Journal of
*Sensor and
Actuator Networks*

MDPI

Article

Cyber–Physical Systems Forensics: Today and Tomorrow

Nader Mohamed [1,*], Jameela Al-Jaroodi [2] and Imad Jawhar [3]

[1] Department of Computer Science, Information Systems, and Engineering, California University of Pennsylvania, California, PA 15419, USA
[2] Department of Engineering, Robert Morris University, Moon Township, PA 15108, USA; aljaroodi@rmu.edu
[3] Faculty of Engineering, Al Maaref University, Beirut 1600, Lebanon; ihjawhar@gmail.com
[*] Correspondence: mohamed@calu.edu

Received: 7 July 2020; Accepted: 31 July 2020; Published: 5 August 2020

check for updates

Abstract: Cyber–Physical Systems (CPS) connect the physical world (systems, environments, and humans) with the cyber world (software, data, etc.) to intelligently enhance the operational environment they serve. CPS are distributed software and hardware components embedded in the physical world and possibly attached to humans. They offer smart features, such as enhancing and optimizing the reliability, quality, safety, health, security, efficiency, operational costs, sustainability, and maintainability of physical systems. CPS are also very vulnerable to security attacks and criminal activities. In addition, they are very complex and have a direct impact on their environment. Therefore, it is hard to detect and investigate security attacks, while such attacks may have a catastrophic impact on the physical world. As a result, CPS must incorporate security measures in addition to suitable and effective forensics capabilities. When the security measures fail and an attack occurs, it becomes imperative to perform thorough forensics analysis. Adding effective forensics tools and capabilities will support the investigations of incidents. This paper defines the field of CPS forensics and its dimensions: Technical, Organizational, and Legal. Then, it reviews examples of current research efforts in the field and the types of tools and methods they propose for CPS forensics. In addition, it discusses the issues and challenges in the field that need to be addressed by researchers and developers of CPS. The paper then uses the review outcomes to discuss future research directions to address challenges and create a more effective, efficient, and safe forensics tools and for CPS. This discussion aims to create a starting point for researchers where they can identify the gaps and challenges and create suitable solutions through their research in CPS forensics.

Keywords: cyber-physical systems; CPS; digital forensics; network forensics; cyber-physical systems forensics; data-driven forensics; forensics-by-design

1. Introduction

Cyber–physical Systems (CPS) provide useful integration and interactions between the physical and the cyber worlds [1]. CPS offer promising technology that adds many capabilities to different physical-based applications in diverse domains. CPS can be used to enhance automation capabilities in manufacturing processes for better productivity, efficiency, accuracy, safety, and reliability [2,3]. It can be used in healthcare applications to provide useful real-time services for patients and healthcare professionals [4,5]. CPS can be used in large commercial and residential buildings to improve energy efficiency and living/working conditions [6,7]. They can also be used in transportation systems to enhance safety and efficiency [8]. CPS utilize and integrate numerous technologies, features, and ideas from networking, distributed systems, sensors, embedded systems, software systems, and hardware devices such as microcontrollers and actuators. CPS also encompass different disciplines such as mechanical, biomedical, construction, systems, and electrical engineering along with healthcare, transportation, and energy fields to add value to applications in the physical world [9].

While CPS can offer many smart enhancements for improving physical systems and processes, they are, like any other computerized and distributed system, vulnerable to security attacks and criminal activities. Unlike other systems, however, security attacks may cause not only data, software and hardware damages but also major physical damages. These physical damages may include human deaths and injuries, infrastructure damages, loss of resources, and machine breakdowns or malfunctions. An interesting case involving a security attack on a CPS known as the Stuxnet worm is analyzed in [10]. The Stuxnet worm is a highly sophisticated cyber-attack using several security attack techniques with a specific goal of disabling a manufacturing facility. Another attack was discovered a few years later on the US power grid (Calpine Corporation, Houston, TX, USA) with the intentions of causing a major blackout in the country [11].

When a general-purpose software is attacked or breached, forensics (digital criminal investigations) will involve analyzing operational and access logs, tracking network traffic sources, and figuring out how it was done, who did it, and of course why. Forensics efforts will also use this information and additional software operational information to create defense mechanisms for future attacks. As the applications of CPS are rapidly being developed and deployed in different critical domains, various security measures are considered and included to protect them. Along with the security measures, it is extremely important that CPS also include suitable and effective forensics capabilities. These are critical, yet difficult to achieve, when attacks are detected and investigations to find the culprits and mitigate the damages are needed. In CPS, the forensics process becomes a much wider and more complex endeavor. Analysis, tracking, and investigations will have to cover all software and hardware components, digital and physical evidence, and all interactions across the whole system, which usually involves largely distributed and heterogeneous components. In addition, currently available CPS forensics methods rely mainly on traditional techniques that, despite their effectiveness in some fields, may not be effective enough for CPS forensics. As a result, CPS forensics can benefit from another native behavior/feature of CPS, which is access to huge amounts of data. Data collected before, during and after a security attack are available for analysis to arrive at more definitive forensics evidence. The key is to adapt forensics techniques and create new ones that can take advantage of these data.

In this paper we offer an overview of CPS forensics, then highlight the challenges of adopting different techniques for CPS forensics. The goal is to help outline an overview of possible solutions using different approaches for improved and more effective CPS forensics operations. We will first define and discuss the emerging area of CPS forensics and highlight its different dimensions (technical, organizational, and legal) and introduce some issues and challenges in the field. These issues arise due to several factors such as the connection to the physical world; the intimate integration between heterogeneous components, humans, and software; and the added vulnerability due to the active feedback and control cycles needed for CPS effective operations. Then, we discuss current approaches addressing CPS forensics which leads us to the final goal of this paper, outlining new approaches and techniques t for CPS forensics so that researchers and practitioners in the field will have an overview of what is happening and what is possible in terms of creating and effectively applying CPS forensics approaches.

The rest of the paper is organized as follows. Section 2 provides background information about CPS, forensics, and related work. Section 3 discusses security attack and risks on CPS. Section 4 introduces CPS forensics from three different perspectives: technical, organizational, and legal. The current approaches for enabling CPS forensics are discussed in Section 5. Section 6 provides some discussion regarding potential future research and development directions, and Section 7 concludes the paper.

2. Background

This section covers some related work and background information about CPS, forensics, and the relevant work in these fields.

2.1. Cyber-Physical Systems

CPS are networked embedded systems, categorized by solid and constant interactions between physical and cyber components [9]. CPS are being progressively utilized everywhere to enhance physical domains. A great part of CPS is designed to support smart and context-aware mission-critical applications [1]. Predefined objectives of the related application domain are realized through the monitoring and control processes, as provided by CPS. The control decisions are usually performed by the cyber world using smart algorithms constructed by software.

Unlike regular embedded systems, CPS are networked embedded systems that consist of several heterogeneous distrusted components. These components may be computing nodes, sensors, actuators, smart devices, and software. These components are connected through wired and/or different types of wireless networks, as shown in Figure 1. Both sensor and actuator components are tightly attached to their physical environment. Sensors and actuators provide the interface between the cyber world and the physical world. Sensors are used to monitor the physical world, while the actuators are used to manipulate the physical world. One or more computation units are used to execute control software for the environment. These computation units can be computers or microcontrollers.

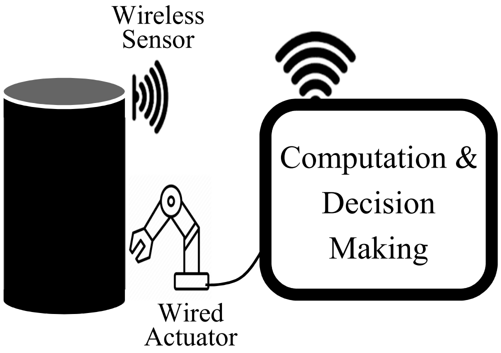

Figure 1. Cyber–physical Systems (CPS) components connected by wired and wireless networks.

The three main functions in CPS of operations are: monitoring using sensors, making decisions using smart software, and applying actions using actuators [12]. These three functions operate within a feedback loop covering the whole CPS as shown in Figure 2.

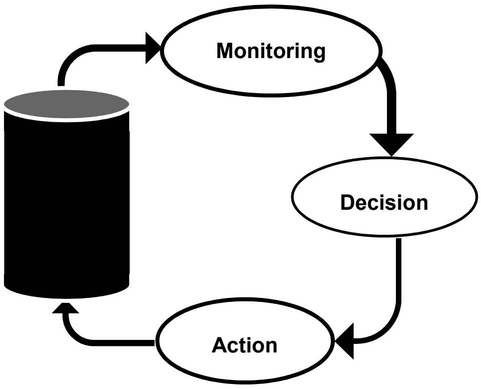

Figure 2. Closed-loop control steps of CPS.

Multiple connected CPS can also work together to complete a task or mission. These CPS form large-scale CPS that consist of multiple resources utilized for completing the assigned task or mission. Each CPS has its own sensors, actuators, and computation resources, but they need to work together. These CPS can be homogenous or heterogeneous in terms of their resources and capabilities. However, these collaborative CPS share their resources for the benefit of the application they are being used for. Such a system is referred to as a Collaborative Cyber-Physical System (CCPS) [13]. One example of CCPS is industrial collaborative robotic CPS that form the main requirement to create smart manufacturing [14].

CPS can also be connected to other systems such as cloud and fog computing to use the advanced services and large-scale resources provided by such systems. Cloud computing can provide scalable and flexible computational and storage services as well as advanced software services to support CPS. In smart manufacturing, for example, CPS collected data can be off-loaded to the cloud for storage and future analysis [15]. Fog computing can provide more localized services such as limited processing services, real-time services, data caching, short-term storage services, and efficient communication services [12]. In the smart manufacturing CPS, fog nodes can be the points of control and decision making based on the data collected locally in the area. Such functions require some storage and processing power but cannot tolerate the delays of using the cloud. When CPS utilize cloud and fog computing for their operations, they are referred to as Cyber-Physical Cloud Systems (CPCS) [16].

2.2. Forensics

Forensic science is an ancient profession associated with any type of criminal activity. Criminal investigations and the use of forensic science advanced a lot over time [17–19]. In the past few decades computers and software applications supporting forensics have been created and are in use for various activities such as facial recognition, DNA analysis, examining crime scene devices and content, and crime scene simulations [20]. Quickly, computers and computing devices became the crime scene for criminal activities such as stealing data, disrupting operations, or spying on others. Digital crimes led to the need for new and more sophisticated forensic approaches to computing devices, software, and data to collect evidence [21,22].

The technical and the law enforcement communities had to work together to address digital crimes and digital investigations. In addition, the legal system needed to extend some of its laws and regulations to incorporate these developments. A lot of effort and advances were made in this direction [23–26]. These rapid advancements in computing and technology increased the complexity of computer systems, and, as a result, forensics also became difficult and complex. A study of the historical development in this area is presented in [27]. A simple example to illustrate this is securing the evidence found. In a physical crime scene, the location can be isolated and access control is implemented. With digital crimes, access points to crime scenes can be unlimited and change can be done quickly and remotely. Investigators have to work methodically and fast to identify and isolate evidence before anyone can remove or modify it through digital means. This will involve severing all physical connections, disabling wireless connectivity, and possibly finding components (cyber and/or physical) that may change or destroy evidence. With CPS, the issues are combined and magnified, adding more requirements to achieve effective and efficient forensics.

2.3. Related Work

Several researchers investigated and highlighted the importance of securing CPS and the associated issues. General security issues and challenges in CPS are investigated by many researchers such as Humayed et al. [28], Ashibani and Mahmoud [29], Wang et al. [30], Alguliyev et al. [31], Neuman [32], Banerjee et al. [33], Burg et al. [34], and Cardenas et al. [35]. Some research efforts focused mainly on security for specific CPS applications. Sridhar et al. [36] and Sun et al. [37], for example, studied the CPS security of power grids. Huang et al. [38] investigated CPS security for industrial processes. Wells et al. [39] investigated the challenges of securing manufacturing CPS.

Other research efforts offered different techniques and frameworks to evaluate CPS security. Wurm et al. [40] investigated the security vulnerabilities of some implemented CPS from a cross-layer perspective. This investigation includes the CPS and the underlying hardware platforms. DiMase et al. [41] developed a system engineering framework to evaluate the well-being of CPS security. Hahn et al. [42] developed a framework for understanding cyber-attacks and the associated security risks to CPS.

Forensic issues and solutions were investigated in many emerging related areas. Some examples of these areas are in cloud computing [43–46], fog and edge computing [47–49], smartphones [50–53], and internet of things (IoT) [54–57]. Cloud computing, fog computing, smartphones, and IoT are usually components of and enabling technologies for CPS. Therefore, all their challenges will be inherited by the CPS using them. Moreover, there are two major differences between the forensics of CPS and those of the other technologies. The first one is that the forensics of the other technologies are mainly of the cyber/digital type. That is the issues investigated are mostly in the software part of the system or sometimes in the directly connected devices in this system. CPS forensics, in addition to the two types above, also involve forensics on the physical environment the CPS is serving. The second difference is that CPS operations rely heavily on the utilization of the feedback and control loops. These loops span all parts of the CPS (physical, cyber/physical, and cyber). This means that the effects of an attack may cause more damage or generate effects in areas not directly connected to the location of the attacks. This unique feature in CPS will also affect the methods by which forensic data are collected and preserved for analysis. These two differences create additional challenges for CPS forensics investigations. Yet, these same unique features in CPS create opportunities to create better proactive CPS security and forensics.

Some researchers also investigated issues and proposed solutions for forensics in specific areas of CPS. One area is concerning SCADA (Supervisory Control and Data Acquisition), which is used for monitoring and controlling industrial facilities such as oil and gas refineries as illustrated in [58–60]. Other areas include the electrical power grid [61], smart homes [62], smart cities [63], connected vehicles [64], and additive manufacturing systems [65]. However, these efforts were mainly investigating the cyber/digital and network forensics of the CPS applications in their respective domains.

Recently, there has been some interest in investigating different aspects of general CPS forensics and proposing more generalized solutions for them. We will cover examples of these efforts for CPS forensics in Section 5. Unlike other papers discussing CPS forensics with specific target domains or features, the main contributions of this paper address the CPS forensics in a holistic view. This includes (1) offering a working definition of CPS forensics; (2) studying CPS forensics from three different dimensions: technical, organizational, and legal; (3) surveying the current work and enabling techniques in the field; and (4) discussing potential future CPS forensics research and development directions.

3. Security Attacks on CPS

Implementing and deploying CPS solutions benefit many applications; however, they have major security risks if they are exposed. These risks may escalate to the levels of resulting in human deaths, infrastructure damages, and negative economic impact. In CPS both the cyber part and the physical part need to be protected from any possible attacks, since these can target the physical parts, the cyber parts, or both. In addition, the effects or damages from the attacks initiated on the cyber parts may propagate to the physical parts and vice versa. One example of such an attack is gaining unauthorized access to a control software function (cyber part) leading to the injection of fake control messages, such as one making one of the actuators in the CPS perform unwanted actions. Another example could be blocking a sensor (physical part) from obtaining the correct measurements for a specific condition which may lead the software to generate incorrect results or decisions leading the whole CPS system to operate in the wrong direction.

In actual incidents, many CPS security attacks targeted parts of the CPS that could lead to physical damages by directly attacking SCADA systems or the ICS (Industrial Control System) and affecting the actual operations of the industry. In some cases, the attack may target the computing infrastructure that runs and operates the control systems. Examples include the cyberattack on the Ukrainian power grid leading to massive power outages in 2015 [66] and the cyberattack on Saudi Aramco, where over 30,000 workstations were infected with a virus resulting in operational disruptions company-wide in 2012 [67]. Several additional examples are discussed in [68,69].

Attacks on CPS can be categorized into passive and active attacks and each has some different characteristics and effects. They also differ in modes such as sources, intentions, and targets. Each of these categories is further divided into several other types as shown in Figure 3. Different passive and active attacks can compromise different CPS components and some examples of these attacks are depicted in Figure 4. The attacks may target any or all components (cyber and physical) and have effects on both. For example, attacks on ICS affecting how the device/machine will behave; disrupting or modifying messages causing some software modules to trigger the wrong actions; and hacking into a video camera and using the videos to discover trade secrets. This is in addition to the more typical attacks on the software components.

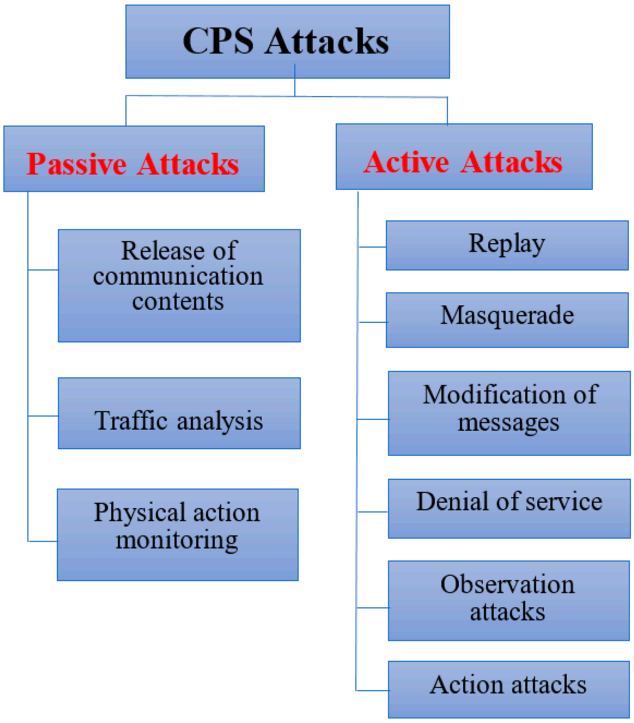

Figure 3. General CPS Attacks.

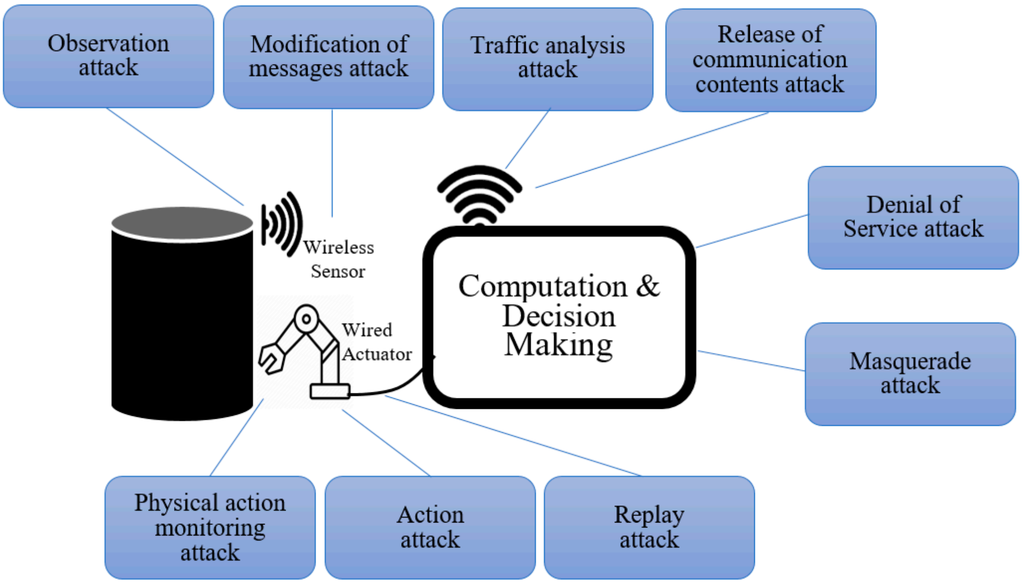

Figure 4. CPS components with possible passive and active security attacks.

3.1. Passive Attacks

Passive security attacks are recognized as attacks that provide access of some form to the CPS but does not directly affect it. Examples include eavesdropping and monitoring information transmissions; reading information stored in the system; or observing actions taken in the CPS. All of these activities will expose the CPS but will not cause any alternations or damages in the transmitted or stored information, or the CPS cyber or physical resources. As this category of attacks will not alter or damage the CPS and their operations, it is difficult to discover them. There are three possible outcomes of passive attacks: the release of communication contents; communication traffic analysis leading to, for example, trade secrets being exposed; and physical action monitoring that may help the attacker learn about operational procedures or trade secrets.

The release of communication contents will expose information that may be sensitive or private such as system information, control information, internal decisions, or other information among CPS components, among collaborative CPS, or between a CPS and other supported systems such as cloud and fog computing. Monitoring communication traffic allows intruders to know the contents of the communications in the CPS if the messages are not encrypted. If encrypted, the monitoring may not disclose the information, but can provide the intruders with the pattern of communication and sensing and control messages among different components of the CPS. Using this information, the intruders could identify the type of sensing or control messages, location of CPS components, and the type and frequency of current CPS operations.

Monitoring physical activities will allow the intruders to learn about the CPS activities and the actual operations taking place in the physical world. All of this can create multiple problems and consequences, such as violating the confidentiality of the system; violating the privacy of consumers, patients, or organizations; and enabling industrial and commercial espionage. Fortunately, many of the passive attacks can be thwarted by employing good physical security measures and using strong encryption/decryption methods for data in transit and at rest to hide exchanged information, control signals, and feedback content.

3.2. Active Attacks

The main characteristic of these attacks is that they will cause some form of alteration or damage to the CPS or some of its components. Intruders could attack by finding ways to access the system and alter communication messages, stored information, or actions to be taken. Unlike passive attacks, active attacks could be noticed relatively quickly through the alterations or damages they cause. There are six general types of active attacks on CPS: replay, masquerade, modification, denial of service, observation, and action attacks.

The first four types are attacks on the cyber parts, while the last two are physical attacks which require physical access to the system. In a replay attack, the intruder passively captures messages or action signals being exchanged and resends them in the CPS to create unauthorized outcomes including erroneous cyber or physical actions. The masquerade attack is when an intruder without any privileges or having limited privileges in the CPS impersonates entities with higher privileges to gain unheroized access and to gain access to restricted data or resources or conduct unauthorized actions. In message modification attacks, the intruders either alter, delay, or reorder some sensing or control messages to produce unauthorized cyber or physical actions. The denial of service attack is when intruders avert the regular use of CPS by flooding it with fake requests and message exchanges. This type of attack is usually performed by overloading some components of the CPS with messages greater than their capacity that will make the component and possibly the whole CPS stop or degrade operational performance. This is usually possible when the components of the CPS are connected through wireless networks or there are possible access points to the CPS components from outside the system (e.g., access through internet connections).

Observation attacks require intruders to have physical access to some sensing components in the CPS. The attack is performed by blocking the sensors or generating wrong observations through these sensors (e.g., deliberately increasing the heat near a temperature sensor to report an incorrect situation). Based on the wrong observations, the CPS may make incorrect decisions and take inappropriate actions (e.g., starting the sprinkler system in the area being monitored due to the faked high temperature readings). This type of attack usually starts as a physical attack but could quickly propagate to the cyber parts leading to software issues as well. The action attacks are also physical attacks targeting the actuators and action controllers in the CPS. Intruders may alter the actuator's responses to change the outcomes of their operations. One example is changing the type of material in a 3D printer in the CPS so that the printed product will be faulty or will not match the specifications. Physical attacks cannot be performed without actual physical access to some CPS components.

Many methods to protect CPS from active attacks are possible such as ramping up physical security of the physical operational sites, implementing strong access and control policies, adding multiple message validation steps in critical parts of the CPS, and including active monitoring techniques in the CPS operations.

3.3. Attack Modes

CPS security attacks, whether passive or active, may come from different sources, have different targets, and have different objectives. Similar to other systems, CPS security attacks may be internal, external, or both. Internal attacks are the ones initiated by a user who is authorized to access CPS resources and services (an employee for example); nonetheless, they use these access privileges to attack the CPS. They may, for example, alter operations, use resources for alternate goals, or steal/corrupt data or information. On the other hand, external attacks are the ones initiated by unauthorized attackers without prior access privileges to the CPS, such as criminals, competitors, terrorists, or hostile governments.

CPS security attacks may also target different parts (physical or cyber) of the CPS or all of it. For example, some passive attacks may only target digital data, for example, obtaining personnel data or spying on the message exchanges in the CPS. While others are initiated to observe physical activities to learn about operations or steal trade secrets. One example of an attack targeting physical parts is described in [65], where a thermal video camera was used to record the process of printing an object on a 3D printer and using that to obtain a detailed view of the structure and design on the object. This is also an insider attack since the camera had to be installed at the 3D printing location and passive since it did not alter the original system attacked. Passive digital security attacks will directly target the data or computational components of the CPS to steal or learn secrets.

Active attacks also have many consequences on any and all the components of the CPS. These could vary from major physical damages and loss of resources (including humans) to minor annoyances. Some catastrophic physical effects could be an explosion in a manufacturing facility, altering the operations of some manufacturing machines leading to unnoticed changes in the product, that later could cause major damages where it is used (e.g., altering the design of a medical device that could result in patients death or injuries). On the other side of the spectrum, attacks could also cause digital damages at varying levels. It could be a complete wipe out of software components or data on one end, to minor alterations of some interface layout. However, most damages in one type of resource will eventually lead to damages in the other. For example, losing some control data may lead to incorrect or delayed physical actions that may cause damages or problems. Furthermore, attacking sensors in the CPS by blocking their sensing mechanisms is a physical attack that could lead to incorrect data and incorrect results. Major examples here are the Stuxnet attack [10] and the Calpine Corporation [11]. More analysis of the propagation of attacks' impact on CPS is presented in [70].

CPS that have direct links to humans, medical CPS for example, could suffer heavily from security attacks because the possibility of human harm is very high. In [71] the authors discuss four possible security attacks on implantable medical devices. One example discussed in the article is an attack on an implantable cardioverter defibrillator, where attackers were able to inject malicious messages that could change the devices treatment actions. Energy CPS can also be affected in many severe ways, but most will not likely cause direct human harm, except when power is lost in a critical situation such as a hospital operating room during surgery. However, massive infrastructure and loss of resources is possible. Plumer [72] discusses the possibility of causing a national blackout due to security attacks. With less severe effects, a water pipeline monitoring CPS failure due to a security attack may delay the discovery of leaks, alter pressure levels, or report nonexistent leaks; all of which can be verified and managed without major losses especially to humans. Table 1 provides a summary of major CPS applications covering their main objectives and potential security risks.

Table 1. CPS Applications Benefits and Potential Security Risks.

CPS Applications	Major Objectives	Potential Security Risks
Medical CPS	- Timely patient monitoring and treatment - Accurate monitoring and treatment	- Loss of lives and injuries - Loss of critical resources
Smart Buildings	- Reduced energy consumption - Enhanced quality of life for occupants	- HVAC (Heating, Ventilating, and Air-Conditioning) systems damages - unnecessary energy consumption - Reduction in the quality of life
Smart Grids	- Optimized energy utilization - Reduced overload risks - Reduced energy waste	- Energy infrastructure damages - Energy efficiency reductions - Negative economic impact - Consumers loss of services
Pipelines Monitoring and Control	- Maintained health and operations of pipelines - Reduced impact of failures, accidents, and possible attacks	- Pipeline infrastructure damages - Possible fires due to natural gas and oil pipelines damages - Human deaths or injuries - Environmental pollution - Negative economic impact
Smart Water Networks	- Reduced water loss - Optimized water production and utilization - Enhanced water quality - Better service availability for consumers	- Water network infrastructure damages - Water networks efficiency reduction - Water pollution - Human health consequences - Negative economic impact
Vehicular Safety	- Reduced possibility of accidents - Reduced congestion - Reduced traffic violations	- Vehicular accidents - Human deaths and injuries - Road infrastructure damages - Traffic delays
Smart Manufacturing	- Optimized production and maintenance - Enhanced product quality - Customizable production processes - Enhanced safety	- Production efficiency reduction - Manufacturing equipment damages - Increase in resources consumption - Manufacturing safety reduction - Human deaths and injuries - Negative economic impact

Table 1. *Cont.*

CPS Applications	Major Objectives	Potential Security Risks
Self-Driving Vehicles	- Reduced transportation costs - Optimized traffic flow - Enhanced safety - Efficient ride sharing systems - Reduced congestion	- Vehicular accidents - Human deaths and injuries - Structure damages - Traffic delays
Intelligent Traffic Lights	- Reduced traffic delays - Minimized vehicles travel times - Increased vehicles average velocity	- Vehicular accidents - Human deaths and injuries - Road infrastructure damages - Traffic delays
Renewable Energy Production (Wind Farms, solar and Hydropower Plants)	- Maximized power generation - Improved ability to integrate with other systems such as smart grids - Better capabilities to balance energy production and consumption	- Renewable energy infrastructure damages - Reduction in energy production - Problems with other integrated systems
Energy Efficiency in Data Centers	- Reduced energy consumption - Maintained good health of the equipment - Reduced maintenance and operations costs	- Equipment damages - Reduction in energy consumption efficiency - Loss of data - Openings for unauthorized access
Greenhouse Efficient Controls	- Enhanced plants growth and produce quantity and quality - Optimized resources utilization	- Plants deaths - Reduction in produce quantity and quality - Increased unnecessary recourses consumption

The last factor to consider is one that many have not addressed or do not consider to be a security attack. This is whether the attack was intentional (pre-meditated) or non-intentional (accidental). The general trend is that any attack of any type and consequence is intentional. However, there are some possibilities of damages caused by an unintentional action or erroneous operations. For example, someone unintentionally forgetting to sign out of the system console, could lead to others exploiting the issue. Sometimes users may install or add something to a device that will later have some impact on the other software leading to damages. There is also the possibility of accidently copying or corrupting data or control signals leading to problems or damages. All these examples show that CPS forensics are also necessary to handle this type of issue. The main idea is that many damages assumed to be caused by a pre-meditated security attack could have simply happened by mistake. Therefore, forensics investigations should be carried out with the understanding of the possible discovery of an error or mistakes.

4. CPS Forensics

The former director of the Defense Computer Forensics Laboratory defined digital forensics as "The application of computer science and investigation procedures for a legal purpose involving the analysis of digital evidence (information of probative value that is stored or transmitted in binary form) after proper search authority, chain of custody, validation with mathematics (hash functions), use of validation tools, repeatability, reporting and possible expert presentation" [73]. Digital forensics and physical evidence forensics can also be considered a special field that overlaps with network forensics as well. Digital forensics have advanced substantially in the past several years. Several digital forensics types were developed. These include computer forensics, network forensics, virtual machine forensics, mobile devices forensics, and cloud computing forensics [74]. Unlike other digital forensics types, CPS forensics is a new type that is still at its early stages of development and deserves more attention. CPS forensics is a cross discipline of CPS's cyber (software, networks, etc.) and physical parts and forensics. Physical forensics have been used and refined over a very long period of time and, thus, offer some good guidelines for using it. Network forensics involves tracking, collecting and analyzing network traffic using a systematic approach [75]. Furthermore, CPS forensics also incorporates elements from all other types of forensics depending on the extent of their deployment and their components. For example, if the CPS uses cloud services, then cloud forensics apply and if attacks occur on mobile devices mobile forensics will be needed.

A model using a framework for analyzing cloud forensics discussed in [43] can be adapted and applied to CPS forensics. In this framework, there are three dimensions to consider: technical, organizational, and legal. Each dimension approaches the forensics from its own perspective. Following the essence of this model we will describe these dimensions within the context of CPS forensics and highlight some important related issues.

4.1. Technical Dimension

The technical dimension involves the processes, techniques, methodologies, and tools required to conduct the forensics in CPS environments. Forensics involve several technical aspects, such as data collection, virtualization/simulations, and incorporating proactive and corrective measures.

1. **Forensics Data Gathering.** When an attack occurs several data collection steps need to be performed while preserving the integrity and validity of this data. This includes finding, recognizing, marking, acquiring, analyzing, and reporting forensics data. Unlike other digital forensics types, data gathering in CPS involves collecting data from and about the digital components along with the corresponding physical environment. This also implies that data gathering will involve traditional physical evidence collection related to the attack and its effects. The physical environment can offer information based on the traces left behind and/or the physical damages incurred. On the cyber side of the operation, data collected and preserved from a variety of computing and control devices must be validated. The tools used to gather this data will differ based on the technologies used in these components. Sources of data will also be extremely different from traditional systems as there will be multiple sources with different storage and reporting methods and formats in addition to different capabilities and resources.
2. **Dynamic Existence**. Discounting the main computing resources in a CPS (full scale devices and resources) that must be present continuously, there are components and devices that drop in and out of the system dynamically. Many components in a CPS will only be available while actively completing an assigned task. For all other times, it remains inactive or disconnects from the system to preserve resources. For example, a wireless motion activated camera will only record and transmit data if there is movement in its range. In addition, some of these components have small storage capabilities. These are usually set up to deliver sensed data and overwrite it periodically to save space. Collecting forensics evidence requires tools that are capable of recognizing these special operational conditions. Furthermore, control signals may not be stored on a continuous basis (only control signals differencing from normal are recorded for example) leading to gaps in information about how the actions were triggered.
3. **Connection to the Physical Environment**. The intimate connection between the different digital components in a CPS with the physical environment they operate in imposes additional unique characteristics on the whole system. Forensics here require tools and methods that can combine many of the digital forensic capabilities with traditional forensic processes. Inspecting the sources of a failure, for example, will require tracing the digital evidence leading to the failure in addition to any possible physical evidence such as tampering. In this regard, virtualization, emulation, and simulation techniques can be used as enablers for CPS forensics by provisioning for virtual simulations of the situation and the factors leading to the problem.

4. **Proactive Measures**. A major contributor to effective forensics is being prepared ahead of time. Generally, most software systems have some level of security measures in place. Authentication, authorization, access controls, encryption, and similar measures are becoming standard practice. In CPS, these measures need to be extended to all components of the system including the physical world. Using secure locations, imposing controlled access to locations of these components, limiting external exposure, and using biometrics for access and control are some examples of proactive measures for CPS security. Other proactive measures in CPS require validation and verification of sensed data and action commands. As these devices are prone to failure and tempering, it is important to create strong measures to ensure the correctness and integrity of the collected data and the issued actions. Several models are available and need to be enabled for security and intrusion detection in CPS. One example is using intrusion detection techniques that can be included within the CPS components and sub-systems [76]. There are several intrusion detection techniques developed specifically for CPS applications that can help to overcome some security and other challenges [77].
5. **Digital Trails**. Another proactive measure that is important for forensics is monitoring and recoding all activates in a system. In the cyber world, monitors and logging features are usually integrated with the software to keep track of all transactions, log all access, and record all events. In the physical world, additional measures are needed to have more information about what is happening in the CPS components and the environment they operate in. Physical access logs to locations, human logins to the system and their locations, maintenance records, and hardware upgrades/replacements are some examples. In addition, recording physical changes in the environment, such as temperature, lighting, and movements, to name a few is necessary for analysis if a security incident occurs in the CPS. Using intrusion detection for example, enables collecting data related to CPS activities during normal operations. Examples include data about the interactions among different sub-systems within, information exchange between the software components and the sensing devices and actuators, interaction logs between the CPS and the external environment. This information is collected for intrusion detection, but a preserved complete record (digital trails) of this data is tremendously useful for forensics analysis when an attack occurs.
6. **Heterogeneity of Components**. In CPS the components differ from each other in many ways. Some are physical user interface devices, others are sensing devices from various types and capabilities, there are also actuators that are responsible for different actions in the system and operate accordingly. Moreover, we have multiple software components, usually from different sources and sub-systems that require compatible interfaces and connections. A CPS must be capable of handling this verity and operating effectively across the whole system. With all these differences, adding features to assist in forensics becomes a challenge. In addition, incorporating proactive measures and logging methods may be hindered by the limited resources in some devices, privacy issues in others, and access controls as well. This also imposes some requirements on the forensics tools being used as some may not be compatible with all the different components or could require resources not usually available on many of them.

4.2. Organizational Dimension

CPS, from the organizational perspective, could be small and self-contained and could grow to become global systems owned and managed by various independent entities. The complexity of the forensics processes increases as the CPS becomes bigger.

1. **Private Limited Ownership CPS**. At the smallest level, we can consider CPS that are owned and operated by a single entity (one or few people). One example could be a home security system or a privately owned self-driving vehicle. Here access, ownership, and tracking of data is manageable and can be secured and validated quickly. In addition, privacy issues are minimal and contained under a single control point.

2. **Intra-Organization CPS**. There are CPS that operate across a single organization such as a small factory using CPS to monitor and control assembly line operations. Here we also have a relatively contained CPS under a single control system. As a result, control, access, and privacy issues are limited within the owning entity.
3. **Separate CPS Ownership/Operations**. CPS can also be owned by an entity but operated and controlled by a different independent entity. For example, a small business using CPS commissioned through a third party such as a cloud service provider or specialized technology company. Here forensic data will be needed from both sides and privacy and access issues may arise as each entity has its own rules and security requirements.
4. **Federated Organizations CPS**. Another type of CPS covers multiple systems and locations owned by a federation of entities. For example, CPS to monitor and control a supply chain for retailers. These systems will operate in collaboration across many independent entities. Take for example a large retailer obtaining merchandise from multiple producers, using different companies for transportation and warehousing in addition to their own retail systems. Here responsibilities further distribute across multiple entities, thus adding more challenges to finding, accessing, and using forensic data.
5. **Large Scale Open Ownership CPS**. CPS can also be implemented and operated across many independent and non-federated entities. The sub-systems interact with each other through specified interfaces, but none of them has direct access or control to the others. For example, ATM machines and point-of-sale (PoS) components can be part of a large CPS that facilitates access to users' accounts through multiple banks and financial institutions. The system operates across all of them; however, each one operates independently and may have very different security and data collection policies.

There are two major aspects to consider in relevance to all the types of CPS, which also link the organizational and the legal dimensions. First, whether consumers or consumer devices/data are part of the CPS. Any of the five types of CSP may be connected to and used by consumers or external clients. This adds an extra security issue that could significantly affect forensic efforts and the privacy of the consumers' data. For example, a smart energy grid may have CPS components belonging to the consumers to monitor energy use. These components could be collecting and storing private consumer data beyond power consumption levels. When an attack occurs, we have to consider how much and what type of data should or should not be examined and how to find evidence while preserving consumers' privacy.

The other aspect is whether the CPS are local or operate across multiple countries (different jurisdictions). The main concern here is how to manage the forensics in terms of responsibilities and governance. In CPS, like any other distributed system, if an attack occurs and forensics begin, it is important to maintain integrity and validity. Data gathered across multiple locations must have clearly defined isolation from individual governance influences. Having the required permissions and tools to access and collect forensic data is important, in addition to creating clear definitions of responsibilities and roles of all sub-systems. To further complicate things, we also have to handle the different compliance requirements, regulations and laws across all parts of the CPS in different countries (discussed next).

Governance creates various issues when it comes to CPS forensics with varying levels of complexity. In essence, the larger the governance circle, the larger the issues we need to handle for forensics. When an attack occurs and the CPS, its environment, and all supporting systems are under one governing body, clearances, privacy and access issues are determined by the governing body and apply to all parts of the system. However, realistically, most CPS are implemented and deployed with the support of various organizations and service providers. Access to forensic data such as audit trails, historical usage data, and any relevant data will have to be orchestrated across all entities involved. Data privacy, access controls, data integrity, and data protections must be preserved, and proper controls and policies should be enforced.

4.3. Legal Dimension

The legal dimension of CPS forensics involves the extension of laws and regulations to include CPS forensic activities and evidence. Furthermore, principles, procedures, and policies for CPS forensics should be developed to make sure that forensics activities do not break any laws and regulations. In addition, it is important to ensure that these processes and methods comply with legally acceptable evidence gathering, handling, and validation procedures. It is important to ensure the different process are perfumed lawfully and the evidence chain of custody is secured and validated to make them admissible in court. Legal procedures similar to regular types of crime investigations must be implemented. Justifying searches, obtaining warrants, and securing and seizing evidence must be done according to the rules of the law. Some steps have been accomplished in relevant domains such as the US E-Government Act of 2002, which includes policies like the Privacy Impact Assessments (PIAs) [78], the introduction of the EU GDPR (European Union General Data Protection Regulation) [79], and the proposal for regulations in EU for robotics and AI law [80].

A key issue to consider is who will be performing the forensic procedures. The mix of physical evidence in the CPS environment and the digital evidence in the software side require different collection methods and experience. Police investigators are well trained to do that with physical evidence and sometimes with some forms of digital evidence. However, when the data needed is part of a complex system, it will require the expertise of software professionals to handle it. The software professionals are capable of finding and analyzing this data; however, they lack the professional training in how to follow legal procedures to maintain the chain of custody and integrity of evidence so that it is admissible. Interesting discussions of digital forensics and law enforcement connections are presented in [81,82].

The organizational dimension heavily impacts this dimension as well. Clear and well-defined ownership and operations reduce legal issues, while large-scale and global CPS systems will require more efforts to properly establish the forensics processes while conforming to the correct legal requirements. In addition, the legal aspects span different concerns each of which further impacts the process. Some of these factors include the following. Furthermore, the ethics and ethical conduct aspects pose an additional area to be considered carefully, for example [83] discusses similar issues in smart cities. Discussing of this aspect is beyond the scope of this paper.

1. **Ownership**. The legal implications of data/evidence ownerships can impede or complicate forensics efforts. Well defined limited ownership of CPS components limits the responsibility chain to the defined owners and can be easier to handle the legal processes like warrants, seizers, and validations. For example, assume an attack on a medical CPS occurred that altered some patients' records. The investigation will require access to many patients' records to identify the full impact of the attack and find traces leading to the attackers. However, these data, although collected and managed by the medical CPS owners, individual records also belong to their respective patients. How will warrants, for example, be handled? Who will be viewing and analyzing this data?
2. **Jurisdiction**. Where is everything? In the United States, many states have different state laws and ways of enforcing them. In addition, law enforcement in one state usually cannot pursue criminals and criminal evidence outside their state. The same applies when considering multiple countries. CPS spanning multiple jurisdiction areas, will cause major problems in terms of handling the legal aspect of the forensics and the use of CPS collected/generated data. A discussion of an example of this issue is available in [84]. Going back to the medical CPS attack. If this system covers multiple states or countries, what happens if some allow access to all patients' records with one warrant, while others require individual warrants for each record? What if a certain activity is considered a crime in one country and not a crime in another? Even if there is some collaboration between these states or countries regarding forensics procedures, which laws should be enforced?

3. **Intellectual Property and Trade Secrets**. Forensic searches in the digital world could lead to the exposure of a lot of information that is intended to be protected by law. Intellectual property data may inadvertently expose certain organizations to competition. Another critical issue is the trade secrets organizations need to be kept private and never exposed. What happens if the forensic analysis exposes this information? What are the legal implications? CPS in a factory, for example, may be monitoring a very complicated fabrication process that is kept secret. If an attack occurs on this CPS, the investigation may outline this process and expose it.
4. **Private Information**. This is probably the most discussed and debated issue regarding digital forensics in general and it is more prevalent when performing CPS forensics. Any CPS will have direct links and interactions to humans and data relevant to their work, living, medical history, etc. Some CPS components may be able to analyze and discard personalized data on the spot, while others do not have the capabilities to do that, so they transmit everything to some storage component in the system. In addition, when dealing with forensic evidence, anonymized data may not be useful, thus investigators will need access to the complete data sets, which could easily violate a person's privacy rights. Many data breaches occurred in the past few years that led to the exposure of huge amounts of sensitive data. CPS have that unique position to collect and record all kinds of data way beyond what a regular user could comprehend. This further violates their privacy when investigated. Within an organization, an attack may warrant full investigation of all employee work and access records. This could still lead to private data exposure not relevant to the attack itself.
5. **Relevance**. CPS gather continuous and detailed data to facilitate smooth and efficient operations and effective controls of the systems they interact with. A lot of this data may not be security relevant but may have some effect on security aspects. The forensic analysts face a big challenge trying to sift through huge amounts of data to pinpoint the relevant data to the security attack being investigated. Some may be easily recognizable, such as IP address access logs and user authentication logs. However, some relevant data may be disguised under the apparent illusion of irrelevance. For example, assume an attacker penetrates a system and initiates executions of specific codes that can allow this attacker to use the CPUs available for their own benefit. When this attack is discovered, network and access logs will be the first to be looked into. However, these may not always offer usable evidence. However, other data such as how long the CPU has been executing at an abnormal or irregular level, how much memory is being in use, or even how fast the user responses are happening for the regular users, can be useful. A careful investigation of this type of (irrelevant) data may lead to more clues about the attack. All of this makes the legal process more difficult in terms of identifying the types of warrants needed, whether or not some evidence will be admissible if it is found outside the warrant boundaries, or to what extent the search methods are acceptable in terms of legality, ethics, and privacy.

4.4. Discussion

The three dimensions combined lead to varying levels of complexity in CPS forensics. Table 2 offers an overview of how complexity levels change with the introduction of additional dimensions to the CPS. Starting from the technical dimensions we provide three levels. Each one of the technical dimensions (1 through 6, see Section 4.1) is associated with relevant technical, organizational (see Section 4.2) and legal (see Section 4.3) sources of complexity. The "Technical Complexity" column assumes a base case where a CPS is small scale and under a single authority and highlights some sources of complexity. The next column takes us into the organizational dimension and shows which of them will further complicate our basic CPS. Similarly, the last column addresses the sources of complexity imposed from the legal dimension. For example, a basic CPS, privately owned will generally have to incorporate some features that will handle organizational and legal issues. However, a large-scale open CPS with multiple owners and locations, will have a huge number of issues to consider for effective forensics. A lot of work has been done in several domains close to and relevant to CPS forensics. In addition, some preliminary work is starting to appear tackling specific aspects of CPS forensics. However, addressing technical issues alone without considering how these challenges will change due to the other two dimensions will not lead to effective solutions for CPS forensics. A lot of technical solutions are needed in addition to mechanisms to address the organizational differences and enforce correct and lawful collection and use of the forensics evidence. Advances in the technological dimension have been progressing quickly and various approaches and solutions for CPS security have been introduced. However, very few address the forensics part in a holistic approach in all dimensions. In this paper we focus on the technical dimension in particular, and we hope to pursue the other two in our next stage of research in this field. The following two sections will discuss current technologies enabling CPS forensics then outline a futuristic view of what this field should be like.

Table 2. Technical dimensions and how legal and organizational dimensions increase CPS forensics complexity.

#	Technical Dimension	Technical Complexity	Organizational Complexity Sources	Legal Complexity Sources
1	Forensics Data Gathering	Preserving data integrity and validity. Finding, recognizing, marking, acquiring, analyzing, and reporting data.	All dimensions add complexity in an increasing level from 1 thru 5.	All dimensions will increase complexity.
2	Dynamic Existence	Components may: Not always be connected Have limited resources Change locations	Complexity increases as CPS grow bigger regardless of the dimension.	Relevance adds complexity. Identifying and legally obtaining ONLY relevant data.
3	Connection to the Physical Environment	Combining digital forensics capabilities and traditional forensics processes.	Federated and large-scale open CPS. Managing highly distributed physical and digital resources.	Privacy and relevance come in play.
4	Proactive Measures	Solutions incorporated at design time. Pre-incident planning. Extending security measures to all CPS components.	All five dimensions increase complexity. Legacy systems, inadequate resources, and operational software.	Managing privacy of people and the intellectual property and trade secrets.
5	Digital Trails	Creating trails for physical and digital activates.	Multiple ownership and control (in community, federated and open).	The major complexity factors here are ownership and privacy. Slight effects from relevance.
6	Heterogeneity of Components	Interoperability, interfaces, inadequate resources in some components.	Community, federated and open add complexity in increasing levels.	Ownership of heterogeneous devices may complicate legal access to CPS components.

5. Current CPS Forensics Approaches

CPS are very complex systems; thus, forensics require very complex processes. This section covers the current CPS forensics approaches being studied and proposed. Most forensics research efforts were dedicated for SCADA. In this section, we will not cover SCADA as it represents a somewhat smaller or specialized representation of CPS. We will focus mainly on the proposed techniques that can be used for any type of CPS. A survey of the tools, techniques, and methodologies of SCADA digital forensics can be found in [85].

CPS attacks usually involve multistage and multiple components in CPS. This makes these attacks difficult to detect, trace, and analyze. Mishra [86] addressed this complexity by proposing a modeling forensic investigation process. An epidemiology model was employed to find the degree of interaction among infectious components of the CPS. This benefits in understanding the propagation steps of the attack in the entire system. Aliabadi et al. [87] developed a real-time-specific invariant inference algorithm, called ARTINALI that incorporates time in the mined invariants, along with the traditional data and event invariants. This approach allows for detecting common attacks with more accuracy. This is because most CPS are real-time systems, and their operational correctness not only requires correct logic but also correct timing behavior.

Vollmer and Manic [88] proposed and verified automatically deploying deceptive virtual network entities in a control system network. This could be used to create dynamic virtual honeypots for observing and attracting network intruder activities. Do et al. [62] studied the potential for exploiting information retrieved from CPS such as smart home devices for forensic purposes. Abedi and Sedaghat [89] investigated this using crawling and spidering techniques to help in CPS forensics. Alrimawi et al. [90] proposed an approach to represent and share incidents knowledge for CPS. This approach recognizes patterns of incidents that occurred in different CPS.

Other efforts focus more on specific components of CPS and mostly on the cyber side. For example, Chan and Chow [91] developed a logging mechanism for a programmable logic controller to enable forensics analysis. Abeykoon and Feng [92] proposed an analytical framework to acquire digital evidence from a Robot Operating System. Al-Sharif et al. [93] investigated the possibility of collecting digital evidence extracted from the main memory (RAM) of the computer components about attacks on CPS. They used Java for their demonstration and found that it is possible to collect some evidence even after the garbage collector is explicitly executed. This work assists investigators to help them recognize and understand the software utilized to start an attack.

There are some research efforts in developing mechanisms and methods to integrate forensic principles and aspects into the design and implementation of CPS to enable forensic investigation processes. This approach is known as a Forensics-by-Design framework. One example of these efforts is to apply this in medical CPS (MCPS) to enable forensic investigations for criminal medical cases and attacks on medical CPS components (equipment, software, patients, etc.) [94]. In another example, the forensics-by-design framework is proposed to be used for cyber-physical cloud systems (CPCS) [95]. In this work, the authors used this framework to integrate forensic requirements into the CPCS design and development phases. The importance of this work is that while cloud computing can provide many benefits for CPS, this integration generates issues relevant to ensuring data confidentially, integrity, and availability. Attacks on a CPCS may be initiated from the CPS components, from the networks that link the CPS with the cloud, or from the cloud. There are six factors defined in the proposed framework to confirm that a CPCS is designed to enable forensic investigations. These are security risk management principles and practices, forensics readiness principles and practices, incident-handling principles and practices, laws and regulations, CPCS hardware and software requirements, and industry-specific requirements. In addition, the authors also highlighted the importance of validation and verification to ensure the reliability of CPCS forensic design and development.

Generally, the forensics-by-design framework can help recognize security breaches including their sources and types. In addition, it maintains and examines evidential data and draws conclusions. This facilitates answering the six key forensics questions—what, why, how, who, when, and where. Moreover, the forensics-by-design framework is a start for important advances in the field as it provides a base for facilitating more systematic forensics processes in CPS.

Unlike other regular systems that have many commercial forensics software and tools that can be used for security incidents, developing forensics tools for CPS can be extremely complex. Consequently, employing the proposed forensics-by-design framework offers significant help.

Although this approach may increase the implementation costs and complexity, it will provide many benefits to enable forensic investigations and protect the CPS. This can easily lead to a high ROI (Return on Investment) for the CPS during operations. These benefits are also extremely important as most CPS are used for critical applications and applications that involve humans.

The current CPS forensic research efforts can also be divided into three categories as shown in Figure 5. The first categories group is for developing frameworks, components, techniques, and tools to use during the development phase of CPS, before attacks, to add proactive measures for CPS forensics. Examples are developing forensics-by-design frameworks; components to enable implementing CPS with forensics capabilities such as logs and audit trails; and testing techniques and tools to ensure the forensic capabilities of the developed CPS. All these tools rely heavily on creating appropriate data collection mechanisms in the design phase of the CPS. The second category is for developing techniques and tools to be used during attacks. For example, tools for intrusion detection, intrusion prevention, and intruder entrapment. The last category is to help incident investigation efforts (after attacks). Some examples are developing investigation tools, investigation approaches, and incident representation techniques to enable sharing, processing, and extracting knowledge from the incidents. Table 3 provides a summary of the discussed research efforts in CPS forensics and their categories. The table shows that most efforts are focusing on the cyber parts of CPS and ignoring the physical parts. Thus, it is necessary to expand the research efforts to cover both and create broader forensic approaches.

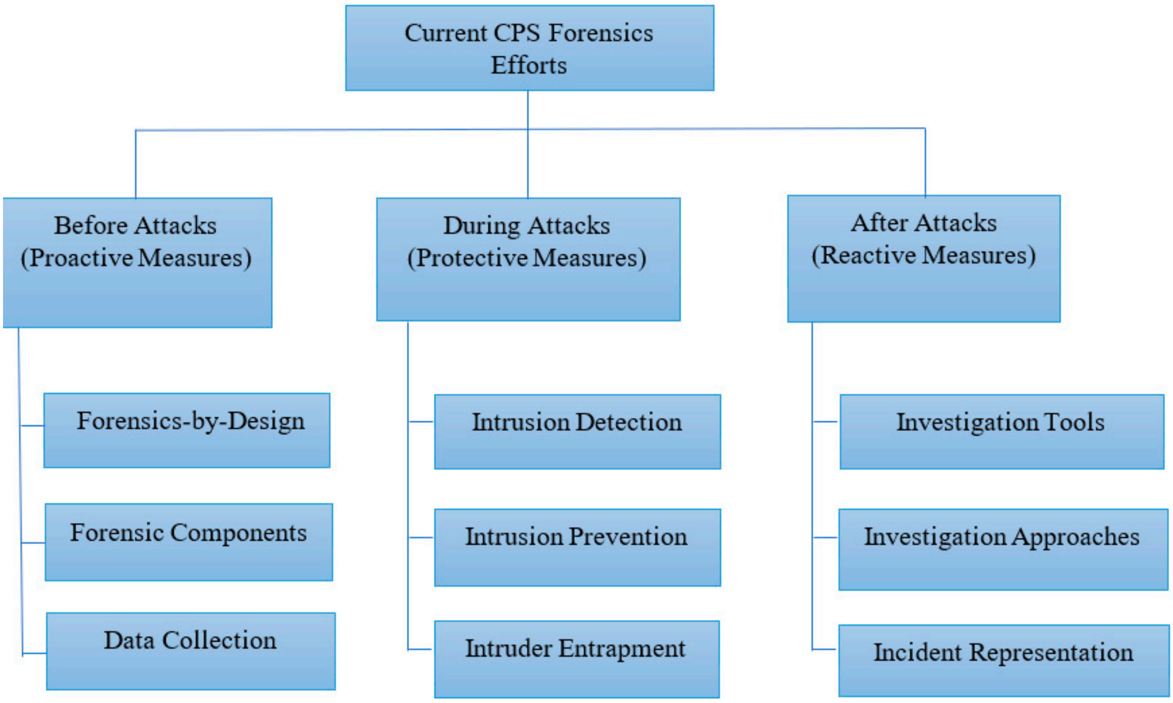

Figure 5. Current CPS Forensics Research Efforts Categories.

Table 3. A Summary of Current Research Efforts for CPS Forensics.

Work	Category	Cyber, Physical, or Both	Main Purpose
Mishra [86]	Investigation approach	Cyber	To understand the propagation steps of multistage CPS attacks in the entire system.
Aliabadi et al. [87]	Investigation approach	Cyber	To detect common CPS attacks with more accuracy by incorporating time in the mined invariants, along with the traditional data and event invariants.
Vollmer and Manic [88]	Intrusion Prevention and Intruder Entrapment	Cyber	To create dynamic virtual honeypots for observing and attracting network intruder activities.
Do et al. [62]	Investigation approach	Cyber	To exploit information retrieved from smart home devices for forensics purposes.
Abedi and Sedaghat [89]	Intrusion detection	Cyber	To use crawling and spidering techniques to help in CPS forensics.
Alrimawi et al. [90]	Incident Representation	Both	To enable sharing incidents knowledge and to recognize patterns that occurred in different CPS.
Chan and Chow [91]	Forensics component	Cyber	To develop logging mechanism for programmable logic controllers to enable forensics analysis.
Abeykoon and Feng [92]	Forensic tool	Cyber	To develop an analytical framework to acquire digital evidence from a Robot Operating System.
Al-Sharif et al. [93]	Investigation approach	Cyber	To enable collecting digital evidence extracted from the main memory.
Grispos et al. [94]	Forensics-by-design	Cyber	To develop a framework for forensics ready medical CPS.
Ab Rahman et al. [95]	Forensics-by-design	Cyber	To develop a framework for forensics ready CPCS.

From these examples we can see that most current research efforts are for digital forensics in CPS. In addition, many address specific features or application domains of CPS. Integrating or considering the different types of components in a CPS (cyber and physical) is essential for creating successful forensic techniques. Research is making some progress; however, direct and specific proposals addressing the forensics of the whole CPS effectively are yet to be investigated and offered.

6. Future CPS Forensics Directions

CPS applications are being and will be implemented and deployed in many areas in our lives. Current CPS forensic techniques are mostly still in the research and evaluation stages (e.g., the overview in [96]), while most forensics work is being done using tools and techniques created for other types of distributed systems, such as cloud computing and enterprise systems. Furthermore, tools and techniques addressing both the cyber and physical parts of the CPS have not been introduced, although discussed on some occasions. Techniques for CPS security and forensics need to be further developed to address all aspects of CPS and in all dimensions (technical, organizational, and legal). Current research also addressed other aspects of CPS including discussions and proposals for the security of CPS. These approaches in related or similar systems should be adapted and extended to create a holistic approach to CPS forensics. Therefore, to achieve quick progress, it is important to learn from, adapt, and expand available technologies for CPS forensics. We discussed several examples in the earlier sections.

There are two main areas in CPS forensics that differ from other systems and need to be extensively addressed: enhancing and adapting current approaches in criminal forensics and available digital forensics methods (Section 6.1); and enhancing and expanding current software solutions through data-driven forensics approaches (Section 6.2). In addition, addressing forensics issues from a holistic CPS view will also facilitate using features and capabilities in CPS to further support and enhance CPS forensics capabilities. Furthermore, moving in this direction will allow for a better understanding of the forensic needs in all three dimensions of CPS (technical, organizational, and legal). We propose to approach this area as CPS forensics engineering (Section 6.3) in an effort to have a more systematic and organized approach to the field and to start treating CPS forensics as a system requirement that must be tackled throughout the system development processes.

6.1. Investigation Approaches

As illustrated in the previous section (Section 5), efforts and advances in CPS forensics are mostly focused on the cyber parts or specialized for specific CPS domains. Here we discuss possible ways to better integrate and use traditional criminal and digital investigation techniques to, overall, improve CPS forensics. Since CPS include and affect various types of physical components and humans, investigations of the digital part alone may not lead to the desired results. The evidence and effects of security attacks will likely be in both the physical and cyber parts of the CPS. Some areas that need further work and improvements include the following.

1. **Investigators**. This is probably an overlooked area. There are ongoing efforts to train criminal investigators on finding and handling digital evidence. Unfortunately, in CPS, the cyber side is a lot more complex and collecting and analyzing digital evidence is practically beyond the capabilities of traditional law enforcement investigators. On the flip side, there are many highly experienced technical investigators capable of performing sophisticated investigation and analysis techniques. Unfortunately, they are not well versed when it comes to the legal aspects of finding and handling evidence. This requires changing how these two categories work and creating models that will allow them to seamlessly collaborate for more effective investigations across the CPS (physical and digital). In addition, more efforts are needed to create systematic procedures and practices to better define and control investigation activities to match the increasing complexity of the process.
2. **Law enforcement**. Laws and law enforcement in the digital world and CPS need to be updated and adjusted to accommodate for the changes. According to [11], cyber security legislations are insufficient and vague. Furthermore, legislations do not precisely address issues in CPS, such as defining what constitutes a digital (or CPS) crime; identifying what is (or not) acceptable as evidence; addressing the legalities of digital enhancements of evidence; issuing and handling digital and physical search warrants; securing the CPS including all its cyber and physical components as a crime scene; and handing CPS court proceedings. In CPS, experts in criminal law need to be aware of, and preferably fluent in, technology. At the same time, technology experts must have a good understanding of the legal aspects of forensics. Researchers, legislators, security experts and criminal investigators need to create collaboration and training models to have experts in CPS forensics.
3. **Observation**. When a security attack is detected on CPS, the process of observing its effects and collecting information about the conditions that led to them starts. Here, physical investigations may be needed if the attack resulted in some form of physical damages, led to abnormal behavior of physical components, or was facilitated by physical actions. Digital search will cover the cyber parts to identify the causes and try to find the culprits. Investigators will need to quickly identify and isolate evidence and ensure the usability (admissibility) of the evidence. A major problem in these scenarios is that CPS components are not always in one location and are not always connected or in use. As a result, deciding on how to secure the crime scene requires more knowledge of the CPS architecture and the physical and digital characteristic and locations of their components. New tools to help in this process are needed to ensure comprehensive coverage

and accurate collection of evidence. One possible example is creating a visualization tool showing all CPS components and their connectivity and operational status in real time. This will help identify the areas and components that need to be secured and investigated.

4. **Analysis**. Collecting and preserving evidence (or what appears to be evidence) is the first step. However, analysis is another critical part of the investigation process. There are various tools used in physical evidence analysis, such as analyzing blood samples, autopsies, visual observations, and profiling. In addition, digital tools, such as facial recognition, DNA analysis, GPS location mapping, and many more are also used for this purpose. On the cyber side, computer crime investigations have also advanced heavily, and technologies are currently capable of handling and processing huge amounts and types of data evidence quickly and accurately. For CPS forensics, all of these tools are useful, yet more is needed to allow for more comprehensive coverage and efficient methods. For example, data analytics tools can be designed to find correlations between digital and physical evidence; creating digital models depicting some aspects of the crime scene using both physical and digital evidence; and introducing reliable and trustworthy computational techniques for more in depth analysis and evidence manipulation. Virtualization of the CPS crime scene and using techniques similar to or adapted from other domain, for example in manufacturing [97], can provide a good investigation platform for investigators. Another useful tool currently in use in many other fields is the information dashboard. Creating a similar tool that allows for different representations of collected evidence also provides investigators with easy methods to create more abstractions and view the data from different angles.

6.2. Data-Driven CPS Forensics

CPS, given the way they are deployed and operated, can collect and generate huge amounts of data. This data will come from both the cyber and physical parts of the CPS, practically creating big data. In other domains big data for digital forensics were defined and its challenges and opportunities were discussed [98,99]. Many of the opportunities mentioned can be observed in CPS forensics. As a result, it is only logical to approach CPS forensics as a data-driven field. Deployed CPS already gather and use huge amounts of data to achieve their objectives. A lot of this data is stored for future analysis and planning. It is then possible to use the same datasets for forensics in case an attack occurs. In addition, proactive measures need to be incorporated in the CPS to collect additional data that could help in forensics. For example, IP addresses are validated for access authorization in a stateless part of the CPS. Therefore, there is no need to store this information. However, keeping this information may help later to analyze incoming traffic and find the source of an attack. Each part of the CPS (cyber or physical) provides a multitude of opportunities to collect data for forensics purposes. The following provides an overview of possible research and development directions that can be pursued in the field.

1. **Data Collection**. Careful planning of CPS operations and data collection and storage functions is necessary to facilitate better forensics. Physical devices, such as video cameras, thermal sensors, and entry log recorders, can provide useful information. Digitally, provisions to record more data for forensics can be made early in the Design phase of the CPS. At that stage, it is easier to add these measures with minimum disruption to the actual functionalities of the CPS. In addition, treating the forensics as a system requirement will ensure accurate integration and resource planning for the CPS operations. Generally, current work does not address CPS forensics (and likely all types of digital forensics) as part of a system's requirements. Therefore, several opportunities to gather useful data are missed. We need to change the way we address this and include better security engineering principles alongside the software/system development principles.
2. **Data Management**. Tools to help organize, move, and access collected data need to be adapted to handle the real-time streams of data and large storage and communications requirements. With this also comes the responsibility to protect data privacy and ensure legitimate access to the data. User friendly and configurable tools to rearrange, aggregate, and anonymize data before presenting it to investigators are going to be a great help in this process. When information

about a specific type of activity is needed and the identity of the users is not important, the investigator should be able to enter the required criteria and the tools will run through the data and present the parts needed, while hiding the rest of it. Another important aspect here is establishing a foundation for data trustworthiness. There are different possible directions for data trustworthiness and sharing including trustworthiness of data based on provenances, formal policy analysis, and security experiments reproducibility. This will require relying on approaches that can establish and maintain trust relationships between the different components of the CPS applications and any other systems interacting with them. One possible method is using blockchain to enhance trust and secure transactions [100,101]. Blockchain was discussed as a tool for smart city security [102,103]. In CPS forensics it can similarly help ensure the authenticity and correctness of shared data and provide a strong base for establishing proofs.

3. **Automation**. The existence of a multitude of data about CPS allows for the opportunity to create automation techniques for some forensics methods. There are various applications in use for evidence analysis such as facial recognition, video analysis, and DNA comparisons. These techniques can be adapted to analyze CPS forensics data for specific goals. For example, algorithms that can compare different data streams and identify anomalies between the two, or tools to overlay different activities in different parts of the CPS to find overlaps or correlations between them. Another area of automation is controlling the operations of different parts of the CPS. In this case, a tool that can automatically shut down specific components, divert traffic from one path to another, or isolate specific parts of the network will allow investigators to have better control over the CPS, which will help in terms of securing evidence, preserving instantaneous data and operational conditions, and ensuring restricted access to the components during the investigation. Furthermore, many security attack detection and mitigation operations can be automated and used to provide solutions to detect and react to attacks like intrusion detection and prevention systems (IDPSs) and deal with challenging CPS security aspects such as advanced persistent threats (APTs) [104] and low and slow vectors [105]. Example possible approaches include context representation and sharing, detecting attacks using reasoning, graph grammars, and stream-based classification [106]. The data is available, and automation will save a lot of time and open up new opportunities to find links and clues.
4. **Intelligent Data Analysis**. Traditional data analytics are important tools for CPS forensics. However, advances in artificial intelligence, data mining, and machine learning techniques can offer tremendous benefits. These approaches have been applied in other areas relevant to CPS such as in smart buildings, self-driving cars, smart water networks, smart manufacturing, smart grids, and smart traffic light controls. Machine learning algorithms can monitor and learn from the CPS components' usage patterns and help identify flows or adjust configurations to enhance security measures and forensics data collection. They can also be used to monitor and learn human behavior and interactions with the CPS to help improve the cyber-physical interactions, identify possible problem areas, and quickly detect abnormal behaviors. In addition, analyzing the human–CPS interactions can facilitate better understanding of the relationship between human behavior and vulnerability to different types of attacks [107]. Intelligent algorithms can be designed to analyze these behaviors and create better interaction policies and monitoring techniques to prevent future attacks [108]. Machine learning algorithms can also be used across multiple CPS operating in similar conditions or performing similar functions. In this case, we have larger datasets and more sources for training the algorithms. As a result, these algorithms can achieve better learning capabilities faster. However, these same capabilities and reliance on training sets could lead to additional security risks and more complex forensics requirements. These threats can be classified as threats against the training phase and threats against the testing/inferring phase [109]. For example, attackers may add more data to the training sets that negatively influences the performance of the learning process (attacking the training phase), thus reducing the effectiveness of the learning algorithm. Another example is the poisoning

attack, which disrupts the availability and the integrity of the machine learning processes via introducing adversarial samples to the training data set. The poisoning attack generally targets the inference process by disrupting or even diverting it from the correct learning path. Different countermeasures to these attacks were discussed in [109]. However, this will require developing CPS forensics mechanisms and tools that are capable of dealing with and taking advantage of artificial intelligence and machine learning algorithms.

5. **Modeling and Simulation**. Creating a model for a system relies heavily on the data available about it. For CPS forensics, data collected can be used to build accurate models for the CPS and the conditions of its components before, during, and after an attack. This creates plenty of opportunities to analyze and compare the models to find clues and to identify weak spots in the CPS. In addition, the use of simulations can help provide better insights about the effects and available evidence in all parts of the CPS, especially the physical parts. The concept of digital twin has been around in other fields, such as smart manufacturing [110]. The same approach can be applied to CPS to provide accurate simulation model of the physical parts and link them to the digital parts. This will assist in creating complete views of the CPS and run different operational scenarios for the investigation. Simulation models can also assist in visualizing and tracing the control loops in the CPS and how each action affects subsequent actions. This will create a systematic time-based view of events that occurred leading to and during an attack.

Data-driven approaches will help discover unknown factors through observations and collective data analytics. While it was difficult to have such applications a few years ago due to the unavailability of the needed datasets, it is possible now as many applications and systems collect an enormous amount of data as they operate. Data-driven approaches generate insights and observations about the CPS security attacks that can be utilized in different ways: (1) CPS developers can use them to plan for designing and implementing better, more effective and secure CPS; (2) governments, security agencies, and legislation bodies can use them to define security requirements, standards, policies, and measures in addition to attack response plans; and (3) organizations deploying and using CPS can define security policies, detection and mitigation plans, and assessment of potential security risks.

6.3. CPS Forensics Engineering

Security engineering emerged in an effort to introduce engineering problem solving process models and software development life cycle approaches to security. It is time to introduce the same concepts to CPS forensics. CPS developers and organizations using CPS need to be more aware of the importance of including forensics (just like security) as part of the CPS requirements specifications. In addition, it is important to take these requirements through the same stages of the system development life cycle. Thus, including the forensics requirements is important when going through the design, implementation, and verification and validation steps.

Adopting the engineering approach will allow for including some or all of the possible approaches discussed in this section. Applying data-driven techniques will be supported by the CPS developers as a core requirement, which will lead to better planning of data collection and management; satisfying requirements ensuring all data needed for analysis, modeling, simulation, and visualization are being collected; and leaving room for further expansions and additions of new techniques when they are developed. Furthermore, this will create opportunities for better verification and validation capabilities for quality assurance. Testbeds need to be implemented and used to explore different attack scenarios, evaluate new forensics approaches, and provide accurate measurements for deployment. Two examples proposed for CPS security testbeds in [111,112] may provide some insights for this type of tool. This systematic approach will also allow for utilizing the same tools for forecasting and detecting security attacks before they actually cause damages to the CPS. Another area where CPS forensics can help with (beyond finding the attackers) is using the information to reverse or minimize the damages in the CPS caused by the attacks.

It is expected that more academic and industrial research will be conducted over the coming years to find applicable, practical, and efficient solutions. These include finding better ways to collect, share, clean, and analyze security data [106] and identifying more security risks and monitoring and mitigation approaches to use. In addition, faster data-driven mechanisms will be introduced to find new observations including finding zero-day attacks. Furthermore, some new security and forensics solutions will be significantly enhanced to provide better security measures and analyses including context-aware security solutions that incorporate information about the current environment context in dealing with security threats [113]. What we hope for is that these developments will have some level of organization that will create well defined CPS forensics process models.

On a side note, we addressed the CPS forensics mostly from the technical dimension. However, many of the current and future techniques developed will introduce additional issues in the remaining two dimensions (organizational and legal), such as handling issues of privacy and confidentiality, ethical conduct, jurisdictions, legal requirements, and human rights. These constitute a huge hurdle in the way of creating effective and efficient security and forensics measures. Discussion of how to reduce their impact is beyond the scope of this paper. In addition, there are many grey areas when it comes to organizational and legal aspects of CPS forensics. Once more, these were lightly incorporated where appropriate, but not detailed in this paper. Both areas will be addressed in future work.

7. Conclusions

Major advances in CPS design and development in various fields allowed for sophisticated and very effective ways to accomplish the goals of the CPS. Yet, this also increased the security risks on CPS as they grow bigger and become integrated into the physical operating environment. Securing CPS is a huge challenge and performing forensic analysis on CPS is also as big a challenge. As a result, our motivation to complete this study is to highlight current CPS forensics efforts, identify the challenges as we consider the different dimensions involved (technical, organizational, and legal). The main goal is to offer researchers and developers an overview of these challenges, the viability of data-driven forensics approaches, what is currently being done to address them, and a vision for possible new data-driven CPS forensics approaches.

In this paper, we defined and discussed a new type of forensics, cyber-physical systems forensics (CPS Forensics). We discussed CPS forensic principles and issues within the three dimensions: technical, organizational, and legal. Based on the current work in this field, we realize there is a strong need to further address this topic and provide effective CPS forensics measures. Efforts to create and cultivate suitable procedures, tools, regulations, and policies for CPS forensics are extremely important. Current approaches available offer partial solutions as they are mostly designed for specific types of CPS or to address very specific types of security aspects. Very few address the CPS forensics in a holistic approach that could meet the general demands of any CPS. One example that offers some promising contribution is the forensics-by-design approach, where forensics efforts are enabled as built-in capabilities in CPS incorporated throughout the development process. As a result, when a security incident occurs, the CPS equipped with these techniques will have built-in measures to provide investigators with the necessary data for the forensics.

Yet, there is room for more enhancements on current approaches to further incorporate fine grain data collecting, advanced algorithmic analysis, and create additional methods and tools to support the forensics activities. Since collecting and analyzing data is a natural feature in CPS, we proposed the data-driven CPS forensics as a viable direction to create effective and efficient CPS forensics tools. We discussed future development and research directions for improving CPS forensics approaches. There is a huge gap to fill and we identified some examples for the investigation approaches that include both the physical and cyber parts of CPS. We also proposed adopting an engineering process approach for identifying forensics requirements, designing appropriate methods, and implementing and testing them in line with the system development stages.

Unfortunately, we did not have room to delve deeper into the organizational and legal challenges, except when they were directly relevant to a technical aspect. The topic is broad and challenges and possible approaches to handle all dimensions are too many to cover in one paper, so we opted to focus mostly on the technical aspects. However, we plan to delve deeper in this direction and investigate the issues further in the future.

Author Contributions: All authors contributed to various sections in the paper according to their background. N.M. and J.A.-J. wrote the main sections of the paper. I.J. contributed to the sections on security attacks on CPS and the technical dimension of CPS forensics. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Lee, E.A. Cyber physical systems: Design challenges. In Proceedings of the 11th IEEE Symposium on Object Oriented Real-Time Distributed Computing (ISORC), Orlando, FL, USA, 5–7 May 2008.
2. Lee, J.; Bagheri, B.; Kao, H. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23. [CrossRef]
3. Mohamed, N.; Al-Jaroodi, J.; Lazarova-Molnar, S. Leveraging the Capabilities of Industry 4.0 for Improving Energy Efficiency in Smart Factories. *IEEE Access* **2019**, *7*, 18008–18020. [CrossRef]
4. Lee, I.; Sokolsky, O.; Chen, S.; Hatcliff, J.; Jee, E.; Kim, B.; King, A.; Mullen-Fortino, M.; Park, S.; Roederer, A.; et al. Challenges and research directions in medical cyber–physical systems. *Proc. IEEE* **2011**, *100*, 75–90.
5. Mohamed, N.; Al-Jaroodi, J. The Impact of Industry 4.0 on Healthcare System Engineering. In Proceedings of the 13th Annual IEEE International Systems Conference (SYSCON), Orlando, FL, USA, 8–11 April 2019; pp. 431–437.
6. Schmidt, M.; Åhlund, C. Smart buildings as Cyber-Physical Systems: Data-driven predictive control strategies for energy efficiency. *Renew. Sustain. Energy Rev.* **2018**, *99*, 742–756. [CrossRef]
7. Lazarova-Molnar, S.; Shaker, H.R.; Mohamed, N. Reliability of Cyber Physical Systems with Focus on Building Management Systems. In Proceedings of the IEEE Int'l Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, USA, 9–11 December 2016.
8. Deka, L.; Khan, S.M.; Chowdhury, M.; Ayres, N. Transportation cyber-physical system and its importance for future mobility. In *Transportation Cyber-Physical Systems*; Elsevier: Amsterdam, The Netherlands, 2018; pp. 1–20.
9. Rajkumar, R.; Lee, I.; Sha, L.; Stankovic, J. Cyber-physical systems: The next computing revolution. In Proceedings of the Design Automation Conference, Anaheim, CA, USA, 13–18 June 2010; pp. 731–736.
10. Karnouskos, S. Stuxnet worm impact on industrial cyber-physical system security. In Proceedings of the IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, Victoria, Australia, 7–10 November 2011; pp. 4490–4494.
11. Viganò, E.; Loi, M.; Yaghmaei, E. Cybersecurity of Critical Infrastructure. In *The Ethics of Cybersecurity*; Christen, M., Gordijn, B., Loi, M., Eds.; The International Library of Ethics, Law and Technology, Springer: Cham, Switzerland, 2020; Volume 21.
12. Al-Jaroodi, J.; Mohamed, N. PsCPS: A Distributed Platform for Cloud and Fog Integrated Smart Cyber-Physical Systems. *IEEE Access* **2018**, *6*, 41432–41449. [CrossRef]
13. Nazarenko, A.A.; Camarinha-Matos, L.M. Towards collaborative cyber-physical systems. In Proceedings of the International Young Engineers Forum (YEF-ECE), Costa de Caparica (Lisbon), Portugal, 5 May 2017; pp. 12–17.
14. Khalid, A.; Kirisci, P.; Khan, Z.H.; Ghrairi, Z.; Thoben, K.D.; Pannek, J. Security framework for industrial collaborative robotic cyber-physical systems. *Comput. Ind.* **2018**, *97*, 132–145. [CrossRef]
15. Al-Jaroodi, J.; Mohamed, N.; Jawhar, I. A service-oriented middleware framework for manufacturing industry 4.0. *ACM SIGBED Rev.* **2018**, *15*, 29–36. [CrossRef]

16. Simmon, E.; Kim, K.S.; Subrahmanian, E.; Lee, R.; De Vaulx, F.; Murakami, Y.; Zettsu, K.; Sriram, R.D. *A Vision of Cyber-Physical Cloud Computing for Smart Networked Systems*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2013.
17. Lyman, M.D. *Criminal Investigation: The Art and the Science*; Prentice Hall: Upper Saddle River, NJ, USA, 2001.
18. Bell, S. *Crime and Circumstance: Investigating the History of Forensic Science*; ABC-CLIO: Santa Barbara, CA, USA, 2008.
19. Catts, E.P.; Goff, M.L. Forensic entomology in criminal investigations. *Annu. Rev. Entomol.* **1992**, *37*, 253–272. [CrossRef]
20. Allen, W.H. Computer forensics. *IEEE Secur. Priv.* **2005**, *3*, 59–62. [CrossRef]
21. Casey, E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*; Academic Press: Cambridge, MA, USA, 2011.
22. *Handbook of Computer Crime Investigation: Forensic Tools and Technology*; Casey, E. (Ed.) Elsevier: Amsterdam, The Netherlands, 2001.
23. Taylor, R.W.; Fritsch, E.J.; Liederbach, J. *Digital Crime and Digital Terrorism*; Prentice Hall Press: Upper Saddle River, NJ, USA, 2014.
24. Reith, M.; Carr, C.; Gunsch, G. An examination of digital forensic models. *Int. J. Digit. Evid.* **2002**, *1*, 1–12.
25. Wang, Y.; Lee, H.C. Research on some relevant problems in computer forensics. In Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 22–23 March 2013; Atlantis Press: Paris, France, 2013.
26. Andersson, V. Standards and Methodologies for Evaluating Digital Forensics Tools: Developing and Testing a New Methodology. Bachelor's Thesis, Halmstad University, Halmstad, Sweden, 2018.
27. Choi, K.-S.; Lee, C.S.; Louderback, E.R. Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Springer Nature Switzerland AG: Cham, Switzerland, 2020; pp. 27–43.
28. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-physical systems security—A survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831. [CrossRef]
29. Ashibani, Y.; Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions. *Comput. Secur.* **2017**, *68*, 81–97. [CrossRef]
30. Wang, E.Y.; Ye, Y.; Xu, X.; Yiu, S.M.; Hui, L.C.K.; Chow, K.P. Security issues and challenges for cyber physical system. In Proceedings of the IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing, Hangzhou, China, 18–20 December 2010; pp. 733–738.
31. Alguliyev, R.; Imamverdiyev, Y.; Sukhostat, L. Cyber-physical systems and their security issues. *Comput. Ind.* **2018**, *100*, 212–223. [CrossRef]
32. Neuman, C. Challenges in security for cyber-physical systems. In *DHS Workshop on Future Directions in Cyber-Physical Systems Security*; 2009; pp. 22–24. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.152.973&rep=rep1&type=pdf (accessed on 7 July 2020).
33. Banerjee, A.; Venkatasubramanian, K.K.; Mukherjee, T.; Gupta, S.K.S. Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. *Proc. IEEE* **2011**, *100*, 283–299. [CrossRef]
34. Burg, A.; Chattopadhyay, A.; Lam, K.Y. Wireless communication and security issues for cyber-physical systems and the Internet-of-Things. *Proc. IEEE* **2017**, *106*, 38–60. [CrossRef]
35. Cardenas, A.; Amin, S.; Sinopoli, B.; Giani, A.; Perrig, A.; Sastry, S. Challenges for securing cyber physical systems. In *Workshop on Future Directions in Cyber-Physical Systems Security*; 2009. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.152.5198&rep=rep1&type=pdf (accessed on 7 July 2020).
36. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber–physical system security for the electric power grid. *Proc. IEEE* **2011**, *100*, 210–224. [CrossRef]
37. Sun, C.C.; Liu, C.C.; Xie, J. Cyber-physical system security of a power grid: State-of-the-art. *Electronics* **2016**, *5*, 40. [CrossRef]
38. Huang, S.; Zhou, C.J.; Yang, S.H.; Qin, Y.Q. Cyber-physical system security for networked industrial processes. *Int. J. Autom. Comput.* **2015**, *12*, 567–578. [CrossRef]
39. Wells, L.J.; Camelio, J.A.; Williams, C.B.; White, J. Cyber-physical security challenges in manufacturing systems. *Manuf. Lett.* **2014**, *2*, 74–77. [CrossRef]

40. Wurm, J.; Jin, Y.; Liu, Y.; Hu, S.; Heffner, K.; Rahman, F.; Tehranipoor, M. Introduction to cyber-physical system security: A cross-layer perspective. *IEEE Trans. Multi-Scale Comput. Syst.* **2016**, *3*, 215–227. [CrossRef]
41. DiMase, D.; Collier, Z.A.; Heffner, K.; Linkov, L. Systems engineering framework for cyber physical security and resilience. *Environ. Syst. Decis.* **2015**, *35*, 291–300. [CrossRef]
42. Hahn, A.; Thomas, R.K.; Lozano, I.; Cardenas, A. A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *11*, 39–50. [CrossRef]
43. Ruan, K.; Carthy, J.; Kechadi, T.; Crosbie, M. Cloud forensics. In *IFIP International Conference on Digital Forensics*; Springer: Heidelberg/Berlin, Germany, 2011; pp. 35–46.
44. Ruan, K.; Carthy, J.; Kechadi, T.; Baggili, I. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digit. Investig.* **2013**, *10*, 34–43. [CrossRef]
45. Dykstra, J.; Sherman, A.T. *Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies*; ADFSL Conference on Digital Forensics, Security and Law: Richmond, VA, USA, 2011.
46. Alex, M.E.; Kishore, R. Forensics framework for cloud computing. *Comput. Electr. Eng.* **2017**, *60*, 193–205. [CrossRef]
47. Huang, C.; Lu, R.; Choo, K.K.R. Vehicular fog computing: Architecture, use case, and security and forensic challenges. *IEEE Commun. Mag.* **2017**, *55*, 105–111. [CrossRef]
48. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.A.; Choudhury, N.; Kumar, V. Security and privacy in fog computing: Challenges. *IEEE Access* **2017**, *5*, 19293–19304. [CrossRef]
49. Esposito, C.; Castiglione, A.; Pop, F.; Choo, K.K.R. Challenges of connecting edge and cloud computing: A security and forensic perspective. *IEEE Cloud Comput.* **2017**, *4*, 13–17. [CrossRef]
50. Mylonas, A.; Meletiadis, V.; Tsoumas, B.; Mitrou, L.; Gritzalis, D. Smartphone forensics: A proactive investigation scheme for evidence acquisition. In *IFIP International Information Security Conference*; Springer: Heidelberg/Berlin, Germany, 2012; pp. 249–260.
51. Mylonas, A.; Meletiadis, V.; Mitrou, L.; Gritzalis, D. Smartphone sensor data as digital evidence. *Comput. Secur.* **2013**, *38*, 51–75. [CrossRef]
52. Grover, J. Android forensics: Automated data collection and reporting from a mobile device. *Digit. Investig.* **2013**, *10*, S12–S20. [CrossRef]
53. Mahalik, H.; Tamma, R.; Bommisetty, S. *Practical Mobile Forensics*; Packt Publishing Ltd.: Birmingham, UK, 2016.
54. MacDermott, A.; Baker, T.; Shi, Q. Iot forensics: Challenges for the ioa era. In Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5.
55. Meffert, C.; Clark, D.; Baggili, I.; Breitinger, F. Forensic State Acquisition from Internet of Things (FSAIoT) A general framework and practical approach for IoT forensics through IoT device state acquisition. In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August–2 September 2017; pp. 1–11.
56. Yaqoob, I.; Hashem, I.A.T.; Ahmed, A.; Kazmi, S.A.; Hong, C.S. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Gener. Comput. Syst.* **2019**, *92*, 265–275. [CrossRef]
57. Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of Things security and forensics: Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *78*, 544–546. [CrossRef]
58. Ahmed, I.; Obermeier, S.; Naedele, M.; Richard, G.G., III. Scada systems: Challenges for forensic investigators. *Computer* **2012**, *45*, 44–51. [CrossRef]
59. Elhoseny, M.; Hosny, A.; Hassanien, A.E.; Muhammad, K.; Sangaiah, A.K. Secure automated forensic investigation for sustainable critical infrastructures compliant with green computing requirements. *IEEE Trans. Sustain. Comput.* **2017**, *5*, 174–191. [CrossRef]
60. Hilal, H.; Nangim, A. Network security analysis SCADA system automation on industrial process. In Proceedings of the 2017 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP), Jakarta, Indonesia, 21–23 November 2017; pp. 1–6.
61. Sohl, E.; Fielding, C.; Hanlon, T.; Rrushi, J.; Farhangi, H.; Howey, C.; Carmichael, K.; Dabell, J. A field study of digital forensics of intrusions in the electrical power grid. In Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, Denver, CO, USA, 12 October 2015; pp. 113–122.
62. Do, Q.; Martini, B.; Choo, K.K.R. Cyber-physical systems information gathering: A smart home case study. *Comput. Netw.* **2018**, *138*, 1–12. [CrossRef]

63. Baig, Z.A.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K.; et al. Future challenges for smart cities: Cyber-security and digital forensics. *Digit. Investig.* **2017**, *22*, 3–13. [CrossRef]
64. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE Commun. Mag.* **2018**, *56*, 50–57. [CrossRef]
65. Al Faruque, M.A.; Chhetri, S.R.; Canedo, A.; Wan, J. *Forensics of Thermal Side-Channel in Additive Manufacturing Systems*; University of California: Irvine, CA, USA, 2016.
66. North America Electric Reliability Corp, Defense Use Case. *Analysis of the Cyber Attack on the Ukrainian Power Grid*; SANS Ind. Control Syst.: Wachington, DC, USA, 2016; Tech. Rep.
67. Bronk, C.; Tikk-Ringas, E. The Cyber Attack on Saudi Aramco. *Survival* **2013**, *55*, 81–96. [CrossRef]
68. Lindsay, J.R. Stuxnet and the Limits of Cyber Warfare. *Secur. Stud.* **2013**, *22*, 365–404. [CrossRef]
69. Al-Mhiqani, M.N.; Ahmad, R.; Yassin, W.; Hassan, A.; Abidin, Z.Z.; Ali, N.S.; Abdulkareem, K.H. Cyber-security incidents: A review cases in cyber-physical systems. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 499–508.
70. Orojloo, H.; Azgomi, M.A. A method for evaluating the consequence propagation of security attacks in cyber–physical systems. *Future Gener. Comput. Syst.* **2017**, *67*, 57–71. [CrossRef]
71. AlTawy, R.; Youssef, A.M. Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. *IEEE Access* **2016**, *4*, 959–979. [CrossRef]
72. Plumer, B. It's Way too Easy to Cause a Massive Blackout in the US. in Vox. Available online: https://www.vox.com/2014/4/14/5604992/us-power-grid-vulnerability (accessed on 30 June 2020).
73. Zatyko, K. Defining Digital Forensics. *Forensic Mag.* **2007**, *4*, 18–22.
74. Nelson, B.; Phillips, A.; Steuart, C. *Guide to Computer Forensics and Investigations*, 5th ed.; Cengage Learning: Boston, MA, USA, 2016.
75. Pilli, E.S.; Joshi, R.C.; Niyogi, R. Network forensic frameworks: Survey and research challenges. *Digit. Investig.* **2010**, *7*, 14–27. [CrossRef]
76. Han, S.; Xie, M.; Chen, H.H.; Ling, Y. Intrusion detection in cyber-physical systems: Techniques and challenges. *IEEE Syst. J.* **2014**, *8*, 1052–1062.
77. Mitchell, R.; Chen, I.R. A survey of intrusion detection techniques for cyber-physical systems. *ACM Comput. Surv. (CSUR)* **2014**, *46*, 55. [CrossRef]
78. E-Government Act of 2002, US Department of Justice. Available online: https://www.justice.gov/opcl/e-government-act-2002 (accessed on 1 June 2020).
79. Bhaimia, S. The General Data Protection Regulation: The next generation of EU data protection. *Leg. Inf. Manag.* **2018**, *18*, 21–28. [CrossRef]
80. Catea, R.M. Challenges of the Not-So-Far Future: EU Robotics and AI Law in Business. *Chall. Knowl. Soc.* **2018**, 213–216.
81. Huang, J.; Ling, Z.; Xiang, T.; Wang, J.; Fu, X. When digital forensic research meets laws. In Proceedings of the 32nd International Conference on Distributed Computing Systems Workshops, Macau, China, 18–21 June 2012.
82. Montasari, R.; Hill, R. Next-generation digital forensics: Challenges and future paradigms. In Proceedings of the 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 16–18 January 2019.
83. Clever, S.; Crago, T.; Polka, A.; Al-Jaroodi, J.; Mohamed, N. Ethical Analyses of Smart City Applications. *Urban Sci.* **2018**, *2*, 96. [CrossRef]
84. Gross, O. Legal Obligations of States Directly Affected by Cyber-Incidents. *Cornell Int. Law J.* **2015**, *48*, 481.
85. Awad, R.A.; Beztchi, S.; Smith, J.M.; Lyles, B.; Prowell, S. Tools, techniques, and methodologies: A survey of digital forensics for scada systems. In Proceedings of the 4th Annual Industrial Control System Security Workshop, San Juan, PR, USA, 4 December 2018; pp. 1–8.
86. Mishra, S. Forensic Investigation Framework for Complex Cyber Attack on Cyber Physical System by Using Goals/Sub-goals of an Attack and Epidemics of Malware in a System. In *Recent Trends in Communication, Computing, and Electronics*; Springer: Singapore, 2019; pp. 491–504.
87. Aliabadi, M.R.; Kamath, A.A.; Gascon-Samson, J.; Pattabiraman, K. ARTINALI: Dynamic invariant detection for cyber-physical system security. In Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering, Paderborn, Germany, 4–8 September 2017; pp. 349–361.

88. Vollmer, T.; Manic, M. Cyber-physical system security with deceptive virtual hosts for industrial control networks. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1337–1347. [CrossRef]
89. Abedi, M.; Sedaghat, S. Crawler and Spiderin usage in Cyber-Physical Systems Forensics. *OIC-CERT J. Cyber Secur.* **2018**, *1*, 53–61.
90. Alrimawi, F.; Pasquale, L.; Mehta, D.; Nuseibeh, B. I've seen this before: Sharing cyber-physical incident knowledge. In Proceedings of the 1st International Workshop on Security Awareness from Design to Deployment, Gothenburg, Sweden, 27 May–3 June 2018; pp. 33–40.
91. Chan, R.; Chow, K.P. Forensic analysis of a Siemens programmable logic controller. In *International Conference on Critical Infrastructure Protection*; Springer: Cham, Switzerland, 2016; pp. 117–130.
92. Abeykoon, I.; Feng, X. A forensic investigation of the robot operating system. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 851–857.
93. Al-Sharif, Z.A.; Al-Saleh, M.I.; Alawneh, L.M.; Jararweh, Y.I.; Gupta, B. Live forensics of software attacks on cyber–physical systems. *Future Gener. Comput. Syst.* **2020**, *108*, 1217–1229. [CrossRef]
94. Grispos, G.; Glisson, W.B.; Choo, K.R. Medical cyber-physical systems development: A forensics-driven approach. In Proceedings of the 2nd IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies, Philadelphia, PA, USA, 17–19 July 2017.
95. Ab Rahman, N.H.; Glisson, W.B.; Yang, Y.; Choo, K.K.R. Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Comput.* **2016**, *3*, 50–59. [CrossRef]
96. Jones, A.; Vidalis, S.; Abouzakhar, N. Information security and digital forensics in the world of cyber physical systems. In Proceedings of the 2016 Eleventh International Conference on Digital Information Management (ICDIM), Porto, Portugal, 19–21 September 2016; pp. 10–14.
97. Babiceanu, R.F.; Seker, R. Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. *Comput. Ind.* **2016**, *81*, 128–137. [CrossRef]
98. Guarino, A. Digital forensics as a big data challenge. In *ISSE 2013 Securing Electronic Business Processes*; Springer: Wiesbaden, Germany, 2013; pp. 197–203.
99. Zawoad, S.; Hasan, R. Digital forensics in the age of big data: Challenges, approaches, and opportunities. In Proceedings of the 17th International Conference on High Performance Computing and Communications, 7th International Symposium on Cyberspace Safety and Security, and 12th International Conference on Embedded Software and Systems, New York, NY, USA, 24–26 August 2015.
100. Al-Jaroodi, J.; Mohamed, N. Blockchain in Industries: A Survey. *IEEE Access* **2019**, *7*, 36500–36515. [CrossRef]
101. Mohamed, N.; Al-Jaroodi, J. Applying blockchain in industry 4.0 applications. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 0852–0858.
102. Hakak, S.; Khan, W.Z.; Gilkar, G.A.; Imran, M.; Guizani, N. Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges. *IEEE Netw.* **2020**, *34*, 8–14. [CrossRef]
103. Melhem, A.; AlZoubi, O.; Mardini, W.; Yassein, M.B. Applications of blockchain in smart cities. In Proceedings of the 2nd International Conference on Data Science, E-Learning and Information Systems, Dubai, Arab Emirate, 2–5 December 2019.
104. Tankard, C. Advanced persistent threats and how to monitor and deter them. *Netw. Secur.* **2011**, *8*, 16–19. [CrossRef]
105. Cambiaso, E.; Papaleo, G.; Chiola, G.; Aiello, M. Slow DoS attacks: Definition and categorization. *Int. J. Trust. Manag. Comput. Commun.* **2013**, *1*, 300–319. [CrossRef]
106. Thuraisingham, B.; Kantarcioglu, M.; Hamlen, K.; Khan, L.; Finin, T.; Joshi, A.; Oates, T.; Bertino, E. A data driven approach for the science of cyber security: Challenges and directions. In Proceedings of the IEEE 17th International Conference on Information Reuse and Integration (IRI), Pittsburgh, PA, USA, 28–30 July 2016; pp. 1–10.
107. Ovelgönne, M.; Dumitraş, T.; Prakash, B.A.; Subrahmanian, V.S.; Wang, B. Understanding the relationship between human behavior and susceptibility to cyber attacks: A data-driven approach. *ACM Trans. Intell. Syst. Technol. (TIST)* **2017**, *8*, 51. [CrossRef]
108. Siminoff, J.; Mitura, M.J.; Amazon Technologies Inc. Behavior-Aware Security Systems and Associated Methods. U.S. Patent Application 16/001,627, 13 December 2018.

109. Liu, Q.; Li, P.; Zhao, W.; Cai, W.; Yu, S.; Leung, V.C. A survey on security threats and defensive techniques of machine learning: A data driven view. *IEEE Access* **2018**, *6*, 12103–12117. [CrossRef]
110. Uhlemann, T.H.J.; Lehmann, C.; Steinhilper, R. The digital twin: Realizing the cyber-physical production system for industry 4.0. *Procedia Cirp* **2017**, *61*, 335–340. [CrossRef]
111. Poudel, S.; Ni, Z.; Malla, N. Real-time cyber physical system testbed for power system security and control. *Int. J. Electr. Power Energy Syst.* **2017**, *90*, 124–133. [CrossRef]
112. Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Trans. Smart Grid* **2013**, *4*, 847–855. [CrossRef]
113. Covington, M.J.; Fogla, P.; Zhan, Z.; Ahamad, M.A. A context-aware security architecture for emerging applications. In Proceedings of the 18th Annual Computer Security Applications Conference, Las Vegas, NV, USA, 9–13 December 2002; pp. 249–258.