, Department of Physics, Faculty of Sciences, International Hellenic University, Kavala Campus, 65404 St. Loukas, Greece
[4] Department of Information and Communication Systems Engineering, University of Aegean, 83200 Samos, Greece; cskianis@aegean.gr
* Correspondence: kdemertzis@teiemt.gr

Abstract: In today's Industrial Internet of Things (IIoT) environment, where different systems interact with the physical world, the state proposed by the Industry 4.0 standards can lead to escalating vulnerabilities, especially when these systems receive data streams from multiple intermediaries, requiring multilevel security approaches, in addition to link encryption. At the same time taking into account the heterogeneity of the systems included in the IIoT ecosystem and the non-institutionalized interoperability in terms of hardware and software, serious issues arise as to how to secure these systems. In this framework, given that the protection of industrial equipment is a requirement inextricably linked to technological developments and the use of the IoT, it is important to identify the major vulnerabilities and the associated risks and threats and to suggest the most appropriate countermeasures. In this context, this study provides a description of the attacks against IIoT systems, as well as a thorough analysis of the solutions for these attacks, as they have been proposed in the most recent literature.

Keywords: IIoT; IoT; Industry 4.0; protocols; cyber threats; attacks; security

check for updates

Citation: Tsiknas, K.; Taketzis, D.; Demertzis, K.; Skianis, C. Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. *IoT* **2021**, *2*, 163–186. https://doi.org/10.3390/iot2010009

Received: 29 January 2021
Accepted: 5 March 2021
Published: 7 March 2021

1. Introduction

According to the Industry 4.0 standard [1], cyber-physical systems within partially structured smart factories play a central role in monitoring and supervising natural processes by taking autonomous and decentralized decisions in order to maximize the production process. An important factor for achieving this target is the IIoT operational network, where the logical systems communicate and collaborate in real time to implement all kinds of intelligent production solutions, organizational services, and operational processes, required to fulfil the production chain [2].

Specifically, IIoT refers to all interconnected sensors, instruments, and other devices, which in combination with industrial applications, including production and energy management, create a complex network of services, which allows the application of automation at a higher level (see Figure 1) [3].

This connectivity allows data collection, exchange, and analysis, as it facilitates the performance improvement across the production chain. It also enables the manufacturing sector to make huge innovative leaps, gain significant extroversion, and develop activities that were previously impossible.

It should be emphasized that the complete transformation of the supply chain into a truly integrated and fully automated process based on the IIoT presupposes the continuous and uninterrupted exchange of information from every stage of the production scale. For the implementation of this communication, IIoT systems are often combined in a multilevel architecture, in which at the hardware level are considered the physical systems (for instance sensors, actuators, control systems, security mechanisms, etc.), at the network level the physical networking media (wired and wireless), and finally at the upper layers the protocols that collect and transmit information from the communications stack.

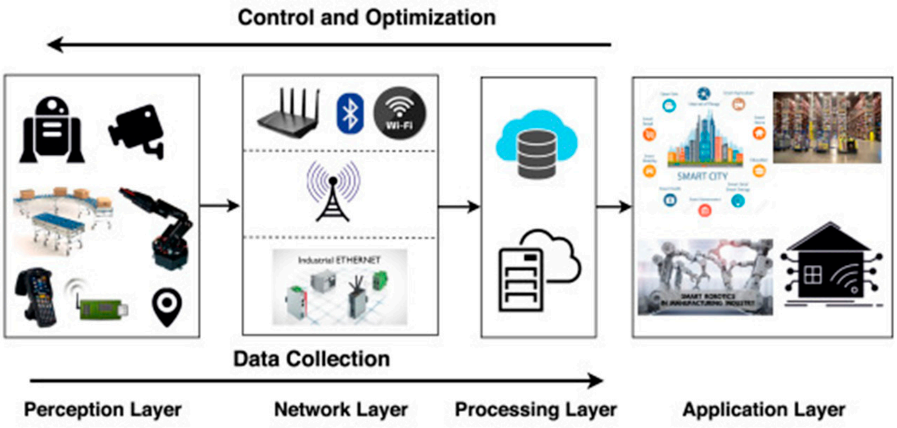


Figure 1. Generalised IIoT system architecture.

The continuous increase of connectivity and the use of standard communication protocols, which are implemented under Industry 4.0 standard, however, creates a strong need to protect critical industrial systems from cyber security threats [4]. The industrial systems that control the production process and the operation of the smart factories have constant access to the internet and the industrial networks, but in addition to the information and data of the company to which they belong. Common devices of this type are called industrial control systems (ICS) [5]. The most common ICS are SCADA (supervisory control and data acquisition) systems and sensors used in control loops to collect measurements and provide process automation [6]. These systems are interconnected within the IIoT network; they are active devices in real-time industrial networks, which allow the remote monitoring and control of processes, even when the devices are located in remote areas.

This networking and connectivity improve the operational efficiency of the system, but at the same time, they pose significant challenges for the means of securing the infrastructure [7] in terms of confidentiality, integrity, and availability. Another very important factor that further deteriorates systems' integrity is that both the machines and the devices in modern industrial facilities are designed initially to facilitate functionality and not to provide a secure environment, which makes them particularly vulnerable to cyber-attacks.

Exploiting the vulnerabilities of the communication protocols that are widely used in the Industrial IoT, as well as the vulnerabilities related to their operational control and how to use them, may result in compromising the critical devices applications, the denial or non-availability of essential services, or even their partial or total destruction, with incalculable consequences [8].

Generally speaking, the most relevant studies conducted so far focus on the security risks in IoT systems. For the particular environment of the Industrial IoT systems, however, there is no available extensive research to our best of our knowledge. In addition, the existing studies fail to contribute substantially to the awareness and clear understanding of the risks associated with IIoT systems as well as the severity of the attacks against them, which in most cases results in great damage and even loss of human lives.

In this sense, this paper presents an extensive study of the most popular ways of attacking industrial applications, as well as the corresponding literature studies related to them, with the aim to provide a more effective, cyber-security-oriented approach and ultimately lead to a more resilient industrial environment.

The main contribution of this work is to provide researchers, but also organizations dealing with Industrial IoT technologies in general, with a comprehensive study on issues related to cyber threats on industrial equipment, as well as the latest countermeasures for the protection of the infrastructure in question, through a critical and benchmarking framework. In this context, the main difference from the other IIoT surveys is the provision of a complete, up to date, and valid reference framework for the identification and the assessment of the risks related to the ever-evolving industrial environment.

The study is organized as follows: Section 2 reviews related work, and Section 3 gives a detailed description of the main risks that can be found in the Industrial IoT environment, the ways they operate, and the associated effective solutions that have been proposed in the most recent literature. Section 4 presents the main results of our study, and finally the last section draws the conclusions and outlines future research directions.

2. Metasurvey

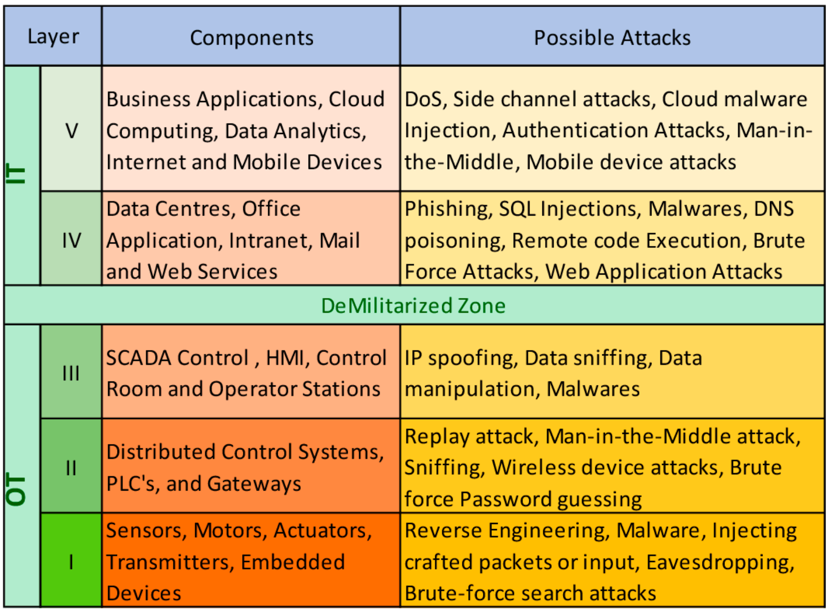
In this section a literature review on the surveys works on the threats associated with the industrial IoT systems. The main security risks are discussed, along with the suggested countermeasures. In particular, we discuss their contribution in the field, and we raise topics of interest that require further investigation and analysis.

Some of the modern attacks on critical infrastructure networks, such as power grids [9], are related to undermining actuators or sensors located in the physical layer, attacks against connections between different devices in the data-link layer, or more specialized attacks to compromise specific control systems such as SCADA devices [10].

SCADA devices are industrial automation control and telemetry systems, consisting of local controllers, which communicate through the industrial IoT network. In cases of advanced cyber-attacks [11], actuators or sensors isolation strategies are usually performed in order to falsify the normal values of the sensors and alter the mode of operation of the cyber-physical systems in an advanced industrial environment. For example, in a cyber-attack on a SCADA potable water disinfection system, the automations related to the treatment and production of clean water, the special flow meters, level, conductivity, and pH analysis, as well as the pumps that calculate the doses of chemicals, could be altered with devastating results for public health.

This study in particular simply lists the building blocks of a functional SCADA architecture, while an analysis of the attacks in the physical layer is completely superficial. In addition, the authors report five types of attacks and attack vectors (source code design and implementation, buffer overflow, SQL injection, cross site scripting (XSS), and effective patch management application), without providing information on the attacks against the software and without giving detailed explanations that could focus on specific methodological approaches on mitigation or prevention. Finally, regarding the communication layer of SCADA systems, the study is devoted to superficial references to the general ways of attacking communication systems and specifically to the unnecessary ports and services, communication channel vulnerabilities, and vulnerabilities of communication protocols. In summary, this study fails to contribute substantially to the awareness and clear understanding of the risks associated with SCADA systems as well as the severity of the attacks against them, which in most cases results in great damage and even loss of human lives.

A more careful approach to the threats related to the industrial IoT systems is presented in [8], where the authors provide a detailed list of possible attacks per layer of the five functional levels of the industrial IoT, with the first three being part of operational technology (OT), while the other two are part of information technology (IT) (see Figure 2). The first functional level includes systems that perform the physical processes of the IIoT, such as embedded devices, sensors, actuators, transmitters, and motors. Attacks aimed at this level require an excellent knowledge of the design of the IIoT system, and access to the specifications of active devices, engineering plans, and detailed information about their installation and operational functionality. The second functional level incorporates the specialized equipment, which communicates and controls the devices of the first level, such as distributed control systems (DCS), programmable logic control (PLCs) and gateways. Attacks at this level aim at preventing legitimate communication between the two levels and controlling the flow of communication. The third functional level is the SCADA and all related industrial automation control and telemetry systems, such as data acquisition devices, master stations, and human machine interfaces, which communicate via the IP protocol. Many of the attacks at the SCADA level rely on IP packet creation techniques with false attributes such as the source address, in order to disguise the identity of the sender of the packet, encouraging the recipient to think that it came from a legitimate network user. The fourth functional level includes business planning services, such as office applications, intranet, web, and mail services. Attacks targeted at this level exploit known or unknown vulnerabilities of these services and enter malicious code where the application expects legitimate data from the user in order to gain access with administrator privileges.



Layer		Components	Possible Attacks
IT	V	Business Applications, Cloud Computing, Data Analytics, Internet and Mobile Devices	DoS, Side channel attacks, Cloud malware Injection, Authentication Attacks, Man-in-the-Middle, Mobile device attacks
	IV	Data Centres, Office Application, Intranet, Mail and Web Services	Phishing, SQL Injections, Malwares, DNS poisoning, Remote code Execution, Brute Force Attacks, Web Application Attacks
DeMilitarized Zone			
OT	III	SCADA Control , HMI, Control Room and Operator Stations	IP spoofing, Data sniffing, Data manipulation, Malwares
	II	Distributed Control Systems, PLC's, and Gateways	Replay attack, Man-in-the-Middle attack, Sniffing, Wireless device attacks, Brute force Password guessing
	I	Sensors, Motors, Actuators, Transmitters, Embedded Devices	Reverse Engineering, Malware, Injecting crafted packets or input, Eavesdropping, Brute-force search attacks

Figure 2. Layered IIoT architecture and possible attacks.

The fifth functional level includes high level services such as analytics, data mining methods handled by the enterprise applications, and cloud computing services. Attacks at this level include a set of malicious actions like interception and deception, but also more advanced types such as adversarial attacks.

It should be noted that the authors of this study, between levels three and four, place a demilitarized zone that includes service servers to which users connect on untrusted networks.

Although this study provides a solid approach on how the IIoT works and the corresponding vulnerabilities associated with it, it is generally considered incomplete, as it does not provide examples of similar attacks, or techniques that could prevent them. It is rather a survey on the known types of attacks, which provides some minimal information that can be easily extracted by the literature.

A holistic approach based on the business planning and the standardization on security requirements designed by the standardization bodies Industrial Consortium and OpenFog Consortium is presented in [12]. Given the complex nature of the IIoT ecosystem, the paper examines the security requirements of industrial connection and communication protocols, based on a three-tier architecture and whether these protocols used at each level provide a certain level of security. In particular, it initially presents an abstract three-tier IIoT architecture, which includes the main components of most IIoT developments, categorizing it in a very clear way (Figure 3).

The edge tier consists of end-points and edge-based gateway devices, composing a proximity network, which connects sensor devices, actuators, and control systems. The gateway devices provide a grouping point for the network, allowing internal inter-level communications, but also layered communications with the higher second level, the platform tier, where the connection is made as an access network for data transfer and control between the levels, which is implemented as connectivity via internet or mobile network. The platform tier contains service-based and middle-ware applications, such as analytics services, data transformation, data integration, etc. The interface with the third and higher level, which is called the enterprise tier, is done with a service network, which is mainly based on the Internet. Finally, the enterprise tier is used for high-level services, such as enterprise applications, cloud computing, domain services, hosting, etc. At this level, end users can interact with the network through specially designed interfaces. Based on this architecture, T. Gebremichael et al. proposed a set of connectivity protocols per level and the security features required for the secure device implementation in IIoT networks. The expansion of these implementation technologies also allows for the distribution of security requirements between the different areas of the network and creates embankments that could serve as backup protection in the event of wide scale breaches.

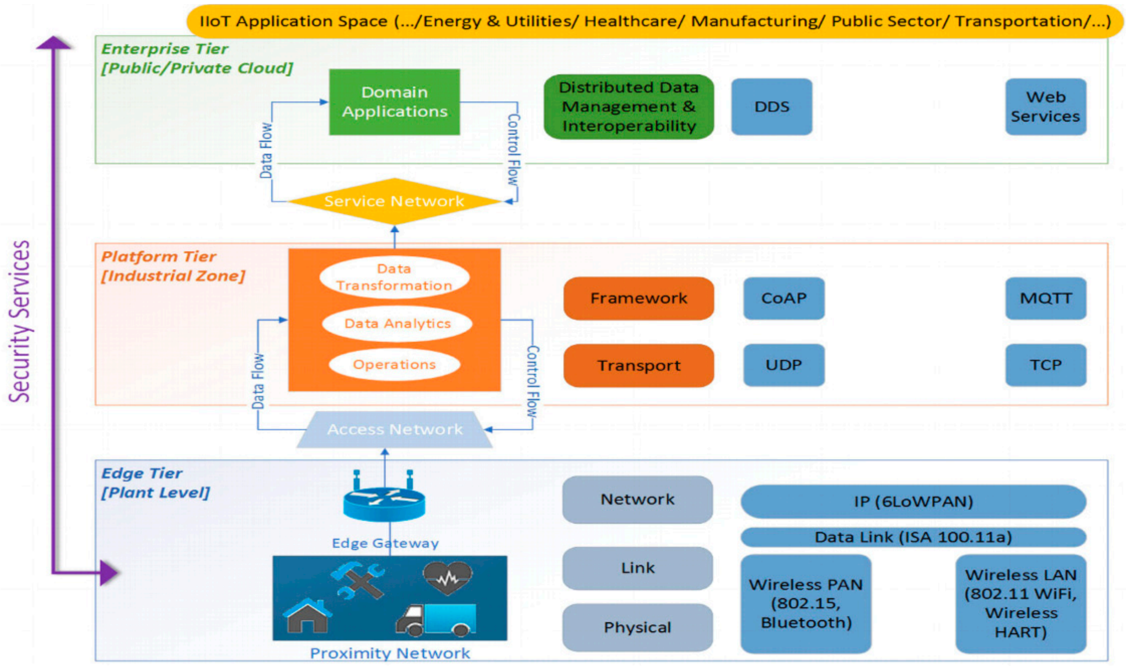


Figure 3. Three-tier architecture of IIoT connectivity and communications standards.

Finally, the authors of study [13] present a detailed study on SCADA attacks. SCADA systems are the main hardware of the IIoT ecosystem, consist of various entities organized in a hierarchical structure, and are used to monitor the various industrial processes. They include techniques of integration of data acquisition systems, data transmission systems, and human–machine interface (HMI). HMI is a user interface that connects a person to a device, mainly used for data visualization and production time monitoring, while also visualizing machine input and output information. The general description of SCADA architecture includes the master station/terminal unit or master unit (MSU/MTU) which is the control center of a SCADA network, the sub-MSU/sub-MTU acting as a sub-control center, the remote station units/remote terminal units (RSUs/RTUs), acting as the intelligent end devices (IEDs), and the programmable logic controller (PLC), used to monitor or collect data from sensors and actuators. This study summarizes the most typical attacks against SCADA systems, the ways in which they occur, and the tools commonly used. More specific, the following modes of attack are presented.

1. Passive or Active Eavesdropping. By accessing the wired or wireless network [14] between MTUs and sub-MTUs or RTUs, an attacker could install spyware [15] and proceed to exploitation [16].

2. Man-in-the-Middle (MitM). In this type of attack, the attacker intercepts and monitors the network traffic, inputs manipulated data during transmission, and sends it to the receiver [17,18]. In the event of a successful breach, he takes over the session and maintains the connection from a spoofed IP to avoid detection [19,20].
3. Masquerade. The attacker uses a fake identity and IP spoofing to pretend to be a legitimate network user in order to steal information from the system or network [21,22]. Then, by launching a brute force attack, stolen passwords can be used to gain unauthorized access to important information [23].
4. Virus, Trojan Horse, and Worms. An attacker could send malicious code to MTU after launching a MitM or Masquerade attack [24–26]. Malicious code can either allow unauthorized users to access the infected system and use it to launch other attacks on other infrastructure, or it could spread to the network and infect MSU/MTU, often causing unstable behavior or even total system collapse [27,28].
5. Denial of Service (DoS) or Distributed Denial of Service (DDoS). Malicious RTUs send random IP packets to the MTU in order to consume the system's resources with the final objective of making it inoperable [1,29–34].
6. Fragmentation. This is a type of DoS attack where the attacker exploits the weaknesses of the network packet reassembly process, so when the size of the transmitted data is larger than the maximum transmission unit, the MSU/MTU fails to service and collapses [3,35–37].
7. Cinderella. This attack occurs when a malicious user, after attacking and gaining access to a system, changes the internal clock of the network, resulting in the premature expiration of the security software, thus increasing the vulnerability of the network [38,39].
8. Doorknob Rattling. It is related to the preparatory actions used to prepare for an attack, including legitimate procedures for testing the system, for instance limited attempts to access the system with random criteria in order to evaluate the readiness and the responsiveness of security measures [40,41].

Given the complexity of the architectures associated with SCADA systems and related prototypes, Ghosh and S. Sampalli provide a comprehensive study of the current security standards (IEEE 1402, ISO 17799, ISO 15408, NERC security guidelines, NERC 1200, API 1164), the detection of SCADA mechanisms (including machine learning algorithms such as Naïve Bayes, Random Forest, Decision Tree Algorithm, etc.), and prevention of SCADA attacks which involve the adaptation of key management schemes such as cryptography (SCADA key establishment (SKE)), SCADA key management architecture (SKMA), and logical key hierarchy (LKH).

3. Cyber Threats and Its Countermeasures

Automation and remote control are today the most important methods by which critical infrastructures [42] improve the productivity and quality of their services. Under this spectrum, the efficient management of IIoT systems requires maximum accuracy, reliability, and security. The digital technologies that are part of the IIoT ecosystem undoubtedly improve the efficiency of critical infrastructures, but at the same time, they are associated with significant challenges related to the ongoing threats to the digital security of the infrastructures in question [43]. In this spirit, the protection of the IIoT is now paralleled with the general need to protect the critical infrastructure of a country, such as telecommunications, water and energy networks, government infrastructure, etc., as the systems emerged in these infrastructures are directly related to the IIoT environment, which is an ideal target for large-scale cyber-attacks.

In the following subsections, we classify the IIoT threats in five generic categories: phishing attacks, ransomwares, protocol, supply chain, and system attacks [44]. This separation enables a clear and comprehensive presentation of the security risks and the associated counter-measures as specialized in the Industrial IoT environment.

3.1. Phishing Attacks

This is a very popular type of attack often used to steal user sensitive data. It occurs when an attacker, pretending to be a trusted entity [45], misleads users into entering personal information into a fake website or downloading an attachment, which results in the installation of a malware or the disclosure of sensitive information. For critical infrastructures, specialized phishers use advanced techniques, called compromised attacks, that combine social engineering, aiming at both the lack of specialized active security measures by systems, and the lack of information or vigilance of users. The techniques include zero-days malware, link manipulation, filter evasion, obfuscating brand logos, website forgery, covert redirect, etc., aimed primarily at vendor/remote websites and then the breach of IIoT systems and in general the control of operation systems that linked to it. In general, the malicious user tries to enter or access the IIoT through a front-end level. He remains there for a period of reconnaissance and mapping of the general network, until the most appropriate time is found to start the extensive attack and then with pivoting (the action of moving from one system to another) to apply the appropriate exploits and compromise ICS systems.

In general, there are several papers that focus on malicious website crawling based on specialized techniques. Madhusudhanan et al. [46] propose a new technique called PHONEY, which automatically detects and analyzes phishing attacks. The main idea behind this technique is a web browser extension, which provides information on the quality of the sites, the security certificates they have, and information that they have been confirmed to contain malicious code or misleading URLs (see Figure 4).

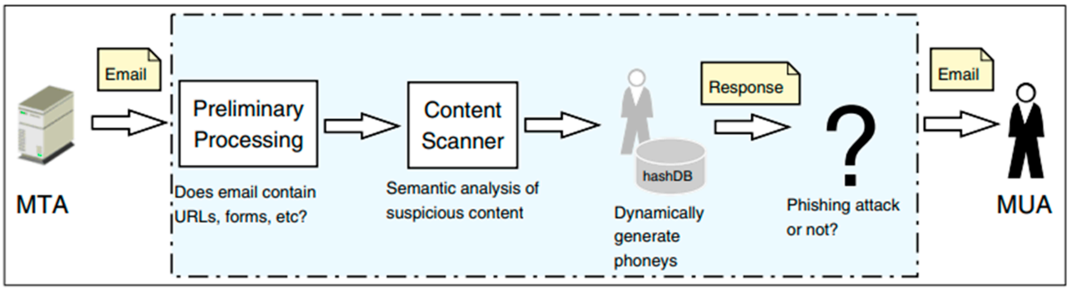

Email
MTA
Preliminary Processing
Does email contain URLs, forms, etc?
Content Scanner
Semantic analysis of suspicious content
hashDB
Dynamically generate phoneys
Response
?
Phishing attack or not?
Email
MUA

Figure 4. Block diagram of PHONEY architecture.

McRae and Vaughn [47] introduced a new method to detect sites that contain phishing content using honey tokens. Accordingly, Ajlouni et al. [48] use a methodology based on association rules and the classification and detection of phishing sites. This algorithm generates correlations between objects and then creates correlation rules between objects, where each correlation rule signals the dependence of a set of objects on another set of objects, for the purpose of final ranking and locating content that indicates if a site is relevant with deceptive actions. It should be noted that the authors applied these algorithms to phishing data sets, and the obtained result was very accurate and surpassed more advanced algorithmic standardizations such as the SVM algorithm. Finally, Jain and Richariya [49] implemented a prototype web browser used as an agent to process data from phishing attacks. The user uses the web browser to open the email in a secure environment, and if an attack is detected, they will be notified and asked to delete the email.

An advanced machine learning technique is proposed by the work of [50] and specifically the intelligence web application firewall (IWAF) to critical infrastructure protection (CIP), an advanced phishing attacks detection system. It is an extremely innovative and fully automated active security tool, which uses an evolving Izhikevich spiking neuron model for the automated identification of phishing web sites and builds group policy objects (GPO) and pushes them into Windows domain. This system optimally implements a decision rule for the categorization and detection of phishing attacks, while at the same time, this knowledge is translated into firewall rules to enhance the active response capabilities of critical infrastructure.

In particular, IWAF initially receives network traffic between Industrial IoT devices as a PCAP (packet capture) file, from which the features of interest are extracted and are able to detect phishing attacks. The proposed Izhikevich spiking model algorithm uses the exported features and performs categorization to detect phishing attacks. When such an attack is detected, a list of indicators of compromise (IoCs) is created. IoCs are forensic data, such as data found in system logs or file logs, that detect potentially malicious activity on a system or network. IoCs are converted to group policy objects (GPOs). GPOs are a set of settings that determine what a system will look like and how it will behave for a defined group of users in the Windows environment. With a scheduled task, these policies are forwarded to specific organizational units (OUs) of Windows Active Directory and are applied to all users, effectively creating rules to prevent and limit phishing attacks.

A promising technique called URL embedding (UE) was introduced by Yan et al. [51]. This new algorithm is used to investigate the correlations between different domain names, in order to calculate correlation coefficients between different URLs. Obviously, this technique creates serious demands on computing resources, especially when analyzing domains with sparse representations, as URLs can be distributed over the Internet. In this case, the distributed representation is transformed into a small vector with the help of a neural network, and thus the mapping between the URLs and their distributed representations is stored without much trouble. An obvious disadvantage of the method is the complexity of the space, and it takes a lot of space to store the domain integration model, as many dimensional vectors have to be stored. To solve this problem, the authors suggest that malicious websites be treated as words and then use intelligent machine learning algorithms to locate the words in question in DNS queries, so that misleading malicious addresses are detected before they are even executed.

Gu et al. [52] proposed a method for detecting botnets by mapping a sequence model based on extracting URLs from spam mails. Additionally, Ma et al. [53] studied various machine learning methods for classifying sites based on their characteristics and the content they included. Features such as IP addresses, WHOIS records, and lexical features of phishing URLs have been analyzed by McGrath and Gupta in their work [54], with their findings constituting an index of heuristic methods for filtering phishing-related emails, but also more generally in detecting suspicious domain registrations. Xie et al. [55] focus on detecting spamming botnets by developing regular signatures based on expressions from a set of spam address data. Stalmans [56] proposed a technique for detecting and mitigating botnet infection on a network, using features from DNS queries such as multiple Address (A) and NS Records, IP ranges, Time-To-Leave (TTL), and alphanumeric characters from domains.

Finally, the work of [50] proposes the creation of an innovative protection system from fast-flux botnets, which use as communication points domain names created with the domain generation algorithm (DGA) technique. Unlike other techniques that have been proposed and focus on DNS traffic analysis, this system proposes the creation of a Smart URL Filter in a zone-based policy firewall for detecting algorithmically generated malicious domain names. It is a biologically inspired artificial intelligence computer security technique, as it uses the evolving spiking neural network (eSNN), which is the third and most advanced generation of neural networks, which simulates in the most realistic way the functioning of the human brain.

The superiority of the proposed method was demonstrated after a thorough comparison of the prediction accuracy and the ability to generalize to new data, with corresponding evolving and bio-inspired learning methods.

3.2. Ransomware Attacks

This type of attack inserts a malware into the IIoT system in order to cause denial of service (DoS) or access to personal files and demands the users pay a fee in order to regain access. In contrast with the conventional ransomwares, which are distributed massively, IIoT ransomwares are usually targeted, i.e., they focus on critical system entities in order to cause as much damage as possible. Due to this limitation, the research conducted on the common ransomwares cannot be considered as applicable in IIoT ransomwares. The authors of [57] offer a detailed and systematic analysis of the various threats imposed by IIoT ransomwares and recommend some potential countermeasures. Their analysis suggests that the IIoT edge gateways are very vulnerable to ransomware attacks in IIoT systems. In an industrial environment, the IIoT gateways have some common properties, despite their partial differences in functionality and architectures. A typical IIoT edge gateway acts as a bridge between the external world and the critical IIoT infrastructure, that is, program logic controllers (PLCs) or input/output (I/O) devices. When an attacker launches a successful ransomware attack against an IIoT gateway, it can take full access of it by replacing the gateway's password with a new one and then updating the existing firmware with a malicious one. Even if the user bypasses the locking, the attacker can still access and encrypt all user and data files, including those collected from the PLCs and I/O devices, and those exchanged between the cloud and the enterprise. Then the attacker can ask for ransom in order to decrypt the data, or threaten the victim to gradually delete the data if the ransom is not paid.

To analyze the vulnerabilities of IIoT edge systems, M. Al-Hawawreh et al. built an experimental testbed of an IIoT system, which follows the industrial internet reference architecture (IIRA) (see Figure 5) [26].

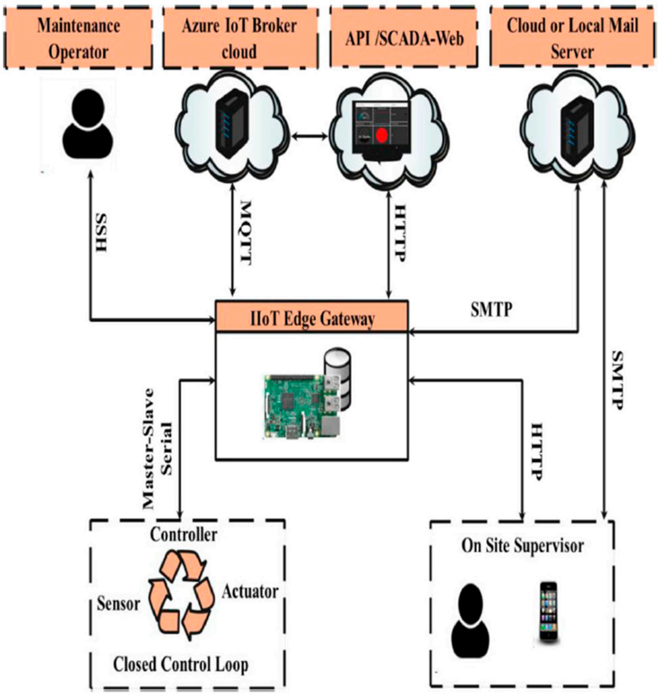


Figure 5. IIoT system Testbed for the analysis of ransomware attacks.

Their platform consists mainly of three parts: the IO devices (IoT sensors, controllers, and actuators), the cyber world entities (maintenance operators, mail and cloud servers for processing the collected IoT data, and SCADA web monitoring devices), and the IIoT gateways. Then they conducted proof of concept (PoC) ransomware attacks on this platform using python scripts resembling the well-known Erebus Linux Ransomware attack. This targeted IIoT ransomware attack affected a big number of web services and database and multimedia files of a web hosting company when launched [55]. According to Reference [58], the main steps of this attack include sniffing for data and system files in predefined directories of the IIoT edge gateway, data encryption and deletion of the original files, sending the stolen data as an attachment in a message to a fake email address via simple mail transfer protocol (SMTP), and eventually sending notification messages to the user that a ransom is requested. In the compromised IIoT edge gateway, M. Al-Hawawreh et al. collected and processed data related to the system's activities in terms of CPU, memory, and I/O device usage and CPU processing load, and they compared with the corresponding data collected by the system when no ransomware attack is carried out. Their results suggest that the targeted ransom attack at the IIoT edge gateway caused much higher usage and processing power of system resources in comparison with a similar ransom attack in a workstation. Based on these observations and measurements, the authors concluded that the monitoring of the kernel-related activity parameters can be a significant indicator of a crypto-ransomware attack launched towards IIoT edge gateways. Then M. Al-Hawawreh suggested some countermeasures that should be taken to protect more efficiently the IIoT infrastructure from these attacks, including the deployment of Next-Generation firewalls with improved traffic filtering capabilities, the employment of monitoring tools, such as intrusion detection systems (IDSs), for detecting attacks in the early stage, and the separation of the IIoT edge gateway from the other IIoT infrastructure, by placing the IIoT edge gateway in a specific trusted zone.

Apart from the conventional methods for identifying ransomware attacks, there are many studies that have utilized machine and deep learning techniques for ransomware detection. The authors of [59] introduced a detection model using dynamic machine learning techniques, such as conversation-based network traffic features, for consistent detection of windows ransomware network attacks. Their experiments demonstrated that the database created by these features achieves a high performance in terms of accuracy. The authors of [60] implemented a network-based intrusion detection system, by employing two independent classifiers operating in parallel on two different levels: packet and flow levels for detecting the Locky ransomware. Experimental evaluation of the proposed model found very efficient in tracking ransomware attacks with high detection accuracy.

Finally, the authors of [24] suggested a hybrid detection model combining classical auto-encoding (CAE) and variational auto-encoding (VAE) deep learning techniques to reduce data dimension and obtain a precise representation of the activities. The extracted features were combined to form a new vector used to train a deep neural network (DNN) classifier. The proposed model was compared with other models including random forest [61], decision trees [59], logistic regression (LR), support vector machine (SVM) [62], and DNN [63] and it was found that it achieves the best performance as measured by the detection rate (DR) and the false negative rate (FNR).

3.3. Protocols Attacks

The OSI networks structure consists of five layers for IoT: physical, data-link, network, transport, and application layer (see Figure 6) [64].

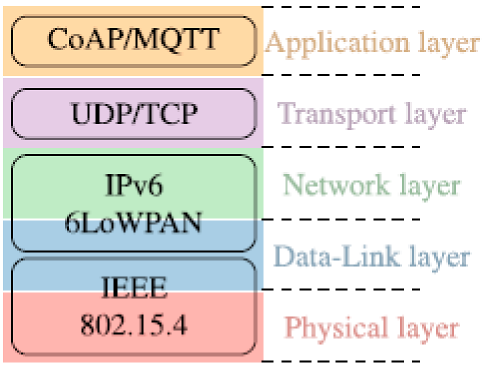


Figure 6. An example of IoT protocol stack compared to TCP/IP stack.

The IIoT systems may use the same protocols with the common IoT systems for implementing the first four layers of the stack, like for instance IEEE 802.15.4 6LoWPAN, Bluetooth Low Energy (BLE), IEEE 802.11 (used by WiFi), Long-Term Evolution (LTE), and

UDP/TCP (see also Figure 5). In our review, we provide a brief overview of the threats and countermeasures at the first four layers and focus on the fourth (application) layer, which is particularly applicable for the IIoT applications.

3.3.1. Attacks in Physical, Data-Link, Network, and Transport Layers

There are many works devoted to the attacks towards the layers and suggest the appropriate countermeasures [64–67]. Amongst the most common threats in physical and data-link layers is the denial of service (DoS) attacks. In this type of threat, the malicious device degrades the processing ability of the nodes, to make the system unavailable. Jamming, collision, exhaustion, and unfairness are the three most important methods in DoS attacks [67] In jamming DoS attacks, the attacker jams the signal by transmitting at the same frequency, whereas in tampering, the attacker takes over the control of the sensor node by physical means, for instance by wiring on the electronic board, or by attaching cables to the circuit board. For the detection of jamming DoS attacks, the authors of [65,67,68] propose a cross-layer security detection mechanism and a jammed area mapping model (JAM), which avoids the jammed part of the wireless sensor network (WSN) by re-routing the packets to alternative routes. Tampering threats can be identified and prevented by physical checking of the WSN by eye or with the use of special equipment.

In collision DoS attacks, the malicious device starts transmitting packets on the victim's frequency, causing collisions and packet retransmissions. If the collision attack continues until the energy resources of the targeted node are exhausted [69], it is also known as an exhaustion attack. The unfairness attack is caused when the exhaustion attack results in degrading the system ability in the advantage of the malicious users. Efficient defense against jamming and collision attack involves the employment of frequency-hopping spread spectrum (FHSS) technique [70,71] Data transit attacks are very common in physical and data-link layers of the IoT systems involving wireless sensor networks (WSN) and RFID sensor networks (RRSN) and include packet sniffing and Man in the Middle (MitM) attacks. Countermeasures to this type of threat include applying data encryption algorithms, such as asymmetric encryption standard (AES) in IEEE 802.15.4 and 6LoWPAN networks [72], wired equivalent privacy (WEP), and Wi-Fi Protected Access II (WPA2) in Wi-Fi and LTE networks [73].

The most popular threats at the network layer of IoT systems include routing and DoS, data transit attacks, and the attacks at the neighbor discovery protocol (NDP) [65] In routing attacks, the malicious device forwards the ongoing messages to the wrong paths, while in DoS, it causes traffic congestion and resource exhaustion by injecting a big amount of data into the network. Effective countermeasures at these types of attack include egress filtering, authorization, and monitoring tools, such as intrusion detection system (IDS) solutions specifically adapted for IoTs like SVELTE [74] Data transit attacks affect data integrity and confidentiality. Countermeasures include the use of compressed transport protocols, for instance datagrams transport layer security (DTLS) [72]. The threats against the neighbor discovery protocol (NDP) are presented in [75]. In this work, a detailed description of the operation and the most common attacks towards NDP is performed. In addition, the protection mechanisms for NDP have been thoroughly analyzed in this work, including the tunneling (IPSec) and the secure neighbor discovery (SEND) protocols. The analysis results indicate that for NDP, SEND is the most efficient protection mechanism against DNP protocol attacks, but it still lacks good support levels by most of the operating systems.

The most popular IoT attacks at the transport layer include de-synchronization, SYN-flooding, and message queue telemetry transport (MQTT) exploit attacks [65]. In de-synchronization attacks, the intruder injects packets with fake sequence numbers of control flags that de-synchronize endpoints. Effective countermeasures include message authentication [76–78]. In SYN-flooding attacks, the malicious device sends a large volume of SYN packets to the victim. The victim responds with SYN-ACKs, but the spoofed device does not send acknowledgements (ACKs). As a result, the victim's queue is filled up and cannot receive and process legitimate SYN requests. Defense against SYN-flooding attacks involves interventions and optimizations on the transport protocols themselves, by making the memory and the queue management more efficient in handling of SYN packets and by hardening the network security with the employment of packet filtering and proxy techniques [79]. The deficiencies of the message queue telemetry transport (MQTT) protocol are presented by the authors of [80]. MQTT is a simple messaging protocol, which adapts the publish-and-subscribe messaging approach and is specifically designed for the remote control of devices with bandwidth constraints, such as the IoT applications. MQTT is, however, very vulnerable to attacks, since it does not provide by default any data encryption and authentication mechanism. Defense against MQTT exploit includes the adaption of scalable and robust security mechanisms, such as the secure MQTT protocol, which enforces the security features of the attribute based encryption (ABE) algorithm. ABE supports broadcast encryption for secure message delivery to multiple intended recipients, which is a desired feature in IoT applications [81]. Table 1 summarizes the most common protocol attacks in IIoT, the threats, and the proposed countermeasures.

Table 1. Common attacks in the first four layers of IoT stack and possible countermeasures.

Layer/Level	Protocols	Threats	Countermeasures
Physical Layer and Data Link layer	IEEE 802.15.4 BLE WiFi LTE	Jamming DoS attacks	Packets' rerouting to alternative routes [68]
		Collision/Exhaustion/ Unfairness attacks	FHSS techniques [70,71]
		Data Transit Attacks	Data encryption algorithms [72,73]
Network Layer	IPv4/IPv6 RPL 6LoWPAN	Routing and DoS Attacks	Ingress filtering and IDS solutions [65,74]
		Data Transit Attacks	Compressed Transport protocols (for instance DTL) [72]
		Threats to Neighbor Discovery Protocol (IPv4/IPv6)	Use of IPsec, SEND protocols [75]
Transport Layer	De-Synchronization	Sending control flags that synchronize endpoints	Message authentication [77]
	SYN-flooding	System flooding during the SYN handshaking phase	Optimizations in transport layer apply network filtering [79]
	MQTT	Data Transit Attacks, Scalable Key management	Secure MQTT, ABE algorithm [81]

3.3.2. Attacks in Application Layer

Among the most popular attacks towards the application layer of IIoT systems is related with the Modus protocol used by SCADA systems and is studied by the authors of [82]. In particular, they present a very specialized study, a model in the way of attacks against the sensors, used by the control loops for the collection of measurements in SCADA infrastructure in gas pipeline and water storage tank implementations. Sensors, which are active devices in the infrastructure network, are PLCs that are conveniently interconnected to allow remote monitoring and control of high-speed response processes, even in cases where the devices are distributed between different remote points. Communication (sending and receiving data) is achieved with the widely used SCADA Modbus messaging protocol, which provides client–server communication between devices connected to different types of bus or network, via serial lines.

In the simulation performed in this study, Modbus Masters devices request information on the transfer of discrete, or analog IO communication and the recording of data by a slave Modbus. A simple request–response scheme is used for all executed transactions, where the master device starts a request and the slave responds. The authors, considering that the implementation of the Modbus protocol contains many vulnerabilities, simulate these vulnerabilities, in a context of recording and evaluating the different types of attacks that can take place.

A vulnerability lies in protocol's inability to recognize a forged slave–master IP address in the SCADA network. An unauthorized, remote intruder performing a Man in the Middle (MitM) attack exploits this vulnerability, by sending queries containing invalid addresses, and then collects information about the network MSUs/MTUs from the returned messages.

Another vulnerability is the lack of adequate security checks and control of the physical identity/certification address to validate the communication between the Modbus master and slave devices. This defect allows remote intruders to issue arbitrary commands without authentication towards any slave device, via a Modbus master. The SCADA Modbus protocol is also vulnerable due to the protocol implementation errors when processing request messages and separate input read responses. Thus, an unauthorized, remote intruder can perform a DoS or DDoS attack on a SCADA network, by sending request or response parameters containing malicious values to select a data field on the system that contains a vulnerable Modbus application.

Finally, Modbus TCP is the protocol commonly used in SCADA networks for process control. Modbus limits the PDU size to 253 bytes to allow the package to be sent in serial RS-485 interface. Modbus TCP adds 7 bytes to the Modbus protocol header. This sets a limit on the legal package size. When an attacker creates a specially designed packet larger than 260 bytes and sends it to a Modbus master–slave, if the devices for rejecting such packets are not properly configured, it leads to a successful buffer overflow attack.

The most common security countermeasure is the use of intrusion detection and prevention systems with deep packet inspection capabilities or industrial firewalls that have the ability to detect and stop highly specialized attacks hidden deep in the communication flow [83]. For example, Liang et al. [84] propose an industrial network intrusion detection algorithm based on a multi feature data clustering optimization model. The novel features are twofold: to rapidly select a node with high-security coefficient as the cluster center, and match the multi feature data around the center into a cluster. The detection accuracy of abnormal data reaches 97.8%, and the fault positives of detection are decreased by 8.8%. Additionally, a novel network intrusion prevention system that exploits the benefits of incremental machine learning frameworks that utilizes a self-organizing incremental neural network along with a support vector machine is proposed by Constantinides et al. [85]. The results show that the proposed framework can achieve on-line updated incremental learning in a fast and efficient manner, making it suitable for efficient and scalable industrial applications. Moreover, intrusion detection methods are based on machine learning to access the Modbus TCP protocol development by Deng et al. [86]. It is a data preprocessing method based on the frequency of Modbus protocol function code and coil that appears in Modbus TCP traffic in order to detect the abnormal Modbus TCP traffic by a support vector machine model. On the other hand, cloud-based intrusion and prevention systems for industrial networks are promising solutions to secure these infrastructures. Brugman et al.) propose a highly accurate novel cloud based intrusion detection and prevention architecture to identify and prevent cybersecurity threats in industrial networks using software defined networking to route traffic to the cloud for inspection using network function virtualization and service function chaining. The proposed method uses Amazon Web Services to create a virtual private cloud for packet inspection that ensures scalability, resilience, and visibility.

3.4. *Supply Chain Attacks*

Supply chain attacks are particularly dangerous. The major challenge for IIoT integration in the Industry 4.0 supply chain is security. Hardware chips with embedded malicious code are hard to find, since this code has the ability to be executed without being easily noticed for a long period of time. One of the causes of security vulnerabilities in the IIoT environment is the involvement of many stakeholders. This means that there are different components of devices being manufactured by different vendors, everything getting assembled by another vendor, and finally being distributed by yet another one. This situation today, which is not easy to avoid, usually leads to security issues (backdoors installed) that can put an entire production line at risk (see Figure 7). In general, what is today called third party is gaining the attention of risk management more and more. M. Farooq, in their study [87], presents and highlights the supply chain threats, and they suggest approaches concerning the risk management procedures. They present and describe the IoT supply chain risk landscape, characterizing it as extremely diverse.

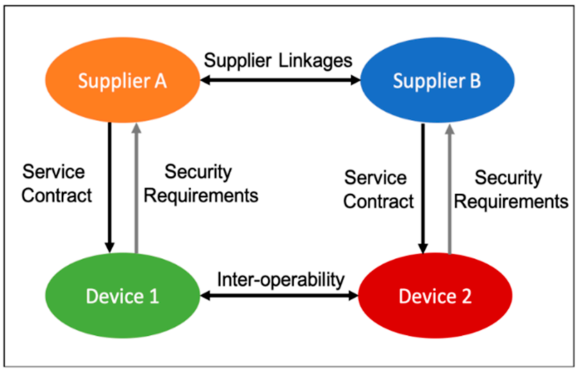


Figure 7. Key interactions between different players in the supply chain ecosystem of the IoT.

This work may describe the IoT, but the situation is similar in the Industrial IoT environment, since they share a number of protocols. A vendor has the ability to embed backdoor channels in their devices, inject viruses, or provide faulty chips. The supply chain risks are hard to observe and hard to control. The risk propagates from one device to the other and gets amplified as the IoT ecosystem becomes more complex. Another issue is to dissect the supply chain links in IoT, meaning that the interactions between devices, between suppliers, and among them are always difficult to determine. Further, they highlight the IoT risk implications and consequences, and finally as a countermeasure, they propose to view the ecosystem from a supply chain viewpoint and then take appropriate measures to control the risks. They describe two approaches, the top-down approach, which is more centralized, and the bottom-up approach, which focuses on decentralization.

This work gives a general understanding of the supply chain risks, but it does not provide technical countermeasures to deal with these types of attack for an environment that already faces this threat and does not have the ability to change the whole risk management approach.

Petar Randaliev [88], in their study, presents a dynamic and self-adapting supply chain system supported with artificial intelligence (AI), machine learning (ML), and real-time intelligence for predictive cyber risk analytics. This approach is used to develop a transformational roadmap for the Industrial Internet of Things in Industry 4.0 supply chains of small and medium enterprises (SMEs), because these types of companies usually lack the resources needed to effectively mitigate the high risks that the cyber threats are posing. One interesting point of discussion from the main findings is the weakness of existing cyber risk impact assessment models to calculate the impact of supply chain infrastructure. Additionally, there is an inconsistency in measuring the supply chain cyber risks, caused by the lack of understanding of supply chain operations in Industry 4.0.

Timothy Kieras et al. [89] presented in their study the RIoTS (risk analysis of IoT supply chain threats), which is risk analysis methodology in networked systems such as the IoT that emanate from the suppliers of individual components. They argue that risk analysis must shift from a vulnerability-centered approach to the modeling of suppliers and components as a system. They propose an adaptation of the attack tree techniques in order to include the risk associated from suppliers and supplier groupings. Their intention is to highlight and reveal hidden threats posed to the IoT ecosystem from potential supplier collusion. As we see, most studies focus on risk management approaches for supply chain attacks.

3.5. Systems Attacks

One of the most common attacks on industrial infrastructure is related to SCADA systems, which due to their proliferation and usability are found in many industrial infrastructures worldwide. Given the complexity of the devices in question, the heterogeneity of industrial networks, and the seriousness of the implementations in which these systems are located, such as water, energy, etc., networks, ref. [90] presented a study of how to attack SCADA devices, while at the same time they studied, applied, and proposed a specialized solution for their timely and valid detection. They deal in particular with the case where the attacker is taking advantage of the fieldbus communication in the industrial EtherNet/IP protocol, after performing a Man-In-the-Middle (MitM) attack in an Ethernet ring using the device level ring (RLR) protocol, and finally they carry out a stealthy sensor attack. Fieldbus is an industrial network system for distributed real-time control. It operates on a network structure that typically allows daisy-chain, star, ring, branch, and tree network topologies. In fieldbus communication in the industrial EtherNet/IP protocol, devices use IO settings, messages that do not follow specific formats and sizes, as they are specified by the controller designer. Additionally, the analog sensor control signals are coded using 4–20 mA measurements. This means that the attacker must have, in addition to detailed knowledge of the system design, access to the specifications of the devices, engineering, and installation drawings in order to fully understand the information exchanged and rearrange the sensors to his advantage.

Wireless communication between sensors and control devices is performed via multicast EtherNet/IP connection over user datagram protocol (UDP). While only devices that subscribe to a specific multicast address will receive multicast packets, multicast is IP-level, so all UDP packets arriving at a specific destination address will be accepted. The IP version 4 (IPv4) multicast service uses Class D address space (224.0.0.0–239.255.255.255). The data transmission in IPv4 multicast is done without ensuring the accurate transmission of data to the information receivers, unlike what happens to the other datagrams of the Class A–Class C address spaces. As IPv4 multicast is organized, the data are transferred to UDP datagrams. Each address in the Class D address space represents the group of those who wish to receive the data. A host joins the group by sending a JOIN Internet Group Message Protocol (IGMP) message. He can then participate in the group without time restrictions (there is no concept of group ownership). Additionally, in order to send data to a group, it is not necessary to be a member of the group, or to monitor the transmitted information, so it is generally very easy to install an intruder as MItM.

After establishing MItM, the attacker launches a stealthy sensor attack. This attack configures the sensors and actuators settings, in order to change the operation of specific mechanisms, but this is not perceived by the monitoring mechanisms of the system. More specifically, in this attack, there is a raw water storage tank, which includes a water level sensor, a valve that opens when a sensor shows the level <0.5 m and closes when the level is >0.8 m, and a pump whose action depends on the UF process, in which forces such as pressure or concentration gradients lead to separation through a semipermeable membrane. If the water level in the tank is below 0.25 m, the pump is immediately switched off, which is interpreted as a safety mechanism. The attacker's goal is to exaggerate the water without being detected by a typical detection mechanism based on the detection of anomalies. This is achieved by modifying the sensor and actuator information by constructing appropriate packets, which are adapted so that the fieldbus communication can change the functionality of the devices.

F. Mercaldo, et al. operate in a very intelligent and simple way, as through a time logic and specifically taking advantage of high-level features related to SCADA infrastructure and modeling the system logs in a network of synchronous automata, they characterize the behavior of SCADA system, whether it accepts an attack or not. More specifically, the process initially involves distinguishing logs from SCADA system logs. The record values are associated with the actual measurements performed by the system operating personnel. The received distinguished values are then classified into three classes (up, basal, and low). The values in question are then entered into an automated system (The automated systems implement automata, i.e., mathematical objects that maintain abstract finite state machines for resolving complex problems. In an automated system, specific transitions are allowed among the states.). As the automaton sees an input symbol, it performs a transition to another state, depending on the transition function. For each discrete situation, an automatic is implemented, which is synchronized with a specific clock. For every status change, a status table is implemented, in which the system states are presented in time format. To detect overflow or underflow, the automatons are checked at random times, and if there is a deviation from the status table, then they are related to the attacks against the system.

Although various intelligent techniques have been proposed for the analysis of Internet traffic between IIoT devices and which have achieved very high success [91–93], a specialized standardization is proposed in the work blockchain security architecture for IIoT [94], which is based on deep learning smart contracts for the security and functionality of industrial applications, providing a decentralized, reliable, peer-to-peer network for communication between SCADA devices. In essence, this architecture is called upon to fill a key gap in the way IIoT operates, in the context of the convergence of heterogeneous infrastructures based on blockchain. More specifically, this system takes advantage of the functions of the blockchain network by implementing advanced anomaly recognition functions through the two-way, bilateral agreement provided by smart contracts, ensuring in the most efficient and intelligent way the secure network communication between the trading devices in the trading system. The proposed deep learning smart contract, which incorporates a sophisticated deep autoencoder into its code, provides an intelligent mechanism that can categorize with great precision the harmful irregularities in IIoT transactions, which in most cases involve advanced cyber-attacks.

Autoencoder is a neural network that is divided into a pair of two connected networks, one of which acts as an encoder and the other as a decoder. The encoder network takes in the data of the network traffic between master/slave devices and converts it into a smaller, denser representation, which can be used by the decoder's second network to convert it to the original input. Essentially, Autoencoder aims at the realistic representation of the inputs and outputs of the network, compressing the input to latent representation and then rebuilding the output from this representation.

In this way, it learns to compress the original data from the input layer into an abstract form, which it then decompresses, turning it into something that fits perfectly with the original data. This forces Autoencoder in addition to reducing the size of an initial problem and learning how to ignore noise and thus recognize any vulnerabilities associated with attacks in the SCADA Modbus protocol.

Attacks on industrial control systems (ICS) are aimed at mechanically controlling the dynamically rearranging centrifugation, or reprogramming the complex programmable logic controller (PLC) devices in order to speed up or slow down their operations, driving overall industrial equipment in its destruction or permanent damage. Such an attack scenario is described in [95], where the optimal power flow (OPF) algorithm is maliciously applied, which is widely used in power system control centers, in order to find the optimal power system control strategy, while minimizing the overall cost while ensuring security of the system.

Power system safety is usually defined by a set of lower and upper limits for various system parameters, such as power line power and minimum/maximum allowable power frequency 59.5–61 Hz (60 Hz is the rated power grid frequency in the US). The control strategy is essentially a set of control commands that the PLC sends to the actuators, e.g., output control points on the generators that determine the power to be generated by each generator, the margin of error to be ensured for system security, on/off commands, etc.

Luis et al. apply the OPF control algorithm to PLC, after making three malicious modifications: they removed the state that ensures that the system is within safe margins, replaced the cost minimization function with maximizing so that the hostile impact is maximized, and added predefined hidden conditions to ensure that malicious actions are not detected or detected by operators on local imaging devices as well as on the SCADA device overview website.

To solve behavioral deviations, abnormality detection techniques have been proposed in the literature, which can work even when the nature of the attack is new and therefore unknown, as they are based on a tactic of comparing the current situation with a model or more generally with a set of parameters that are considered to describe the normal operation of the system. To achieve these results, behavioral analysis related to basic network parameters such as operating specifications, average power per time window, etc., is widely used. Additionally, the detection of anomalies is related to other technical or heuristic forms of analysis, in order to identify patterns that help detect, identify, and predict their appearance, without leading to false alarms [96,97]. In general, types of anomalies are considered patterns that show different or deviant behavior from the expected and can be categorized into point anomalies, contextual anomalies, collective anomalies, protocol anomalies, etc. [98–100].

In cases of highly specialized attacks such as those simulated by Luis et al., a simple anomaly detection system is not enough, but it requires more sophisticated and obviously complex methods. On the contrary, the method proposed by [101] is an extremely simple and at the same time dynamic methodology, which as it turns out is able to detect with great precision advanced attacks like the one described. Specifically, the CUmulative SUM (CUSUM) algorithm is used, which works intuitively, based on the idea of adding the difference between a variable and the expected value over time. If this cumulative amount exceeds a certain threshold, then the decision is made that a change has been made. More specifically, CUSUM uses Equation (1) to detect a change, where S_n represents the cumulative value in sample n, x_n represents the value monitored in sample number n, and w_n is the usual mean of the monitored value. A change is detected when S_n rises above a predetermined threshold, which is a function of the relative magnitude of the change and the noise of x.

$$S_0 = 0,\ S_{n+1} = max(0,\ S_n + x_n - w_n) \tag{1}$$

This anomaly detection algorithm is used and tested with great success in the detection of anomalies performed by the experiment of Luis et al., where x is a scan cycle execution time detector. Essentially, this simple change detection algorithm allows the monitoring of the execution time of the deterministic PLC control program in real time and implements alerts for changes, in order to detect early anomalies that are usually associated with cyber-attacks. It is important to note that with very high percentages of correct alerts, almost all abnormalities were detected within seconds and within up to five minutes in the worst case, significantly limiting the attackers' ability to damage equipment. Finally, another important advantage of this algorithm is its simplicity, which reinforces the hypothesis that it can be integrated into PLCs that lack resources to provide stronger guarantees of the overall security of the IIoT ecosystem.

4. Discussion

The universal protection of the infrastructure and the reliability of the proposed solutions presented should not be taken for granted, because the cyber security of the IIoT ecosystem is a multifactorial problem, as described above [102].

In particular, due to the nature of the IIoT and the wide range of vulnerabilities that can arise from the complexity of the systems involved in it, important features related to complex patterns, systems, or processes are identified and maintained, which do not evolve in parallel with the overtime and which are potential vulnerabilities of the overall network [103]. More generally, the problem lies in the fact that in the particular high complexity environment under examination, while standardization systems are multivariate, high heterogeneity exists and is maintained, as this can be attributed to the age of systems that have not been upgraded, to the complex relationship that describes them, and the subtle differences that distinguish them [7].

An overview of the discussed cyber threats and countermeasures is presented in Table 2.

Table 2. Cyber Threats and their countermeasures.

ID	Cyber Threats		Countermeasures
1	Phishing attacks The attacker, masquerading as a trusted entity.	Breach of IIoT systems Control of operation systems that are linked to it	PHONEY for auto detection and analysis of phishing attacks [46] Intelligence Web Application Firewall (IWAF) [104] URL Embedding (UE) [51] Detecting botnets by mapping a sequence model based on extracting URLs from spam mails [56] Smart URL Filter in a zone-based policy firewall for detecting algorithmically generated malicious domains names [50]
2	Ransomware attacks Type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid.	DoS attacks, data encryption	Next Generation firewalls with improved traffic filtering capabilities [57] Machine learning techniques [59] Intrusion detection system [60] Hybrid detection systems [105]
3	Protocols Attacks Any threat in protocol stack of IIoT	Jamming DoS attacks	Packets' rerouting to alternative routes [68]
		Collision/exhaustion/unfairness attacks	FHSS techniques [70,71]
		Data transit attacks	Data encryption algorithms [72,73]
		Routing and DoS Attacks	Ingress filtering and IDS solutions [65,74]
		Data transit attacks	Compressed transport protocols (for instance DTL) [72]
		Threats to neighbor discovery protocol (IPv4/IPv6)	Use of IPsec, SEND protocols [75]
		Sending control flags that synchronize endpoints	Message authentication [77]
		System flooding during the SYN handshaking phase	Optimizations in transport layer apply network filtering [79]
		Data transit attacks, scalable key management	Secure MQTT, ABE algorithm [81]
		SCADA modbus attacks	Intrusion detection and prevention system [106,107]
4	Supply chain attacks A cyber-attack that seeks to damage an industry or organization by targeting less-secure elements in the supply chain.	Backdoors installation Very hard to detect	View the ecosystem from a supply chain viewpoint and control the risk [87] Self-adapting supply chain system with artificial intelligence (AI), machine learning (ML), and real-time intelligence for predictive cyber risk analytics [88]
5	Systems Attacks Unauthorized access into an industrial system in order to cause harm.	Man-in-the-Middle attacks Mechanically control the dynamically rearranging centrifugation, or reprogram the complex programmable logic controller (PLC) devices in order to speed up or slow down their operations	System logs modelling [90] Deep learning smart contracts for the security and functionality of industrial applications, providing a decentralized, reliable, peer-to-peer network for communication between SCADA devices [90] Hybrid network anomaly and intrusion detection approach based on evolving spiking neural network classification [108] CUmulative SUM (CUSUM) algorithm [101]

Among the threats discussed, the supply chain attacks are becoming a serious concern, because significant factors like complexity and stealth do not provide easy solutions [109]. To mitigate these types of attacks, usually risk management approaches are utilized. Another major drawback is the fact that older industrial systems, which in most cases do not have security as a prerequisite in their construction specifications, are turning points of the overall security of the system, significantly increasing the overall risk of attacks, even if access control or encryption techniques are added in them [110,111]. In addition, the standardization and harmonization procedures with the existing institutionalized standards raise serious concerns, as most of the existing IIoT systems have a high degree of dependence on their development company, which creates problems of rearrangement or adaptation of their mechanisms, such as functions that they include or can support [7].

Furthermore, due to the real-time operation and development of the IIoT [88,90,94], the management of data with time difference, taking into account correlations and interdependencies from other devices that may be included in the data flow sequence, creates additional requirements in the ways of ensuring accuracy and integrity of information. The encryption [102] and key management techniques that have been proposed and used in the IIoT environment, while providing strict specifications, lag behind in the implementation of mechanisms that will be executed quickly and without much complexity, so that they can be used by low-resource devices.

Finally, another important conclusion drawn from the use of most of the machine learning methods presented in this study is the fact that only statistics on the operation of devices or network traffic are used [96,104] with the result that smoothing is ineffective, as the parameters trained do not include a variety of elements from different usage or behavior parameters of the overall system. The problem stems from the erroneous assumption that the original model and all its updated replicates had similar feature distributions, and therefore the current statistics could be shared with all the intelligent learning inner loop updates. Obviously, this hypothesis is not correct. A better alternative, which was applied to the proposed method, is to store statistics during steps and to read the optimization parameters step by step for each of the internal loop iterations.

5. Conclusions

Given the growing complexity of threats in the ever-changing environment of the Industrial IoT and the parallel weakness of traditional security systems to detect serious threats of escalating depth and duration, it is necessary to acknowledge the risks that threaten the specific infrastructures and provide confidentiality of industrial information [110]. Similarly, while there is a risk that cybercriminals may gain access to the production process, with serious, perhaps incalculable consequences, most industrial companies seek security know-how in order to secure their infrastructure. It should be noted that IIoT architectures, and industrial systems in general [5,6,13,90], need a different kind of protection from standard networks, as conventional security solutions, such as virus scanners or conventional firewalls, do not meet industry standards and requirements.

In this study, a thorough description of attacks against Industrial IoT systems was carried out, taking into account the most important features and vulnerabilities that they incorporate, while at the same time a thorough analysis of indicative solutions against these vulnerabilities, as proposed in the most recent literature. In this context, it is a validated reference framework and an indicative scientific presumption for the identification and assessment of risks related to the ever-evolving industrial environment.

One element that could be considered in the direction of the future expansion of this research is the investigation of unconventional methods of attacks or advanced methods of combination methodology of unknown attacks such as zero-days attacks. Additionally, an important development in this study, concerns the bibliographic investigation of methods with possibilities of self-improvement and self-adaptation to new unknown threats in IIoT systems. Finally, the research could be expanded by the search for special protection techniques against the physical security of IIoT devices, from malicious configuration of mechatronic subsystems that are part of this network, with the aim of their exploitation by third parties.

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

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: MDPI Research Data Policies.

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

References

1. Kannengiesser, U.; Müller, H. Towards viewpoint-oriented engineering for Industry 4.0: A standards-based approach. In Proceedings of the 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, Russia, 15–18 May 2018; pp. 51–56. [CrossRef]
2. Banafa, A. 2 The Industrial Internet of Things (IIoT): Challenges, requirements and benefits. In *Secure and Smart Internet of Things (IoT): Using Blockchain and AI*; River Publishers: Gistrup, Denmark, 2018; pp. 7–12.
3. Mumtaz, S.; Alsohaily, A.; Pang, Z.; Rayes, A.; Tsang, K.F.; Rodriguez, J. Massive internet of things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation. *IEEE Ind. Electron. Mag.* **2017**, *11*, 28–33. [CrossRef]
4. Juarez, F.A.B. Cybersecurity in an Industrial Internet of Things Environment (IIoT) challenges for standards systems and evaluation models. In Proceedings of the 2019 8th International Conference On Software Process Improvement (CIMPS), Leon, Guanajuato, Mexico, 23–25 October 2019; pp. 1–6. [CrossRef]
5. Kargl, F.; van der Heijden, R.W.; Konig, H.; Valdes, A.; Dacier, M.C. Insights on the security and dependability of industrial control systems. *IEEE Secur. Priv.* **2014**, *12*, 75–78. [CrossRef]
6. Falco, G.; Caldera, C.; Shrobe, H. IIoT cybersecurity risk modeling for SCADA systems. *IEEE Internet Things J.* **2018**, *5*, 4486–4495. [CrossRef]
7. Lee, C.-H.; Wu, Z.-L.; Chiu, Y.-T.; Chen, V.-S. Heterogeneous industrial iot integration for manufacturing production. In Proceedings of the 2019 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), Taipei, Taiwan, 3–6 December 2019; pp. 1–2. [CrossRef]
8. Panchal, A.C.; Khadse, V.M.; Mahalle, P.N. Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures. In Proceedings of the 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 23–24 November 2018; pp. 124–130. [CrossRef]
9. Zhou, C.; Wang, Z.; Huang, W.; Guo, Y. Research on network security attack detection algorithm in smart grid system. In Proceedings of the 2017 International Conference on Computer Technology, Electronics and Communication (ICCTEC), Dalian, China, 19–21 December 2017; pp. 1407–1410. [CrossRef]
10. Irmak, E.; Erkek, I. An overview of cyber-attack vectors on SCADA systems. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–5. [CrossRef]
11. Kang, D.-H.; Kim, B.-K.; Na, J.-C. Cyber threats and defence approaches in SCADA systems. In Proceedings of the 16th International Conference on Advanced Communication Technology, Pyeongchang, Korea, 16–19 February 2014; pp. 324–327. [CrossRef]
12. Gebremichael, T.; Ledwaba, L.P.I.; Eldefrawy, M.H.; Hancke, G.P.; Pereira, N.; Gidlund, M.; Akerberg, J. Security and privacy in the industrial internet of things: Current standards and future challenges. *IEEE Access* **2020**, *8*, 152351–152366. [CrossRef]
13. Ghosh, S.; Sampalli, S. A survey of security in SCADA networks: Current issues and future challenges. *IEEE Access* **2019**, *7*, 135812–135831. [CrossRef]
14. Physical Layer Security in Wireless Networks with Passive and Active Eavesdroppers—IEEE Conference Publication. Available online: https://ieeexplore.ieee.org/document/6503890 (accessed on 16 February 2021).
15. Zeng, Y.; Zhang, R. Active eavesdropping via spoofing relay attack. In Proceedings of the 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Shanghai, China, 20–25 March 2016; pp. 2159–2163. [CrossRef]
16. Shafie, A.E.; Chihaoui, H.; Hamila, R.; Al-Dhahir, N.; Gastli, A.; Ben-Brahim, L. Impact of passive and active security attacks on MIMO smart grid communications. *IEEE Syst. J.* **2019**, *13*, 2873–2876. [CrossRef]
17. Eigner, O.; Kreimel, P.; Tavolato, P. Detection of man-in-the-middle attacks on industrial control networks. In Proceedings of the 2016 International Conference on Software Security and Assurance (ICSSA), St. Polten, Austria, 24–25 August 2016; pp. 64–69. [CrossRef]

18. Lan, H.; Zhu, X.; Sun, J.; Li, S. Traffic data classification to detect man-in-the-middle attacks in industrial control system. In Proceedings of the 2019 6th International Conference on Dependable Systems and Their Applications (DSA), Harbin, China, 3–6 January 2020; pp. 430–434. [CrossRef]
19. Andreica, G.R.; Bozga, L.; Zinca, D.; Dobrota, V. Denial of service and man-in-the-middle attacks against IoT devices in a GPS-based monitoring software for intelligent transportation systems. In Proceedings of the 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet), Bucharest, Romania, 11–12 December 2020; pp. 1–4. [CrossRef]
20. Esfahani, A.; Mantas, G.; Ribeiro, J.; Bastos, J.; Mumtaz, S.; Violas, M.A.; De Oliveira Duarte, A.M.; Rodriguez, A. An efficient web authentication mechanism preventing man-in-the-middle attacks in industry 4.0 supply chain. *IEEE Access* **2019**, *7*, 58981–58989. [CrossRef]
21. Wardega, K.; Tron, R.; Li, W. Resilience of multi-robot systems to physical masquerade attacks. In Proceedings of the 2019 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 19–23 May 2019; pp. 120–125. [CrossRef]
22. Ustun, T.S.; Farooq, S.M.; Hussain, S.M.S. A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard. *IEEE Access* **2019**, *7*, 156044–156053. [CrossRef]
23. Xiang, Z.; Guangyu, H.; Zhigong, W. Masquerade detection using support vector machines in the smart grid. In Proceedings of the 2014 Seventh International Joint Conference on Computational Sciences and Optimization, Beijing, China, 4–6 July 2014; pp. 30–34. [CrossRef]
24. Al-Rabiaah, S. The 'Stuxnet' virus of 2010 as an example of a 'APT' and its 'Recent' variances. In Proceedings of the 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 25–26 April 2018; pp. 1–5. [CrossRef]
25. Zou, J.; Jin, X.; Zhang, L.; Wang, Y.; Li, B. A case study of anomaly detection in industrial environments. In Proceedings of the 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), New York, NY, USA, 1–3 August 2019; pp. 294–298. [CrossRef]
26. Lin, J.; Liu, L. Research on security detection and data analysis for industrial internet. In Proceedings of the 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), Sofia, Bulgaria, 22–26 July 2019; pp. 466–470. [CrossRef]
27. Berhe, A.B.; Kim, K.; Tizazu, G.A. Industrial control system security framework for ethiopia. In Proceedings of the 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, Italy, 4–7 July 2017; pp. 814–817. [CrossRef]
28. Shang, W.; Cui, J.; Song, C.; Zhao, J.; Zeng, P. Research on industrial control anomaly detection based on FCM and SVM. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 218–222. [CrossRef]
29. Borgiani, V.; Moratori, P.; Kazienko, J.F.; Tubino, E.R.; Quincozes, S.E. Towards a distributed approach for detection and mitigation of denial of service attacks within industrial internet of things. *IEEE Internet Things J.* **2020**, 1. [CrossRef]
30. Tan, Z.; Jamdagni, A.; He, X.; Nanda, P.; Liu, R.P.; Hu, J. Detection of denial-of-service attacks based on computer vision techniques. *IEEE Trans. Comput.* **2015**, *64*, 2519–2533. [CrossRef]
31. Serror, M.; Hack, S.; Henze, M.; Schuba, M.; Wehrle, K. Challenges and opportunities in securing the industrial internet of things. *IEEE Trans. Ind. Inform.* **2020**, 1. [CrossRef]
32. Biswas, R.; Wu, J.; Li, X. A capacity-aware distributed denial-of-service attack in low-power and lossy networks. In Proceedings of the 2019 IEEE 40th Sarnoff Symposium, Newark, NJ, USA, 23–24 September 2019; pp. 1–6. [CrossRef]
33. Sahu, S.S.; Priyadarshini, P.; Bilgaiyan, S. Curbing distributed denial of service attack by traffic filtering in wireless sensor network. In Proceedings of the Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Hefei, China, 11–13 July 2014; pp. 1–6. [CrossRef]
34. Ficco, M.; Palmieri, F. Introducing fraudulent energy consumption in cloud infrastructures: A new generation of denial-of-service attacks. *IEEE Syst. J.* **2017**, *11*, 460–470. [CrossRef]
35. Memmi, G.; Kapusta, K.; Qiu, H. Data protection: Combining fragmentation, encryption, and dispersion. In Proceedings of the 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 5–7 August 2015; pp. 1–9. [CrossRef]
36. Suciu, I.; Vilajosana, X.; Adelantado, F. An analysis of packet fragmentation impact in LPWAN. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6. [CrossRef]
37. Makris, P.; Skoutas, D.N.; Skianis, C. A survey on context-aware mobile and wireless networking: On networking and computing environments' integration. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 362–386. [CrossRef]
38. Li, Y. A vulnerability risk assessment method for industrial control system. In Proceedings of the 2020 International Conference on Computer Communication and Network Security (CCNS), Xi'an, China, 21–23 August 2020; pp. 146–152. [CrossRef]
39. Delignat-Lavaud, A.; Fournet, C.; Kohlweiss, M.; Parno, B. Cinderella: Turning shabby X.509 certificates into elegant anonymous credentials with the magic of verifiable computation. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 235–254. [CrossRef]
40. Repp, P. Diagnostics and assessment of the industrial network security expert system. In Proceedings of the 2017 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), St. Petersburg, Russia, 16–19 May 2017; pp. 1–5. [CrossRef]

41. Chen, H.; Hu, M.; Yan, H.; Yu, P. Research on industrial internet of things security architecture and protection strategy. In Proceedings of the 2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), Jishou, China, 14–15 September 2019; pp. 365–368. [CrossRef]
42. Mikhalevich, I.F.; Trapeznikov, V.A. Critical infrastructure security: Alignment of views. In Proceedings of the 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 20–21 March 2019; pp. 1–5. [CrossRef]
43. Kolowrocki, K.; Soszynska-Budny, J. Critical infrastructure safety indicators. In Proceedings of the 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand, 16–19 December 2018; pp. 1761–1764. [CrossRef]
44. Liu, X.; Qian, C.; Hatcher, W.G.; Xu, H.; Liao, W.; Yu, W. Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities. *IEEE Access* **2019**, *7*, 79523–79544. [CrossRef]
45. Roman, R. Trust and reputation systems for wireless sensor networks. In *Security and Privacy in Mobile and Wireless Networking*; Troubador Publishing Ltd.: Leicester, UK, 2009; pp. 105–128.
46. Chandrasekaran, M.; Chinchani, R.; Upadhyaya, S. PHONEY: Mimicking user response to detect phishing attacks. In Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks(WoWMoM'06), Buffalo-Niagara Falls, NY, USA, 26–29 June 2006. [CrossRef]
47. McRae, C.M.; Vaughn, R.B. Phighting the phisher: Using web bugs and honeytokens to investigate the source of phishing attacks. In Proceedings of the 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Waikoloa, HI, USA, 3–6 January 2007; p. 270c. [CrossRef]
48. Ajlouni, M.I.A.; Hadi, W.; Alwedyan, J. Detecting phishing websites using associative classification. *J. Inf. Eng. Appl.* **2013**, *3*, 6–10.
49. Jain, A.; Richariya, V. Implementing a web browser with phishing detection techniques. *arXiv* **2011**, arXiv:1110.0360.
50. Demertzis, K.; Iliadis, L. Evolving smart URL filter in a zone-based policy firewall for detecting algorithmically generated malicious domains. In *Statistical Learning and Data Sciences*; Springer: Cham, Switzerland, 2015; pp. 223–233. [CrossRef]
51. Yan, X.; Xu, Y.; Cui, B.; Zhang, S.; Guo, T.; Li, C. Learning URL embedding for malicious website detection. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6673–6681. [CrossRef]
52. Gu, G.; Porras, P.; Yegneswaran, V.; Fong, M. BotHunter: Detecting Malware Infection through IDS-Driven Dialog Correlation. Presented at the 16th {USENIX} Security Symposium ({USENIX} Security 07). 2007. Available online: https://www.usenix.org/conference/16th-usenix-security-symposium/bothunter-detecting-malware-infection-through-ids-driven (accessed on 24 January 2021).
53. Ma, J.; Saul, L.K.; Savage, S.; Voelker, G.M. Beyond blacklists: Learning to detect malicious web sites from suspicious URLs. In Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining—KDD'09, Paris, France, 28 June–1 July 2009; p. 1245. [CrossRef]
54. McGrath, D.K.; Gupta, M. Behind phishing: An examination of phisher modi operandi. In Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, Bloomington, IN, USA, 15 April 2008; pp. 1–8.
55. Xie, Y.; Yu, F.; Achan, K.; Panigrahy, R.; Hulten, G.; Osipkov, I. Spamming Botnet: Signatures and Characteristics. August 2008. Available online: https://www.microsoft.com/en-us/research/publication/spamming-botnet-signatures-and-characteristics/ (accessed on 24 January 2021).
56. Stalmans, E.; Irwin, B. A framework for DNS based detection and mitigation of malware infections on a network. In Proceedings of the 2011 Information Security for South Africa, Johannesburg, South Africa, 15–17 August 2011; pp. 1–8. [CrossRef]
57. Al-Hawawreh, M.; den Hartog, F.; Sitnikova, E. Targeted ransomware: A new cyber threat to edge system of brownfield industrial internet of things. *IEEE Internet Things J.* **2019**, *6*, 7137–7151. [CrossRef]
58. Erebus Linux Ransomware: Impact to Servers and Countermeasures—Security News. Available online: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/erebus-linux-ransomware-impact-to-servers-and-countermeasures (accessed on 20 January 2021).
59. Alhawi, O.M.K.; Baldwin, J.; Dehghantanha, A. Leveraging machine learning techniques for windows ransomware network traffic detection. In *Cyber Threat Intelligence*; Dehghantanha, A., Conti, M., Dargahi, T., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 93–106.
60. Almashhadani, A.O.; Kaiiali, M.; Sezer, S.; O'Kane, P. A multi-classifier network-based crypto ransomware detection system: A case study of locky ransomware. *IEEE Access* **2019**, *7*, 47053–47067. [CrossRef]
61. Maiorca, D.; Mercaldo, F.; Giacinto, G.; Visaggio, C.A.; Martinelli, F. R-PackDroid: API package-based characterization and detection of mobile ransomware. In Proceedings of the Symposium on Applied Computing, Marrakech, Morocco, 3–7 April 2017; pp. 1718–1723. [CrossRef]
62. Sgandurra, D.; Muñoz-González, L.; Mohsen, R.; Lupu, E.C. Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection. ArXiv160903020 Cs. September 2016. Available online: http://arxiv.org/abs/1609.03020 (accessed on 20 January 2021).
63. Tseng, A.; Chen, Y.; Kao, Y.; Lin, T. Deep learning for ransomware detection. *IEICE Tech. Rep.* **2016**, *116*, 87–92.
64. Tournier, J.; Lesueur, F.; Mouël, F.L.; Guyon, L.; Ben-Hassine, H. A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet Things* **2020**, 100264. [CrossRef]
65. Butun, I.; Osterberg, P.; Song, H. Security of the internet of things: Vulnerabilities, attacks, and countermeasures. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 616–644. [CrossRef]

66. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017; pp. 1–6. [CrossRef]
67. Hossain, M.M.; Fotouhi, M.; Hasan, R. Towards an analysis of security issues, challenges, and open problems in the internet of things. In Proceedings of the 2015 IEEE World Congress on Services, New York City, NY, USA, 27 June–2 July 2015; pp. 21–28. [CrossRef]
68. Muraleedharan, R.; Osadciw, L. Cross layer denial of service attacks in wireless sensor network using swarm intelligence. In Proceedings of the 2006 40th Annual Conference on Information Sciences and Systems, Princeton, NJ, USA, 22–24 March 2006; pp. 1653–1658. [CrossRef]
69. Antonopoulos, A.; Verikoukis, C.; Skianis, C.; Akan, O.B. Energy efficient network coding-based MAC for cooperative ARQ wireless networks. *Ad Hoc Netw.* **2013**, *11*, 190–200. [CrossRef]
70. Mouaatamid, O.E.; Lahmer, M.; Belkasmi, M. Internet of Things Security: Layered Classification of Attacks and Possible Countermeasures. *Electron. J. Inf. Technol.* **2016**. Available online: http://www.webmail.revue-eti.net/index.php/eti/article/view/98 (accessed on 20 January 2021).
71. Usman, M.; Raponi, S.; Qaraqe, M.; Oligeri, G. KaFHCa: Key-Establishment via Frequency Hopping Collisions. arXiv201009642 Cs. *Octember 2020.* Available online: http://arxiv.org/abs/2010.09642 (accessed on 20 January 2021).
72. Hennebert, C.; Santos, J.D. Security protocols and privacy issues into 6LoWPAN stack: A synthesis. *IEEE Internet Things J.* **2014**, *1*, 384–398. [CrossRef]
73. Adnan, A.H.; Abdirazak, M.; Shamsuzzaman Sadi, A.B.M.; Anam, T.; Khan, S.Z.; Rahman, M.M.; Omar, M.M. A comparative study of WLAN security protocols: WPA, WPA2. In Proceedings of the 2015 International Conference on Advances in Electrical Engineering (ICAEE), Dhaka, Bangladesh, 17–19 December 2015; pp. 165–169. [CrossRef]
74. Raza, S.; Wallgren, L.; Voigt, T. SVELTE: Real-Time intrusion detection in the internet of things. *Ad Hoc Netw.* **2013**, *11*, 2661–2674. [CrossRef]
75. Ahmed, A.S.A.M.S.; Hassan, R.; Othman, N.E. IPv6 neighbor discovery protocol specifications, threats and countermeasures: A survey. *IEEE Access* **2017**, *5*, 18187–18210. [CrossRef]
76. Unsal, E.; Çebi, Y. Denial of Service Attacks in WSN. In Proceedings of the International Symposium on Computing in Science & Engineering, Izmir, Turkey, 4–6 September 2013.
77. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. Authentication protocols for internet of things: A comprehensive survey. *Secur. Commun. Netw.* **2017**, *2017*, 1–41. [CrossRef]
78. El-hajj, M.; Chamoun, M.; Fadlallah, A.; Serhrouchni, A. Analysis of authentication techniques in Internet of Things (IoT). In Proceedings of the 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, 18–20 October 2017; pp. 1–3. [CrossRef]
79. Eddy, W.M. Defenses against TCP SYN flooding attacks. *Internet Protoc. J.* **2006**, *9*, 2–16.
80. Andy, S.; Rahardjo, B.; Hanindhito, B. Attack scenarios and security analysis of MQTT communication protocol in IoT system. In Proceedings of the 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Yogyakarta, Indonesia, 19–21 September 2017; pp. 1–6. [CrossRef]
81. Singh, M.; Rajan, M.A.; Shivraj, V.L.; Balamuralidhar, P. Secure MQTT for Internet of Things (IoT). In Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 4–6 April 2015; pp. 746–751. [CrossRef]
82. Morris, T.H.; Thornton, Z.; Turnipseed, I. Industrial control system simulation and data logging for intrusion detection system research. In Proceedings of the 7th Annual Southeastern Cyber Security Summit, Huntsville, AL, USA, 3–4 June 2015; pp. 3–4.
83. Chromik, J.; Remke, A.; Haverkort, B.R.; Geist, G. A Parser for Deep Packet Inspection of IEC-104: A practical solution for industrial applications. In Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks—Industry Track, Portland, OR, USA, 24–27 June 2019; pp. 5–8. [CrossRef]
84. Liang, W.; Li, K.-C.; Long, J.; Kui, X.; Zomaya, A.Y. An industrial network intrusion detection algorithm based on multifeature data clustering optimization model. *IEEE Trans. Ind. Inform.* **2020**, *16*, 2063–2071. [CrossRef]
85. Constantinides, C.; Shiaeles, S.; Ghita, B.; Kolokotronis, N. A novel online incremental learning intrusion prevention system. In Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 24–26 June 2019; pp. 1–6. [CrossRef]
86. Deng, L.; Peng, Y.; Liu, C.; Xin, X.; Xie, Y. Intrusion detection method based on support vector machine access of modbus TCP protocol. In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15–18 December 2016; pp. 380–383. [CrossRef]
87. Farooq, M.J.; Zhu, Q. IoT supply chain security: Overview, challenges, and the road ahead. ArXiv190807828 Cs. July 2019. Available online: http://arxiv.org/abs/1908.07828 (accessed on 19 January 2021).
88. Radanliev, P.; De Roure, D.; Page, K.; Nurse, J.R.C.; Montalvo, R.M.; Santos, O.; Maddox, L.T.; Burnap, P. Cyber Risk at the Edge: Current and Future Trends on Cyber Risk Analytics and Artificial Intelligence in the Industrial Internet of Things and Industry 4.0 Supply Chains. December 2020. Available online: https://www.preprints.org/manuscript/201903.0123/v2 (accessed on 19 January 2021).

89. Kieras, T.; Farooq, J.; Zhu, Q. RIoTS: Risk analysis of IoT supply chain threats. In Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020.
90. Mercaldo, F.; Martinelli, F.; Santone, A. Real-Time SCADA attack detection by means of formal methods. In Proceedings of the 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Napoli, Italy, 12–14 June 2019; pp. 231–236. [CrossRef]
91. Demertzis, K.; Iliadis, L.; Bougoudis, I. Gryphon: A semi-supervised anomaly detection system based on one-class evolving spiking neural network. *Neural Comput. Appl.* **2020**, *32*, 4303–4314. [CrossRef]
92. Xing, L.; Demertzis, K.; Yang, J. Identifying data streams anomalies by evolving spiking restricted Boltzmann machines. *Neural Comput. Appl.* **2020**, *32*, 6699–6713. [CrossRef]
93. 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]
94. Demertzis, K.; Iliadis, L.; Tziritas, N.; Kikiras, P. Anomaly detection via blockchained deep learning smart contracts in industry 4.0. *Neural Comput. Appl.* **2020**, *32*, 17361–17378. [CrossRef]
95. Garcia, L.A.; Brasser, F.; Cintuglu, M.H.; Sadeghi, A.-R.; Mohammed, O.; Zonouz, S.A. Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit. In Proceedings of the Network and Distributed System Security Symposium, San Diego, CA, USA, 26 February–1 March 2017. [CrossRef]
96. Zhou, L.; Guo, H. Anomaly detection methods for IIoT networks. In Proceedings of the 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Singapore, 31 July–2 August 2018; pp. 214–219. [CrossRef]
97. Genge, B.; Haller, P.; Enachescu, C. Anomaly detection in aging industrial internet of things. *IEEE Access* **2019**, *7*, 74217–74230. [CrossRef]
98. Cook, A.A.; Misirli, G.; Fan, Z. Anomaly detection for IoT time-series data: A survey. *IEEE Internet Things J.* **2020**, *7*, 6481–6494. [CrossRef]
99. Gaddam, A.; Wilkin, T.; Angelova, M. Anomaly detection models for detecting sensor faults and outliers in the IoT—A survey. In Proceedings of the 2019 13th International Conference on Sensing Technology (ICST), Sydney, NSW, Australia, 2–4 December 2019; pp. 1–6. [CrossRef]
100. Deorankar, A.V.; Thakare, S.S. Survey on anomaly detection of (IoT)—Internet of Things cyberattacks using machine learning. In Proceedings of the 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 11–13 March 2020; pp. 115–117. [CrossRef]
101. Formby, D.; Beyah, R. Temporal execution behavior for host anomaly detection in programmable logic controllers. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 1455–1469. [CrossRef]
102. Nakamura, E.T.; Ribeiro, S.L. A privacy, security, safety, resilience and reliability focused risk assessment methodology for IIoT systems steps to build and use secure IIoT systems. In Proceedings of the 2018 Global Internet of Things Summit (GIoTS), Bilbao, Spain, 4–7 June 2018; pp. 1–6. [CrossRef]
103. Sengupta, J. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
104. Demertzis, K.; Kikiras, P.; Tziritas, N.; Sanchez, S.; Iliadis, L. The next generation cognitive security operations center: Network flow forensics using cybersecurity intelligence. *Big Data Cogn. Comput.* **2018**, *2*, 35. [CrossRef]
105. Al-Hawawreh, M.; Sitnikova, E. Leveraging deep learning models for ransomware detection in the industrial internet of things environment. In Proceedings of the 2019 Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, 12–14 November 2019; pp. 1–6. [CrossRef]
106. Brugman, J.; Khan, M.; Kasera, S.; Parvania, M. Cloud based intrusion detection and prevention system for industrial control systems using software defined networking. In Proceedings of the 2019 Resilience Week (RWS), San Antonio, TX, USA, 4–7 November 2019; pp. 98–104. [CrossRef]
107. Nyasore, O.N.; Zavarsky, P.; Swar, B.; Naiyeju, R.; Dabra, S. Deep packet inspection in industrial automation control system to mitigate attacks exploiting modbus/TCP vulnerabilities. In Proceedings of the 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Baltimore, MD, USA, 25–27 May 2020; pp. 241–245. [CrossRef]
108. Demertzis, K.; Iliadis, L. A hybrid network anomaly and intrusion detection approach based on evolving spiking neural network classification. In *E-Democracy, Security, Privacy and Trust in a Digital World*; Sideridis, A.B., Kardasiadou, Z., Yialouris, C.P., Zorkadis, V., Eds.; Springer International Publishing: Cham, Switzerland, 2014; Volume 441, pp. 11–23.
109. Hu, W.; Li, M.; Yuan, C.; Zhang, C.; Wang, J. Diversity in neural architecture search. In Proceedings of the 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, UK, 19–24 July 2020; pp. 1–8. [CrossRef]
110. McLaughlin, S.; Konstantinou, C.; Wang, X.Y.; Davi, L.; Sadeghi, A.-R.; Maniatakos, M.; Karri, R. The cybersecurity landscape in industrial control systems. *Proc. IEEE* **2016**, *104*, 1039–1057. [CrossRef]
111. Li, Y.; Xu, L.; Shu, W.; Tao, J.; Mei, K. AutoGesNet: Auto gesture recognition network based on neural architecture search. In Proceedings of the 2020 12th International Conference on Advanced Computational Intelligence (ICACI), Dali, China, 14–16 August 2020; pp. 257–262. [CrossRef]