




Article

Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures

Kyriaki Tsantikidou * and Nicolas Sklavos 

SCYTALE Group, Computer Engineering and Informatics Department, University of Patras, 26504 Patra, Greece; nsklavos@upatras.gr

* Correspondence: k.tsantikidou@upatras.gr

Abstract: Critical Infrastructures (CIs), such as healthcare facilities, power grids, transportation systems, and financial institutions, are vital components of a functioning society, with the economy and safety being dependent on them. Nevertheless, they have become increasingly vulnerable to cyber threats and attacks in recent years. The main reason is their inability to quickly adapt to technological changes, employ updated cryptographic frameworks, and implement a thoroughly secure architecture based on their characteristics. In this study, the unique complexities of these systems are highlighted. Various verified cyberattacks that were executed against CIs in recent years are analyzed. Moreover, the general framework of CIs is demonstrated together with the employed technologies and cryptographic primitives. A thorough architecture of said technologies is developed to better understand the targeted components and easily identify potentially hidden threats. Afterwards, threat, adversary, and attack models that target critical systems and services are designed. The purpose is a better comprehension of the systems' vulnerabilities, attack structures, motives, and targets for assisting CIs' designers in creating secure frameworks and mechanisms, with the ability to mitigate such threats. Lastly, security controls and cryptography frameworks are demonstrated together with efficient mitigation architectures and implementations from the research community.

Keywords: Critical Infrastructures; cybersecurity; cryptography; threats and attacks; mitigation; smart health; Internet of Things (IoT); SCADA



Citation: Tsantikidou, K.; Sklavos, N. Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures. *Cryptography* **2024**, *8*, 7. <https://doi.org/10.3390/cryptography8010007>

Academic Editor: Josef Pieprzyk

Received: 26 January 2024

Revised: 21 February 2024

Accepted: 23 February 2024

Published: 25 February 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

A Critical Infrastructure (CI) consists of either physical or digital systems and assets that are essential to nation-wide executed services [1]. These services can facilitate various aspects of daily life, such as healthcare, heating, transportation, irrigation, water supply, electricity supply, and information and communication services. These systems include, but are not limited to, healthcare and public health, financial systems, transportation systems, energy facilities, and oil and gas providers. Various frameworks have been introduced in recent years that propose the integration of such facilities with novel technologies, such as Internet of Things (IoT), Big Data Analysis, Cyber-Physical Systems (CPSs), robotics, etc. [2,3]. Moreover, Supervisory Control and Data Acquisition (SCADA) systems, which are employed for monitoring and controlling industrial services and infrastructures, are starting to employ mechanisms for connecting to the internet and integrating with other technologies. Overall, the main purpose is the enhancement of traditional infrastructures by digitizing the services and introducing new tools for enabling real-time and autonomous capabilities and better satisfying the constantly increasing applications' requirements, scalability, and heterogeneity.

Nevertheless, as these infrastructures become more reliant on information technologies and interconnected networks, they also become more vulnerable to cyber threats and attacks [4]. IoT, CPS, and SCADA systems have many innate vulnerabilities, due to their

architectures, employed mechanisms, and implemented cryptographic primitives, that can create opportunities for adversaries to gain access to or control over the CI and achieve their intended malicious purposes [5–7]. Possible disruption to these services has a great impact on national security, the economy, public health, and safety, with catastrophic results and the endangerment of human lives. Moreover, due to obvious or hidden interdependencies between different infrastructures, a successful attack that targets a specific critical system can lead to the complete shut-down of another CI or service.

The European Union has also stressed in the past the importance of CIs and their cybersecurity and safety [8]. Increased awareness, focused training and research, accurate information, and better understanding regarding CIs' interdependencies, threats, vulnerabilities, security incidents, cryptography frameworks, and mitigation and countermeasure techniques are demanded. Therefore, research that focuses on these objectives is needed to facilitate the integration of cybersecurity into CIs.

Various papers have investigated the vulnerabilities and threats of CIs from different perspectives. This work investigates recent issues and incidents of the last five years, from 2018 to 2023. It also discusses different aspects and technologies of various CIs, instead of focusing only on specific architectures. For additional reference, some international series of standards and guides that provide extensive analyses of appropriate security requirements for CIs and models for the proper implementation of cryptographic mechanisms can be found in [9–11].

In [12], various attack categorization methods are explored and reviewed within the context of IoT wireless devices in CIs. It also discusses the challenges that are encountered with cybersecurity detection methods. However, recent cyberattack incidents or mitigation methods are not presented as well as a developed unified architecture of the employed technologies. Major cyber incidents of industrial control systems (ICSs) and CIs are analyzed in [13]. Threat types, an adversary model, and practical and theoretical shortcomings are also presented. Nevertheless, a unified approach that integrates all employed technologies is not followed. Moreover, contrariwise to [13], the Health 4.0 framework is also explored in the current paper. In [5], IoT-enabled attacks are modeled. These types of attack aim at affecting some critical system or service by compromising IoT devices. It provides a taxonomy of realistic attack vectors and suggestions of mitigation solutions. However, this approach can be limited, as the IoT is not the only target of attackers, even if it is the most susceptible component of the architecture. Moreover, a unified architecture that clearly presents the integration of the IoT with CIs, SCADA, and CPSs is not demonstrated, contrariwise to this study. Lastly, ref. [14] introduces the vulnerabilities and cyberattacks of various CIs, being thorough with the recent development of attacks in each infrastructure. Nevertheless, it only focuses on these characteristics and omits any analysis in the architecture and technologies of CIs and mitigation approaches.

Moreover, ref. [4] only presents a survey of cyberattacks that targeted oil and gas infrastructures. The application and challenges of smart energy grids is the main component that is analyzed in [15]. In [16], smart cities and their current challenges and systems are presented. Furthermore, ref. [17] focuses on the security protocols and vulnerabilities of only SCADA systems. In [7], CPS security and a CPS-specific risk assessment are analyzed. Lastly, refs. [18–20] focus on the security, threats, and vulnerability assessment of the IoT as an independent entity and not as a part of a CI. Contrasting these related works, this study does not focus on a single aspect of CIs but analyzes the whole structure and many of its most employed technologies.

This study aims at providing researchers the appropriate knowledge and tools for better understanding CIs' architecture, threats, and vulnerabilities and modeling potential attacks based on the architecture's structure, the adversaries' characteristics, and attack patterns. This is achieved by first analyzing some recent real cyberattacks against CIs together with the CIs' structure and their most utilized technologies, namely SCADA, the IoT, and CPSs [7,17,21]. Moreover, the main concept of newly proposed frameworks, such as Industry 4.0 and Health 4.0, is these technologies' smooth integration with each

other and further with traditional CIs. Therefore, a unified architecture is developed that combines these three technologies and their mechanisms, while also maintaining their independence and characteristics. Two cryptography frameworks that can be applied on top of this architecture are also analysed to comprehend common techniques for security and privacy. The final created three layers can then be utilized as a tool by the CI designers for better developing their system and consequently identify each layer's vulnerabilities, interdependencies, and attacks. This provides a huge advantage against adversaries that try to exploit, disrupt, and destroy CIs, as the designers can foresee their system's characteristics, weaknesses, and challenges and quickly manage or eliminate them before any irreversible damage is inflicted.

This study also models threats, adversaries, and attacks. A threat model is a systematic approach to highlight and assess potential vulnerabilities and threats in the CIs' architecture. An adversary model demonstrates the characteristics, capabilities, and motivations of an attacker. They are categorized based on their available resources, access, specificity, and knowledge. An attack model specifies the strategies that are followed in order for attackers to complete their intended purposes. Three types of attacks are analyzed based on the target and vulnerabilities of each layer of the architecture. These models are the second important tool provided to CI designers to better understand the vulnerabilities and dangers of the environment they are working on and then carefully and securely develop their systems. Once again, by carefully analyzing and comprehending these models, CI developers and employees can anticipate threats and attacks, take measures against them, and completely mitigate them.

Finally, this study demonstrates various proposed security and mitigation approaches that enhance the security of a targeted component, offer mitigation policies, and train or assist the CI's supervisors. Overall, they provide a third tool of knowledge with the purpose of guiding future researchers toward finding appropriate solutions to their security problems. This step properly completes the previously mentioned tools as suitable solutions are presented with examples to be followed.

The contributions of this study, and specifically the provided tools for CI designers, are as follows:

- A presentation of the most recent cybersecurity attacks against CIs;
- An analysis and development of a thorough architecture that integrates the most common technologies and cryptographic mechanisms of CIs;
- The creation of a threat model, an adversary model, and an attack model based on this architecture and the structure of CIs;
- A demonstration of some published security and mitigation techniques and approaches.

The value of presenting collective standards and architectures that can be clearly followed by designers has been demonstrated by the constant efforts of the research community to develop exemplary combinational frameworks, such as Health 4.0, Industry 4.0, etc., together with NIST's efforts to provide cryptography solutions and security requirements [1–3,5,8,22,23]. Furthermore, by utilizing the demands of the European Union as a measurable value, this study increases awareness, directs training and research, provides accurate information, and facilitates better comprehension regarding CIs' interdependencies, threats, vulnerabilities, security incidents, cryptography frameworks, and mitigation and countermeasure techniques. Interdependencies are demonstrated in the developed unified architecture of CIs. Threats and vulnerabilities are analysed by easy-to-follow models. Finally, the most recent security incidents are mentioned, and cryptography frameworks, mitigation techniques, and security solutions are presented in detail. Thus, all demands are followed.

The rest of this paper is structured as follows: Section 2 highlights recent incidents of cyberattacks against different CIs to demonstrate common attack types and the consequences. In Section 3, the overall framework of CIs is analyzed together with the architectures of the most employed technologies and systems. A unified architecture that integrates these technologies together with the commonly employed cryptographic mechanisms is also

developed to better comprehend each of its components and their obvious and hidden vulnerabilities. Section 4 presents a threat, an adversary, and an attack model against the unified architecture and the cryptography frameworks of CIs for identifying the potential threats and vulnerabilities; as the characteristics, motivations, and capabilities of adversaries; and the attack types that can cause irreversible damage to the structure. Section 5 highlights recently proposed security and mitigation solutions by the scientific community for cryptography and general CIs. Finally, Section 6 concludes this paper.

2. Recent Incidents in Critical Infrastructures

In this section, recent real-world incidents will be presented. Their type of attack, the target, and the consequences will be demonstrated for each critical infrastructure to better demonstrate their vulnerabilities and the security importance.

2.1. Health

According to ENISA's threat landscape 2023 report, healthcare data and service availability have been the target of many attacks throughout the years [24]. In 2022, the Professional Finance Company had a data breach that impacted the patients of 650 healthcare providers across the USA. A similar attack accumulated a huge amount of medical data from different hospitals in Indonesia and sold them to the dark web. The availability of a website that is employed for facilitating patients' medical needs is also the target of attacks. A large DDoS cyberattack in Israel targeted various ministries' domains, resulting in the unavailability of their gov websites.

Medical devices can also become the target of malicious attacks because they can be utilized to access the whole system and perform DoS attacks that disturb the operational flow. Insulin pumps that were sold to 4000 patients were recalled by the FDA due to their vulnerability in unauthorized connections. A potential hacker could connect to the device wirelessly and change the pump's settings, leading to the over-delivery of insulin [25]. Overall, various types of attacks have been proven effective against medical devices, such as pacemakers, activity monitors, cardiac defibrillators, etc., resulting in data breaches and malfunctions [26].

2.2. Energy Facilities

In 2020, SolarWinds' Orion Platform was targeted, specifically its software updates versions 2019.4 hotfix 5, 2022.2 unpatched and 2022.2 hotfix 1 [27]. This platform is a tool that is utilized by IT professionals and government organizations, especially in the United States. The adversaries gained access to the platform via reconnaissance, thus extracting sensitive information and authorized credentials about the platform and its clients. This compromised authorization entity was then employed to gain access to the overall network. The result was the insertion of malicious code to a developing software that was going to be added in the next platform update. The devices that installed that update were then compromised, allowing adversaries to communicate with these client devices, further corrupting the network and executing remote operations. A lot of client data was stolen, with the company losing revenue and its trustworthiness.

Other attacks against power grids, as presented in [28], targeted components of the cyber and physical domains. An example is the exploitation of an unnoticed software bug in order to compromise a substation's controls. These attacks can have serious consequences, derailing the timely operation of power grids, disconnecting lines and equipment, and even causing failures and blackouts.

2.3. Intelligent Transportation Systems

According to ENISA's 2023 report regarding cyber threats in transport, malicious attacks have increased in number in recent years [29]. Specifically, ransomware attacks have doubled and attacks linked to cybercriminals and hacktivists are on the rise. Fraudulent websites which impersonate airlines official websites, DDoS attacks against railway

companies, and ransomware attacks that led to production disruptions in the automobile industry are some recent examples of attacks being executed by money-driven or political groups. The main purpose is the extraction of companies' and clients' sensitive data or credentials and operational disruptions to the system. These can lead to losses in revenue or major accidents due to malfunctions.

2.4. Oil and Gas Facilities

In 2019, various attacks were performed and targeted oil and gas facilities, mainly in the Middle East [4]. These attacks tried to gain access to the system by employing spear phishing and password spraying. Many email accounts and credentials were compromised with a DNS and HTTP communication-based trojan that remotely executed arbitrary operations.

Another attack that targeted oil and gas facilities was also performed in 2021. The Colonial Pipeline, which is a critical infrastructure that provides a huge percentage of the U.S. East Coast's fuel, was targeted, and requested to pay ransom for the decryption keys that would restore the system [13]. A VPN account that was believed to be deactivated was compromised and utilized as an entry point to the system. Even though the exact method with which the username and password of the account were extracted is not known, that VPN account had notably not enabled any multi-factor authentication protection. Afterwards, ransomware that was designed by the cybercriminal group DarkSide was easily installed. This ransomware gains foothold of the network and installs itself to other MS Window machines via network shares. The next steps are to exfiltrate private information and encrypt all files by utilizing a combinational encryption mechanism. Overall, the adversaries had a money-driven motivation, resulting in an outrage lasting almost six days.

2.5. Financial Services

Constant attacks target finance platforms, payment systems, or even mobile e-banking apps in order to extract enough information and credentials and then execute requests and operations that seem legitimate. Various vulnerabilities had been exploited in the past, such as update failure, fake calls mimicking trojans, software defects, etc. [14,30]. The main motives are the theft of either the money or data information of users, monitoring the financial activities of specific target clients, and tampering with the critical operations being executed.

3. Framework of Critical Infrastructures

In this section, various proposed frameworks and protocols of each type of CI will be presented, with each highlighting specific requirements that must be fulfilled for their proper functionality. Furthermore, the basic technologies and cryptographic primitives that support these frameworks, together with their architectures, are analyzed.

3.1. Frameworks for Different Critical Infrastructure Systems

The systems that are employed by Critical Infrastructures can be described by either the Health 4.0 or Industry 4.0 frameworks, depending on the structures' application. E-Health services have been employed in hospital environments and for near-patient applications, which assist disabled or elderly people with their everyday life from the comfort of their home. Health 4.0 is a new framework that analyzes the design and performance requirements for integrating new technologies into health services [2]. Furthermore, there are various application protocols that complement these requirements, such as Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP) and the Extensible Message and Presence Protocol (XMPP) [6]. Each has unique properties and capabilities while enabling smooth communication and data exchange between the components of the system. Overall, the developed systems must abide by the following design principles:

- Interoperability: the ability of heterogeneous devices to constantly communicate with each other via wired and wireless networks;
- Virtualization: the automation of healthcare processes by monitoring the environment;
- Decentralization: the ability of each employed component of the system to decide on their next operation based on the collected data;
- Real-time capability: the ability to quickly react to environmental changes and communicate it with the rest of the system's components;
- Service orientation: the categorization of the system's operations as services which are easily accessible to all related parties;
- Modularity: the scalability of the system that enables it to constantly adapt and adopt new requirements and technologies.

The security requirements are generally defined by the Health 4.0 framework and are followed by the application protocols. The main security requirements are availability, authorization, authentication, confidentiality, safety, privacy, integrity, and non-reputability. These requirements can be maintained by implementing appropriate cryptographic primitives to the employed devices of the framework. These cryptographic primitives include block ciphers, stream ciphers, hash functions, message authentication codes (MACs), and Authenticated Encryption Schemes [6]. Depending on the application and mainly on the available resources, one or multiple heavy or lightweight primitives can be utilized for security.

Nevertheless, even though security and privacy are thoroughly analyzed, their implementation is sometimes lacking. For example, the MQTT protocol does not provide security or implement any cryptographic primitives on its own. Instead, it must incorporate an additional security protocol, such as the Transport Layer Security (TLS) protocol, on top of its own layers. These security protocols consist of various mechanisms for authenticating the parties that communicate with each other, handling key and communication parameters and finally encrypting and safely transmitting the data. This is mainly achieved by utilizing appropriate cryptographic primitives, key scheduling and management schemes, network certificates, and hello functions. This computation and time addition can be critical, with some designers omitting this solution or being unable to implement appropriate approaches in a timely manner [13]. Therefore, as the healthcare domain integrates more technologies, such as the Internet of Things (IoT), Cyber-Physical Systems and Big Data Analytics, cybersecurity together with more suitable cryptographic mechanisms must be considered and become an interchangeable part of the systems.

Industry 4.0 provides guidance on CIs' advancements and a general framework that must be followed for the proper integration of digital technologies, automation, and data exchange. It is employed for all industrial and manufacturing processes and specifically for industrial control systems [3]. Moreover, the design principles of Industry 4.0 are the same as mentioned above. Health 4.0 simply adopted these principles from Industry 4.0 while adding specific application parameters [2]. Nevertheless, interoperability, virtualization, decentralization, real-time capability, service orientation, and modularity are once again the main principles that efficiently demonstrate the requirements of an industrial application. Industry 4.0 also employs the same types of technologies, such as the Internet of Things (IoT), Big Data Analysis, Cyber-Physical Systems, robotics, etc. Therefore, the same application protocols can be employed as with healthcare systems. Lastly, the security requirements and integration of cybersecurity is also discussed by the framework. The same requirements as with Health 4.0 must be fulfilled. The same cryptographic primitives and security protocols can be implemented to better achieve the mentioned requirements. Nevertheless, once again, their implementation is difficult with similar vulnerabilities being presented.

Overall, the enhancement of CIs is indisputable. Smart energy grid systems can improve the functionality and control of traditional power system networks by incorporating new technologies [15]. They enhance the efficiency, reliability, and sustainability of the electrical grid by enabling an intelligent two-way communication path. Oil and gas sys-

tems can maintain the control of operations in real time while enhancing the safety and environmental monitoring remotely [4]. Intelligent Transportation Systems (ITSs) consist of various vehicles and control mechanisms whose interconnection is enhanced via Industry 4.0 and its integrated technologies [5]. Finally, smart cities improve the quality of service for their citizens via the constant collection and analysis of data and the creation of new data-oriented functionalities [16]. Nevertheless, the security of all these systems must be approached with caution, as more threats and attacks, which can cause damage to national functionality and endanger human lives, are emerging.

3.2. Differences between Frameworks

The Industry 4.0 framework was the inspiration for the creation of the Health 4.0 framework. The integration of novel technologies, which was presented by Industry 4.0, was the required next step for enhancing healthcare structures and their services. Nevertheless, despite all their similarities, there is a slight difference between them to better ensure the fulfilment of the performance and security requirements of health systems. The only difference is that, in some cases, the devices that are employed by industry systems can have more resources available compared to healthcare applications. Therefore, more advanced technologies, together with more computationally complex security and cryptography mechanisms, can be employed by industrial control systems. In e-Health systems, this option is unsuitable due to the more lightweight approach of health services that require the system to be wearable with a long-lasting battery in order to allow the user to continue with their normal everyday life without any disruptions. Some Industry Control Systems may also present these types of resource-constraint difficulties, such as smart home applications, that cannot be necessarily included in the Health 4.0 framework. Therefore, in this study, instead of the blind adoption of a specific framework, their appropriate combination is presented with flexible solutions that can be changed depending on the application.

3.3. Architecture of Employed Technologies

3.3.1. SCADA Architecture

The proper functionality of CIs depends on various systems that support and implement their services. The basic system that is being employed for monitoring and controlling industrial processes and infrastructures is Supervisory Control and Data Acquisition (SCADA) [17]. It remotely collects data from sensors and equipment and transmits them to central control services. SCADA systems typically operate in protected and isolated environments with dedicated communication protocols and infrastructure. However, due to the integration of CIs and information technology /the internet, SCADA systems have been exposed to more threats and attacks, deeming their framework outdated [5]. New secure and safety-driven operational mechanisms are demanded.

A typical SCADA architecture consists of four layers [5,17]. In the bottom layer of the architecture, various field devices, such as sensors, actuators, motors, and robotics, are presented. These devices collect data from the environment and execute transmitted commands. They also closely communicate with the next layer, which contains the Remote Terminal Units (RTUs). The RTUs collect the field devices' data and transmit them to the next layer, namely the control center. They also send commands or control signals to the field devices. The control center contains the human-computer interface (HCI) and one or more distributed supervisory devices that support the HCI. The SCADA operators are then responsible for utilizing this center and interface to correspond to alerts and perform necessary control operations. The employed supervisory device is the Master Terminal Unit (MTU). MTUs constantly exchange data with all RTUs and further send the received data to the HCI. They then transmit back the appropriate commands and signals that were produced by the operators or by the last layer, namely the cloud services. This fourth layer consists of computing and storing services that store and perform analytics and processing operations with the collected data, which were received from the control center. The cloud

services can also communicate with other remote operators via the internet or possibly autonomously create commands to be executed by the other layers.

The SCADA architecture employs various networks and communication protocols based on the processing abilities of the components and the technical requirements which are mandatory to the application. A SCADA application can vary in its employment from a small factory to a big city; thus, communication can be achieved by combining different network structures, such as wired approaches, namely dedicated or power lines, Local Area Networks (LANs) and Wide Area Networks (WANs). The most popular protocols that facilitate the heterogeneity and scalability of the systems are Ethernet/IP, Modbus/TCP, IEC-60870, BITBUS, Distributed Network Protocol 3, etc.

3.3.2. IoT and CPS Architectures

Other systems that are employed for CIs are the Internet of Things (IoT) [21] and Cyber-Physical Systems (CPSs) [7]. According to Industry 4.0, various technologies and principles must be integrated with CIs. The IoT is one of these technologies that can fulfill many requirements and efficiently enhance systems. It is a network of interconnected devices, sensors, actuators, and systems that communicate by data sharing over various communication protocols and the internet [31]. Even though the IoT offers many capabilities, such as real-time function and scalability, it also consists of various vulnerabilities and threats [6]. This, in turn, exposes the CIs that depend on the IoT technology. Lastly, CPSs present a close connection to the IoT, as both concepts involve the integration of physical objects with the digital world [32]. The CPS emerged from a systems engineering and control perspective, while the IoT emerged from a networking and information technology perspective.

The IoT architecture presents distinct components that are similar to the SCADA architecture's components. The IoT architecture can also be divided to three main and one optional layer [31]. In the bottom layer of the IoT architecture, resource-constrained devices, sensors, and actuators that collect data from the environment are presented. These devices function as publishers, which receive requests to either transmit collected data or perform commands. The following layer, which communicates with the IoT devices, includes gateway devices that have more computation resources and function as brokers, handling routing services and enabling the resource-constrained devices to communicate with the external world securely and efficiently. The next layer contains edge/fog devices that strive to resolve the resource limitations of the IoT by allowing a part-processing of the large amount of data before being transmitted to the last layer, namely the cloud services. This results in the reduction of the network and response latency. In various applications, the gateway device also operates as an edge/fog computing device, thus making these two components interchangeable. This choice depends on the capabilities of the employed gateway device and the requirements of the application. Moreover, either the gateway or the edge/fog device can create commands for the resource-constrained devices by quickly analyzing specific points and data. Finally, the cloud services are responsible for storing and fully processing the received data, producing commands after high-resource-demanding computations and communicating with remote authorized users.

The IoT networks that are employed are once again either wired or wireless. There are two different kinds of wireless communication networks, similar to the SCADA architecture. The LANs can be employed for connecting the resource-constrained devices with the gateway devices and perhaps the gateway devices with the edge/fog computing devices. The WANs can be employed for connecting the middle components with the cloud services, as these devices have more computation and memory resources and can completely execute these more resource-demanding networks. Some exemplary communication protocols are IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), ZigBee[®]14, Wireless HART, etc.

Lastly, similarly to the SCADA and IoT architecture, the CPS architecture consists of a bottom layer, which contains the actuators and sensors, and a computing and control

center [33]. The bottom layer has more resource limitations compared to the control center that is responsible for handling the intercommunication and network management and controlling service execution. These two components also communicate with each other via the previously mentioned communication networks. As an extent of the CPS architecture, communication with cloud services is accomplished in order to better digitize the structures.

3.3.3. Unified Architecture

SCADA, the IoT, and CPSs are three distinct and yet interconnected technologies. They can function as a separate system, supporting and implementing CIs, or they can be integrated, creating new opportunities for flexibility, connectivity, and operational efficiency [34]. The comprehension of their architecture and functionality as distinct and unified entities is essential for proper vulnerability identification and classification.

Overall, these architectures can be combined with two different methods. First, the architectures can function as different systems that communicate with each other via cloud services, as was demonstrated in [35]. Second, the architectures can create a single generic architecture that better facilitates all CIs' requirements while also demonstrating scalability due to its ability to support both IoT, CPS, and SCADA technologies. This architecture is presented in Figure 1. It is divided into three main layers, namely the sensor layer, the control center, and the cloud services.

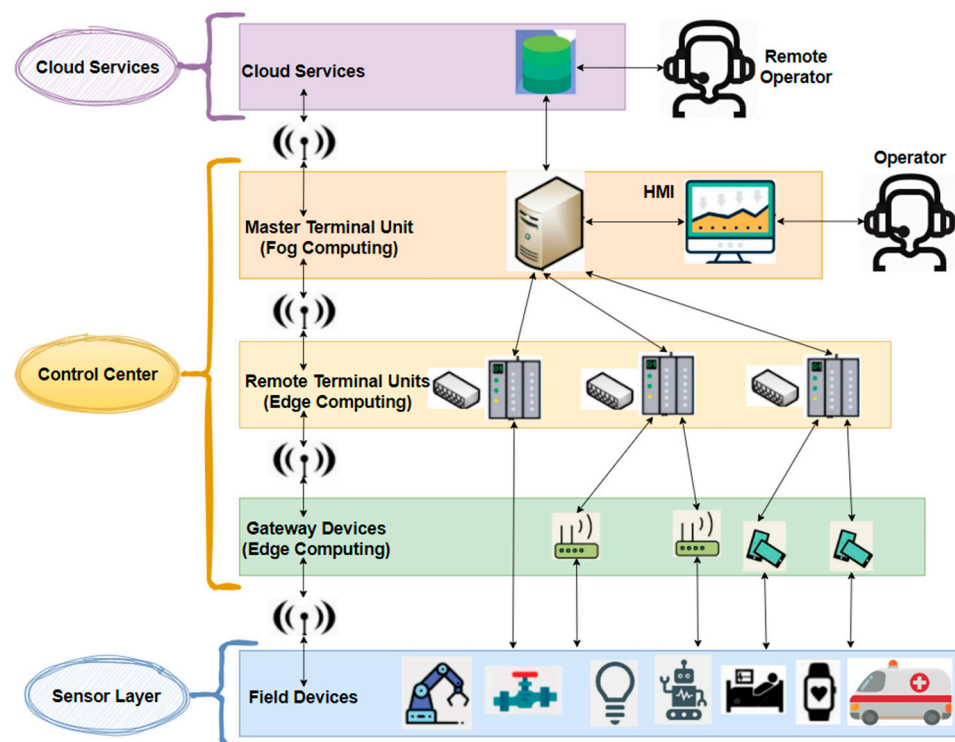


Figure 1. Unified architecture of a CI.

The sensor layer consists of the field devices and the resource-constrained IoT devices of the analyzed architectures' bottom layers. The control center is a combination of the two middle components and consists of the same devices, namely the gateway, edge/fog devices, RTUs, MTUs, and an HCI. It is responsible for handling the communication between the sensor layer, the users or operators, and the cloud services. It functions as a broker, handling routing and being able to employ both LANs and WANs. Each component of the control center implements one or multiple communication and network protocols from IoT or SCADA architectures, depending on the type of device from the sensor layer it communicates with. ZigBee, LoRaWAN, or 6LoWPAN protocols are employed for the communication with IoT resource-constrained devices [20]. Distributed Network Protocol

(DNP3), BITBUS, or Modbus protocols are employed for the interconnection of industrial and control devices [17]. The communication of the components inside this layer can be achieved by employing one of these protocols. Different types of communication protocols can be enabled by this layer as it has more computing and memory capabilities. These resources can also be utilized for edge/fog computing. Overall, the center control component contains an interconnected network of devices that directly communicate with the field devices, process part of the data, give simple commands, transmit all data to the cloud services for further processing, and, lastly, provide an interface for human–computer interaction. Finally, the cloud services layer remains unchanged. The method of communication with the control center is achieved via internet protocols or the already mentioned industrial and IoT protocols.

This unified architecture can be employed by different CI systems. Health systems can now provide remote communication and supervision of patients without extra consumption of human and hospital resources. Some services can be executed automatically due to the different layers of the control center that handle various cases by processing the transmitted data without the direct and constant supervision of the operators, in this case, doctors and hospital personnel. This configuration of the control center also ensures the real-time operation of the services, as middle devices exist between the cloud services, operators, and actuators, quickly responding and transmitting commands and alerting reports. Moreover, the accuracy of the diagnosis can be enhanced as timely records of data are appropriately stored and handled by various layers that can clear the noise and reduce the packet losses between transmissions. In a similar way, the industrial control systems are enhanced. More access capabilities are provided that enable the operators to control the systems from different end points: at the beginning with the gateway devices, which can be mobile phones; at the middle with the MTU and the HMI; and, finally, at the end via the cloud services. The procedures are controlled and supervised in real time with more data being measured via different methods and appropriate communication protocols. Therefore, the operators have a more detailed understanding of their system by clearly dividing the architecture into sections and responsibilities, with potential problems being easier and faster to discover and solve. These are all extremely beneficial to smart energy grid systems, ITs, oil and gas systems, etc., with their control being structured and appropriately handled with multiple layers and autonomous services as safety nets.

3.4. Cryptography in CIs

In this section, cryptographic mechanisms will be analysed with the purpose of better understanding their functionality and proper implementation for the security of the unified architecture. Specific cryptographic primitives regarding key generation and device authentication, namely Physical Unclonable Functions (PUFs) and random number generators, are also mentioned. Afterwards, two cryptography frameworks will be presented that display different methodologies, security levels, and implementation requirements. The selection of a framework depends on the demands of each CI.

3.4.1. Cryptographic Mechanisms

Cryptography is a fundamental piece in maintaining the security of CIs [2,17]. Specifically, cryptographic primitives satisfy many security requirements, with their proper implementation being the main solution for safe data transmission. Confidentiality and data protection, authentication and access control, key management and distribution schemes, and secure communication channels are some cryptographic mechanisms that must always be considered throughout the design of a CI that employs the previously mentioned technologies [36,37]. Based on these mechanisms and the CI's ability to implement them, two basic cryptography frameworks that are based on the designed unified architecture are presented.

The first two cryptographic mechanisms are the most basic and easier to implement even in the resource-limited layers of the architecture. Many lightweight cryptographic

primitives have been standardized for their proper application in the IoT or other resource-constrained technologies [22]. First, confidentiality and data protection are ensured via the application of encryption algorithms, such as block ciphers and stream ciphers, that encrypt the transmitted data and prevent unauthorized access. Thus, the communication between the layers of the architecture can be safely executed while preserving the privacy and mitigating malicious attacks that aim at alternating, injecting, or extracting sensitive information. Second, authentication and access control can also be executed via the application of proper cryptographic algorithms and modes of operation, such as MACs, Digital Certificates, Counter Mode (CTR), Galois Counter Mode (GCM), etc. These types of mechanisms complement block and stream ciphers by offering methods of authenticating data, verifying the identities of authorized parties, and ensuring the maintenance of integrity and authenticity.

The employment of key management and distribution schemes is more complicated and consumes additional resources. Key management and distribution schemes handle the generation, storage, distribution, and rotation of the keys that are employed for either symmetric or asymmetric encryption. This specific mechanism is heavily important for the proper performance of cryptographic algorithms, as the mismanagement of the encryption keys can lead to their extraction via malicious attacks or brute force. This, in turn, leads to the unauthorized decryption of sensitive information and the loss of data integrity and authenticity. Key management and distribution schemes can either be sufficiently implemented by the resources of the CI's architecture or they can be handled by third-party corporations that design and execute these schemes as an independent component that is separate from the other layers of the architecture. Nevertheless, in a CI, and especially in the defense or national security domain, third parties are difficult to be trusted with these important responsibilities.

The last mechanism refers to secure communication channels. Various protocols create a channel that allows the secure communication and transmission of data between nodes and endpoints. This mechanism requires more resources, as additional functions are needed to properly ensure the channel's security. Overall, the employment of TLS, Secure Shell (SSH), or other security protocols establish these channels and protect them from data-related attacks.

Depending on the system, different mechanisms are selected in various forms. For example, in a very resource-restricted e-Health environment, the first two mechanisms will take priority, as the employed primitives can have a compact architecture while providing enough security for data privacy and authentication. Key management schemes can be handled by more resource-available devices in the system or third parties. This results in a lightweight approach that unfortunately reduces the security, as not all end points of the system are independent. Access and authentication schemes must also be included in systems that have a huge network of heterogeneous devices constantly connecting and exchanging data, such as smart homes. All devices must implement them either via a compact or high-throughput design, depending on the resources available. The secure communication channel is very important in systems with a high possibility of losing crucial real-time information. In both e-Health and smart energy grid environments, which include more high-processing systems that communicate from a high distance, the existence of packet loss and the easy execution of malicious attacks against communication channels is inevitable. Finally, in oil and gas systems that are constantly targeted by attackers, a high-randomness and high-processing key management scheme must be implemented in order to completely secure the whole system from its foundation.

3.4.2. Physical Unclonable Functions (PUFs) and Random Number Generators (RNGs)

Physical Unclonable Functions (PUFs) are specific cryptographic primitives that utilize the unique physical properties that are inherent in electronic devices with the purpose of generating unpredictable values. Small differences in physical properties, such as temperature gradients, electrical characteristics, etc., are appropriately exploited and converted to

identifiers. Specifically, they produce at least one unclonable (ideally) or a hard-to-clone output given a selected input [38]. Thus, they can be employed for generating secure encryption keys and parameter bitstreams, creating unique physical signatures and tags for device authentication and circuit anti-counterfeiting. The uniqueness of these parameters is important, as both encryption keys and identifiers are an extreme weak point for cryptographic frameworks. If the encryption key is easily extracted or generated by brute force, all the encrypted packets can be revealed to the attackers. Similarly, if the unique tag that identifies the circuit of the architecture is easily generated, attacks such as reverse engineering can steal the product, grant access to vulnerable points of the system, and allow alterations to its hardware [39].

There are two basic types of PUFs as presented in [39]. The first type is the silicon PUFs that are engineered on the same dice as part of the circuit. The second type includes the non-silicon PUFs that are fabricated on the silicon system, thus requiring specific practices for assembling them. Moreover, depending on the number of challenges, available resources, and accessibility from the outside, different levels of security can be provided. Strong PUFs, which create the highest number of unique bitstreams, are mostly employed for device authentication properties. Contrariwise, weak PUFs are mainly utilized for secret key generation for cryptographic algorithms.

Other primitives that can generate random bitstreams are Random Number Generators (RNGs) [40,41]. There are two types of RNGs, namely the Pseudo Random Number Generators (PRNGs) and the True Random Number Generators (TRNGs). The first one does not depend on the physical characteristics of the device, but instead on mathematical equations and algorithms. The second one extracts the produced random bits from physical sources, such as electronic noise, health sensors, signals, etc. Overall, when RNGs are suitably implemented, they can be characterized by unpredictability, independence, and reproducibility, features greatly important for the creation of unique keys and communication parameters.

3.4.3. Cryptography Frameworks

Two cryptography frameworks can be applied to the unified architecture that was presented previously. These two are the most basic frameworks that allow for the proper application and execution of cryptographic primitives and mechanisms. Enhancements based on these two can be found or designed based on the more specific requirements of each CI application.

The first framework depends on basic security protocols, such as TLS, Datagram Transport Layer Security (DTLS), Secure Sockets Layer (SSL), etc., that consist of two security mechanisms that regulate the safety of the communication between two parties, namely the server and the client [37]. These two mechanisms are a handshake-based protocol and a record-layer-based protocol. A handshake protocol includes specific functions that enable the transmission of, first, HELLO messages; second, encryption and key parameters; and last, verification and authentication messages between the client and server. An example of a Key Exchange algorithm is the Elliptic Curve Diffie–Hellman Ephemeral (ECDHE), and an example of a Server Certificate Authentication Scheme is the Rivest–Shamir–Adleman (RSA). These methods create a secure communication channel with appropriate key management and distribution schemes. The data can be safely encrypted and then transmitted to the corresponding party without being susceptible to simple attacks.

The purpose of a record-layer protocol is simple and perfectly complements the handshake protocol. Specifically, it includes cryptographic algorithms that encrypt data with the utilization of an encryption key. This encryption key was previously generated by the key parameters that were transmitted via the handshake protocol. A variety of algorithms can be implemented for this protocol, such as AES, CHACHA20-POLY1305, ASCON, etc. Moreover, various modes of operation can be added to enhance the privacy and authentication of data. The most common one is the Authenticated Encryption with Associated Data (AEAD) mode of operation, such as GCM, Counter with Cipher Block Chaining Message Authentication Code (CCM), etc. Depending on the application's resources and require-

ments, specific implementations and algorithm designs can be inserted to the protocol to better facilitate these needs.

Cryptography architectures that are based on security protocols require many resources to implement and execute all these different cryptographic primitives, thus adding high computation overhead [36]. Furthermore, the performance flow of the handshake protocol adds high time overhead to the architecture that can be crucial for real-time-based operations. This problem is countered with the second cryptography framework that omits parts of the handshake protocol, only implementing or relying on a third party for a key management and distribution scheme. It also establishes an end-to-end encryption scheme by utilizing the record-layer protocol. Specifically, it does not encrypt parts of the data that are needed for routing, called metadata, with the purpose of enabling its proper transmission without all layers of the architecture needing to decrypt the whole message. Thus, when a message needs to be transmitted from the sensor layer to the cloud services layer, the middle layer, namely the control layer, is not required to know the encryption key or decrypt the message, because it needs to only read the routing data that are not encrypted. Overall, this method requires less computation and time overhead, but it comes with a trade-off regarding security and authentication that can be critical in a CI infrastructure. The implementation of appropriate cryptography frameworks is extremely challenging and equally important.

3.4.4. Cryptography of the Unified Architecture

Each layer of the presented unified architecture can be divided into three categories, namely publishers, brokers, and subscribers. The sensor layer that includes devices that collect data acts as the main publisher. The components of the control center act as brokers that handle data routing and the cloud services layer is the most frequent subscriber that request data. The control center can act as a subscriber too, depending on the specific operation that is executed. Overall, all of these categories must implement a cryptography framework to establish a secure method for transmitting data and commands.

Figures 2 and 3 demonstrate the two different cryptography frameworks and their general application in the unified architecture. For the first cryptography framework in Figure 2, all categories implement the required security protocols and can exchange parameters and encrypted data. Cloud services request data and communicate with the control center via a secure communication channel. Afterwards, the control center requests and then receives encrypted data from the sensor layer via a similar secure communication channel. The data are decrypted, processed if necessary, and then encrypted again. Finally, they are sent to the appropriate cloud service component that requested them. One of the components of the control center can request data from the sensor layer. In that case, the procedure is the same, with the in-between components of the control center functioning as a broker.

For the second cryptography framework in Figure 3, each category implements different mechanisms, because the required operations might not be the same. Furthermore, an additional component must be created, which is either independent from the employed devices or is integrated into them, for key generation, management, and distribution. For example, the sensor layer and the cloud services can implement only data encryption and decryption mechanisms, and perhaps some key generation schemes, as they only function as a publisher and a subscriber, respectively. Moreover, for each component of the control center that is not required to read the published and forwarded data and only functions as a broker, no encryption or decryption mechanisms are needed.

As was mentioned before, each framework has its own advantages and disadvantages. An appropriate choice must be made by CI designers to better satisfy the security requirements of their specific application. Nevertheless, all CI architectures must abide to the four mentioned cryptography mechanisms, namely confidentiality and data protection, authentication and access control, key management and distribution schemes, and secure communication channels, and implement them in various forms.

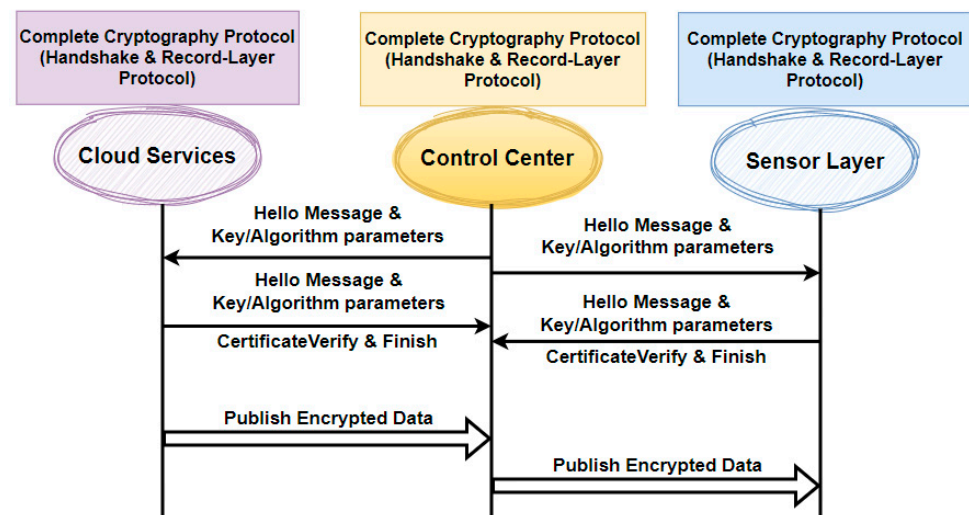


Figure 2. Cryptography framework of unified architecture based on security layer protocols.

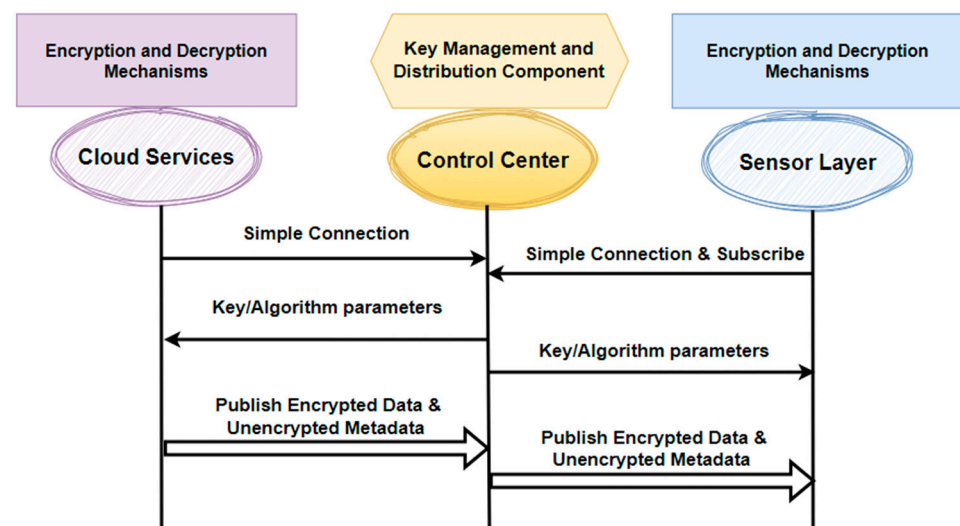


Figure 3. Cryptography framework of unified architecture based on end-to-end security.

4. Threat, Adversary, and Attack Models for Critical Infrastructures' Architecture

In this section, the threat model of the previously analyzed architecture, which employs the SCADA, IoT, and CPS technologies, will be presented. Afterwards, the adversary model, which identifies the characteristics, capabilities, and motivations of potential attackers, will be demonstrated. Finally, an attack model, which describes the types of attacks against CIs, will be created.

4.1. Threat Modeling

4.1.1. General Threat Modeling

The vulnerabilities can be categorized into five different levels, namely hardware, software, firmware, network, and process [4]. Hardware-level vulnerabilities refer to the device's state throughout its life cycle, namely from its creation in the supply chain until its destruction. The software and firmware levels focus on vulnerabilities in the application's code, data injection mechanisms, and update failures. Network-level vulnerabilities define the lack of proper communication protocols and network load handling. Finally, the process level contains the logical vulnerabilities of the design or programming processes that are utilized.

Each layer of the architecture, which is depicted in Figure 1, is susceptible to one or multiple of these vulnerabilities. All hardware components in all layers are, in a different form, susceptible to physical attacks, namely tampering of any kind and the alteration or destruction of the hardware that is employed. The devices that are utilized in the sensor layer can function remotely and unattended in questionable environments [42]. Therefore, an adversary that is close to the hardware can easily execute various physical attacks, causing damage, reverse-engineering, or adding malicious hardware, namely a trojan, to the infrastructure's equipment. The hardware that is employed by the rest of the layers can also be tampered with, even though they do not exist in extremely remote environments. Specifically, malicious hardware can be imbedded into the components' hardware during all stages of the supply chain [43]. This malware hardware can then be employed to orchestrate an attack on the system or leak sensitive data to the adversary. Finally, as most applications do not implement physical mitigation algorithms or even leave ports of the devices unnecessarily open and thus accessible to unauthorized parties, the adversary can once again easily control or corrupt the system and leak data [18].

Firmware- and software-level vulnerabilities are also present in all layers of the architecture. The sensor layer consists of resource-constrained devices, resulting in their inability to execute high-computing, demanding security algorithms to completely protect the system and each component from malicious attacks, such as malware and firmware injection, improper access control, etc. [18]. The control center, which consists of devices with higher processing capabilities, can be affected by more types of attacks, as they connect to more general communication protocols and with the cloud services and internet. Attacks targeting web applications or the HCI can be also performed. Moreover, all three layers can execute unpatched or not properly tested operating systems, leading to errors that can impact the process and performance flow, such as buffer overflow [4]. This can also extend to the employed security algorithms and authorization protocols.

The network level consists of all the communication protocols and remote access points that enable the components to exchange data with each other. The sensor layer devices cannot implement heavyweight security and network mechanisms due to their resource limitations. Thus, the data may be transmitted without prior encryption or access can be given without proper authentication [19]. This vulnerability is also present in many application and communication protocols that are employed by all layers, as they do not ensure the security of the communication channels or the addition of security and authentication protocols, such as TLS [4,36]. Nevertheless, even some functions of TLS are vulnerable. The zero round-trip time (0-RTT) in the TLS's handshake protocol contributes to faster transmission by starting the exchange of less sensitive data without awaiting additional confirmation regarding authentication. However, it is highly susceptible to replay attacks [37]. Therefore, in a critical infrastructure with most data being considered sensitive, this vulnerability can lead to data leaks or disruptions of service.

Other vulnerabilities at the network level stem from the unresolved challenges of the wireless networks that are utilized between the architecture's layers [4,20]. Various attacks have been successfully performed against IoT networks, such as ZigBee, Bluetooth Low Energy, 6LoWPAN, and LoRaWAN. Due to the heterogeneity and scalability of the networks, the routing, key management, authentication, and traffic-redireciting mechanisms cannot handle the excessive transmission load, either because there are not enough resources or not enough quick mitigation policies. They also can be easily fooled by malicious entities that legally join the network, either because of improper security/identification parameter management or a lack of strong authentication mechanisms. The other networks that are usually employed in SCADA architectures also have similar vulnerabilities. More importantly, as SCADA systems are traditionally isolated from the internet, their communication protocols do not implement any security measures against network attacks [17]. Thus, their integration with IoT networks that closely connect with internet services deem SCADA networks extremely vulnerable.

Finally, the process level consists of logic vulnerabilities, such as improper business logic validation testing and security training of CI employees [17]. In many applications, the user is allowed to insert invalidated data and thus causes software performance malfunctions. This vulnerability can even be extended to those employees of the systems who have not been trained to properly operate the functions. In the security domain, the user can be the most critical vulnerability of the architecture.

4.1.2. Threat Modeling in Cryptography Frameworks

Cryptographic primitives require an encryption key in order to properly encrypt and decrypt messages. This key distribution to all components of the CI's architecture must be executed in such a way that attackers cannot extract the key and decipher sensitive information. Therefore, direct transmission of this key to other components is not advised, as attackers can easily perform an eavesdrop attack and extract it. Asymmetric cryptography is the main solution to this problem. However, this mechanism requires many resources and a high execution time that can be prohibitive for resource-constrained architectures [36]. Moreover, most devices cannot afford to spare memory space to store encryption keys. The devices that are included in the sensor layer are also prone to probe attacks that can physically extract sensitive information regarding the encryption key.

Independently of the key management schemes, cryptographic primitives have various vulnerabilities of their own. The improper implementation of these primitives with bad trade-offs are constantly presented throughout the research community, resulting in weak security methods and endangerments to privacy [6]. Furthermore, in many cases, authentication methods are not integrated into encryption algorithms in order to achieve better hardware measurements. Finally, as the Quantum era is approaching, the complexity and computation requirements of security are rising, creating many challenges for the resource-constrained and network-complex CIs [22,23].

The protocols that depend on PUFs are vulnerable to PUF modeling attacks, for example, approximation attacks [39]. They are also limited in their performance impact because of the PUF-based embedded systems' temperature rises. RNGs also present various vulnerabilities. TRNGs are slow and require more hardware resources than PRNGs but provide more security and produce a higher number of random bitstreams than PRNGs [41]. PRNGs constantly require an unpredictable seed in order to maintain their randomness. Overall, all of these cryptographic primitives have great computation and communication costs that must be carefully approached for resource-constrained environments.

Finally, the existing security protocols present vulnerabilities in their security. For example, a particular mechanism of the TLS, namely the zero round-trip time (0-RTT), is susceptible to replay attacks [37]. An attacker can duplicate these 0-RTT data and initiate communication between two components. Additionally, in case of the end-to-end cryptography mechanism, the transmission of unencrypted metadata can reveal sensitive information regarding the reason of communication and create an opportunity for the attacker to disrupt the communication flow.

4.2. Adversary Modeling

Adversaries are individuals or groups of people that execute various attacks against CIs to accomplish various purposes [7]. Outsiders, which exist outside the CI's environment, and insiders, which are employed by the CIs, can attack the architecture while having various types of motives. Financial gain, political or military objectives, cyber-terrorism, hacktivism, or, in some cases, emotional satisfaction can be strong motives that drive criminals, script kiddies, industrial espionage actors, nation-state actors, etc. [5,7,13].

Depending on the resources, access, specificity, and knowledge of the adversary, different attack models must be consisted for mitigation policies [7]:

- **Resources:** Adversaries can be either driven by their own personal motivations, with little to no fundings and resources, or they can be funded by individuals, organizations, or even nations, thus having many access privileges and tools for more sophisticated

attacks. As cryptographic primitives heavily depend on the complexity of their employed mathematic computations and their key size, the resources that are available to the adversary can play a critical role in their ability to safely encrypt the data and protect the key from brute force-based attacks. When the adversary has high computation power available, key extraction and cryptographic vulnerabilities' exploitation is easier.

- **Access:** The possession of access to the system is also important to the adversary, as more types of attacks and more information can be gained by having physical access to targeted components. In the case of the described architecture of CIs, the sensor layer, which contains many resource-constrained devices, is isolated or far away from the center of the architecture. This results in being an easy target for physical attacks, such as side-channel and power analysis, microprobing, and memory flashing attacks. Moreover, some components of the control center can also execute their functionalities remotely without constant human supervision. This can also result in them being easy targets, especially in the case of insiders being adversaries. Nevertheless, even without physical access, network interfaces can also be targeted with replay or rollback attacks and grant accessibility to the system by proximity.
- **Specificity:** Attackers can maliciously intend for a specific output to be produced by the CI's control and monitoring system in order to reshape its functionality according to their own motivations. On the other hand, a specific output cannot be the target of the executed attack. Instead, the misguidance of the system to produce other kinds of outputs except the correct one can be the targeted result.
- **Knowledge:** An adversary can have complete or no knowledge of the system and its functionalities. The system model, parameters, and state vectors can be either already known to the attackers, because they are an insider or in contact with an insider, or because they steadily acquired access to this information by exploiting vulnerabilities of the system. The types of attacks that are executed with zero knowledge of the CI are called black-box attacks.

4.3. Attack Model

The overall target of an attack can be either the cyber or physical domain [7]. The information contained on the transmitted sensitive data together with their integrity, accuracy and non-repudiation can be targeted via the vulnerabilities of the communication protocols, networks, access control commands, and data storage. Moreover, performance, power, and hardware information of the physical devices can also be targeted via non-invasive attacks, such as power analysis attacks, timing attacks, electromagnetic emission attacks, etc.; semi-invasive attacks, such as fault injection, laser scanning, etc.; or invasive attacks, such as reverse engineering and hardware trojan attacks. This type of information is equally critical because security parameters can be extracted by analyzing and exploiting the device's specific patterns, such as power consumption [44]. Lastly, the corruption of the availability without obtaining any information can also be a target of the adversaries. This is achieved by Distributed Denial of Service (DDoS) attacks that disrupt the regular operation of the CI's network, service, website, etc., by flooding them with illegitimate traffic and network load or physically tampering with a device.

There are three main attack methods that aim at the architecture's vulnerabilities, as are depicted in Figure 4. Each attack focuses on a different architecture's layer. In the first type of attacks, the target is the sensor layer. Specifically, an IoT device can be physically approached by an attacker to install malware, tamper with its functionality, or destroy it. An adversary can also gain the trust of the IoT device by obtaining authorization and communicating with it remotely via a network. These result in the adversary disturbing the availability and functionality of the services and gaining access to the system, thus being able to execute their own operations and commands while obtaining the sensitive data transmitted to the devices. Moreover, the resource constraints of these devices can result in the implementation of weak cryptographic algorithms or the absence of important

cryptographic mechanisms [6]. Therefore, attacks that focus on the extraction of the encryption key, the decipher of encrypted data, or the enabling of unauthorized actions regarding these primitives can be easily executed against this layer.

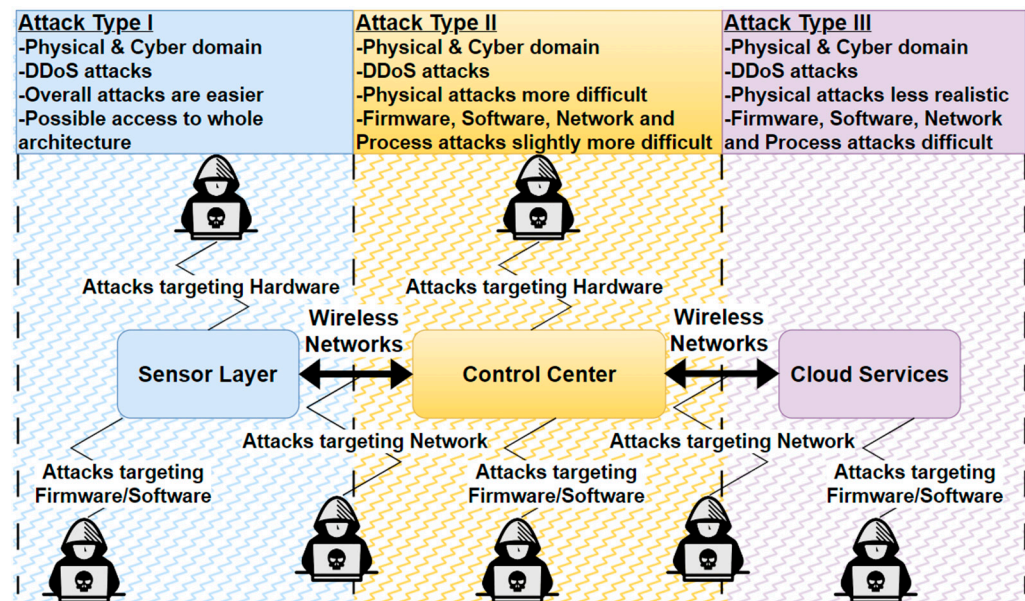


Figure 4. Types of attacks in the attack model.

The second type of attack focuses on the vulnerabilities of the control center. Once again, physical and cyber vulnerabilities can be exploited with the purpose of entering the main system and either causing disturbances in operation or manipulating data and software code. The execution of these attacks can be more difficult due to their physical inaccessibility and control center components' ability to perform slightly higher resource-demanding security and cryptographic mechanisms. Nevertheless, due to the scalability and constant technological evolution, new vulnerabilities are bound to be created and exploited.

The final type of attack exploits the SQL or authentication vulnerabilities of cloud services via the employed network. Physical attacks are nearly impossible in the case of outsider adversaries. Insiders can physically access the servers' rooms when safety mechanisms are not employed by the structure. Cloud services usually implement high-level security and cryptographic mechanisms, being most difficult to directly gain access to. Nevertheless, as presented in [5], the component that is targeted by the adversary can be different from the actual target. Specifically, the IoT devices that implement weak or no security and cryptographic mechanisms are directly connected with the control center and indirectly with the cloud services, which can be the actual targets. Therefore, obvious or hidden attack paths are created, deeming the sensor layer a very attractive target for fulfilling various purposes.

5. Security and Mitigation Solutions

In this section, security and mitigation solutions will be presented. First, general security solutions will be analysed, and afterwards, cryptography specific solutions will be demonstrated.

5.1. General Security Solutions

Many security solutions have been proposed by the research community with the purpose of ensuring security in the targeted systems. The secure data exchange between systems that enable the interoperability of healthcare services is presented in [45]. Vehicle authentication and secure communication between vehicles and healthcare enterprises

is ensured in [46] via a zero-knowledge proof and statistical fingerprinting. In [47], a cybersecurity method for enhancing Modbus/TCP-based industrial automation and control systems is presented. It employs message authentication codes (MACs) as an underlining security mechanism without impacting the communication performance. Reference [48] proposes a memory attack detection mechanism with a response framework with the purpose of being practical without specific hardware or unrealistic defense assumptions. In [49], defensive mechanisms for monitoring and mitigating critical IP-centric issues are implemented. It focuses on SoC designs and provides solutions for hardware-based attacks. These are some examples of the security mechanisms and methodologies that were approached by researchers regarding specific components and systems in CIs.

Other papers from the scientific literature aim at providing a more thorough guidance in securing CIs and specifically mitigating cyberattacks. A new vulnerability mitigation framework through an empirical paradigm is proposed in [50]. A computation system which ranks, weights, and prioritizes the criteria is developed with the purpose of providing detailed cybersecurity analysis and mitigation plans. In [51], an impact assessment of cyberattacks that is based on a hierarchical flow model is presented. The proposed approach models the CI while considering its characteristics, cyber-physical interactions, and the topological structure of its network and components. It receives as input the cybersecurity evidence that is provided by an intrusion detection system and produces the loss value of the cyberattack impact. In [52], a modelling approach that presents a risk dependency and calculation methodology is developed. Based on the CI's production chain topology, a framework that depicts a threat's probability regarding unwanted disruptions assists the designer experts during the designing stages of a CI. Lastly, ref. [53] proposes a combinational framework that assesses the system's resilience during its operational stage by using real-time data and chaos engineering.

Other proposed frameworks focus on the training and assistance of the employees of the CIs to better understand and make appropriate mitigation decisions in case of cyberattacks. In [54], a gamification-based cybersecurity training tool for critical facilities is developed. It is modeled based on real-world industrial control system cyberattacks and adapts to the player's decisions in order to facilitate formative learning. In [55], the Multicriteria Decision Aid Constructivist (MCDA-C) method was employed for enabling easier decision making and facilitating the information security manager's work for mitigating cyber risks. This is achieved by modeling the CI structure and collecting data for criteria analysis. An alert prioritization-based framework, which includes various methods in a mixed approach, was designed in [56]. The focus of this work is the assistance of the network supervisor with an alert assortment that improves and prioritizes thousands of alerts of potential security risks and intrusion attacks. This is achieved by collecting a vast amount of data from the whole system, visualizing latent spaces, and identifying anomalies based on automatic encoders. Finally, a Stackelberg solution can be utilized by the infrastructure administrator to strategically allocate the available resources by modeling the interactions between the attacker and defender in [57].

5.2. Solutions in Cryptography

Various papers propose the development of a communication and authentication protocol that provides fast data transfer between the components of IoT-based architectures. The purpose is a reduction in the computation and especially time overhead with better authentication policies. Ref. [36] proposes a hierarchical identity-based encryption (HIBE) for MQTT-based applications with the aim of reducing the time complexity of common security protocols, such as TLS. Ref. [58] proposes a key management scheme that is based on both the Elliptic Curve Cryptography (ECC) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and provides a lightweight solution to cryptography mechanisms. Likewise, ref. [59] designs a CP-ABE-based access control model with encryption and decryption techniques for less computation and time overhead. In [60,61], end-to-end

communication schemes are developed to better facilitate the requirements and resource constraints of IoT networks.

Other papers develop different approaches in implementing security layer protocols. Ref. [37] implements a lightweight version of the TLS protocol that introduces the ephemeral secret ticket mechanism. In [62], a compact cryptography and security parameter exchange mechanism is proposed, while being compatible with the DTLS handshake protocol. Lastly, a Domain Name System-over-TLS (PDOT) architecture is implemented with the purpose of addressing the challenges of DNS traffic.

Solutions are also presented for the proper implementation of PUFs. Specifically, ref. [38] presents a PUF architecture that is based on the NAND SR-latch and achieves minimal resource consumption without undermining the performance. In [63], an extensive analysis regarding two single-slice-based bit cells on an FPGA device is performed with the vulnerabilities as well as the advantages of each presented. Lastly, ref. [64] demonstrates an area-efficient design approach of latch-based PUFs.

Finally, there is a variety of papers that introduce new architectures and implementations of cryptographic mechanisms, only focusing on a specific primitive and its improvement or a combination of two primitives together. Many papers propose efficient random number generators that can be employed for key and parameter generation [40,65]. For TRNGs, various papers present different architectures that aim at balancing resource consumption and high performance, creating appropriate trade-offs and exploiting mechanisms such as edge sampling, entropy sources in programmable logic, etc. [41,66,67]. Other published research papers develop a unified architecture of PUFs and TRNGs with the purpose of enhancing the compactness, scalability, flexibility, and reconfigurability of the system while increasing the security and privacy [68,69]. Lightweight or accelerated versions of block ciphers and stream ciphers are also developed for more efficient encryption/decryption of data and authentication policies [70–73]. Lastly, a novel authentication scheme has been developed by the research community, named Privacy-Preserving Mutual Authentication (PPMA). This scheme enhances the security of the employed systems by utilizing appropriate cryptographic mechanisms, such as PUFs, ID-based signature schemes, and self-generated pseudonyms. Two important examples are presented in [74,75], each being applied to an Internet of Drones environment and a Vehicular ad hoc network, respectively.

6. Conclusions

Critical Infrastructures (CIs) contain services and operations that are essential for national safety, humans' well-being, the economy, and overall daily-life functionality. Therefore, their security is of the utmost importance. However, as CIs' demands are constantly increasing, these traditional infrastructures are being integrated with novel technologies, such as the IoT, CPSs, etc. The main control mechanism of CIs, namely SCADA, is also being inserted into an interconnected world where everything communicates over networks and the internet. Even though this integration enhances the capabilities of the infrastructures, it also forces them into a hostile environment without the time and necessary tools to adapt. This leads to various CIs' vulnerabilities being exploited by attackers in recent years and sometimes causing irreversible damage [4].

This study aimed to analyze the framework and vulnerabilities of these infrastructures with the purpose of assisting researchers and designers in comprehending the threats, adversaries, and possible security and mitigation approaches. This is achieved by providing the following tools of knowledge to the CI designers. First, recent incidents against common CIs are presented while analyzing their motives, consequences, and attack methods. Afterwards, promising frameworks of CIs are investigated, namely Industry 4.0 and Health 4.0, to highlight the necessary requirements and suggested technologies for the smooth transition of traditional structures to the digital world. The architectures of commonly employed technologies, together with cryptographic mechanisms, are introduced, and a unified architecture, which better facilitates this transition, is being developed. The

utilization of this unified architecture and its cryptography frameworks can function as a tool for CI designers to quickly categorize the components of the system they develop and better understand its communication, security mechanisms, performance flow, and interdependencies. Moreover, a threat model, which identifies the vulnerabilities and threats of the architecture, an adversary model, which analyzes the characteristics of attackers, and an attack model, which presents the methods of attack against the architecture, are demonstrated. These models present another important tool that is necessary for CI designers regarding the implementation of security and privacy. Specifically, before the implementation of a CI, CI designers can consult these models and better understand the type of security challenges and particular threats and attacks that await them. Consequently, the developed CIs are more prepared while being ready to face various threat scenarios. Lastly, exemplary security, cryptography, and mitigation solutions that were recently proposed by the scientific community are mentioned. These examples are welcomed to be followed by CI designers to secure their systems in advance. Overall, this paper thoroughly discusses the whole structure and technologies of CIs, contrariwise to other published related works, presented in [4,5,7,12–20], that focus on a single component or analyze separately the implemented technologies. It also satisfies the European Union demands regarding CIs and their security by providing targeted knowledge and proper models as tools [8].

Author Contributions: K.T. and N.S. contributed to the research, investigation, results analysis, resources, and writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: The research work was supported by the Hellenic Foundation for Research and Innovation (HFRI) under the 4th Call for HFRI PhD Fellowships (Fellowship Number: 11093, “Cryptographic and Security Mechanisms, Applied in Healthcare Technology”).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All reported data are included in the manuscript.

Acknowledgments: The authors would like to express their sincere appreciation to the Hellenic Foundation for Research and Innovation (HFRI) for their support.

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

References

1. Alcaraz, C.; Zeadally, S. Critical infrastructure protection: Requirements and challenges for the 21st century. *Int. J. Crit. Infrastruct. Prot.* **2015**, *8*, 53–66. [CrossRef]
2. Al-Jaroodi, J.; Mohamed, N.; Abukhousa, E. Health 4.0: On the Way to Realizing the Healthcare of the Future. *IEEE Access* **2020**, *8*, 211189–211210. [CrossRef] [PubMed]
3. Rikalovic, A.; Suzic, N.; Bajic, B.; Piuri, V. Industry 4.0 Implementation Challenges and Opportunities: A Technological Perspective. *IEEE Syst. J.* **2022**, *16*, 2797–2810. [CrossRef]
4. Stergiopoulos, G.; Gritzalis, D.A.; Limnaios, E. Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns. *IEEE Access* **2020**, *8*, 128440–128475.
5. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3453–3495. [CrossRef]
6. Tsantikidou, K.; Sklavos, N. Hardware Limitations of Lightweight Cryptographic Designs for IoT in Healthcare. *Cryptography* **2022**, *6*, 45. [CrossRef]
7. Zografopoulos, I.; Ospina, J.; Liu, X.; Konstantinou, C. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. *IEEE Access* **2021**, *9*, 29775–29818. [CrossRef]
8. European Commission. *Communication from the Commission on a European Programme for Critical Infrastructure Protection*, COM(2006) 786 Final; European Commission: Brussels, Belgium, 2006.
9. International Society of Automation, ISA/IEC 62443 Series of Standards. Available online: <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards> (accessed on 19 February 2024).
10. Stouffer, K.; Pease, M.; Tang, C.; Zimmerman, T.; Pillitteri, V.; Lightman, S.; Hahn, A.; Saravia, S.; Sherule, A.; Thompson, M. *NIST Special Publication: NIST SP 800-82r3 Guide to Operational Technology (OT) Security*; NIST: Gaithersburg, MD, USA, 2023.

11. Knapp, E.D.; Langill, J.T. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, 2nd ed.; Syngress: St. Rockland, MA, USA, 2015.
12. Staddon, E.; Loscri, V.; Mitton, N. Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey. *Appl. Sci.* **2021**, *11*, 7228. [\[CrossRef\]](#)
13. Makrakis, G.M.; Kolias, C.; Kambourakis, G.; Rieger, C.; Benjamin, J. Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents. *IEEE Access* **2021**, *9*, 165295–165325. [\[CrossRef\]](#)
14. Lehto, M. Cyber-Attacks Against Critical Infrastructure. In *Cyber Security. Computational Methods in Applied Sciences*; Springer: Cham, Switzerland, 2022; p. 56.
15. Abir, S.M.A.A.; Anwar, A.; Choi, J.; Kayes, A.S.M. IoT-Enabled Smart Energy Grid: Applications and Challenges. *IEEE Access* **2021**, *9*, 50961–50981. [\[CrossRef\]](#)
16. Rahouti, M.; Xiong, K.; Xin, Y. Secure Software-Defined Networking Communication Systems for Smart Cities: Current Status, Challenges, and Trends. *IEEE Access* **2021**, *9*, 12083–12113. [\[CrossRef\]](#)
17. Pliatsios, D.; Sarigiannidis, P.; Lagkas, T.; Sarigiannidis, A.G. A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1942–1976. [\[CrossRef\]](#)
18. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2702–2733. [\[CrossRef\]](#)
19. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of Threats to the Internet of Things. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1636–1675. [\[CrossRef\]](#)
20. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet Things J.* **2019**, *6*, 8182–8201. [\[CrossRef\]](#)
21. Khurshid, A.; Alsaaidi, R.; Aslam, M.; Raza, S. EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme. *IEEE Access* **2022**, *10*, 129932–129948. [\[CrossRef\]](#)
22. McKay, K.A.; Bassham, L.; Turan, M.S.; Mouha, N. *NISTIR 8114. Report on Lightweight Cryptography*; NIST: Gaithersburg, MD, USA, 2017.
23. Chen, L.; Jordan, S.; Liu, Y.; Moody, D.; Peralta, R.; Perlner, R.; Smith-Tone, D. *NISTIR 8105. Report on Post-Quantum Cryptography*; NIST: Gaithersburg, MD, USA, 2016.
24. European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2023*; ENISA: Athens, Greece, 2023.
25. Medtronic Recalls MiniMed Insulin Pumps as FDA Warns about Hacking Risk. CNN. Available online: <https://edition.cnn.com/2019/06/27/health/medtronic-insulin-pump-recall-cybersecurity-fda-bn/index.html>. (accessed on 4 December 2023).
26. Sethuraman, S.C.; Vijayakumar, V.; Walczak, S. Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles. *J. Med. Syst.* **2020**, *44*, 29. [\[CrossRef\]](#)
27. Sterle, L.; Bhunia, S. On SolarWinds Orion Platform Security Breach. In Proceedings of the 2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI), Atlanta, GA, USA, 18–21 October 2021.
28. Rajkumar, V.S.; Ştefanov, A.; Presekal, A.; Palensky, P.; Torres, J.L.R. Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures. *IEEE Access* **2023**, *11*, 103154–103176. [\[CrossRef\]](#)
29. Understanding Cyber Threats in Transport. European Union Agency for Cybersecurity (ENISA). Available online: <https://www.enisa.europa.eu/news/understanding-cyber-threats-in-transport>. (accessed on 4 December 2023).
30. Timeline of Cyber Incidents Involving Financial Institutions. Carnegie. Available online: <https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline>. (accessed on 4 December 2023).
31. Hu, F. *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations*; CRC Press: Boca Raton, FL, USA, 2016.
32. Greer, C.; Burns, M.; Wollman, D.; Griffor, E. *Cyber-Physical Systems and Internet of Things, Special Publication (NIST SP)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019.
33. Duo, W.; Zhou, M.; Abusorrah, A. A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 784–800. [\[CrossRef\]](#)
34. Falco, G.; Caldera, C.; Shrobe, H. IIoT Cybersecurity Risk Modeling for SCADA Systems. *IEEE Internet Things J.* **2018**, *5*, 4486–4495. [\[CrossRef\]](#)
35. Alanazi, M.; Mahmood, A.; Chowdhury, M.J.M. SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Comput. Secur.* **2023**, *125*, 103028. [\[CrossRef\]](#)
36. Fan, C.; Shie, C.; Tseng, Y.; Huang, H. An Efficient Data Protection Scheme Based on Hierarchical ID-Based Encryption for MQTT. *ACM Trans. Sens. Netw.* **2023**, *19*, 61. [\[CrossRef\]](#)
37. Li, P.; Su, J.; Wang, X. iTLS: Lightweight Transport-Layer Security Protocol for IoT With Minimal Latency and Perfect Forward Secrecy. *IEEE Internet Things J.* **2020**, *7*, 6828–6841. [\[CrossRef\]](#)
38. Della Sala, R.; Scotti, G. A Novel FPGA Implementation of the NAND-PUF with Minimal Resource Usage and High Reliability. *Cryptography* **2023**, *7*, 18. [\[CrossRef\]](#)
39. Mall, P.; Amin, R.; Das, A.K.; Leung, M.T.; Choo, K.-K.R. PUF-Based Authentication and Key Agreement Protocols for IoT, WSNs, and Smart Grids: A Comprehensive Survey. *IEEE Internet Things J.* **2022**, *9*, 8205–8228. [\[CrossRef\]](#)

40. Garcia-Bosque, M.; Pérez-Res, A.; Sánchez-Azqueta, C.; Aldea, C.; Celma, S. Chaos-Based Bitwise Dynamical Pseudorandom Number Generator On FPGA. *IEEE Trans. Instrum. Meas.* **2019**, *68*, 291–293. [\[CrossRef\]](#)
41. Della Sala, R.; Bellizia, D.; Scotti, G. A Novel Ultra-Compact FPGA-Compatible TRNG Architecture Exploiting Latched Ring Oscillators. *IEEE Trans. Circuits Syst. II Express Briefs* **2022**, *69*, 1672–1676. [\[CrossRef\]](#)
42. Zhou, W.; Cao, C.; Huo, D.; Cheng, K.; Zhang, L.; Guan, L.; Liu, T.; Jia, Y.; Zheng, Y.; Zhang, Y.; et al. Reviewing IoT Security via Logic Bugs in IoT Platforms and Systems. *IEEE Internet Things J.* **2021**, *8*, 11621–11639. [\[CrossRef\]](#)
43. Arafat, M.T.; Stanley, A.; Sharma, P. Hardware-based anti-counterfeiting techniques for safeguarding supply chain integrity. In Proceedings of the 2017 IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, USA, 28–31 May 2017.
44. Utyamishv, D.; Partin-Vaisband, I. Real-Time Detection of Power Analysis Attacks by Machine Learning of Power Supply Variations On-Chip. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **2020**, *39*, 45–55. [\[CrossRef\]](#)
45. Liu, Y.; Shan, G.; Liu, Y.; Alghamdi, A.; Alam, I.; Biswas, S. Blockchain Bridges Critical National Infrastructures: E-Healthcare Data Migration Perspective. *IEEE Access* **2022**, *10*, 28509–28519. [\[CrossRef\]](#)
46. Chaudhry, J.A.; Saleem, K.; Alazab, M.; Zeeshan, H.M.A.; Al-Muhtadi, J.; Rodrigues, J.J.P.C. Data Security Through Zero-Knowledge Proof and Statistical Fingerprinting in Vehicle-to-Healthcare Everything (V2HX) Communications. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3869–3879. [\[CrossRef\]](#)
47. Katulić, F.; Sumina, D.; Groš, S.; Erceg, I. Protecting Modbus/TCP-Based Industrial Automation and Control Systems Using Message Authentication Codes. *IEEE Access* **2023**, *11*, 47007–47023. [\[CrossRef\]](#)
48. Geng, Y.; Chen, Y.; Ma, R.; Wei, Q.; Pan, J.; Wang, J.; Cheng, P.; Wang, Q. Defending Cyber-Physical Systems Through Reverse-Engineering-Based Memory Sanity Check. *IEEE Internet Things J.* **2023**, *10*, 8331–8347. [\[CrossRef\]](#)
49. Tan, B.; Elnaggar, R.; Fung, J.M.; Karri, R.; Chakrabarty, K. Toward Hardware-Based IP Vulnerability Detection and Post-Deployment Patching in Systems-on-Chip. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **2021**, *40*, 1158–1171. [\[CrossRef\]](#)
50. Gouriseti, S.N.G.; Mylrea, M.; Patangia, H. Cybersecurity Vulnerability Mitigation Framework Through Empirical Paradigm (CyFER): Prioritized Gap Analysis. *IEEE Syst. J.* **2020**, *14*, 1897–1908. [\[CrossRef\]](#)
51. Zhu, Q.; Qin, Y.; Zhou, C.; Fei, L. Hierarchical Flow Model-Based Impact Assessment of Cyberattacks for Critical Infrastructures. *IEEE Syst. J.* **2019**, *13*, 3944–3955. [\[CrossRef\]](#)
52. Dedousis, P.; Stergiopoulos, G.; Arampatzis, G.; Gritzalis, D. A Security-Aware Framework for Designing Industrial Engineering Processes. *IEEE Access* **2021**, *9*, 163065–163085. [\[CrossRef\]](#)
53. Dedousis, P.; Stergiopoulos, G.; Arampatzis, G.; Gritzalis, D. Enhancing Operational Resilience of Critical Infrastructure Processes Through Chaos Engineering. *IEEE Access* **2023**, *11*, 106172–106189. [\[CrossRef\]](#)
54. Ashley, T.D.; Kwon, R.; Gouriseti, S.N.G.; Katsis, C.; Bonebrake, C.A.; Boyd, P.A. Gamification of Cybersecurity for Workforce Development in Critical Infrastructure. *IEEE Access* **2022**, *10*, 112487–112501. [\[CrossRef\]](#)
55. Moreira, F.R.; Da Silva Filho, D.A.; Nze, G.D.A.; de Sousa Júnior, R.T.; Nunes, R.R. Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology. *IEEE Access* **2021**, *9*, 129605–129618. [\[CrossRef\]](#)
56. Feijoo-Martínez, J.R.; Guerrero-Curieses, A.; Gimeno-Blanes, F.; Castro-Fernández, M.; Rojo-Álvarez, J.L. Cybersecurity Alert Prioritization in a Critical High Power Grid With Latent Spaces. *IEEE Access* **2023**, *11*, 23754–23770. [\[CrossRef\]](#)
57. Ferdowsi, A.; Eldosouky, A.; Saad, W. Interdependence-Aware Game-Theoretic Framework for Secure Intelligent Transportation Systems. *IEEE Internet Things J.* **2021**, *8*, 16395–16405. [\[CrossRef\]](#)
58. Sowjanya, K.; Dasgupta, M.; Ray, S. A lightweight key management scheme for key-escrow-free ECC-based CP-ABE for IoT healthcare systems. *J. Syst. Archit.* **2021**, *117*, 102108. [\[CrossRef\]](#)
59. Das, S.; Namasudra, S. Multiauthority CP-ABE-based Access Control Model for IoT-enabled Healthcare Infrastructure. *IEEE Trans. Ind. Inform.* **2023**, *19*, 821–829. [\[CrossRef\]](#)
60. Ar-Reyouchi, E.M.; Ghomid, K.; Ar-Reyouchi, D.; Rattal, S.; Yahiaoui, R.; Elmazria, O. Protocol Wireless Medical Sensor Networks in IoT for the Efficiency of Healthcare. *IEEE Internet Things J.* **2022**, *9*, 10693–10704. [\[CrossRef\]](#)
61. Hamad, M.; Finkenzeller, A.; Liu, H.; Lauinger, J.; Prevelakis, V.; Steinhorst, S. SEEMQTT: Secure End-to-End MQTT-Based Communication for Mobile IoT Systems Using Secret Sharing and Trust Delegation. *IEEE Internet Things J.* **2023**, *10*, 3384–3406. [\[CrossRef\]](#)
62. Pérez, S.; Hernández-Ramos, J.L.; Raza, S.; Skarmeta, A. Application Layer Key Establishment for End-to-End Security in IoT. *IEEE Internet Things J.* **2020**, *7*, 2117–2128. [\[CrossRef\]](#)
63. Gu, C.; Chang, C.H.; Liu, W.; Hanley, N.; Miskelly, J.; O'Neill, M. A large-scale comprehensive evaluation of single-slice ring oscillator and PicoPUF bit cells on 28-nm Xilinx FPGAs. *J. Cryptogr. Eng.* **2021**, *11*, 227–238. [\[CrossRef\]](#)
64. Habib, B.; Kaps, J.P.; Gaj, K. Efficient SR-Latch PUF. Applied Reconfigurable Computing, ARC 2015. In *Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2015; pp. 205–216.
65. Madani, M.; Tanougast, C. FPGA Implementation of an Enhanced Chaotic-KASUMI Block Cipher. *Microprocess. Microsyst.* **2021**, *80*, 103644. [\[CrossRef\]](#)
66. Yang, B.; Rožic, V.; Grujic, M.; Mentens, N.; Verbauwhe, I. ES-TRNG: A high-throughput, low-area true random number generator based on edge sampling. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2018**, *3*, 267–292. [\[CrossRef\]](#)
67. Addabbo, T.; Fort, A.; Moretti, R.; Mugnaini, M.; Takaloo, H.; Vignoli, V. A New Class of Digital Circuits for the Design of Entropy Sources in Programmable Logic. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2020**, *67*, 2419–2430. [\[CrossRef\]](#)

68. Baturone, I.; Román, R.; Corbacho, Á. A unified multibit PUF and TRNG based on ring oscillators for secure IoT devices. *IEEE Internet Things J.* **2023**, *10*, 6182–6192. [[CrossRef](#)]
69. Wang, Y.; Liang, H.; Wang, Y.; Yao, L.; Yi, M.; Huang, Z.; Lu, Y. A reconfigurable PUF structure with dual working modes based on entropy separation model. *Microelectron. J.* **2022**, *124*, 105445. [[CrossRef](#)]
70. Tsantikidou, K.; Boufeas, D.; Sklavos, N. Area-Delay Efficient Security Scheme for Smart Hospital Systems. In Proceedings of the 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 31 July–2 August 2023.
71. Tsantikidou, K.; Sklavos, N. Minimal Resource Required E-Health System with End-to-End Authenticated Encryption Mechanism. In Proceedings of the 2023 12th International Conference on Modern Circuits and Systems Technologies (MOCASST), Athens, Greece, 28–30 June 2023.
72. Yang, G.; Shi, Z.; Chen, C.; Xiong, H.; Li, F.; Hu, H.; Wan, Z. Hardware Optimizations of Fruit-80 Stream Cipher: Smaller than Grain. *ACM Trans. Reconfigurable Technol. Syst.* **2023**, *16*, 22. [[CrossRef](#)]
73. Bahadori, M.; Järvinen, K.; Niemi, V. FPGA Implementations of 256-Bit SNOW Stream Ciphers for Postquantum Mobile Security. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2021**, *29*, 1943–1954. [[CrossRef](#)]
74. Pu, C.; Wall, A.; Choo, K.-K.R.; Ahmed, I.; Lim, S. A Lightweight and Privacy-Preserving Mutual Authentication and Key Agreement Protocol for Internet of Drones Environment. *IEEE Internet Things J.* **2022**, *9*, 9918–9933. [[CrossRef](#)]
75. Sun, C.; Liu, J.; Xu, X.; Ma, J. A Privacy-Preserving Mutual Authentication Resisting DoS Attacks in VANETs. *IEEE Access* **2017**, *5*, 24012–24022. [[CrossRef](#)]

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