*Type of the Paper (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] Democritus University of Thrace, Department of Electronics and Computer Engineering, Vas. Sofias 12, 67100, Xanthi, Greece; ktsiknas@ee.duth.gr

[2] Hellenic National Defence General Staff, Stratopedo Papagou, Mesogeion 227-231, 15561 Athens, Greece; d.taketzis@hndgs.mil.gr

[3] Laboratory of Complex Systems, Department of Physics, Faculty of Sciences, International Hellenic University, Kavala Campus, St. Loukas, 65404, Greece; kdemertzis@teiemt.gr

[4] University of Aegean, 83200, Karlovassi, Samos, Greece; cskianis@aegean.gr

* Correspondence: e-mail@e-mail.com; Tel.: (optional; include country code; if there are multiple corresponding authors, add author initials)

**Abstract:** In today's Industrial IoT (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, 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 against these attacks, as they have been proposed in the most recent literature**.**

**Keywords:** IIoT; IoT; Industry 4.0; Protocols; Cyber Threats; Attacks; Security

## 1. Introduction

According to the Industry 4.0 standard (Kannengiesser and Müller), 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 (Banafa).

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 Fig. 1) (Sengupta).

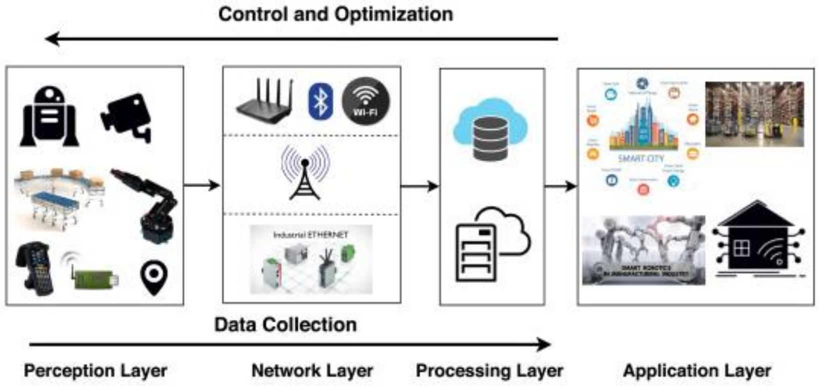


**Figure 1.** Generalised IIoT system architecture.

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.

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 (Juárez). 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) (Kargl et al.). 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 (Falco et al.). 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, it poses significant challenges in the ways of securing the infrastructure (Lee et al.), 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, even their partial or total destruction, with incalculable consequences (Panchal et al.).

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, 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.

The study is organized as follows: Section 2 reviews related work, 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. Sections 4 presents the main results of our study and finally the last section draws the conclusions and outlines future research directions.

## 2. Metasurvey

Some of the modern attacks on critical infrastructure networks, such as power grids (Zhou et al.) are related to undermining actuators or sensors located in the physical layer, attacks against connections between different devices in the data-link layer, or to more specialized attacks to compromise specific control systems such as SCADA devices (Irmak and Erkek).

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 (Kang et al.), 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.

Given the importance of being able to specify attacks against SCADA systems, (Irmak and Erkek) presented a study on the digital threats targeting these systems and specifically evaluating the three main aspects of these systems, namely hardware, software and communication.

In particular, this study makes a simple reference to the building blocks of a functional SCADA architecture, while the reference concerning the attacks against the physical layer is completely superficial. Also, while they provide no specific references on attacks against software, 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 detailed explanations that could focus on specific methodological approaches on mitigation or prevention. Finally, regarding the communication layer of SCADA systems, the study is spent on 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 security of Industrial IoT systems is presented in (Panchal et al.), 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).

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, access to the specifications of active devices, engineering plans and detailed information about their installation and operational functionality. This type of information can only be disclosed by intercepting the basic electrical drawings or by tricking the personnel that designed it so that the attacker can fully understand the existing environment and then modify the sensor's operation to his advantage.

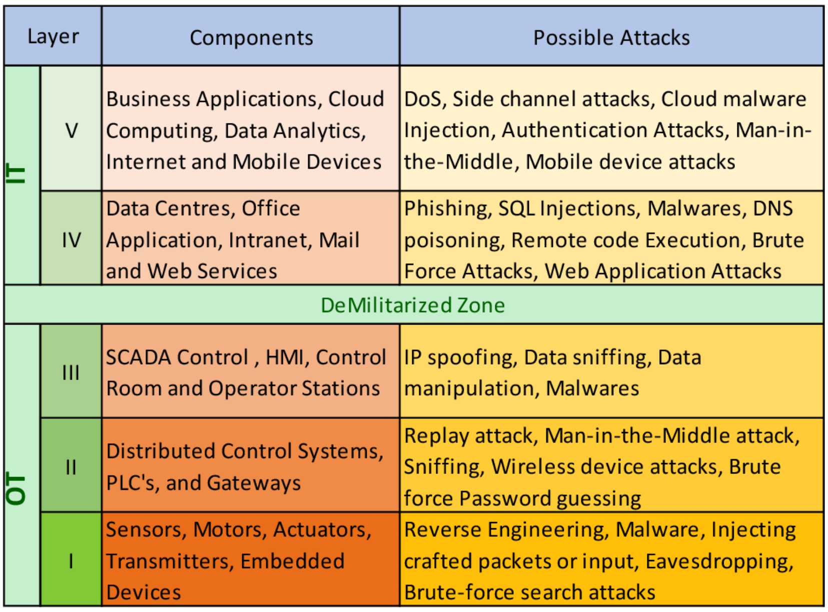
The second functional level, incorporates the specialized equipment which communicates and controls the devices of the first level, such as Distributed Control Systems (DCS), Programmable Logic Control (PLC's) and Gateways. Attacks at this level are aimed at preventing legitimate communication between 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 and 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 for legitimate data from the user, in order to gain access with administrator privileges.

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. An overview of the stack is shown in Fig. 2.



| 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.

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, but it is a rathera survey of the known types of attacks and provides some minimal information that can be easily extracted from the literature.

A holistic approach based on business planning and standardization on security requirements designed by the standardization bodies Industrial Consortium and OpenFog Consortium is presented in (Gebremichael et al.). 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 (Fig 3).

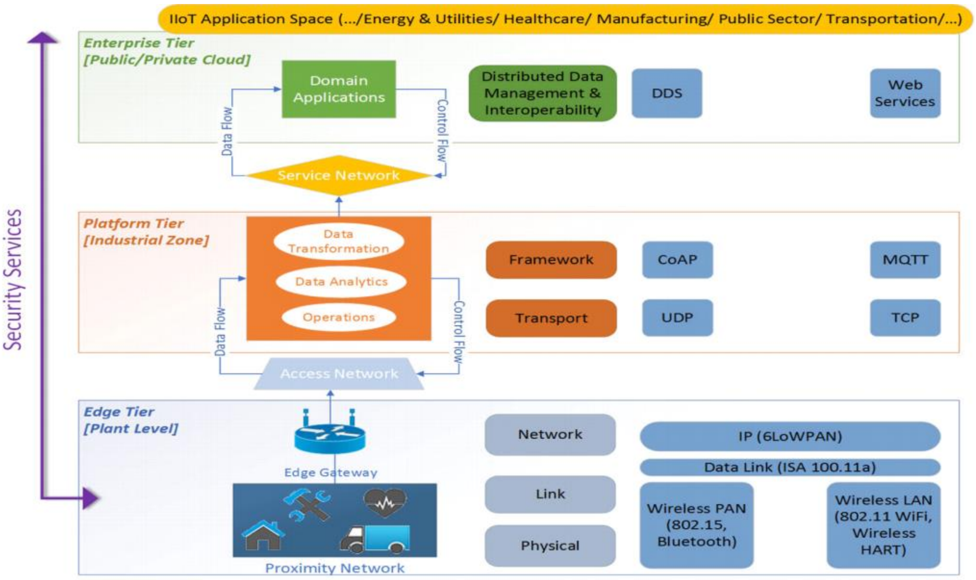


**Figure 3.** Three-tier architecture of IIoT connectivity and communications standards.

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 Enterprise Tier, is done with a service network, which is mainly based on the Internet. Finally, 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 create embankments that could serve as backup protection in the event of wide scale breaches.

In particular, based on the categorization of the study, in the Edge Tier, are classified, presented and explained connectivity protocols like Bluetooth [IEEE 802.15.1] (WPAN), ZigBee 802.15.4 (WPAN), IEEE 802.15.4 (WPAN), NB-IoT (WWAN), WirelessHART (WLAN), LoRaWAN (WWAN), ISA100.11a (Data Link) and 6LoWPAN (Network Layer), while in the Platform Tier, the Connectivity Protocols, CoAP and MQTT.

The specifications and recommendations of the Industrial Consortium and OpenFog Consortium for secure communication with these protocols, include nine basic categories of recommendations and challenges, which are directly related to the proper and safe operation of the Industrial IoT.

The first and perhaps most basic of these specifications concerns the authentication and more specifically the ways of distributing and ensuring correct credentials, non-repudiation techniques and integrity control. For powerful authentication mechanisms, hardware-based systems such as Hardware Root of Trust (HRoT) or Hardware Security Module (HSM) or Trusted Platform Module (TPM) are proposed, as well as advanced mechanisms based on encrypted bitstreams in FPGA physically unclonable functions or hardware-based Trusted Computing Bases (TCBs) for edge devices.

For Access Control mechanisms and the impose of access control rules, encryption mechanisms such as CP-ABE-based are proposed, for grouping devices and configuring them into groups with different access levels. It is also appropriate that the data is encrypted in such a way that only a device with defined access permissions can decrypt it.

Powerful Identity Management mechanisms and solutions are also required to solve naming, addressing and discovery problems in the IIoT ecosystem. Proposed solutions, such as OpenID and Library Alliance, address trust management by managing device identities on proprietary networks, by manipulating a naming and addressing mechanism that escalates to the ever-increasing number of devices involved in IIoT. Key Management for the secure storage and exchange of encryption keys on restricted devices, where intruders have even physical access to such devices, is a problem that manifests itself at various levels of IIoT connectivity protocols. Basic management solutions based on public cryptography are impossible for IIoT due to the complex calculations inherent in public key cryptography. Solutions to this problem involve the use of basic management systems combining lightweight and easy-to-use encryption mechanisms.

Another important function that should be considered, is the data flow confidentiality on Fog Computing process, where data flow encryption techniques should be applied in order to protect the communication in the IIoT. Fog is a distributed computing infrastructure for IIoT, that extends computing capacity and therefore data analytics applications to the periphery of networks. It allows for customers to analyze and manage data locally and thus receive information from connections. The proposed solution was the devices and the connectivity protocols to support a variety of open, proven cryptographic algorithms, capable of being implemented in Fog Computing.

The use of data isolation techniques in IIoT communication is used to protect parts of the IIoT network in the event of adverse reactions, caused by network failing components. Isolation techniques can be scaled to provide security separately by level using container technologies to isolate the business processes, as it currently applies in communication between the legacy applications and the wider IIoT network.

The distributed access control approach recognizes endpoint devices as intelligent resources that can access, process, and distribute access control information to other services and devices. Authorization decisions are then based on site status information provided by the cooperating neighboring nodes. For the implementation of predefined security and authorization policies, the use of filtering and access control in the IIoT is required, based on a distributed access control model so that there is no single point of failure, such as Capability based Access Control (CapBAC). The general idea is based on the logic that a device has a key that gives access to resources or access to a protected area, in order to minimize the communication transactions required during the authentication and access process. The Manufacturer Usage Description (MUD) model is recommended to specify how the devices operate in order to minimize the attack surface. This model in particular defines communication strategies and the corresponding access control mechanisms which limit the interaction with other services or devices, and in particular with publicly known models, in order to minimize the effectiveness of the automated distributed threats.

For the integration of cloud services in the IIoT environment, techniques such as Network Function Virtualization (NFV) are recommended, which collects the various operations performed by the hardware and replaces them with the corresponding functions implemented by the software. In this context all problems and restrictions linked with the hardware do not exist, like for instance the high capital cost of hardware equipment, the requirement for the physical presence of technicians in the area and the possible hardware failures. In addition, the use of software makes the maintenance a much easier, safer, more reliable and financially effective process. Respectively, for the introduction of control and various rules and the management of natural resources and infrastructure for the best service of users on the internet and the achievement of Quality of Service (QoS) and Quality of Experience (QoE) of different users, it is recommended the Software Defined Networking (SDN), which provides controllers, based on the OpenFlow protocol. It is also worth mentioning that this work includes extensive study case examples from the literature, and and also provides some basic guidelines for the protection of the privacy in IIoT systems

Finally, (Ghosh and Sampalli) present a detailed study on SCADA attacks. SCADA systems is the main hardware of the IIoT ecosystem and consists 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, 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 (PLCs), 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 between MTUs and sub-MTUs or RTUs, an attacker could install spyware and proceed to exploitation.
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. In the event of a successful breach, he takes over the session and maintains the connection from a spoofed IP to avoid detection.
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. Then by launching a brute force attack, stolen passwords can be used to gain unauthorized access to important information.
4. *Virus, Trojan Horse and Worms.* An attacker could send malicious code to MTU after launching a MitM or Masquerade attack. 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.
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.
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.

doi:10.20944/preprints202102.0148.v1

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.
8. *Doorknob Rattling.* It is related with 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.

Given the complexity of the architectures associated with SCADA systems and related prototypes, Ghosh and S. Sampalli provide a comprehensive study of:

1. *Current Standards.* These are international certifications of standards by IT security experts and are divided into security guidelines-based standards and crypto-suites based standards. The security guidelines-based standards presented in this study are IEEE 1402, ISO 17799, ISO 15408, NERC security guidelines, NERC 1200, API 1164 and refer to techniques that demonstrate ways such as toolkits, policies, security concepts, guidelines, approaches risk management, training, best practices, safeguards and technologies that can reduce risks, including preventing or mitigating cyber-attacks. The crypto-suites based standards presented in this study are IEC 62210, IEC 62,351 and AGA-12, which provide mechanisms for the participants in the IIoT ecosystem to exchange messages, without being decrypted or revealed by malicious intermediate users.
2. *Detection of SCADA attacks.* Traditional methods such as firewalls used in SCADA networks are not effective enough to withstand complex attacks. In recent years, machine learning algorithms such as Naïve Bayes, Random Forest, Decision Tree Algorithm, Support Vector Machine, Extreme Learning Machines, Spiking Neural Networks have been used to significantly increase and strengthen the active protection measures of these infrastructures. This research presents various techniques that have been used in the literature to protect SCADA infrastructures such as rule-based intrusion detection systems, network anomaly detection methods, one-class classification approaches and hybrid models.
3. *Prevention of SCADA attacks*. The basic approach of preventing attacks on SCADA networks, according to the study in question, concerns encryption and key management techniques. In particular, key management schemes help integrate, control, manage and monitor the entire life cycle of keys and security certificates, while providing visibility to administrators to fully control keys to prevent breaches and compliance issues. In this research the key management implementation is generally categorized as centralized or decentralized, while the basic categorization of the analysis presented concerns symmetric key cryptography (SCADA Key Establishment (SKE), SCADA Key Management Architecture (SKMA), Logical Key Hierarchy (LKH) and Advanced Key-Management Architecture (ASKMA)), asymmetric key cryptography (ID-based Key Management Architecture and NTRU Cryptographic Algorithm for SCADA Networks), hybrid key cryptography (Hybrid Key Management Architecture (HKMA), Advance Hybrid Key Management Architecture (AHSKMA)) and self-healing management (Limited Self-Healing Key Distribution (LISHC)).

In conclusion, this study lists all the current standards used by organizations in the Industrial IoT environment, while providing the security threats of each standard and appropriate solutions that enhance the security posture of this type of infrastructure.

## 3. Cyber Threats and its Countermeasures

Automation and remote control are today the most important methods by which critical infrastructures (Mikhalevich and Trapeznikov) 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 (Kołowrocki and Soszyńska-Budny). 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 sections we review the most popular threats in the IIoT environment, as classified in five generic categories: phishing attacks, ransomwares, protocol, supply chain and system attacks (Liu et al.).

### *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 a trusted entity misleads users to enter personal information at a fake website or download 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 or 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 its 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. (Madhusudhanan Chandrasekaran et al.) 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. McRae and Vaughn (McRae and Vaughn) presented a new method to detect sites that contain phishing content using honey tokens. Accordingly, Ajlouni et al. (Ajlouni et al.) propose 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 (Jain and Richariya) 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 (Demertzis and Iliadis) 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, is using 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. (Yan et al.). 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. (Gu et al.) proposed a method for detecting botnets by mapping a sequence model based on extracting URLs from spam mails. Also, Ma, et al. (Ma et al.) 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 (McGrath and Gupta) 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 (Xie et al.) focus on detecting spamming botnets by developing regular signatures based on expressions from a set of spam address data. Stalmans (Stalmans and Irwin) proposed a technique for detecting and mitigating botnet infection on a network, using features from DNS queries such as A and NS Records, IP ranges, TTL and alphanumeric characters from domains.

Finally, the work of (Demertzis and Iliadis) 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 Domains Names. It is a biologically inspired artificial intelligence computer security technique as it uses the evolving Spiking Neural Network (eSNN) which are the 3rd 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 on personal files and demands from the users to 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 (Al-Hawawreh et al.) offer a detailed and systematic analysis of the various threats imposed by IIoT ransomwares and recommended 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 act as a bridge between the external world and the critical IIoT infrastructure, that is Program Logic Controllers (PLCs) or Input/Output (IO) devices. When an attacker launches a successful ransomware attack against an IIoT gateway, it can take full access on 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 analyse 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) (Lin et al.). Their platform consists mainly of three parts: the I/O 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, database and multimedia files of a web hosting company when launched (*Erebus Linux Ransomware: Impact to Servers and Countermeasures - Security News*). 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 attack on early stage and the separation of the IIoT edge gateway from the other IIoT infrastructure, by placing IIoT edge gateway into a specific trusted zone.

Apart from the conventional methods for identifying ransomware attacks, there are many studies that have utilised machine and deep learning techniques for ransomware detection. The authors of (Alhawi et al.) 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 (Almashhadani et al.) 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 (Al-Hawawreh and Sitnikova) 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 (Maiorca et al.), decision trees (Alhawi et al.), Logistic Regression (LR), support vector machine (SVM) (Sgandurra et al.) and DNN (Tseng et al.) and 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 5 layers for IoT: Physical, Data-link, Network, Transport and Application layer (see Fig.2) (Tournier et al.)

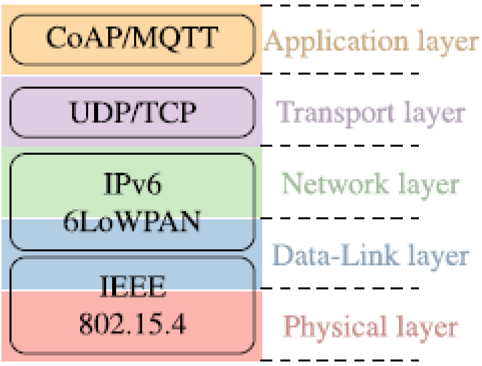


**Figure 2.** An example of IoT protocol stack compared to TCP/IP stack.

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) and Long-Term Evolution (LTE) and UDP/TCP (see also Fig. 2). 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 (Butun et al.; Tournier et al.; Varga et al.; Hossain et al.). 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 (Hossain et al.). 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 (Muraleedharan and Osadciw) proposed 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, it is also known as *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  (Mouatamid et al.; Usman et al.). *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 in this type of threat is to applying data encryption algorithms, such as Asymmetric Encryption Standard (AES) in IEEE 802.15.4 and 6LoWPAN networks (Hennebert and Santos), Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access II (WPA2) in Wi-Fi and LTE networks (Adnan et al.; Sulaiman and Fakhri).

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)* (Butun et al.). In *Routing* attack, 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, authorisation and monitoring tools, such as Intrusion Detection System (IDS) solutions specifically adapted for IoTs like for instance SVELTE (Raza et al.). *Data transit attacks* affect data integrity and confidentiality. Countermeasures include the use of compressed transport protocols, for instance Datagrams Transport Layer Security (DTLS) (Hennebert and Santos). The threats against the *Neighbor Discovery Protocol (NDP)* are presented in (Ahmed et al.). 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 analysed in this work, including the Tunneling (IPSec) and the SEcure Neighbor Discovery (SEND) protocols. The analysis results indicate that NDP that 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 Transport layer include de-synchronisation, SYN-Flooding and Message Queue Telemetry Transport (MQTT) Exploit attacks (Butun et al.). In de-synchronisation attacks the intruder injects packets with fake sequence numbers of control flags that de-synchronise endpoints. Effective countermeasures include message authentication (Unsal and Çebi; Ferrag et al.; El-hajj et al.). 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 involve interventions and optimisations on the transport protocols itself, 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  (Eddy). The deficiencies of the Message Queue Telemetry Transport (MQTT) protocol are presented by the authors of (Andy et al.). 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 include 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 (Singh et al.). 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<br>BLE<br>WiFi<br>LTE | Jamming DoS attacks | Packets' rerouting to alternative routes (Muraleedharan and Osadciw) |
| | | Collision/Exhaustion/ Unfairness attacks | FHSS techniques (Mouatamid et al.; Usman et al.) |
| | | Data Transit Attacks | Data encryption algorithms (Hennebert and Santos; Adnan et al.) |
| Network Layer | IPv4/IPv6<br>RPL<br>6LoWPAN | Routing and DoS Attacks | Ingress filtering and IDS solutions (Raza et al.; Butun et al.) |
| | | Data Transit Attacks | Compressed Transport protocols (for instance DTL) (Hennebert and Santos) |
| | | Threats to Neighbor Discovery Protocol (IPv4/IPv6) | Use of IPsec, SEND protocols (Ahmed et al.) |
| Transport Layer | De-Synchronisation | sending control flags that synchronise endpoints | Message authentication (Ferrag et al.) |
| | SYN-flooding | system flooding during the SYN handshaking phase | Optimisations in transport layer apply network filtering (Eddy) |
| | MQTT | Data Transit Attacks, Scalable Key management | Secure MQTT, ABE algorithm (Singh et al.) |

### 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 (Morris et al.). 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 (Chromik et al.; Nyasore et al.; Wakchaure et al.; Zamfir et al.). For example Liang et al. (Liang et al.) propose an industrial network intrusion detection algorithm based on multifeature 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 is decreased by 8.8%. Also, a novel network intrusion prevention system that exploits the benefits of incremental machine learning frameworks that utilises a self-organizing incremental neural network along with a Support Vector Machine proposed by the Constantinides et al. (Constantinides et al.). 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 based on Machine Learning to access Modbus TCP protocol development by Deng et al. (Deng et al.). 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. (Brugman et al.) propose a high 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 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. In general, what is nowadays called third party is gaining the attention of risk management more and more. M. Farooq in their study (Farooq and Zhu), present and highlight the supply chain threats and they suggest approaches concerning the risk management procedures. They present and describe the IoT supply chain risk landscape characterising it as extremely diverse.

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.

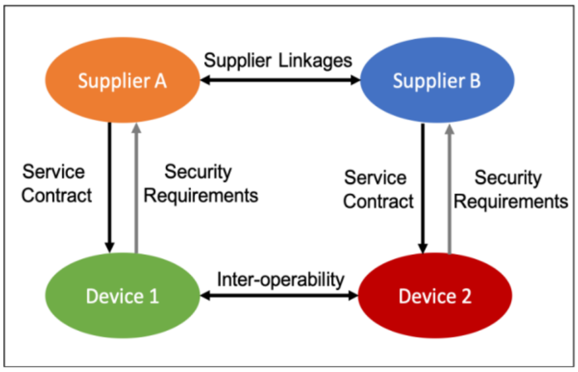


**Figure 3.** Key interactions between different players in the supply chain ecosystem of the IoT.

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 which already faces this threat and does not have the ability to change the whole risk management approach.

Petar Randaliev (Radanliev et al.) in their study, present 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. Also, 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. (Kieras et al.) 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, the (Mercaldo et al.) 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 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. Also, 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 is 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). Also, 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 specific, 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, characterize the behavior of SCADA system, whether it accepts or not an attack. 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 valuesare then classified into 3 classes (Up, Basal, and Low). The values in question are then entered into an automated system[1]. 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 (Konstantinos Demertzis, Iliadis, and Bougoudis; Xing et al.; K. Demertzis, L. Iliadis, and Anezakis), a specialized standardization is proposed in the work Blockchain Security Architecture for IIoT (Konstantinos Demertzis, L. Iliadis, Tziritas, et al.) 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 he learns to compress the original data from the input layer into an abstract form, which 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 (PLCs) devices in order to speed up or slow down their operations,

[1] The automated systems implement automata, i.e. mathematical objects which maintain abstract finite state machines for resolving complex problems. In an automated system specific transitions are allowed among the states

driving overall industrial equipment in its destruction or permanent damage. Such an attack scenario is described in (Garcia et al.) 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 59.5-61Hz (60Hz 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, they replaced the cost minimization function with maximizing so that the hostile impact is maximized and they 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 (Demertzis; Iliadis, et al. and Anezakis; Konstantinos Demertzis, L. Iliadis, and Anezakis; Demertzis and Iliadis) 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. Also, 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 (Zhou and Guo; Genge et al.). In general, as types of anomalies are considered patterns that show different or deviant behavior from the expected and which can be categorized into Point Anomalies, Contextual Anomalies, Collective Anomalies, Protocol Anomalies, etc (Cook et al.; Gaddam et al.; Deorankar and Thakare).

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 (Formby and Beyah) 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 Sn represents the cumulative value in sample n, xn represents the value monitored in sample number n, and wn is the usual mean of the monitored value. A change is detected when Sn 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 to monitor 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 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 (Nakamura and Ribeiro).

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 (Sengupta).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 in capturing the subtle differences that distinguish them (Lee et al.).

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

**Table 2.** Cyber Threats and its Countermeasures.

| ID | Cyber Threats | | Countermeasures |
|---|---|---|---|
| 1 | ***Phishing attacks***<br>The attacker, masquerading as a trusted entity. | Breach of IIoT systems<br>Control of operation systems that are linked to it | PHONEY for auto detection and analysis of phishing attacks (Madhusudhanan Chandrasekaran et al.)<br>Intelligence Web Application Firewall (IWAF) (Demertzis and Iliadis)<br>URL Embedding (UE) (Yan et al.)<br>Detecting botnets by mapping a sequence model based on extracting URLs from spam mails (Stalmans and Irwin)<br>Smart URL Filter in a Zone-based Policy Firewall for detecting Algorithmically Generated Malicious Domains Names (Demertzis and Iliadis) |
| 2 | ***Ransomware attacks***<br>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 (Al-Hawawreh et al)<br>Machine Learning techniques (Alhawi et al.)<br>Intrusion detection system (Almashhadani et a.l)<br>Hybrid detection systems (Al-Hawawreh and SitnikovaMaiorca et al.;Alhawi et al.; Sgandurra et al.; Tseng et al.) |

| | | | |
|---|---|---|---|
| 3 | ***Protocols Attacks***<br>Any threat in protocol stack of IIoT | Jamming DoS attacks | Packets' rerouting to alternative routes (Muraleedharan and Osadciw) |
| | | Collision/Exhaustion/Unfairness attacks | FHSS techniques (Mouatamid et al.; Usman et al.) |
| | | Data Transit Attacks | Data encryption algorithms (Hennebert and Santos; Adnan et al.) |
| | | Routing and DoS Attacks | Ingress filtering and IDS solutions (Raza et al.; Butun et al.) |
| | | Data Transit Attacks | Compressed Transport protocols (for instance DTL) (Hennebert and Santos) |
| | | Threats to Neighbor Discovery Protocol (IPv4/IPv6) | Use of IPsec, SEND protocols (Ahmed et al.) |
| | | sending control flags that synchronise endpoints | Message authentication (Ferrag et al.) |
| | | system flooding during the SYN handshaking phase | optimisations in transport layer<br>apply network filtering (Eddy) |
| | | Data Transit Attacks, Scalable Key management | Secure MQTT, ABE algorithm (Singh et al.) |
| | | SCADA Modbus Attacks | Intrusion Detection and Prevention System (Brugman et al.; Nyasore et al.) |
| 4 | ***Supply chain attacks***<br>*a cyber-attack that seeks to damage an industry or organization by targeting less-secure elements in the supply chain.* | Backdoors Installation<br>Very hard to detect | View the ecosystem from a supply chain viewpoint and control the risk (Farooq and Zhu)<br>Self-adapting supply chain system with Artificial Intelligence (AI), Machine Learning (ML) and real-time intelligence for predictive cyber risk analytics (Radanliev et al.) |
| 5 | ***Systems Attacks***<br>*Unauthorized access into an industrial system in order to cause harm.* | Man-in-the-Middle attacks<br>Mechanically control the dynamically rearranging centrifugation, or reprogramming the complex Programmable Logic Controller (PLCs) devices in order to speed up or slow down their operations | System logs modelling (Mercaldo et al.)<br>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 (Mercaldo et al.)<br>Hybrid Network Anomaly and Intrusion Detection Approach Based on Evolving Spiking Neural Network Classification (Demertzis; Iliadis et al.)<br>CUmulative SUM (CUSUM) algorithm (Formby and Beyah) |

Among the threats discussed, the supply chain attacks are becoming a serious concern because significant factors like complexity and stealthiness do not provide easy so-

doi:10.20944/preprints202102.0148.v1

lutions (Hou et al.). 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 added in them access control or encryption techniques (McLaughlin et al.; Li et al.). 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 it includes or can support (Lee et al.).

Furthermore, due to the real-time operation and development of the IIoT (Mercaldo et al.; Radanliev et al.; K. Demertzis, L. Iliadis, and Anezakis), 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 (Nakamura and Ribeiro) 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 (Konstantinos Demertzis, P. Kikiras, Tziritas, et al.; Zhou and Guo), 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 (McLaughlin et al.). 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 (Ghosh and Sampalli; Mercaldo et al.; Falco et al.; Kargl et al.), 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. Also, 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.

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

## References

1. Brugman, J., et al. “Cloud Based Intrusion Detection and Prevention System for Industrial Control Systems Using Software Defined Networking.” 2019 Resilience Week (RWS), vol. 1, 2019, pp. 98–104. IEEE Xplore, doi:10.1109/RWS47064.2019.8971825.
2. Chromik, J., et al. “A Parser for Deep Packet Inspection of IEC-104: A Practical Solution for Industrial Applications.” 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks – Industry Track, 2019, pp. 5–8. IEEE Xplore, doi:10.1109/DSN-Industry.2019.00008.
3. Constantinides, C., et al. “A Novel Online Incremental Learning Intrusion Prevention System.” 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2019, pp. 1–6. IEEE Xplore, doi:10.1109/NTMS.2019.8763842.
4. Deng, L., et al. “Intrusion Detection Method Based on Support Vector Machine Access of Modbus TCP Protocol.” 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), 2016, pp. 380–83. IEEE Xplore, doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2016.90.
5. Liang, W., et al. “An Industrial Network Intrusion Detection Algorithm Based on Multifeature Data Clustering Optimization Model.” IEEE Transactions on Industrial Informatics, vol. 16, no. 3, Mar. 2020, pp. 2063–71. IEEE Xplore, doi:10.1109/TII.2019.2946791.
6. Nyasore, O. N., et al. “Deep Packet Inspection in Industrial Automation Control System to Mitigate Attacks Exploiting Modbus/TCP Vulnerabilities.” 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), 2020, pp. 241–45. IEEE Xplore, doi:10.1109/BigDataSecurity-HPSC-IDS49724.2020.00051.
7. Wakchaure, M., et al. “Reconnaissance of Industrial Control System by Deep Packet Inspection.” 2016 IEEE International Conference on Engineering and Technology (ICETECH), 2016, pp. 1093–96. IEEE Xplore, doi:10.1109/ICETECH.2016.7569418.
8. Zamfir, S., et al. “Solutions for Deep Packet Inspection in Industrial Communications.” 2016 International Conference on Communications (COMM), 2016, pp. 153–58. IEEE Xplore, doi:10.1109/ICComm.2016.7528337.
9. Ahmed, A. S. A. Mohamed Sid, et al. “IPv6 Neighbor Discovery Protocol Specifications, Threats and Countermeasures: A Survey.” *IEEE Access*, vol. 5, 2017, pp. 18187–210. *IEEE Xplore*, doi:10.1109/ACCESS.2017.2737524.
10. Ajlouni, Moh’d Iqbal AL, et al. “Detecting Phishing Websites Using Associative Classification.” *Journal of Information Engineering and Applications*, vol. 3, no. 7, 2013, pp. 6–10.
11. Al-Hawawreh, M., et al. “Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things.” *IEEE Internet of Things Journal*, vol. 6, no. 4, Aug. 2019, pp. 7137–51. *IEEE Xplore*, doi:10.1109/JIOT.2019.2914390.
12. Al-Hawawreh, M., and E. Sitnikova. “Leveraging Deep Learning Models for Ransomware Detection in the Industrial Internet of Things Environment.” *2019 Military Communications and Information Systems Conference (MilCIS)*, 2019, pp. 1–6. *IEEE Xplore*, doi:10.1109/MilCIS.2019.8930732.
13. Alhawi, Omar MK, et al. “Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection.” *Cyber Threat Intelligence*, Springer, 2018, pp. 93–106.
14. Almashhadani, A. O., et al. “A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware.” *IEEE Access*, vol. 7, 2019, pp. 47053–67. *IEEE Xplore*, doi:10.1109/ACCESS.2019.2907485.
15. Andy, S., et al. “Attack Scenarios and Security Analysis of MQTT Communication Protocol in IoT System.” *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2017, pp. 1–6. *IEEE Xplore*, doi:10.1109/EECSI.2017.8239179.
16. Banafa, A. “2 The Industrial Internet of Things (IIoT): Challenges, Requirements and Benefits.” *Secure and Smart Internet of Things (IoT): Using Blockchain and AI*, River Publishers, 2018, pp. 7–12. *IEEE Xplore*, https://ieeexplore.ieee.org/document/9226906.
17. Butun, I., et al. “Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures.” *IEEE Communications Surveys Tutorials*, vol. 22, no. 1, Firstquarter 2020, pp. 616–44. *IEEE Xplore*, doi:10.1109/COMST.2019.2953364.
18. Cook, A. A., et al. “Anomaly Detection for IoT Time-Series Data: A Survey.” *IEEE Internet of Things Journal*, vol. 7, no. 7, July

2020, pp. 6481–94. *IEEE Xplore*, doi:10.1109/JIOT.2019.2958185.

19. Demertzis, K., L. Iliadis, and V. Anezakis. "MOLESTRA: A Multi-Task Learning Approach for Real-Time Big Data Analytics." *2018 Innovations in Intelligent Systems and Applications (INISTA)*, 2018, pp. 1–8. *IEEE Xplore*, doi:10.1109/INISTA.2018.8466306.
20. Demertzis, Konstantinos, Lazaros Iliadis, and Vardis-Dimitris Anezakis. "A Dynamic Ensemble Learning Framework for Data Stream Analysis and Real-Time Threat Detection." *Artificial Neural Networks and Machine Learning – ICANN 2018*, edited by Věra Kůrková et al., Springer International Publishing, 2018, pp. 669–81. *Springer Link*, doi:10.1007/978-3-030-01418-6_66.
21. Demertzis, Konstantinos, Lazaros S. Iliadis, and Vardis-Dimitrios Anezakis. "An Innovative Soft Computing System for Smart Energy Grids Cybersecurity." *Advances in Building Energy Research*, vol. 12, no. 1, Jan. 2018, pp. 3–24. *Taylor and Francis+NEJM*, doi:10.1080/17512549.2017.1325401.
22. Demertzis, Konstantinos, Lazaros Iliadis, Nikos Tziritas, et al. "Anomaly Detection via Blockchained Deep Learning Smart Contracts in Industry 4.0." *Neural Computing and Applications*, vol. 32, no. 23, Dec. 2020, pp. 17361–78. *Springer Link*, doi:10.1007/s00521-020-05189-8.
23. Demertzis, Konstantinos, Lazaros Iliadis, and Ilias Bougoudis. "Gryphon: A Semi-Supervised Anomaly Detection System Based on One-Class Evolving Spiking Neural Network." *Neural Computing and Applications*, vol. 32, no. 9, May 2020, pp. 4303–14. *Springer Link*, doi:10.1007/s00521-019-04363-x.
24. Demertzis, Konstantinos, Panayiotis Kikiras, Nikos Tziritas, et al. "The Next Generation Cognitive Security Operations Center: Network Flow Forensics Using Cybersecurity Intelligence." *Big Data and Cognitive Computing*, vol. 2, no. 4, Dec. 2018, p. 35. *www.mdpi.com*, doi:10.3390/bdcc2040035.
25. Demertzis, Konstantinos, and Lazaros Iliadis. "A Hybrid Network Anomaly and Intrusion Detection Approach Based on Evolving Spiking Neural Network Classification." *E-Democracy, Security, Privacy and Trust in a Digital World*, edited by Alexander B. Sideridis et al., Springer International Publishing, 2014, pp. 11–23. *Springer Link*, doi:10.1007/978-3-319-11710-2_2.
26. Demertzis, Konstantinos, and Lazaros Iliadis. "Cognitive Web Application Firewall to Critical Infrastructures Protection from Phishing Attacks." *Scienpress Ltd*, vol. 9, no. 2, 2019, p. 26.
27. Demertzis, Konstantinos, and Lazaros Iliadis. "Evolving Smart URL Filter in a Zone-Based Policy Firewall for Detecting Algorithmically Generated Malicious Domains." *Statistical Learning and Data Sciences*, edited by Alexander Gammerman et al., Springer International Publishing, 2015, pp. 223–33. *Springer Link*, doi:10.1007/978-3-319-17091-6_17.
28. Deorankar, A. V., and S. S. Thakare. "Survey on Anomaly Detection of (IoT)- Internet of Things Cyberattacks Using Machine Learning." *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, 2020, pp. 115–17. *IEEE Xplore*, doi:10.1109/ICCMC48092.2020.ICCMC-00023.
29. Eddy, Wesley M. *Defenses Against TCP SYN Flooding Attacks-The Internet Protocol Journal*. Dec, 2006.
30. El-hajj, M., et al. "Analysis of Authentication Techniques in Internet of Things (IoT)." *2017 1st Cyber Security in Networking Conference (CSNet)*, 2017, pp. 1–3. *IEEE Xplore*, doi:10.1109/CSNET.2017.8242006.
31. *Erebus Linux Ransomware: Impact to Servers and Countermeasures - Security News*. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/erebus-linux-ransomware-impact-to-servers-and-countermeasures. Accessed 20 Jan. 2021.
32. Falco, G., et al. "IIoT Cybersecurity Risk Modeling for SCADA Systems." *IEEE Internet of Things Journal*, vol. 5, no. 6, Dec. 2018, pp. 4486–95. *IEEE Xplore*, doi:10.1109/JIOT.2018.2822842.
33. Farooq, Muhammad Junaid, and Quanyan Zhu. "IoT Supply Chain Security: Overview, Challenges, and the Road Ahead." *ArXiv:1908.07828 [Cs]*, July 2019. *arXiv.org*, http://arxiv.org/abs/1908.07828.
34. Ferrag, Mohamed Amine, et al. "Authentication Protocols for Internet of Things: A Comprehensive Survey." *Security and Communication Networks*, vol. 2017, Hindawi, 6 Nov. 2017, p. e6562953, doi:https://doi.org/10.1155/2017/6562953.
35. Formby, D., and R. Beyah. "Temporal Execution Behavior for Host Anomaly Detection in Programmable Logic Controllers." *IEEE Transactions on Information Forensics and Security*, vol. 15, 2020, pp. 1455–69. *IEEE Xplore*, doi:10.1109/TIFS.2019.2940890.
36. Gaddam, A., et al. "Anomaly Detection Models for Detecting Sensor Faults and Outliers in the IoT - A Survey." *2019 13th International Conference on Sensing Technology (ICST)*, 2019, pp. 1–6. *IEEE Xplore*, doi:10.1109/ICST46873.2019.9047684.
37. Garcia, Luis, et al. "Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit." *NDSS*, 2017. *Semantic Scholar*, doi:10.14722/NDSS.2017.23313.
38. Gebremichael, T., et al. "Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges." *IEEE Access*, vol. 8, 2020, pp. 152351–66. *IEEE Xplore*, doi:10.1109/ACCESS.2020.3016937.
39. Genge, B., et al. "Anomaly Detection in Aging Industrial Internet of Things." *IEEE Access*, vol. 7, 2019, pp. 74217–30. *IEEE Xplore*, doi:10.1109/ACCESS.2019.2920699.
40. Ghosh, S., and S. Sampalli. "A Survey of Security in SCADA Networks: Current Issues and Future Challenges." *IEEE Access*, vol. 7, 2019, pp. 135812–31. *IEEE Xplore*, doi:10.1109/ACCESS.2019.2926441.
41. Hennebert, C., and J. D. Santos. "Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis." *IEEE Internet of Things Journal*, vol. 1, no. 5, Oct. 2014, pp. 384–98. *IEEE Xplore*, doi:10.1109/JIOT.2014.2359538.
42. Hossain, M. M., et al. "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things." *2015 IEEE World Congress on Services*, 2015, pp. 21–28. *IEEE Xplore*, doi:10.1109/SERVICES.2015.12.

43. Hou, Y., et al. "Understanding Security Requirements for Industrial Control System Supply Chains." *2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, 2019, pp. 50–53. *IEEE Xplore*, doi:10.1109/SEsCPS.2019.00016.
44. Irmak, E., and İ. Erkek. "An Overview of Cyber-Attack Vectors on SCADA Systems." *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 2018, pp. 1–5. *IEEE Xplore*, doi:10.1109/ISDFS.2018.8355379.
45. Jain, Aanchal, and Vineet Richariya. *Implementing a Web Browser with Phishing Detection Techniques*. 2011, p. 3.
46. Juárez, F. A. B. "Cybersecurity in an Industrial Internet of Things Environment (IIoT) Challenges for Standards Systems and Evaluation Models." *2019 8th International Conference On Software Process Improvement (CIMPS)*, 2019, pp. 1–6. *IEEE Xplore*, doi:10.1109/CIMPS49236.2019.9082437.
47. Kang, D., et al. "Cyber Threats and Defence Approaches in SCADA Systems." *16th International Conference on Advanced Communication Technology*, 2014, pp. 324–27. *IEEE Xplore*, doi:10.1109/ICACT.2014.6778974.
48. Kannengiesser, U., and H. Müller. "Towards Viewpoint-Oriented Engineering for Industry 4.0: A Standards-Based Approach." *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, 2018, pp. 51–56. *IEEE Xplore*, doi:10.1109/ICPHYS.2018.8387636.
49. Kargl, F., et al. "Insights on the Security and Dependability of Industrial Control Systems." *IEEE Security Privacy*, vol. 12, no. 6, Nov. 2014, pp. 75–78. *IEEE Xplore*, doi:10.1109/MSP.2014.120.
50. Kieras, Timothy, et al. *RIoTS: Risk Analysis of IoT Supply Chain Threats*. 2019.
51. Kołowrocki, K., and J. Soszyńska-Budny. "Critical Infrastructure Safety Indicators." *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 2018, pp. 1761–64. *IEEE Xplore*, doi:10.1109/IEEM.2018.8607552.
52. Lee, C., et al. "Heterogeneous Industrial IoT Integration for Manufacturing Production." *2019 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, 2019, pp. 1–2. *IEEE Xplore*, doi:10.1109/ISPACS48206.2019.8986308.
53. Li, J., et al. "Industrial Internet: A Survey on the Enabling Technologies, Applications, and Challenges." *IEEE Communications Surveys Tutorials*, vol. 19, no. 3, thirdquarter 2017, pp. 1504–26. *IEEE Xplore*, doi:10.1109/COMST.2017.2691349.
54. Lin, Shi-Wan, et al. "The Industrial Internet of Things Volume G1: Reference Architecture." *Industrial Internet Consortium*, 2017, pp. 10–46.
55. Liu, X., et al. "Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities." *IEEE Access*, vol. 7, 2019, pp. 79523–44. *IEEE Xplore*, doi:10.1109/ACCESS.2019.2920763.
56. Ma, Justin, et al. "Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs." *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining - KDD '09*, ACM Press, 2009, p. 1245. *DOI.org (Crossref)*, doi:10.1145/1557019.1557153.
57. Madhusudhanan Chandrasekaran, et al. "PHONEY: Mimicking User Response to Detect Phishing Attacks." *2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks(WoWMoM'06)*, 2006, pp. 5 pp. – 672. *IEEE Xplore*, doi:10.1109/WOWMOM.2006.87.
58. Maiorca, Davide, et al. "R-PackDroid: API Package-Based Characterization and Detection of Mobile Ransomware." *Proceedings of the Symposium on Applied Computing*, Association for Computing Machinery, 2017, pp. 1718–1723. *ACM Digital Library*, doi:10.1145/3019612.3019793.
59. McGrath, D. Kevin, and Minaxi Gupta. "Behind Phishing: An Examination of Phisher Modi Operandi." *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, USENIX Association, 2008, pp. 1–8.
60. McLaughlin, S., et al. "The Cybersecurity Landscape in Industrial Control Systems." *Proceedings of the IEEE*, vol. 104, no. 5, May 2016, pp. 1039–57. *IEEE Xplore*, doi:10.1109/JPROC.2015.2512235.
61. McRae, C. M., and R. B. Vaughn. "Phighting the Phisher: Using Web Bugs and Honeytokens to Investigate the Source of Phishing Attacks." *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 2007, pp. 270c–270c. *IEEE Xplore*, doi:10.1109/HICSS.2007.435.
62. Mercaldo, F., et al. "Real-Time SCADA Attack Detection by Means of Formal Methods." *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, 2019, pp. 231–36. *IEEE Xplore*, doi:10.1109/WETICE.2019.00057.
63. Mikhalevich, I. F., and V. A. Trapeznikov. "Critical Infrastructure Security: Alignment of Views." *2019 Systems of Signals Generating and Processing in the Field of on Board Communications*, 2019, pp. 1–5. *IEEE Xplore*, doi:10.1109/SOSG.2019.8706821.
64. Morris, T., et al. *Industrial Control System Simulation and Data Logging for Intrusion Detection System Research*. 2015,/paper/Industrial-Control-System-Simulation-and-Data-for-Morris-Thornton/bb9714e0c661576f5df19fb54e0e26567ca37372.
65. Mouaatamid, Otmane El, et al. "Internet of Things Security: Layered Classification of Attacks and Possible Countermeasures." *Electronic Journal of Information Technology*, vol. 0, no. 9, 9, Dec. 2016. *www.webmail.revue-eti.net*, http://www.webmail.revue-eti.net/index.php/eti/article/view/98.
66. Muraleedharan, R., and L. A. Osadciw. "Cross Layer Denial of Service Attacks in Wireless Sensor Network Using Swarm Intelligence." *2006 40th Annual Conference on Information Sciences and Systems*, 2006. *Semantic Scholar*, doi:10.1109/CISS.2006.286400.
67. Nakamura, E. T., and S. L. Ribeiro. "A Privacy, Security, Safety, Resilience and Reliability Focused Risk Assessment Methodology for IIoT Systems Steps to Build and Use Secure IIoT Systems." *2018 Global Internet of Things Summit (GIoTS)*, 2018, pp. 1–6. *IEEE Xplore*, doi:10.1109/GIOTS.2018.8534521.

68. Panchal, A. C., et al. "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures." *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, 2018, pp. 124–30. *IEEE Xplore*, doi:10.1109/GCWCN.2018.8668630.
69. Radanliev, Petar, et al. *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*. Preprints, Dec. 2020. *www.preprints.org*, https://www.preprints.org/manuscript/201903.0123/v2.
70. Raza, Shahid, et al. "SVELTE : Real-Time Intrusion Detection in the Internet of Things." *Ad Hoc Networks*, vol. 11, no. 8, Elsevier, 2013, pp. 2661–74.
71. Sengupta, Jayasree. "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT." *Journal of Network and Computer Applications*, 2020, p. 20.
72. Sgandurra, Daniele, et al. "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection." *ArXiv:1609.03020 [Cs]*, Sept. 2016. *arXiv.org*, http://arxiv.org/abs/1609.03020.
73. Singh, M., et al. "Secure MQTT for Internet of Things (IoT)." *2015 Fifth International Conference on Communication Systems and Network Technologies*, 2015, pp. 746–51. *IEEE Xplore*, doi:10.1109/CSNT.2015.16.
74. Stalmans, E., and B. Irwin. "A Framework for DNS Based Detection and Mitigation of Malware Infections on a Network." *2011 Information Security for South Africa*, 2011, pp. 1–8. *IEEE Xplore*, doi:10.1109/ISSA.2011.6027531.
75. Sulaiman, Alyaa, and Imad Fakhri. *Comparative Study on 4G/Lte Cryptographic Algorithms Based on Different Factors*. 1 July 2014.
76. Tournier, Jonathan, et al. "A Survey of IoT Protocols and Their Security Issues through the Lens of a Generic IoT Stack." *Internet of Things*, July 2020, p. 100264. *hal.inria.fr*, doi:10.1016/j.iot.2020.100264.
77. Tseng, Aragorn, et al. "Deep Learning for Ransomware Detection." *IEICE Tech. Rep.*, vol. 116, no. 282, 2016, pp. 87–92.
78. Unsal, Emre, and Yalçin Çebi. *DENIAL OF SERVICE ATTACKS IN WSN*. 2013. *ResearchGate*, doi:10.13140/2.1.4040.9929.
79. Usman, Muhammad, et al. "KaFHCa: Key-Establishment via Frequency Hopping Collisions." *ArXiv:2010.09642 [Cs]*, Oct. 2020. *arXiv.org*, http://arxiv.org/abs/2010.09642.
80. Varga, P., et al. "Security Threats and Issues in Automation IoT." *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*, 2017, pp. 1–6. *IEEE Xplore*, doi:10.1109/WFCS.2017.7991968.
81. Xie, Yinglian, et al. *Spamming Botnet: Signatures and Characteristics*. Aug. 2008. *www.microsoft.com*, https://www.microsoft.com/en-us/research/publication/spamming-botnet-signatures-and-characteristics/.
82. Xing, Lining, et al. "Identifying Data Streams Anomalies by Evolving Spiking Restricted Boltzmann Machines." *Neural Computing and Applications*, vol. 32, no. 11, June 2020, pp. 6699–713. *Springer Link*, doi:10.1007/s00521-019-04288-5.
83. Yan, X., et al. "Learning URL Embedding for Malicious Website Detection." *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, Oct. 2020, pp. 6673–81. *IEEE Xplore*, doi:10.1109/TII.2020.2977886.
84. Zhou, C., et al. "Research on Network Security Attack Detection Algorithm in Smart Grid System." *2017 International Conference on Computer Technology, Electronics and Communication (ICCTEC)*, 2017, pp. 1407–10. *IEEE Xplore*, doi:10.1109/ICCTEC.2017.00307.
85. Zhou, L., and H. Guo. "Anomaly Detection Methods for IIoT Networks." *2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, 2018, pp. 214–19. *IEEE Xplore*, doi:10.1109/SOLI.2018.8476769.