Article

Cyber-Physical Systems and Smart Cities in India: Opportunities, Issues, and Challenges

Md. Onais Ahmad [1], Mohd Abdul Ahad [1,*], M. Afshar Alam [1], Farheen Siddiqui [1] and Gabriella Casalino [2]

[1] Department of Computer Science and Engineering, Jamia Hamdard, New Delhi 110062, India; oahmad@jamiahamdard.ac.in (M.O.A.); aalam@jamiahamdard.ac.in (M.A.A.); fsiddiqui@jamiahamdard.ac.in (F.S.)

[2] Department of Computer Science, University of Bari Aldo Moro, 70125 Bari, Italy; gabriella.casalino@uniba.it

* Correspondence: aahad@jamiahamdard.ac.in

Abstract: A large section of the population around the globe is migrating towards urban settlements. Nations are working toward smart city projects to provide a better wellbeing for the inhabitants. Cyber-physical systems are at the core of the smart city setups. They are used in almost every system component within a smart city ecosystem. This paper attempts to discuss the key components and issues involved in transforming conventional cities into smart cities with a special focus on cyber-physical systems in the Indian context. The paper primarily focuses on the infrastructural facilities and technical knowhow to smartly convert classical cities that were built haphazardly due to overpopulation and ill planning into smart cities. It further discusses cyber-physical systems as a core component of smart city setups, highlighting the related security issues. The opportunities for businesses, governments, inhabitants, and other stakeholders in a smart city ecosystem in the Indian context are also discussed. Finally, it highlights the issues and challenges concerning technical, financial, and other social and infrastructural bottlenecks in the way of realizing smart city concepts along with future research directions.

Keywords: CPS; smart cities; smart governance; smart economy; security

1. Introduction

There is no universal definition of a smart city [1]. Different regions connote its meaning differently. Every country has its own conceptualization of a smart city. It varies from country to country, city to city, and place to place [2]. Every country has their own set of requirements and abilities and thus has a different viewpoint and willingness to reform, which affects the migration from classical city setups to urban smart city settlements [3]. In this paper, we aim to give an overview of the smart city setups along with the opportunities, issues, and challenges associated with their successful implementation. With the rapid migration of inhabitants towards urban settlements, governments and policymakers face huge challenges [4]. A typical smart city setup involves facilities equipped with smart and state-of-the-art technology which includes smart transportation, smart energy, smart education, smart healthcare, smart sanitation and waste management, and smart governance, etc. [5]. In the present era of technological advancements, almost everything is converging into digitalization. In the same manner, the word "smart" is being applied everywhere and in every field [6]. With the rapid growth in the economy, the role of digitalization is highly critical to upgrade infrastructural support including physical, societal and institutional. This transformation is seen as a probable solution to several inherent and obvious city problems since it focuses on smart governance, smart IT and Communication, smart environment, smart buildings, smart businesses, and smart transportation, etc. [7]. Information Communication Technology (ICT) is considered the backbone of any smart city initiative; in the absence of ICT, imagining a smart city is baseless and will fail [8]. Smart city core infrastructural support systems such as sensor networks, IoT and wireless devices, and

well-equipped data centers, etc., constitute vital infrastructural mechanisms that provide the key enabling services to the smart city. Smart cities are certainly the future habitat of citizens around the globe; hence, it will be a great infrastructural asset for them. Smart city projects can be thought of as an area of opportunity for all stakeholders, especially for the infrastructural companies as well as developers [9]. In large countries such as India, demographics and diversity pose great challenges as well as opportunities. Naturally, smart city projects will attract high investment and a network of state-of-the-art technology that will create environmentally sustainable solutions, smooth operational efficiencies, and better civic amenities for urban populations and citizens.

The rest of the paper is organized as follows. Section 2 discusses the concept of cyber-physical systems in the context of smart cities and the underlying security threats. Section 3 highlights the enabling technologies for smart city setups. Section 4 provides the opportunities, issues, and challenges associated with the successful realization of smart city ecosystems. The final Section 5 provides the discussion and conclusion.

1.1. Key Action Areas of Smart City

A typical smart city consists of several key focus areas which need to be analyzed to provide holistic planning and designing. Figure 1 shows the key action areas of a typical smart city.
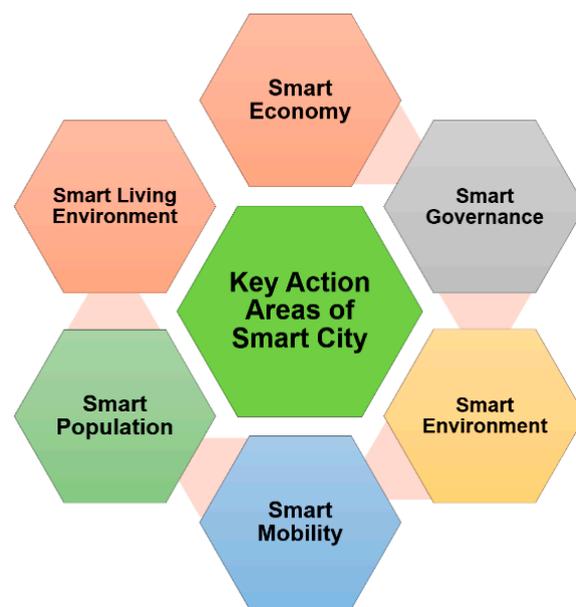
Figure 1. Key Action Areas of a Smart City.

1.1.1. Smart Economy

A smart economy relates to stimulating innovation as well as technological creativity based on scientific research, which cares for a smart environment and superior technology with an aim for attaining economic superiority and prosperity [10]. It further provides independence to a nation and creates equal economic opportunities for all stakeholders including inhabitants, governments, service providers, and other businesses, etc. [11–14].

1.1.2. Smart Governance

Smart governance constitutes performing governance through digital means, a city where public services use digital platforms, e.g., wi-fi and other ICT-based online services. All the policies and projects are implemented, tracked, and maintained using digital technologies to maintain transparency, tracking, and security. Smart governance also provides flexibility in terms of dynamic updating of policies and regulations based on realtime data from the citizens in the form of feedback, suggestions, polls, etc. Smart

governance follows the "citizen first" model of working where data-driven decisions are made to improve governance and involve greater participation by the citizens [15–18].

1.1.3. Smart Environment

A smart environment is an environment with miniature sensors embedded in it, which continuously collect data on the subjects and their surroundings for providing bettering realtime insights into different atmospheric and other environmental parameters such as temperature, pressure, humidity, and other impurities present in the air, water, and soil. A smart environment is an essential part of any smart city. Such an environment promotes the use of ICT for taking automated self-corrective measures when the threshold limit of any parameter is exceeded [19–23]. The monitoring of the environment can be achieved through specialized CPS made for the purpose [24,25]. The specifically designed CPS makes use of the data collected through the IoT devices to perform analytics and make data-driven decisions according to the current needs [26].

1.1.4. Smart Mobility

Smart mobility aims to automate classical transportation management through the use of sensors embedded in traffic signals, street lights, zebra crossings, etc. The concept of smart mobility ensures smooth traffic management and dynamic handling of traffic congestions, providing safe, secured, and free passage to emergency services, including ambulances, police vehicles, government vehicles, etc. Optimal routes are identified and conveyed for effective management and mobility of the masses. Smart mobility ensures pollution-free, environmentally-friendly, and congestion-free mobility leading to an effective means of sustainability in travel and transportation. CPS can be effectively used in smart mobility solutions to provide fault-tolerant and robust transportation across the smart city [27–29].

1.1.5. Smart Population

A smart population includes citizens participating in the development of the nation including various initiatives of the government in an environmentally-friendly, secure, and privacy-preserved manner. There should not be any bias, digital divide, or other forms of inequality concerning age, race, caste, or creed. CPS can be used to build intelligent and smart communities. The data collected and shared between different stakeholders through the CPS can be used to provide deeper insights into the real challenges and issues faced by the inhabitants [30–32].

1.1.6. Smart Living Environment

The concept regarding a smart living environment is related to good health and a hygienic environment. CPS can aid in the development of automated smart living spaces where the errors of the system or networks are mitigated automatically based on self-learning through AI/ML algorithms. These smart spaces are self-reliant and can scale as and when required to accommodate more and more entities. Since every aspect is largely automated, it is easier to identify and diagnose a fault, track the progress, as well as trace the system logs to identify any irregularities [33–35].

Apart from these, there are other areas that are of utmost importance to smart cities. These include smart energy and smart manufacturing. Smart energy systems aim to provide a clean source of energy to the users with minimum or no negative impact on the environment [36–38]. These include energy from renewable sources such as solar, etc. Smart manufacturing refers to adopting ICT for automation of all aspects in the manufacturing domain [39,40].

1.2. Major Contributions

The following are the major contributions of this paper.

- Comprehensive analysis of the CPS, highlighting its working mechanism, application areas, opportunities, issues, and challenges in its realization.
- Highlighting the advancements in CPS from an Indian perspective.
- Identifying the role of various enabling technologies in a smart city with regard to cyber-physical systems.

1.3. Smart Cities-Indian Perspective

The concept of smart cities in India poses several different kinds of issues and challenges. The size of the nation and the diverse population make India a unique case for smart city setups. Most of the existing cities are unplanned and have several issues of waterlogging, sanitation, proper water supply, etc. Tackling all these issues is a very challenging task. In a typical smart city architecture, cities are divided into different areas for better governance, administrative, and utility purposes, and each one keeps its service outlets [41]. The Indian government initiated the mission of smart city development in 2015 (https://smartcities.gov.in/. Accessed on: 12 September 2021). Initially, 20 cities were selected for the mission through an open competition. The core aim of the mission was to provide an underlying infrastructure and quality of life to the inhabitants of the city through sustainable, cost-effective, efficient, and environment-friendly measures. The development was planned by identifying key areas within the city limits and, in parallel, focusing on each selected area of development (http://mohua.gov.in/#skip. Accessed on: 14 September 2021). Figure 2 gives an overview of India's commitment to smart city initiatives (https://smartnet.niua.org/mis/drupal/scm.php. Accessed on: 17 September 2021).
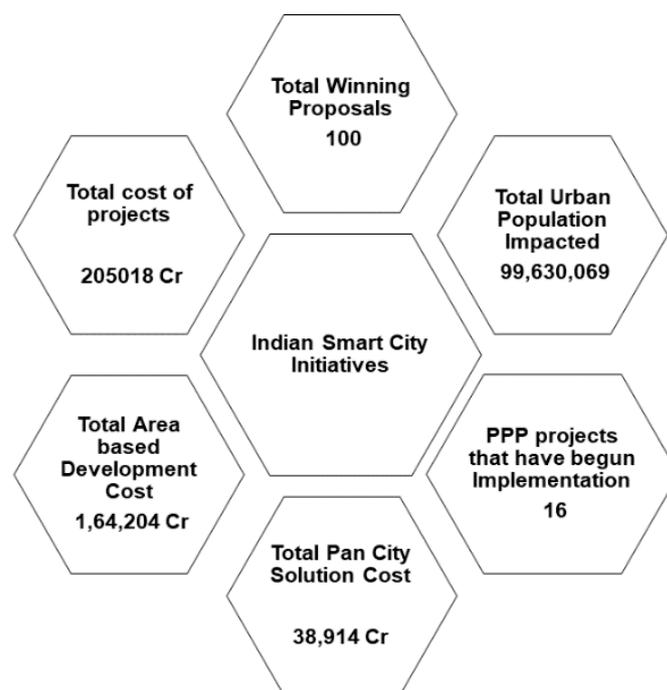
Figure 2. India's Commitment towards Smart City Initiatives.

2. Cyber-Physical Systems (CPS) in Smart Cities

Cyber-physical systems (CPS) were introduced in the year 2006 by Ellen Gill. The concept was based on the combination of cyber (computation and communication) and physical components (devices, gadgets, and systems) that can use smart computation techniques to interact with real-world objects [42]. Figure 3 shows the architectural components of a CPS [43–46].
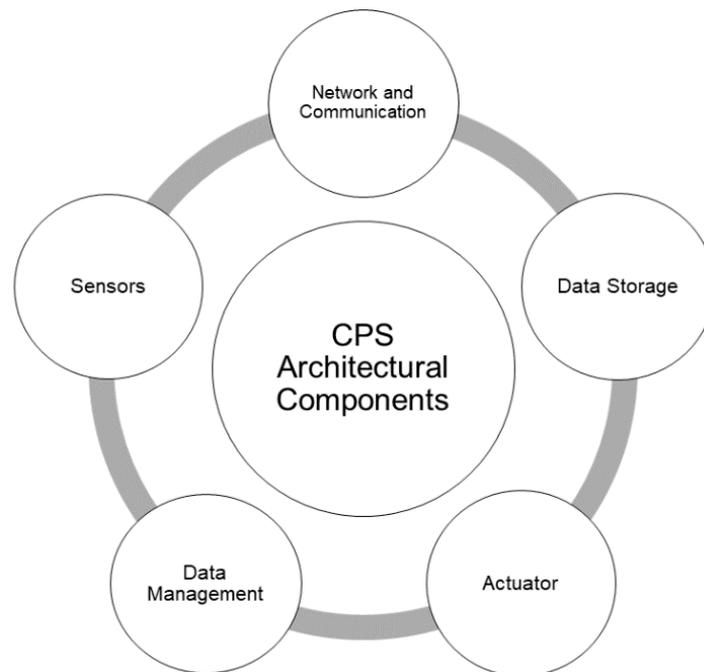
Figure 3. Architectural components of Cyber Physical Systems (CPS).

- Actuator

  The role of an actuator in a typical CPS is to convert the control command into mechanical work. The actuators may be susceptible to hacking where the illegitimate hackers can take control of the actuator device to alter the mechanical work being carried out. This may include locking/unlocking doors, starting, stopping, or changing the speed of clinical wearables, etc. Actuators are the actual controlling mechanism behind the CPS. Since there are multiple resources and services to be controlled, the choice of selecting an optimal actuator plays an important role. There are several actuator-selection approaches as discussed in [47,48].

- Data Management

  This module is responsible for managing the data that are being sensed by the sensors embedded in the different IoT devices in the CPS. This may include data cleaning, preprocessing, data standardization, normalization, etc. Effective management of data generated from sensors is highly crucial for extracting value and taking optimal decisions based on that data. Several data management issues that need to be resolved include selection of appropriate data management systems, data cleaning, and removing data outliers (if any), and security of data at rest and in transit. Apart from these issues, the choice of data management systems also depends upon the type of activity and application [49,50].

- Sensors and Sensing Module

  This module is responsible for sensing the data about the subject and its surroundings. The sensed data are transferred to the data management unit through the internet gateways. Wireless sensors networks (WSN) are the backbone of any CPS. The collection of multiple sensors in the WSN works in synchronization to integrate and perform the task of sensing the data. The data thus collected contain much deeper insights that were not possible with individual sensing capabilities [51,52]. Furthermore, optimal dynamic network topologies can be adopted to place the sensors at appropriate positions within the CPS ecosystem to cater to the needs of changing subjects and their surroundings. The concept of relay nodes is also adopted to provide multihop communication reducing the energy required for data transmission [53].

- Network and Communication

This module consists of communication protocols for establishing the connection among different entities within the CPS. This module governs all the communication including routing, rerouting, error handling, acknowledgments, etc. Several state-of-the-art approaches can be adopted for managing the communications within the CPS ecosystem. With a wide variety of diverse devices connected in a typical CPS, there are several issues and challenges, which include device schemas, data capturing formats, communication protocols, energy efficiency, etc. [54–56]. To overcome these issues several robust approaches have been proposed in the literature. In addition, SDN and NFV technology can also be adopted to control network communication more flexibly and optimally. SDN and NFV approaches provide a software-based controlling of the network parameters including congestion control, route management, placement of relay nodes, number and types of network hops, etc. [57,58].

- Data Storage Module

This module contains cloud and edge-based storage services where the sensed and cleansed data finally reside. It also includes cached data and metadata records. A typical CPS generates huge volumes of rapidly expanding big data. This massive amount of data needs specialized tools and techniques for storage and management. Several big data storage and management approaches, for example, Hadoop, Casandra, HDInsight, NoSQL, etc., can be used. It is generally considered appropriate to partition the data into smaller portions and store it in a distributed manner with an optimal number of copies to provide better control and immediate availability as and when required [59,60]. In [61], the authors proposed a large-scale framework for realtime monitoring in CPS. They used industrial CPS as a use-case to evaluate the effectiveness of the proposed approach.

2.1. Working of CPS

A typical CPS system tends to integrate physical components with the computational components present in cyberspace through a network. Once a successful connection is established, the physical processes can be controlled and managed through software programs. CPS provides abstraction by modeling the dynamics of physical processes with the help of software. This automated controlling of physical processes is improved by providing feedbacks through data generated by different connected entities within the CPS. As shown in Figure 4, a typical CPS can be considered as an embedded system with computations, communications, and control capabilities. In a transportation management CPS, the realtime data of the traffic conditions are captured through sensors embedded in the roads, traffic signals, footpaths, sign boards, etc. The number of vehicles passing through the footpaths or at a stationary position can be measured through the pressure measuring sensor chips embedded in the footpaths. Similarly, inductive loop detectors sensors are used to detect the number of vehicles arriving at any point on the road. The acoustic and ultrasonic sensors are used to measure pressure and sound waves produced through the friction between vehicle tires and roads lanes for identifying the speed and lane detection. These data are then fed into the CPS system to take dynamic decisions for updating traffic signals, enforcing speed limits, giving free passage to emergency services vehicles (if any). In addition, the duration of the signals is also managed dynamically based on the traffic conditions to manage the smooth flow of vehicles without congestion. Apart from the sensors embedded on the roadside signals, footpaths, and signboards, the users (as an entity of the CPS) also share data about realtime traffic conditions and alternative routes with the system to provide optimal management of traffic. Möller and Vakilzadian [28] discussed the different components of CPS for smart transportation. They showcased the importance of vehicle-to-vehicle communication, realtime feedback for traffic conditions, and the integration of information from different entities. Kukkala et al. [62] provided a survey of advanced driver assistance systems (ADAS). They described different hardware-based sensors and corresponding software used in ADAS highlighting the pros and cons of each. In similar ways, the environmental cyber-physical systems (ECPS) are designed to monitor the ecological conditions of the subject and its surroundings. The subject can be

any indoor unit (house, factory, building, etc.) and the surroundings include all the nearby outdoor areas of the subject. Criado et al. in [63] proposed a web socket-based approach for the integration of various heterogeneous components in a smart home environment to ensure interoperability and seamless connectivity. Through the help of smart dust (minute sensors based microelectromechanical systems) the different parameters of the environment such as light, temperature, pressure, humidity, composition of gases, magnetism, and chemicals, etc., can be sensed and detected [64]. Smart dust works on the principle of IEEE 802.11 b/g standards for wireless communications [65]. Different kinds of sensors such as trace metal sensors, radio isotopic sensors, compound detection sensors, etc., are used to detect the presence of environmental pollutants in the air, water, or soil [23,66]. The data collected from such sensors are processed and analyzed to take appropriate countermeasures. Similarly, motion detection sensors and temperature sensors are used in indoor units to control the different devices and appliances based on user preference and conveniences. This may include automatic controlling of AC units, turning off/on the lights, fans, and other appliances, with respect to user availability and preferences.
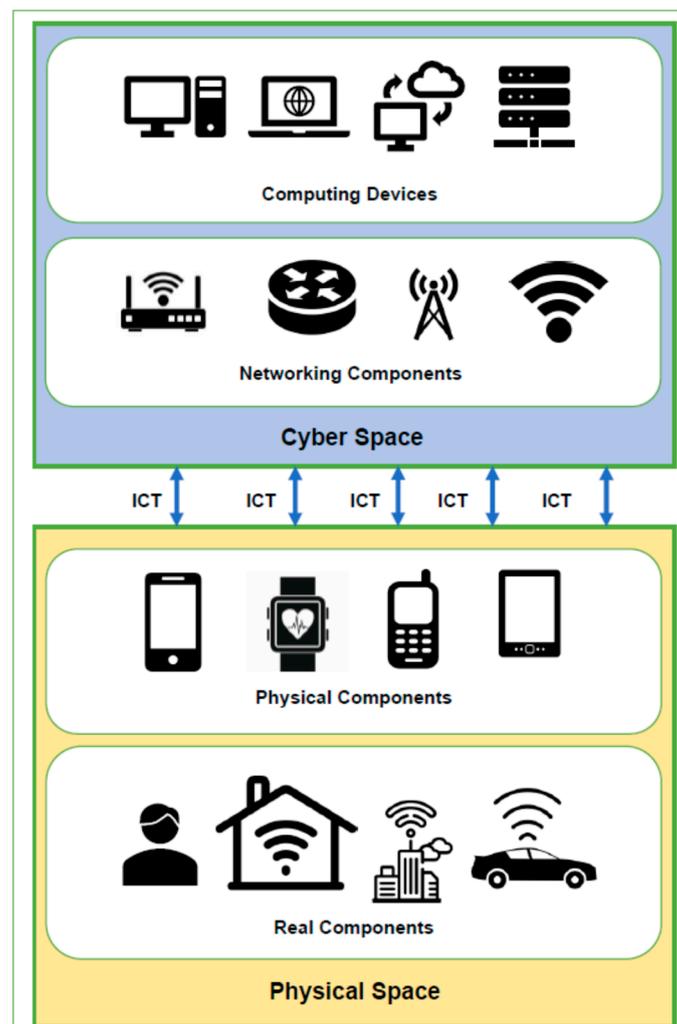
Figure 4. A typical CPS Diagram [45].

To explain the working of cyber physical systems, we use the example of the healthcare domain. The Medical CPS (MCPS) can collect and process data from the clinical and wearable sensors worn by the patients. The biosensors have the potential to sense the critical physiological parameters of the patient and send them to the computing and analytics unit for further processing. There are multiple advantages of biosensors, which include

noninvasive delivery of drugs (in the form of smart pills) and sensing of blood glucose parameters. Hussain and Park [67] proposed a portable EMG-based gait monitoring system. They further identified the effectiveness of myoelectric biomarkers for the classification of stroke-impaired muscular activity. Similarly, there are several other wearable devices such as EMG, ECG, and EEG devices, and sensors such as blood flow sensors and chemical sensors for identifying chemical concentration, PH value, and glucose concentration in the blood. Force sensors are used in kidney dialysis devices. The biosensors are used to sense enzymes, antibodies, and other microbes within the human body. Petropoulos et al. in [68] discussed an IMU-enabled posture monitor for identifying the wrong sitting posture through motion sensors attached to the back of the users. These devices and sensors are used in the medical CPS to provide valuable information about the condition of the patients. With medical CPS, the sensed data are cleaned, standardized, and finally forwarded to the processing and analytics unit to perform analysis. The type of processing depends upon the services required. For example, for realtime requests and queries, the data need to be processed as close to the source (of data generation) as possible. It is vital to provide an immediate response for the requested services. Further, processing the data close to the source reduces network latency and communication bottlenecks, if any. To do so, the MCPS uses an edge computing paradigm in which the sensed data are processed at the edge of the network to provide realtime or near realtime services [69]. Similarly, for non-immediate requests and services, the processing is completed on the cloud. Since moving the sensed data to the cloud is a bandwidth-hungry process, optimal routing and congestion controlling mechanisms are needed to reduce the time of data transfer. Wang et al. in [70] proposed an edge computing-based approach for mitigating coupling issues in CPS. The different wearable point-of-care devices, which are also equipped with miniature sensors are used to provide monitoring and analysis on the go or at homes as well [71–75]. Figure 5 shows a typical medical CPS.

A medical CPS as a whole consists of several components which include sensing, analysis, security, storage, and management. Each of these units has its specific functionality. The data collected from the patients in some cases are highly sensitive and thus must be protected from any kind of theft or hacking. To do so, the medical CPS makes use of different cryptographic techniques to encrypt the data before sending them across the network. Casalino et al. in [76], proposed the concept of fuzzy inference systems in telehealth for critical disease care. Similarly, there are several data management and storage techniques employed within the CPS, which provide optimal data storage and fetching as and when required by the care providers.

With the advancement in technologies including IoT, WSN, big data, and enhancement of computational capabilities, the concept of CPS is widely implemented across multiple domains. The applications of CPS can be found in diverse areas such as aerospace, healthcare, energy, transportation, manufacturing, etc. [77–81]. Smart city ecosystems can be viewed as a large-scale CPS implementation that facilitates the cooperation between various computational, communication, and physical aspects and also helps to provide a better quality of life. These CPS are an integration of components of different natures, which aim to control, manage, and monitor a physical process and also adapt to the changes based on the feedback. A CPS can be thought of as a driver of the smart city services having the capability to completely transform the way of life of the inhabitants. A CPS may be used to collect and share data about realtime traffic conditions, health conditions of the patients, environmental phenomenon, land-use planning, air/water/soil quality, structural health of buildings, roads, and other structures such as bridges, rail tracks, monuments, etc. Since it involves a complex integration of multiple miniature devices (sensors, actuators, and ICs) and larger devices (mobile phones, servers, and clouds), securing such systems is a very challenging task. There are always chances of data leakage and or security breaches from one or the other vulnerable systems or devices. Therefore, it is of utmost importance to implement granular and layered security mechanisms for such types of complex CPS. MFA can greatly help in providing an extra layer of security to the CPS, but we need to

make sure that implementing this extra layer of security is not an overhead and does not increase latency, thus compromising the primary aim of the CPS systems. Table 1 provides the applications of CPS in different domains.
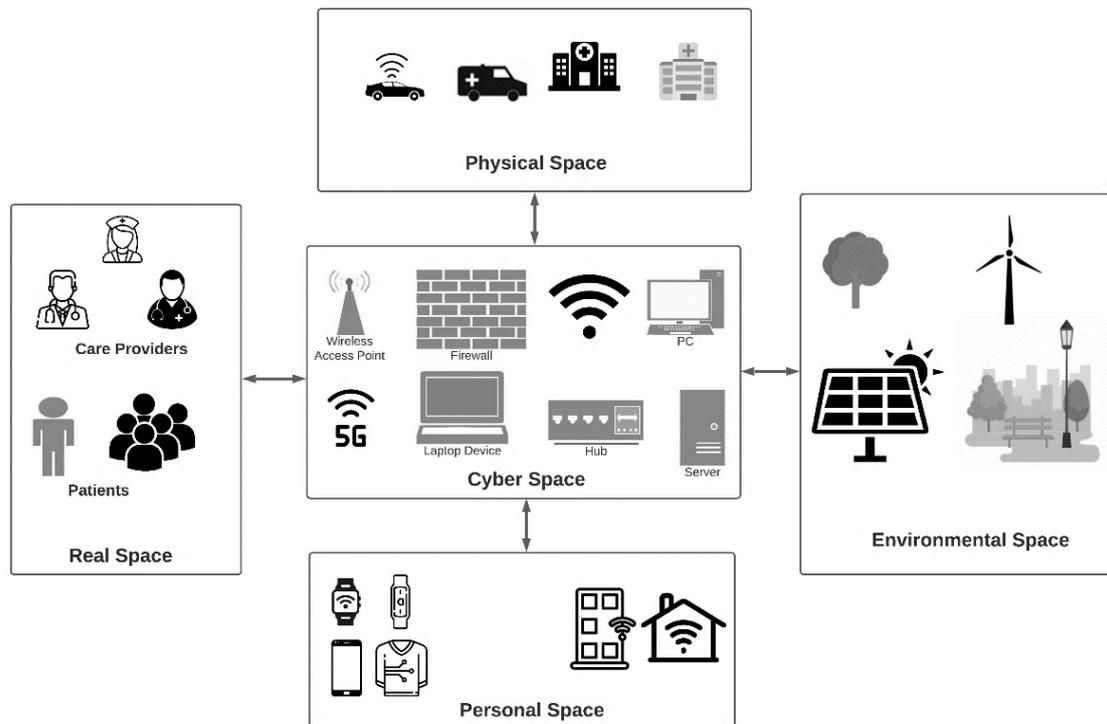
Figure 5. A typical medical CPS [45].

Table 1. Application areas of CPS.

S. No	Smart City Component	Application	Ref
1	Manufacturing	The manufacturing process can be automated to optimize the productivity of goods and enhance the delivery of services.	[82,83]
2	Healthcare	Smart Healthcare systems are designed for realtime monitoring of patients and support remote healthcare services using semiautomatic medical devices.	[76,84–87]
3	Transportation	A smart transportation system in a smart city uses embedded sensors for realtime information sharing and processing for traffic management. Advanced sensing, communication, control, and computations enable the efficient working of autonomous vehicles.	[88–92]
4	Energy	The integration of cyber and physical systems helps to provide a reliable, safe, and secure supply of energy and led to the development of smart grids.	[93,94]
5	Infrastructure	The use of sensors in buildings helps to minimize the overall cost of functioning by optimizing the processes based on the data analysis and feedback mechanism.	[95,96]

Table 1. *Cont.*

S. No	Smart City Component	Application	Ref
6	Agriculture	Regular monitoring of environmental conditions helps to improve agricultural production. Using IoT and sensor technologies helps to implement smart water management, soil monitoring, and efficient supply chains.	[97–99]
7	Education	CPS implementation into conventional education systems can help to develop smart learning environments where all entities can share information and data.	[100–109]
8	Business	The integration of smart techniques to enhance and automate business processes has led to the development of Industry 4.0.	[110–115]
9	Environment monitoring	CPS implementation in geographical areas such as rivers, forests, etc., can be used for remote monitoring and quick response systems. The process of monitoring can be completed using minimal energy and no human intervention in the circumstances of natural and manmade disasters.	[116,117]
10	Security	The information collected from various sensors and other connected devices can be processed for fast decision making and enhancing security and privacy in a smart city ecosystem.	[118–124]
11	Smart homes	Smart homes are one of the most widely adopted applications of CPS. The various components of a regular household such as a security camera, electronic devices, home assistants, etc., are connected to automate the various processes.	[125–130]

2.2. Security Threats in CPS with Respect to Smart Cities

Smart cities incorporate a broad range of cyber-physical systems (CPSs) to boost their efficiency by minimizing expenses and resources. These CPSs, such as smart healthcare, smart transportation, and smart grids, interact with the residents in an active, coordinated, and reliable manner, thereby strengthening the public infrastructure and lowering the living costs [131]. The incorporation of CPSs in smart cities aims to enhance transport, infrastructure, healthcare, safety, and other utilities, but these enhancements result in an elevated risk and susceptibility [132]. Moreover, linking additional devices to the current CPSs introduces additional security threats. The rapid use of CPSs in critical frameworks such as medical equipment and defense puts human lives at serious risk, owing to cyberattacks. In the context of smart cities, some of the security threats prevalent in CPSs are given below [130–133]

- The deployment of ICT-based smart vehicles enables malicious individuals to gain control of the automobile, endangering the lives of the driver and other passengers [131] The attacker might ask for a ransom to release control of the automobile. Similarly, hackers may encrypt important files on a CPS-connected device and ask the owner for a ransom to grant access (ransomware).
- The lack of security updates in CPS linked devices, together with device misconfiguration and the prevalent use of default passwords and settings, as well as the absence of encrypted communication between devices, also presents a serious security loophole. Similarly, poor credentials threaten the security of both the user and their business, as cybercriminals can set up remote sessions to track them. These intruders can identify a user's physical location by using IP addresses or GPS modules of the CPS devices [130–132].

- In a smart city, the prevalence of "actuators" that regulate the physical skeleton (filters, heating components, faucets, filters, etc.) renders the city vulnerable to physical damage if the systems are compromised [132,133].
- Artificial intelligence applications in CPSs are susceptible to data manipulation attacks where cybercriminals can steal sensitive information to generate superficially legitimate input to mislead the algorithm. These attacks could be driven by financial or political rivalry, powered by the tremendous expansion of built-in computing capacity.
- Hackers could seize control of CPS linked devices and use them to disrupt business activities, use them as spam email servers, or turn them into botnets for carrying out DDoS (Distributed Denial of Service) attacks. Individuals with malice can access all smart appliances such as televisions, cameras, and refrigerators, and transform them into attack carriers.

Emerging technologies such as software-determined networks (SDN), blockchain, and game theory have surfaced as promising solutions to alleviate the threats described above. Additionally, it is crucial that the vulnerabilities stemming from deployment settings and implemented technologies be addressed at the initial stages of design and individual security roles be defined for cybersecurity staff and administration in a smart city. Table 2 provides the summary of security attacks and their corresponding mitigation measures adopted in recent literature.

Table 2. Security Attacks in CPS.

S.No	Ref	Focus Area	Threats	Mitigation
1	[134]	Context-Aware CPS security. Provided the notion of context-awareness in CPS.	False data injection, DoS attacks	Different categories of context concerning CPS were identified and a corresponding security mechanism was proposed
2	[135]	CPS in operational technology	Near realtime cyber attacks	Trap-based monitoring systems were proposed using a big data fusion model
3	[136]	CPS for smart grid	Malicious adversaries	STREAM approach for improving integrity and availability
4	[137]	CPS for healthcare	Data theft, impersonation, user profiling attacks, etc.	Cognitive cybersecurity framework using AI
5	[138]	WSN in CPS	Internal and external threats in WSN	Several mitigation approaches were discussed along with a comparison among them
6	[139]	Cross-domain CPS security	DoS and DDoS attacks, hacking, etc.	A security analysis framework was proposed identifying both discrete and continuous signal information flow in cross domain CPS
7	[140]	CPS for pervasive health monitoring systems	BAN attacks	PSKA and CAAC mechanisms were proposed
8	[141]	Securing big data in CPS	Identified various big data security issues	Discussed various security mechanisms for big data security using Weibull distribution.
9	[142]	Security of sensors in CPS	False data injection, spoofing, etc.	Discussed sensor attacks on edge and point of positions. Proposed classification of different kinds of attacks on sensors.
10	[143]	CPS for industrial processes	Deception attacks, DoS attacks, etc.	The concept of intrusion tolerance was proposed to secure industrial control systems.

2.3. Current Developments in CPS in India

With the massive population and area of coverage, the Indian subcontinent poses its unique challenges. The administration in India is keenly focused on realizing the true potential of CPS. Many flagship programs are being organized which have invited academia and research institutions across the country to work on the development of interdisciplinary CPS (https://serbonline.in/ICPS/HomePage. Accessed on 15 September 2021). The national mission on ICPS is focused primarily on the development of cyber-physical systems to solve country-specific problems through the development of embedded systems using IoT for smart homes and services, promote entrepreneurship, social inclusion, etc. (https://nmicps.gov.in/Home/ICPSNMHOME/HomeNM. Accessed on 18 September 2021) One of the premier institutions in India IIT Guwahati launched Intelligent CPS for developing indigenous technologies (https://timesofindia.indiatimes.com/gadgets-news/iit-guwahati-launches-centre-for-intelligent-cyber-physical-systems/articleshow/86295156.cms. Accessed on 17 September 2021). Apart from these, there are several other initiatives started in India for developing state-of-the-art solutions for tackling societal issues and problems utilizing the concept of CPS.

3. Role of Technology in Smart Cities

In a smart city, technological literacy or knowledge is a significant factor for bringing intelligence to the city entities and services. This concept not only provides smart services to its citizens but also plays a pivotal role in good governance, as it provides inputs/feedbacks to the government [144]. Thus, it can be concluded that all these things cannot be achieved without technical support and facilities [145]. Another important technology that is highly significant for a smart city setup is two-way communication. It enables the interaction among different entities of the smart city ecosystem. Keeping the city's requirements, the government can plan and build that city in line with the citizen's needs. ICT, acting as synergic resources for a dynamic communication system between the citizens and the government enables government agencies to have very clear analytical views of the demand pattern of the citizens. ICT also helps in the collective intelligence (CI) that can be established for the optimization of resources with the support of analytics and deep learning [146].

3.1. Internet of Things

Internet of things (IoT) may be termed as the veins of the smart city as it is present in all entities of the smart city ecosystem and connects each dot (node), as every device of the smart city is required to be interconnected [146–148]. Such arrangements make it possible for the devices to connect and communicate amongst themselves and make decisions for the efficient management of the smart city services. Almost all smart cities are based on IoT for deciding and acting.

3.2. ICT and Sensors

It is imperative to have proper knowhow of the underlying technology for smart city development. Modern-day technologies such as IoT, deep and machine learning, geospatial, ICT, sensors, etc., are all needed for a comprehensive smart city experience [149]. Undoubtedly, ICT technology is a thread that can channel all data from every entity and stakeholders including utilities, waste management, better healthcare, etc., to surveil or monitor to provide improved services [150–152].

3.3. Artificial Intelligence

Artificial intelligence is considered the most important technology for smart city setups. With the ability to perform automated, data-dependent, precise, and human-independent decisions, AI systems are widely used in smart city ecosystems [153]. The various services of security surveillance, traffic management, healthcare, and governance, etc., are all being improved with the help of AI technology [154,155].

3.4. Blockchain Technology

Blockchain technology is applied in several domains including healthcare, supply chain, resource management, tracking and tracing, identification and authentication, etc. In the smart city ecosystem, blockchain technology can be used to provide improved authentication of entities, users, and services [156–164].

3.5. 5G and SDN Technology

The advancement in 5G technology has opened a new horizon of opportunities for the smart city ecosystem. Bandwidth-hungry tasks can be more easily carried out seamlessly through the use of 5G networks. 5G technology further provides better connectivity and faster data transmissions needed for realtime or near realtime applications and services [165–167]. The ability to control and manage the network dynamically through SDN provides flexibility in terms of improving the scalability and dynamic routing and rerouting of data packets in case of any hindrances in the network [168–170].

3.6. Deep Learning

Deep learning approaches provide deeper insights into the system and its components making it easier to take better and informed data-driven decisions. The unparalleled data analyzing capabilities of deep learning technology aid in the pre-identification of any errors or future conditions of the systems and their components to provide predictive analysis and maintenance of the faulty components [171–173].

4. Opportunities, Issues and Challenges in Smart Cities

This section provides the various opportunities, issues, and challenges associated with the realization of smart city initiatives [4–7,79,83,132–136,157–168].

4.1. Opportunities

Since India is a very large country in terms of area as well as population, there are several opportunities for stakeholders in smart city initiatives. Since there are large cities needing to be developed, there is consequently a large amount of work involved in the planning, development, and maintenance. The cost of such projects will be huge as already shown in Figure 5. Moreover, such projects will create job opportunities for several classes including skilled and unskilled laborers. Apart from this, many manufacturing and building construction opportunities will be created for medium and small-scale industries, apart from the MNCs. The development of smart cities serves two purposes. Firstly, it promotes reduction in resource usage, and secondly, it reduces resource wastage. Figure 6 highlights some of the opportunities of smart city initiatives [4,9,77–81,174].

4.1.1. Businesses and Manufacturing

With the large-scale adoption of smart city projects, MSME businesses are bound to grow. Raw materials, spare parts, construction materials, operational and maintenance infrastructure, etc., will provide new business opportunities for all small or large market players alike [174,175].

4.1.2. Jobs

The massive setups will require a large workforce at all levels for the completion of smart city projects. Skilled, semi-skilled, and unskilled labor will be required, and thus a large job market will be created with the large-scale adoption of smart city projects [176,177].

4.1.3. Innovations

With sustainability at the core of smart city initiatives, legacy approaches will be replaced by new and innovative approaches and mechanisms for performing tasks. Thus, it will promote and boost innovative capabilities. The Government of India is already aware of this fact and therefore massive national level open challenges and competitions are arranged

where they are inviting innovative solutions for the grassroots problems faced by the society, for example, Smart India Hackathon (https://www.aicte-india.org/Initiatives/smart-india-hackathon. Accessed on 29 October 2021), Atal Innovation Mission (https://aim.gov.in/. Accessed on 29 October 2021), Drug Discovery Hackathon (https://www.mygov.in/task/drug-discovery-hackathon-2020/. Accessed on 29 October 2021), etc.

| New Businesses |
| Innovations |
| Startups |
| Jobs |
| Manufacturing |
| Optimal Utilization of Resources |
| Promotes Sustainability |

Figure 6. Opportunities of Smart City Initiatives.

4.1.4. Startups

There are several issues and challenges that exist in classical city setups. For all such issues and challenges, the concept of startups has emerged in recent years in India. These startups identify the grassroots level basic problems of the society and provide innovative solutions to such problems. Smart city initiatives will surely boost the startup culture as there will be several intrinsic and extrinsic problems associated with such massive ecosystems, which may be hidden initially but may arise as the concept matures. Therefore, startups will be focused on solving such issues for providing better services to the inhabitants. The government is also focusing on promoting startup culture with several flagship initiatives, for example, Startup India (https://www.startupindia.gov.in/ Accessed on 30 October 2021), etc.

4.1.5. Optimal Utilization of Resources

One of the most crucial opportunities that smart city initiatives bring is the optimal utilization of resources. With intelligent and smart data-driven measures, city resources can be optimally utilized by the inhabitants and it can further promote a reduction in the wastage of valuable resources, for example, smart water meters can reduce water wastage, the smart grid can reduce electricity consumption, etc. [178,179].

4.1.6. Promotes Sustainability

The prime aim of smart city initiatives is to promote sustainability in every aspect. The data-driven mechanisms for different purposes through sustainable means are the key driving forces for attaining overall sustainability [180,181].

4.2. Issues and Challenges

There exist very unique issues and challenges in the development of smart city initiatives. They are broadly classified into five categories namely technical, socioeconomic, environmental, societal, and ethical, as detailed in Figure 7 [144–149,157–164].
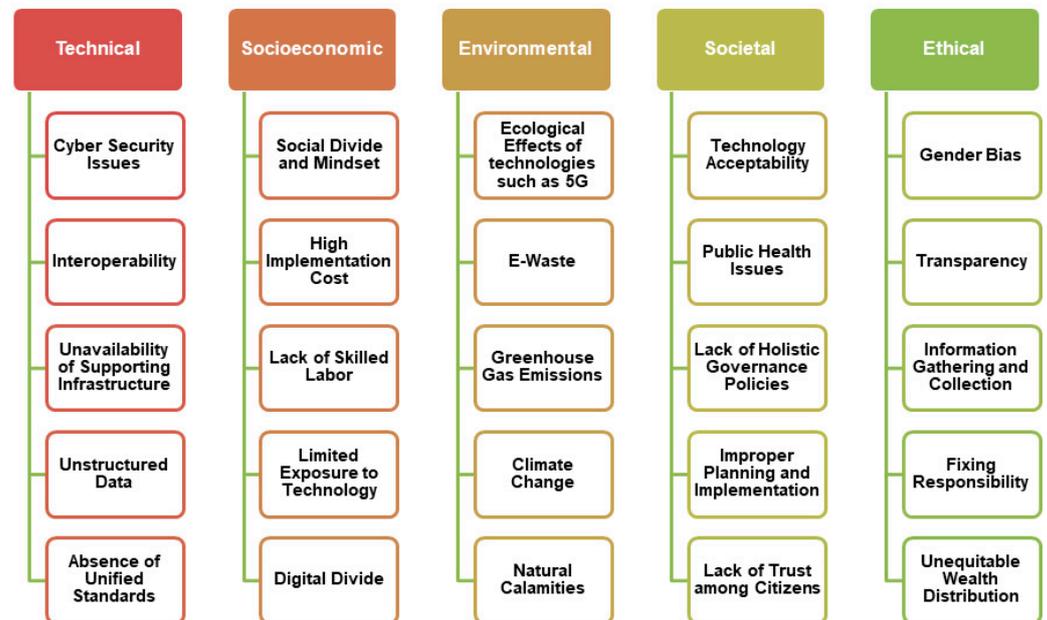
Technical	Socioeconomic	Environmental	Societal	Ethical
Cyber Security Issues	Social Divide and Mindset	Ecological Effects of technologies such as 5G	Technology Acceptability	Gender Bias
Interoperability	High Implementation Cost	E-Waste	Public Health Issues	Transparency
Unavailability of Supporting Infrastructure	Lack of Skilled Labor	Greenhouse Gas Emissions	Lack of Holistic Governance Policies	Information Gathering and Collection
Unstructured Data	Limited Exposure to Technology	Climate Change	Improper Planning and Implementation	Fixing Responsibility
Absence of Unified Standards	Digital Divide	Natural Calamities	Lack of Trust among Citizens	Unequitable Wealth Distribution

Figure 7. Issues and Challenges in Smart City Development.

4.2.1. Technical Issues

These issues comprise a lack of infrastructure, scarcity of technical knowhow, privacy, and security issues [4,77–81,133,134,144,157,164,165,172–178,181–188].

Lack of Infrastructure

The smart city ecosystem is heavily dependent upon a state-of-the-art infrastructure consisting of sophisticated network devices, sensors, IoT devices, heavy-duty servers, security devices, etc. These devices are not readily available or they are too expensive for some nations who have to search for more economical alternatives. The architectural scalability must pertain to the smart city so that processing of data and also analytics requirements could be increased. The critical system cannot afford downtime as it needs high availability.

Scarcity of Technical Knowhow

There is an acute shortage of skilled labor to handle the complex underlying systems of the smart city ecosystem. The available workforce is not well-versed in the technical knowhow of the new devices and thus cannot effectively handle those devices.

Privacy and Security

Privacy and security are the two most important issues associated with smart city initiates. Since all the data are available in digital form and stored on the cloud (mostly), its privacy and security are always questionable when a third party is involved. Several approaches have been proposed in the recent literature to mitigate the security issues in CPS within smart cities [52,60,119,122,124,129,131–143].

Interoperability

The majority of IoT manufacturers focus on providing immediate services to their users rather than focusing on other internal details including security, interoperability, etc.

These IoT devices are generally proprietary devices and lack interoperability, which limits their use [187,188].

Unstructured Data

The vast amount of data generated through ubiquitously available sensors is usually unstructured, which makes it very hard to handle effectively. Different data cleaning and structuring techniques are required to preprocess the data before feeding them to the decision-making unit. Since the services and functionalities of typical smart cities are data-dependent, the veracity and trustworthiness of the data are highly vital [189].

Absence of Unified Standards

To the best of our knowledge, there are no unified standards available for handling sensors and IoT devices deployed in CPS. The lack of unified standards makes it difficult to provide seamless integration and communication among various participating entities of the CPS systems in smart cities.

4.2.2. Socioeconomic Issues

These issues comprise budgetary constraints and rigid policies in place to implement smart city initiatives.

Budget Constraints

Several smaller nations are not able to bear the costs involved in setting up smart city ecosystems and thus are not able to start the initiatives. There are several situations where nations have started initiatives but have to keep the project on hold due to lack of funds.

Rigid Policies

Legacy policies of nations are also considered a hindrance to smart city initiatives. The lack of a single-window clearance system, rigid governance, and regulatory norms are inherent issues that need to be tackled to provide a flexible and open system of clearance for such innovative projects.

4.2.3. Social Issues

In a country like India, which is so diverse in terms of religion, color, caste, and creed, social issues are one of the most prominent factors influencing the decisions of the authorities and citizens alike. Dense population, conventional mindset, illiteracy, and digital divide are the prime factors that hinder smart city projects in this context.

Social Divide and Mindset

The conventional mindset and social divide also hinder the widespread adoption of smart city initiatives. Generally, older people are reluctant to adopt new technologies because of the fear of data theft or lack of technological knowhow.

High Implementation Costs

The implementation cost of smart city initiatives is usually very high. This is a serious issue that prevents smaller nations from readily adopting these initiatives. The CPS systems are highly costly and sophisticated and require expert handling and management.

Lack of Skilled Labor

There is a scarcity of skilled labor capable of handling the sophisticated CPS systems within the smart city ecosystems. Since every CPS is made up of thousands and millions of IoT devices and sensors, it becomes very difficult to manage them effectively without the help of trained professionals.

4.2.4. Environmental Challenges

There are several hazardous effects of technology such as carbon emissions, e-waste, etc. These are termed as "environmental challenges". Research is ongoing across the globe to study the negative effects of technologies such as 5G and 6G, in terms of E-waste generation, carbon emissions, etc. [190]. Other environmental challenges include natural calamities such as earthquakes, floods, lightning, snowfall, draughts, etc.

4.2.5. Societal Issues

These issues pertain to common citizens, which include technological acceptance, public health, lack of knowledge about the existing policies, schemes, and regulations, and lack of trust among citizens.

4.2.6. Ethical Issues

These issues are usually ignored by the majority of policymakers. However, in recent years, ethical issues have been an emerging topic of research. With the adoption of automation in several service domains issues of unconscious gender bias, transparency, rights of the machine, fixing responsibility in case of any mistakes, etc., are hard to identify and mitigate. Other ethical challenges include fear of job loss, unequal distribution of wealth among the stakeholders, dependency on machines, etc. From the smart city perspective, ethical issues play a vital role in governance [191,192]. Self-awareness and education about the pros and cons of technology must be considered while using smart city services.

5. Conclusions and Discussion

The concept of a smart city has gained ground in recent years across the globe. It is most likely that it will continue in the future. Modern-day smart technologies are providing solutions such as saving money, maintaining a sustainable environment by reducing carbon emission, reducing capital and operational costs, promoting better wellbeing and livelihoods, etc. Rapid and unprecedented urbanization severely posed traffic congestion. Consequently, air pollution became a big problem for cities. Transportation and traffic snarls led to another major issue in the transportation system. However, it is hoped that it may be eliminated by succinctly applying the principles of smart city concepts. Smart infrastructure responds intelligently to changes in its environment, including user demands and other infrastructure to achieve better and improved performance. The data-driven approach of smart cities provides exemplary benefits in all spheres of life for the inhabitants. "Data", being the nerve center, means governments must collaborate and coordinate with start-ups and entrepreneurs to obtain effective collaborative outcomes which can be a win-win situation for all stakeholders. It is quite obvious that smart city networks are based on execution, not just planning. It is not an exaggeration that smart city projects can only be achieved when we intersect them with the basic infrastructure. The concept of a smart city has many benefits to its stakeholders if it is a data-driven, robust, dynamic, scalable, and responsive ecosystem. If we have an effective channel of communication, it would automatically connect each stakeholder for improved connectivity and synchronization. Cyber-physical systems being the building blocks of any smart city ecosystem, extensive research is being carried out around the globe to improve their performance, associated security, and privacy issues and improve the maintenance and lifetime of the systems. In recent years, India has also focused on realizing the adoption of CPS in different domains within the smart city framework for the improved management of services with optimal utilization of resources and sustainability as a prime focus. Extensive research and initiatives are being started to take up the challenge.

The enabling technologies facilitate an effective and cost-effective mechanism, thus, applying all the available technologies at our disposal, we can make robust networks of infrastructure and services making an excellent smart city ecosystem to provide better wellbeing and sustainable livelihoods for the inhabitants. Future research must be focused on the security and ethical aspects of these CPS for their widespread adoption in mainstream

city developments. One of the latest technologies slowly coming into the mainstream is the passwordless authentication approach where the users are not required to memorize a username or password, and the authentication takes place with the help of some hardware keys, biometrics, or login tokens, etc. It will be interesting to see its application in the CPS domain as well.

Author Contributions: Conceptualization, M.O.A., M.A.A.(Mohd Abdul Ahad) and F.S.; methodology, F.S., M.A.A. (M. Afshar Alam), and M.O.A., G.C.; validation, M.O.A., M.A.A. (Mohd Abdul Ahad), G.C., and F.S.; formal analysis, M.A.A. (Mohd Abdul Ahad) and F.S.; investigation, M.O.A., M.A.A. (Mohd Abdul Ahad) and F.S.; resources, F.S. and M.A.A. (M. Afshar Alam), G.C.; data curation, M.O.A.; M.A.A. (Mohd Abdul Ahad) and F.S.; writing—original draft preparation, M.O.A. and M.A.A. (Mohd Abdul Ahad); writing—review and editing, M.O.A.; M.A.A., G.C.; and F.S.; visualization, M.A.A. (M. Afshar Alam); M.O.A., G.C.; supervision, M.A.A. (M. Afshar Alam), F.S. and M.A.A. (Mohd Abdul Ahad). All authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

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

References

1. Ruhlandt, R.W.S. The governance of smart cities: A systematic literature review. *Cities* **2018**, *81*, 1–23. [CrossRef]
2. Batty, M.; Axhausen, K.W.; Giannotti, F.; Pozdnoukhov, A.; Bazzani, A.; Wachowicz, M.; Ouzounis, G.; Portugali, Y. Smart cities of the future. *Eur. Phys. J. Spec. Top.* **2012**, *214*, 481–518. [CrossRef]
3. Bakıcı, T.; Almirall, E.; Wareham, J. A smart city initiative: The case of Barcelona. *J. Knowl. Econ.* **2013**, *4*, 135–148. [CrossRef]
4. Jha, P.P.; Iqbal, M.A. A perspective on migration and community engagement in Smart Cities. In *Smart Cities—Opportunities and Challenges*; Springer: Singapore, 2020; pp. 521–526.
5. Kramers, A.; Höjer, M.; Lövehagen, N.; Wangel, J. Smart sustainable cities–Exploring ICT solutions for reduced energy use in cities. *Environ. Model. Softw.* **2014**, *56*, 52–62. [CrossRef]
6. Glasmeier, A.; Christopherson, S. Thinking about smart cities. *Camb. J. Reg. Econ. Soc.* **2015**, *8*, 3–12. [CrossRef]
7. Lee, J.; Lee, H. Developing and validating a citizen-centric typology for smart city services. *Gov. Inf. Q.* **2014**, *31*, S93–S105. [CrossRef]
8. Hernández-Muñoz, J.M.; Vercher, J.B.; Muñoz, L.; Galache, J.A.; Presser, M.; Gómez, L.A.H.; Pettersson, J. Smart cities at the forefront of the future internet. In *Future Internet Assembly*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 447–462.
9. Arroub, A.; Zahi, B.; Sabir, E.; Sadik, M. A literature review on Smart Cities: Paradigms, opportunities and open problems. In Proceedings of the 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, Morocco, 26–29 October 2016; pp. 180–186.
10. Mboup, G.; Oyelaran-Oyeyinka, B. Relevance of smart economy in smart cities in Africa. In *Smart Economy in Smart African Cities*; Springer: Singapore, 2019; pp. 1–49.
11. Kumar, T.V.; Dahiya, B. Smart economy in smart cities. In *Smart Economy in Smart Cities*; Springer: Singapore, 2017; pp. 3–76.
12. Letaifa, S.B. How to strategize smart cities: Revealing the SMART model. *J. Bus. Res.* **2015**, *68*, 1414–1419. [CrossRef]
13. Razmjoo, A.; Østergaard, P.A.; Denai, M.; Nezhad, M.M.; Mirjalili, S. Effective policies to overcome barriers in the development of smart cities. *Energy Res. Soc. Sci.* **2021**, *79*, 102175. [CrossRef]
14. Qian, Y.; Liu, J.; Cheng, Z.; Forrest, J.Y.L. Does the smart city policy promote the green growth of the urban economy? Evidence from China. *Environ. Sci. Pollut. Res.* **2021**, 1–15. [CrossRef] [PubMed]
15. Lopes, N.V. Smart governance: A key factor for smart cities implementation. In Proceedings of the 2017 IEEE International Conference on Smart Grid and Smart Cities (ICSGSC), Singapore, 23–26 July 2017; pp. 277–282.
16. Barns, S. Smart cities and urban data platforms: Designing interfaces for smart governance. *City Cult. Soc.* **2018**, *12*, 5–12. [CrossRef]
17. Razaghi, M.; Finger, M. Smart governance for smart cities. *Proc. IEEE* **2018**, *106*, 680–689. [CrossRef]

18. Bolívar, M.P.R.; Meijer, A.J. Smart governance: Using a literature review and empirical analysis to build a research model. *Soc. Sci. Comput. Rev.* **2016**, *34*, 673–692. [CrossRef]

19. Rashidi, P.; Cook, D.J.; Holder, L.B.; Schmitter-Edgecombe, M. Discovering activities to recognize and track in a smart environment. *IEEE Trans. Knowl. Data Eng.* **2010**, *23*, 527–539. [CrossRef] [PubMed]

20. Kumar, V. Smart environment for smart cities. In *Smart Environment for Smart Cities*; Springer: Singapore, 2020; pp. 1–53.

21. Aletà, N.B.; Alonso, C.M.; Ruiz, R.M.A. Smart mobility and smart environment in the Spanish cities. *Transp. Res. Procedia* **2017**, *24*, 163–170. [CrossRef]

22. Fernández-Caballero, A.; Martínez-Rodrigo, A.; Pastor, J.M.; Castillo, J.C.; Lozano-Monasor, E.; López, M.T.; Zangróniz, R.; Latorre, J.M.; Fernández-Sotos, A. Smart environment architecture for emotion detection and regulation. *J. Biomed. Inform.* **2016**, *64*, 55–73. [CrossRef] [PubMed]

23. Ullo, S.L.; Sinha, G.R. Advances in smart environment monitoring systems using IoT and sensors. *Sensors* **2020**, *20*, 3113. [CrossRef] [PubMed]

24. Kalluri, B.; Chronopoulos, C.; Kozine, I. The concept of smartness in cyber–physical systems and connection to urban environment. *Annu. Rev. Control* **2020**, *51*, 1–22. [CrossRef]

25. Romero, D.; Quinton, C.; Duchien, L.; Seinturier, L.; Valdez, C. SmartyCo: Managing cyber-physical systems for smart environments. In *European Conference on Software Architecture*; Springer: Cham, Switzerland, 2015; pp. 294–302.

26. Ferrer, B.R.; Mohammed, W.M.; Lastra, J.L.M.; Villalonga, A.; Beruvides, G.; Castaño, F.; Haber, R.E. Towards the adoption of cyber-physical systems of systems paradigm in smart manufacturing environments. In Proceedings of the 2018 IEEE 16th International Conference on Industrial Informatics (INDIN), Porto, Portugal, 18–20 July 2018; pp. 792–799.

27. Elshenawy, M.; Abdulhai, B.; El-Darieby, M. Towards a service-oriented cyber–physical systems of systems for smart city mobility applications. *Future Gener. Comput. Syst.* **2018**, *79*, 575–587. [CrossRef]

28. Möller, D.P.; Vakilzadian, H. Cyber-physical systems in smart transportation. In Proceedings of the 2016 IEEE International Conference on Electro Information Technology (EIT), Grand Forks, ND, USA, 19–21 May 2016; pp. 0776–0781.

29. Sargolzaei, A.; Crane, C.D.; Abbaspour, A.; Noei, S. A machine learning approach for fault detection in vehicular cyber-physical systems. In Proceedings of the 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, 18–20 December 2016; pp. 636–640.

30. Xia, F.; Ma, J. Building smart communities with cyber-physical systems. In Proceedings of the 1st International Symposium on from Digital Footprints to Social and Community Intelligence, Beijing, China, 18 September 2011; pp. 1–6.

31. Li, X.; Lu, R.; Liang, X.; Shen, X.; Chen, J.; Lin, X. Smart community: An internet of things application. *IEEE Commun. Mag.* **2011**, *49*, 68–75. [CrossRef]

32. 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]

33. Bai, Z.Y.; Huang, X.Y. Design and implementation of a cyber physical system for building smart living spaces. *Int. J. Distrib. Sens. Netw.* **2012**, *8*, 764186. [CrossRef]

34. Munir, S.; Stankovic, J.A. Depsys: Dependency aware integration of cyber-physical systems for smart homes. In Proceedings of the 2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), Berlin, Germany, 14–17 April 2014; pp. 127–138.

35. Geisberger, E.; Broy, M. (Eds.) *Living in a Networked World: Integrated Research Agenda Cyber-Physical Systems (agendaCPS)*; Herbert Utz Verlag: Munich, Germany, 2015.

36. Papa, R.; Fistola, R. (Eds.) *Smart Energy in the Smart City: Urban Planning for a Sustainable Future*; Springer: Berlin/Heidelberg, Germany, 2016.

37. Pieroni, A.; Scarpato, N.; Di Nunzio, L.; Fallucchi, F.; Raso, M. Smarter city: Smart energy grid based on blockchain technology. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2018**, *8*, 298–306. [CrossRef]

38. Lund, H.; Østergaard, P.A.; Connolly, D.; Mathiesen, B.V. Smart energy and smart energy systems. *Energy* **2017**, *137*, 556–565. [CrossRef]

39. Suvarna, M.; Büth, L.; Hejny, J.; Mennenga, M.; Li, J.; Ng, Y.T.; Herrmann, C.; Wang, X. Smart manufacturing for smart cities—Overview, insights, and future directions. *Adv. Intell. Syst.* **2020**, *2*, 2000043. [CrossRef]

40. Kang, H.S.; Lee, J.Y.; Choi, S.; Kim, H.; Park, J.H.; Son, J.Y.; Kim, B.H.; Do Noh, S. Smart manufacturing: Past research, present findings, and future directions. *Int. J. Precis. Eng. Manuf.-Green Technol.* **2016**, *3*, 111–128. [CrossRef]

41. Gaur, A.; Scotney, B.; Parr, G.; McClean, S. Smart city architecture and its applications based on IoT. *Procedia Comput. Sci.* **2015**, *52*, 1089–1094. [CrossRef]

42. Cyber Physical Systems. Available online: https://ptolemy.berkeley.edu/projects/cps/ (accessed on 5 September 2021).

43. Lee, J.; Bagheri, B.; Kao, H.A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23. [CrossRef]

44. Bagheri, B.; Yang, S.; Kao, H.A.; Lee, J. Cyber-physical systems architecture for self-aware machines in industry 4.0 environment. *IFAC-PapersOnLine* **2015**, *48*, 1622–1627. [CrossRef]

45. Yilma, B.A.; Panetto, H.; Naudet, Y. Systemic formalisation of Cyber-Physical-Social System (CPSS): A systematic literature review. *Comput. Ind.* **2021**, *129*, 103458. [CrossRef]

46. Latif, S.A.; Wen, F.B.X.; Iwendi, C.; Li-li, F.W.; Mohsin, S.M.; Han, Z.; Band, S.S. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Comput. Commun.* **2021**, *181*, 274–283. [CrossRef]

47. Taha, A.F.; Gatsis, N.; Summers, T.; Nugroho, S. Actuator selection for cyber-physical systems. In Proceedings of the 2017 American Control Conference (ACC), Seattle, WA, USA, 24–26 May 2017; pp. 5300–5305.

48. Lu, C.; Saifullah, A.; Li, B.; Sha, M.; Gonzalez, H.; Gunatilaka, D.; Wu, C.; Nie, L.; Chen, Y. Real-time wireless sensor-actuator networks for industrial cyber-physical systems. *Proc. IEEE* **2015**, *104*, 1013–1024. [CrossRef]

49. Gudivada, V.N.; Ramaswamy, S.; Srinivasan, S. Data management issues in cyber-physical systems. In *Transportation Cyber-Physical Systems*; Elsevier: Amsterdam, The Netherlands, 2018; pp. 173–200.

50. Kang, K.D.; Son, S.H. Real-time data services for cyber physical systems. In Proceedings of the 2008 The 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, 17–20 June 2008; pp. 483–488.

51. Wu, F.J.; Kao, Y.F.; Tseng, Y.C. From wireless sensor networks towards cyber physical systems. *Pervasive Mob. Comput.* **2011**, *7*, 397–413. [CrossRef]

52. Ali, S.; Al Balushi, T.; Nadir, Z.; Hussain, O.K. WSN security mechanisms for CPS. In *Cyber Security for Cyber Physical Systems*; Springer: Cham, Switzerland, 2018; pp. 65–87.

53. Vallimayil, A.; Raghunath, K.K.; Dhulipala, V.S.; Chandrasekaran, R.M. Role of relay node in wireless sensor network: A survey. In Proceedings of the 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, India, 8–10 April 2011; Volume 5, pp. 160–167.

54. Liu, T.; Tian, B.; Ai, Y.; Wang, F.Y. Parallel reinforcement learning-based energy efficiency improvement for a cyber-physical system. *IEEE/CAA J. Autom. Sin.* **2020**, *7*, 617–626. [CrossRef]

55. Chinnici, M.; De Chiara, D.; Quintiliani, A. Data center, a cyber-physical system: Improving energy efficiency through the power management. In Proceedings of the 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Orlando, FL, USA, 6–10 November 2017; pp. 269–272.

56. Parolini, L.; Sinopoli, B.; Krogh, B.H.; Wang, Z. A cyber–physical systems approach to data center modeling and control for energy efficiency. *Proc. IEEE* **2011**, *100*, 254–268. [CrossRef]

57. Molina, E.; Jacob, E. Software-defined networking in cyber-physical systems: A survey. *Comput. Electr. Eng.* **2018**, *66*, 407–419. [CrossRef]

58. Moura, J.; Hutchison, D. Modeling cooperative behavior for resilience in cyber-physical systems using SDN and NFV. *SN Appl. Sci.* **2020**, *2*, 1–13. [CrossRef]

59. Alsufyani, A.; Alotaibi, Y.; Almagrabi, A.O.; Alghamdi, S.A.; Alsufyani, N. Optimized intelligent data management framework for a cyber-physical system for computational applications. *Complex Intell. Syst.* **2021**, 1–13. [CrossRef]

60. Chaudhry, N.; Yousaf, M.M.; Khan, M.T. Security assessment of data management systems for cyber physical system applications. *J. Softw. Evol. Process* **2020**, *32*, e2241. [CrossRef]

61. Canizo, M.; Conde, A.; Charramendieta, S.; Minon, R.; Cid-Fuentes, R.G.; Onieva, E. Implementation of a large-scale platform for cyber-physical system real-time monitoring. *IEEE Access* **2019**, *7*, 52455–52466. [CrossRef]

62. Kukkala, V.K.; Tunnell, J.; Pasricha, S.; Bradley, T. Advanced driver-assistance systems: A path toward autonomous vehicles. *IEEE Consum. Electron. Mag.* **2018**, *7*, 18–25. [CrossRef]

63. Criado, J.; Asensio, J.A.; Padilla, N.; Iribarne, L. Integrating cyber-physical systems in a component-based approach for smart homes. *Sensors* **2018**, *18*, 2156. [CrossRef]

64. Park, J.; Park, K. Construction of a remote monitoring system in smart dust environment. *J. Inf. Process. Syst.* **2020**, *16*, 733–741.

65. Warneke, B.; Last, M.; Liebowitz, B.; Pister, K.S. Smart dust: Communicating with a cubic-millimeter computer. *Computer* **2001**, *34*, 44–51. [CrossRef]

66. Jiang, P.; Xia, H.; He, Z.; Wang, Z. Design of a water environment monitoring system based on wireless sensor networks. *Sensors* **2009**, *9*, 6411–6434. [CrossRef] [PubMed]

67. Hussain, I.; Park, S.J. Prediction of myoelectric biomarkers in post-stroke gait. *Sensors* **2021**, *21*, 5334. [CrossRef] [PubMed]

68. Petropoulos, A.; Sikeridis, D.; Antonakopoulos, T. Wearable smart health advisors: An IMU-enabled posture monitor. *IEEE Consum. Electron. Mag.* **2020**, *9*, 20–27. [CrossRef]

69. Wang, X.; Yang, L.T.; Xie, X.; Jin, J.; Deen, M.J. A cloud-edge computing framework for cyber-physical-social services. *IEEE Commun. Mag.* **2017**, *55*, 80–85. [CrossRef]

70. Ma, Y.; Wang, Y.; Yang, J.; Miao, Y.; Li, W. Big health application system based on health internet of things and big data. *IEEE Access* **2016**, *5*, 7885–7897. [CrossRef]

71. Muhammed, T.; Mehmood, R.; Albeshri, A.; Katib, I. UbeHealth: A personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities. *IEEE Access* **2018**, *6*, 32258–32285. [CrossRef]

72. Shishvan, O.R.; Zois, D.S.; Soyata, T. Machine intelligence in healthcare and medical cyber physical systems: A survey. *IEEE Access* **2018**, *6*, 46419–46494. [CrossRef]

73. Hussain, I.; Park, S.J. HealthSOS: Real-Time Health Monitoring System for Stroke Prognostics. *IEEE Access* **2020**, *8*, 213574–213586. [CrossRef]

74. Hussain, I.; Park, S.J. Big-Ecg: Cardiographic Predictive Cyber-Physical System for Stroke Management. *IEEE Access* **2021**, *9*, 123146–123164. [CrossRef]

75. Park, S.J.; Hong, S.; Kim, D.; Hussain, I.; Seo, Y. Intelligent in-car health monitoring system for elderly drivers in connected car. In *Congress of the International Ergonomics Association*; Springer: Cham, Switzerland, 2018; pp. 40–44.

76. Casalino, G.; Castellano, G.; Zaza, G. On the use of FIS inside a Telehealth system for cardiovascular risk monitoring. In Proceedings of the 2021 29th Mediterranean Conference on Control and Automation (MED), Puglia, Italy, 22–25 June 2021; pp. 173–178.

77. Pazienza, A.; Anglani, R.; Fasciano, C.; Tatulli, C.; Vitulano, F. Evolving and Explainable Clinical Risk Assessment at the Edge. In *Evolving Systems*; Springer: Berlin/Heidelberg, Germany, 2021; in press.

78. Khaitan, S.K.; McCalley, J.D. Design techniques and applications of cyberphysical systems: A survey. *IEEE Syst. J.* **2014**, *9*, 350–365. [CrossRef]

79. Gunes, V.; Peter, S.; Givargis, T.; Vahid, F. A survey on concepts, applications, and challenges in cyber-physical systems. *KSII Trans. Internet Inf. Syst. (TIIS)* **2014**, *8*, 4242–4268.

80. Munoz, D.J.; Montenegro, J.A.; Pinto, M.; Fuentes, L. Energy-aware environments for the development of green applications for cyber–physical systems. *Future Gener. Comput. Syst.* **2019**, *91*, 536–554. [CrossRef]

81. Horcas, J.M.; Pinto, M.; Fuentes, L. Context-aware energy-efficient applications for cyber-physical systems. *Ad. Hoc. Netw.* **2019**, *82*, 15–30. [CrossRef]

82. Basile, F.; Chiacchio, P.; Coppola, J.; Gerbasio, D. Automated warehouse systems: A cyber-physical system perspective. In Proceedings of the 2015 IEEE 20th Conf. Emerging Technologies & Factory Automation (ETFA), Luxembourg, 8–11 September 2015; pp. 1–4.

83. Wiesner, S.; Marilungo, E.; Thoben, K.D. Cyber-physical product-service systems—Challenges for requirements engineering. *Int. J. Autom. Technol.* **2017**, *11*, 17–28. [CrossRef]

84. Li, Y.T.; Jacob, M.; Akingba, G.; Wachs, J.P. A cyber-physical management system for delivering and monitoring surgical instruments in the OR. *Surg. Innov.* **2013**, *20*, 377–384. [CrossRef]

85. Tercero, C.; Kodama, H.; Shi, C.; Ooe, K.; Ikeda, S.; Fukuda, T.; Arai, F.; Negoro, M.; Kwon, G.; Najdovski, Z. Technical skills measurement based on a cyber-physical system for endovascular surgery simulation. *Int. J. Med. Robot. Comput. Assist. Surg.* **2013**, *9*, e25–e33. [CrossRef]

86. Sonntag, D.; Zillner, S.; Chakraborty, S.; Lorincz, A.; Strommer, E.; Serafini, L. The medical cyber-physical systems activity at EIT: A look under the hood. In Proceedings of the 2014 IEEE 27th Int. Symp. Computer-Based Medical Systems (CBMS), New York, NY, USA, 27–29 May 2014; pp. 351–356.

87. Dogaru, D.I.; Dumitrache, I. Cyber-physical systems in healthcare networks. In Proceedings of the 2015 E-Health and Bioengineering Conference (EHB), Iasi, Romania, 19–21 November 2015; pp. 1–4.

88. Bradley, J.M.; Atkins, E.M. Optimization and control of cyber-physical vehicle systems. *Sensors* **2015**, *15*, 23020–23049. [CrossRef]

89. Kantarci, B. Cyber-physical alternate route recommendation system for paramedics in an urban area. In Proceedings of the 2015 IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA, 9–12 March 2015; pp. 2155–2160.

90. Zhou, Y.; Mo, Z.; Xiao, Q.; Chen, S.; Yin, Y. Privacy-preserving transportation tra±c measurement in intelligent cyber-physical road systems. *IEEE Trans. Veh. Technol.* **2016**, *65*, 3749–3759. [CrossRef]

91. Ma, M.; An, J.; Huang, Z.; Cao, Z. Sensor data fusion based on an improved dempster- shafer evidence theory in vehicular cyber-physical systems. In Proceedings of the 2015 IEEE International Symposium Intelligent Control (ISIC), Sydney, NSW, Australia, 21–23 September 2015; pp. 683–687.

92. Kumar, N.; Bali, R.S.; Iqbal, R.; Chilamkurti, N.; Rho, S. Optimized clustering for data dissemination using stochastic coalition game in vehicular cyber-physical systems. *J. Supercomput.* **2015**, *71*, 3258–3287. [CrossRef]

93. Li, Y.; Wu, J.; Li, S. State estimation for distributed cyber-physical power systems under data attacks. *Int. J. Model. Identif. Control* **2016**, *26*, 317–323. [CrossRef]

94. Wan, J.; Yan, H.; Li, D.; Zhou, K.; Zeng, L. Cyber-physical systems for optimal energy management scheme of autonomous electric vehicle. *Comput. J.* **2013**, *56*, 947–956. [CrossRef]

95. Gurgen, L.; Gunalp, O.; Benazzouz, Y.; Gallissot, M. Self-aware cyber-physical systems and applications in smart buildings and cities. In Proceedings of the 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 18–22 March 2013; pp. 1149–1154.

96. Schmidt, M.; Åhlund, C. Smart buildings as Cyber-Physical Systems: Data-driven predictive control strategies for energy efficiency. *Renew. Sustain. Energy Rev.* **2018**, *90*, 742–756. [CrossRef]

97. Mehdipour, F. Smart field monitoring: An application of cyber-physical systems in agriculture. In Proceedings of the 2014 IIAI 3rd International Conference Advanced Applied Informatics (IIAIAAI), Kokura, Japan, 31 August–4 September 2014; pp. 181–184.

98. Mehdipour, F.; Nunna, K.C.; Murakami, K.J. A smart cyber-physical systems-based solution for pest control. In Proceedings of the Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE Int. Conf. and IEEE Cyber, Physical and Social Computing, Beijing, China, 20–23 August 2013; pp. 1248–1253.

99. Caramihai, S.I.; Dumitrache, I. Agricultural enterprise as a complex system: A cyber physical systems approach. In Proceedings of the 2015 20th Int. Conf. Control Systems and Computer Science (CSCS), Bucharest, Romania, 27–29 May 2015; pp. 659–664.

100. Cheng, A.M.K. An undergraduate cyber-physical systems course. In Proceedings of the 4th ACM SIGBED Int. Workshop on Design, Modeling, and Evaluation of Cyber-Physical Systems, Berlin, Germany, 14–17 April 2014; pp. 31–34.

101. Peter, S.; Momtaz, F.; Givargis, T. From the browser to the remote physical lab: Programming cyber-physical systems. In Proceedings of the 2015 IEEE Frontiers in Education Conference (FIE), El Paso, TX, USA, 21–24 October 2015; pp. 1–7.

102. Lawlor, O.; Bogosyan, S.; Vural, Y.; Thompson, I.; Moss, M.; Gokasan, M. AERO-beam: An open-architecture test-bed for research and education in cyber-physical systems. In Proceedings of the Industrial Electronics Society, IECON 2015-41st Annual Conference of the IEEE, Yokohama, Japan, 9–12 November 2015; pp. 005080–005086.

103. Pester, A.; Madritsch, C.; Klinger, T. Collaborative learning with cyber-physical systems. In Proceedings of the 2015 IEEE Global Engineering Education Conference (EDUCON), Tallinn, Estonia, 18–20 March 2015; pp. 184–188.

104. Schoitsch, E. Special session TET-DEC (teaching, education and training for dependable embedded and cyber-physical systems) An E&T use case in a European Project. In Proceedings of the 2015 41st Euromicro Conf. Software Engineering and Advanced Applications (SEAA), Madeira, Portugal, 26–28 August 2015; pp. 280–289.

105. Azad, A.K.M.; Hashemian, R. Cyber-Physical Systems in STEM Disciplines. In Proceedings of the 2016 SAI Computing Conference (SAI), London, UK, 13–15 July 2016; pp. 868–874.

106. Van Tendeloo, Y.; Vangheluwe, H. Teaching the fundamentals of the modelling of cyber-physical systems. In Proceedings of the Symp. Theory of Modeling & Simulation, Society for Computer Simulation International, Pasadena, CA, USA, 3–6 April 2016; p. 5.

107. Ardimento, P.; Bernardi, M.L.; Cimitile, M.; De Ruvo, G. Mining Developer's Behavior from Web-Based IDE Logs. In Proceedings of the 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Napoli, Italy, 12–14 June 2019; pp. 277–282.

108. Picerno, P.; Pecori, R.; Raviolo, P.; Ducange, P. Smartphones and exergame controllers as BYOD solutions for the e-tivities of an online sport and exercise sciences university program. In *International Workshop on Higher Education Learning Methodologies and Technologies Online*; Springer: Cham, Switzerland, 2019; pp. 217–227.

109. Casalino, G.; Cafarelli, B.; del Gobbo, E.; Fontanella, L.; Grilli, L.; Guarino, A.; Limone, P.; Schicchi, D.; Taibi, D. Framing automatic grading techniques for open-ended questionnaires responses. A short survey, CEUR Workshop Proceedings. In *teleXbe—Technology Enhanced Learning Environments for Blended Education*; Publisher CEUR-WS: Foggia, Italy, 2021; in press.

110. Klimeš, J. Using formal concept analysis for control in cyber-physical systems. *Procedia Eng.* **2014**, *69*, 1518–1522. [CrossRef]

111. Du, C.; Tan, L.; Dong, Y. Period selection for integrated controller tasks in cyber-physical systems. *Chin. J. Aeronaut.* **2015**, *28*, 894–902. [CrossRef]

112. Medhat, R.; Bonakdarpour, B.; Kumar, D.; Fischmeister, S. Runtime monitoring of cyber-physical systems under timing and memory constraints. *ACM Trans. Embed. Comput. Syst.* **2015**, *14*, 79. [CrossRef]

113. Han, R.; Zhao, X.; Yu, Y.; Guan, Q.; Hu, W.; Li, M. A cyber-physical system for girder hoisting monitoring based on smartphones. *Sensors* **2016**, *16*, 1048. [CrossRef]

114. Sanchez, B.B.; Alcarria, R.; Sańchez-De-Rivera, D.; Sańchez-Picot, A. Enhancing process control in industry 4.0 scenarios using cyber-physical systems. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2016**, *7*, 41–64.

115. Decker, L.; Leite, D.; Giommi, L.; Bonacorsi, D. Real-time anomaly detection in data centers for log-based predictive maintenance using an evolving fuzzy-rule-based approach. In Proceedings of the 2020 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Glasgow, UK, 19–24 July 2020; pp. 1–8.

116. Sierla, S.; O'Halloran, B.M.; Karhela, T.; Papakonstantinou, N.; Tumer, I.Y. Common cause failure analysis of cyber-physical systems situated in constructed environments. *Res. Eng. Des.* **2013**, *24*, 375–394. [CrossRef]

117. Sanislav, T.; Mois, G.; Folea, S.; Miclea, L.; Gambardella, G.; Prinetto, P. A cloud-based cyber-physical system for environmental monitoring. In Proceedings of the 2014 3rd Mediterranean Conf. Embedded Computing (MECO), Budva, Montenegro, 15–19 June 2014; pp. 6–9.

118. Wang, J.; Yu, H. Analysis of the composition of non-deducibility in cyber-physical systems. *Appl. Math. Inf. Sci.* **2014**, *8*, 3137–3143. [CrossRef]

119. Wan, K.; Alagar, V. Context-aware security solutions for cyber-physical systems. *Mob. Netw. Appl.* **2014**, *19*, 212–226. [CrossRef]

120. Lyn, K.G.; Lerner, L.W.; McCarty, C.J.; Patterson, C.D. The trustworthy autonomic interface guardian architecture for cyber-physical systems. In Proceedings of the 2015 IEEE Int. Conf. on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, (CIT/IUCC/DASC/PICOM), Liverpool, UK, 26–28 October 2015; pp. 1803–1810.

121. Niu, H.; Jagannathan, S. Optimal defense and control of dynamic systems modeled as cyber-physical systems. *J. Def. Model. Simul.* **2015**, *12*, 423–438. [CrossRef]

122. Puttonen, J.; Afolaranmi, S.O.; Moctezuma, L.G.; Lobov, A.; Lastra, J.L.M. Security in cloud-based cyber-physical systems. In Proceedings of the 2015 10th Int. Conf. P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Krakow, Poland, 4–6 November 2015; pp. 671–676.

123. Fernandez, E.B. Threat modeling in cyber-physical systems. In Proceedings of the Dependable, Autonomic and Secure Computing, 14th Int. Conf. Pervasive Intelligence and Computing, 2nd Int. Conf. Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Auckland, New Zealand, 8–12 August 2016; pp. 448–453.

124. Nguyen, P.H.; Ali, S.; Yue, T. Model-based security engineering for cyber-physical systems: A systematic mapping study. *Inf. Softw. Technol.* **2017**, *83*, 116–135. [CrossRef]

125. Cassandras, C.G. Smart cities as cyber-physical social systems. *Engineering* **2016**, *2*, 218–219. [CrossRef]

126. Mazumdar, S.; Ayguade, E.; Bettin, N.; Bueno, J.; Ermini, S.; Filgueras, A.; Giorgi, R. AXIOM: A hardware-software platform for cyber physical systems. In Proceedings of the 2016 Euromicro Conf. Digital System Design (DSD), Limassol, Cyprus, 31 August–2 September 2016; pp. 539–546.

127. Seiger, R.; Huber, S.; Schlegel, T. Toward an execution system for self-healing workflows in cyber-physical systems. *Softw. Syst. Model.* **2018**, *2*, 551–572. [CrossRef]

128. Seiger, R.; Struwe, S.; Lemme, D.; Schlegel, T. An interactive mobile control center for cyber-physical systems. In Proceedings of the 2016 ACM Int. Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, ACM, Heidelberg, Germany, 12–16 September 2016; pp. 193–196.

129. Walker-Roberts, S.; Hammoudeh, M.; Aldabbas, O.; Aydin, M.; Dehghantanha, A. Threats on the horizon: Understanding security threats in the era of cyber-physical systems. *J. Supercomput.* **2020**, *76*, 2643–2664. [CrossRef]

130. Coviello, G.; Avitabile, G.; Florio, A. The importance of data synchronization in multiboard acquisition systems. In Proceedings of the 2020 IEEE 20th Mediterranean Electrotechnical Conference (MELECON), Palermo, Italy, 16–18 June 2020; pp. 293–297.

131. Fernandes, E.; Rahmati, A.; Jung, J.; Prakash, A. Security implications of permission models in smart-home application frameworks. *IEEE Secur.* **2017**, *15*, 24–30. [CrossRef]

132. Cui, L.; Xie, G.; Qu, Y.; Gao, L.; Yang, Y. Security and privacy in smart cities: Challenges and opportunities. *IEEE Access* **2018**, *6*, 46134–46145. [CrossRef]

133. Habibzadeh, H.; Nussbaum, B.H.; Anjomshoa, F.; Kantarci, B.; Soyata, T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustain. Cities Soc.* **2019**, *50*, 101660. [CrossRef]

134. Alguliyev, R.; Imamverdiyev, Y.; Sukhostat, L. Cyber-physical systems and their security issues. *Comput. Ind.* **2018**, *100*, 212–223. [CrossRef]

135. Biron, K.; Bazzaza, W.; Yaqoob, K.; Gawanmeh, A.; Fachkha, C. A big data fusion to profile CPS security threats against operational technology. In Proceedings of the 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Cork, Ireland, 31 August–3 September 2020; pp. 397–402.

136. Pal, R.; Prasanna, V. The STREAM mechanism for CPS security the case of the smart grid. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2016**, *36*, 537–550. [CrossRef]

137. Abie, H. Cognitive cybersecurity for CPS-IoT enabled healthcare ecosystems. In Proceedings of the 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 8–10 May 2019; pp. 1–6.

138. Burg, A.; Chattopadhyay, A.; Lam, K.Y. Wireless communication and security issues for cyber–physical systems and the Internet-of-Things. *IEEE* **2017**, *106*, 38–60. [CrossRef]

139. Chhetri, S.R.; Wan, J.; Al Faruque, M.A. Cross-domain security of cyber-physical systems. In Proceedings of the 2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC), Chiba, Japan, 16–19 January 2017; pp. 200–205.

140. Venkatasubramanian, K.K.; Nabar, S.; Gupta, S.K.; Poovendran, R. Cyber physical security solutions for pervasive health monitoring systems. In *E-Healthcare Systems and Wireless Communications: Current and Future Challenges*; IGI Global: Hershey, PA, USA, 2012; pp. 143–162.

141. Gifty, R.; Bharathi, R.; Krishnakumar, P. Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection. *Neural Comput. Appl.* **2019**, *31*, 23–34. [CrossRef]

142. Panoff, M.; Dutta, R.G.; Hu, Y.; Yang, K.; Jin, Y. On Sensor Security in the Era of IoT and CPS. *SN Comput. Sci.* **2021**, *2*, 1–14. [CrossRef]

143. 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]

144. Ahad, M.A.; Paiva, S.; Tripathi, G.; Feroz, N. Enabling technologies and sustainable smart cities. *Sustain. Cities Soc.* **2020**, *61*, 102301. [CrossRef]

145. Albino, V.; Berardi, U.; Dangelico, R.M. Smart cities: Definitions, dimensions, performance, and initiatives. *J. Urban Technol.* **2015**, *22*, 3–21. [CrossRef]

146. Bifulco, F.; Tregua, M.; Amitrano, C.C.; D'Auria, A. ICT and sustainability in smart cities management. *Int. J. Public Sect. Manag.* **2016**, *29*, 132–147. [CrossRef]

147. Saxena, S.; Bhushan, B.; Ahad, M.A. Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *J. Netw. Comput. Appl.* **2021**, *181*, 103050. [CrossRef]

148. Arasteh, H.; Hosseinnezhad, V.; Loia, V.; Tommasetti, A.; Troisi, O.; Shafie-khah, M.; Siano, P. Iot-based smart cities: A survey. In Proceedings of the 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), Florence, Italy, 7–10 June 2016; pp. 1–6.

149. Kim, T.H.; Ramos, C.; Mohammed, S. Smart City and IoT. *Future Gener. Comput. Syst.* **2017**, *76*, 159–162. [CrossRef]

150. Ferro, E.; Caroleo, B.; Leo, M.; Osella, M.; Pautasso, E. The role of ICT in smart cities governance. In *Proceedings of 13th International Conference for E-Democracy and Open Government*; Donau-Universität Krems: Krems an der Donau, Austria, 2013; pp. 133–145.

151. Pla-Castells, M.; Martinez-Dura, J.J.; Samper-Zapater, J.J.; Cirilo-Gimeno, R.V. Use of ICT in Smart Cities. A practical case applied to traffic management in the city of Valencia. In Proceedings of the 2015 Smart Cities Symposium Prague (SCSP), Prague, Czech Republic, 24–25 June 2015; pp. 1–4.

152. Dameri, R.P. Using ICT in smart city. In *Smart City Implementation*; Springer: Cham, Switzerland, 2017; pp. 45–65.

153. Shit, R.C.; Sharma, S.; Puthal, D.; Zomaya, A.Y. Location of Things (LoT): A review and taxonomy of sensors localization in IoT infrastructure. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2028–2061. [CrossRef]
154. Allam, Z.; Dhunny, Z.A. On big data, artificial intelligence and smart cities. *Cities* **2019**, *89*, 80–91. [CrossRef]
155. Ullah, Z.; Al-Turjman, F.; Mostarda, L.; Gagliardi, R. Applications of artificial intelligence and machine learning in smart cities. *Comput. Commun.* **2020**, *154*, 313–323. [CrossRef]
156. Ibba, S.; Pinna, A.; Seu, M.; Pani, F.E. CitySense: Blockchain-oriented smart cities. In Proceedings of the XP2017 Scientific Workshops, Cologne, Germany, 22–26 May 2017; pp. 1–5.
157. 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]
158. Majeed, U.; Khan, L.U.; Yaqoob, I.; Kazmi, S.A.; Salah, K.; Hong, C.S. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. *J. Netw. Comput. Appl.* **2021**, *181*, 103007. [CrossRef]
159. Makhdoom, I.; Zhou, I.; Abolhasan, M.; Lipman, J.; Ni, W. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Comput. Secur.* **2020**, *88*, 101653. [CrossRef]
160. Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Appl. Innov.* **2016**, *2*, 71.
161. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
162. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where is current research on blockchain technology?—A systematic review. *PLoS ONE* **2016**, *11*, e0163477. [CrossRef]
163. Bhushan, B.; Khamparia, A.; Sagayam, K.M.; Sharma, S.K.; Ahad, M.A.; Debnath, N.C. Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustain. Cities Soc.* **2020**, *61*, 102360. [CrossRef]
164. Tripathi, G.; Ahad, M.A.; Paiva, S. S2HS-A blockchain based approach for smart healthcare system. In *Healthcare*; Elsevier: Amsterdam, The Netherlands, 2020; Volume 8, p. 100391.
165. Guevara, L.; Auat Cheein, F. The role of 5G technologies: Challenges in smart cities and intelligent transportation systems. *Sustainability* **2020**, *12*, 6469. [CrossRef]
166. Minoli, D.; Occhiogrosso, B. Practical aspects for the integration of 5G networks and IoT applications in smart cities environments. *Wirel. Commun. Mob. Comput.* **2019**, 1–30. [CrossRef]
167. Rao, S.K.; Prasad, R. Impact of 5G technologies on smart city implementation. *Wirel. Pers. Commun.* **2018**, *100*, 161–176. [CrossRef]
168. Mukherjee, B.K.; Pappu, S.I.; Islam, M.J.; Acharjee, U.K. An SDN based distributed IoT network with NFV implementation for smart cities. In *International Conference on Cyber Security and Computer Science*; Springer: Cham, Switzerland, 2020; pp. 539–552.
169. Rametta, C.; Baldoni, G.; Lombardo, A.; Micalizzi, S.; Vassallo, A. S6: A Smart, Social and SDN-based Surveillance System for Smart-cities. *Procedia Comput. Sci.* **2017**, *110*, 361–368. [CrossRef]
170. Ghosh, U.; Chatterjee, P.; Shetty, S.; Datta, R. An SDN-IoT− Based Framework for Future Smart Cities: Addressing Perspective. In *Internet of Things and Secure Smart Environments*; Chapman and Hall/CRC: London, UK, 2020; pp. 441–468.
171. Bhattacharya, S.; Somayaji, S.R.K.; Gadekallu, T.R.; Alazab, M.; Maddikunta, P.K.R. A review on deep learning for future smart cities. *Internet Technol. Lett.* **2020**, e187. [CrossRef]
172. Muhammad, A.N.; Aseere, A.M.; Chiroma, H.; Shah, H.; Gital, A.Y.; Hashem, I.A.T. Deep learning application in smart cities: Recent development, taxonomy, challenges and research prospects. *Neural Comput. Appl.* **2021**, *33*, 2973–3009. [CrossRef]
173. Atitallah, S.B.; Driss, M.; Boulila, W.; Ghézala, H.B. Leveraging Deep Learning and IoT big data analytics to support the smart cities development: Review and future directions. *Comput. Sci. Rev.* **2020**, *38*, 100303. [CrossRef]
174. Bélissent, J. Getting clever about smart cities: New opportunities require new business models. *Camb. MA USA* **2010**, *193*, 244–277.
175. Ahuett-Garza, H.; Kurfess, T. A brief discussion on the trends of habilitating technologies for Industry 4.0 and Smart manufacturing. *Manuf. Lett.* **2018**, *15*, 60–63. [CrossRef]
176. Sharida, A.; Hamdan, A.; Mukhtar, A.H. Smart cities: The next urban evolution in delivering a better quality of life. In *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*; Springer: Cham, Switzerland, 2020; pp. 287–298.
177. Ménascé, D.; Vincent, C.E.; Martin Moreau, M. Smart Cities and new forms of employment. *Field Actions Sci. Rep. J. Field Actions* **2017**, *16*, 16–21.
178. Куприяновский, В.П.; Щичко, А.С.; Намиот, Д.Е.; Куприяновская, Ю.В. "Reasonable Water": Integrated Water Resources Management on the basis of smart technologies and models for smart cities. *Int. J. Open Inf. Technol.* **2016**, *4*, 20–29.
179. Canizes, B.; Pinto, T.; Soares, J.; Vale, Z.; Chamoso, P.; Santos, D. Smart city: A GECAD-BISITE energy management case study. In *International Conference on Practical Applications of Agents and Multi-Agent Systems*; Springer: Cham, Switzerland, 2017; pp. 92–100.
180. Zavratnik, V.; Podjed, D.; Trilar, J.; Hlebec, N.; Kos, A.; Stojmenova Duh, E. Sustainable and community-centred development of smart cities and villages. *Sustainability* **2020**, *12*, 3961. [CrossRef]
181. De Las Heras, A.; Luque-Sendra, A.; Zamora-Polo, F. Machine learning technologies for sustainability in smart cities in the post-covid era. *Sustainability* **2020**, *12*, 9320. [CrossRef]
182. Pilkington, M. Blockchain technology: Principles and applications. In *Research Handbook on Digital Transformations*; Edward Elgar Publishing: Cheltenham, UK, 2016.

183. Akhtar, M.M.; Rizvi, D.R. Traceability and Detection of Counterfeit Medicines in Pharmaceutical Supply Chain Using Blockchain-Based Architecture. In *Sustainable and Energy Efficient Computing Paradigms for Society*; Ahad Mohd Abdul, P.S., Ed.; Springer/EAI: Cham Switzerland, 2020.
184. Paiva, S.; Ahad, M.A.; Tripathi, G.; Feroz, N.; Casalino, G. Enabling Technologies for Urban Smart Mobility: Recent Trends, Opportunities and Challenges. *Sensors* **2021**, *21*, 2143. [CrossRef]
185. Tripathi, G.; Ahad, M.A.; Sathiyanarayanan, M. The role of blockchain in internet of vehicles (IoV): Issues, challenges and opportunities. In Proceedings of the 2019 International Conference on Contemporary Computing and Informatics (IC3I), Singapore, 12–14 December 2019; pp. 26–31.
186. Ahad, M.A.; Paiva, S.; Tripathi, G.; Haq, Z.A.; Nafis, M.T.; Feroz, N. Big Data and Modern-Day Technologies in COVID-19 Pandemic: Opportunities, Challenges, and Future Avenues. *Emerg. Technol. Battling Covid-19 Appl. Innov.* **2021**, *1*, 79–106.
187. Givehchi, O.; Landsdorf, K.; Simoens, P.; Colombo, A.W. Interoperability for industrial cyber-physical systems: An approach for legacy systems. *IEEE Trans. Ind. Inform.* **2017**, *13*, 3370–3378. [CrossRef]
188. Gürdür, D.; El-Khoury, J.; Seceleanu, T.; Lednicki, L. Making interoperability visible: Data visualization of cyber-physical systems development tool chains. *J. Ind. Inf. Integr.* **2016**, *4*, 26–34. [CrossRef]
189. Zhang, L. A framework to model big data driven complex cyber physical control systems. In Proceedings of the 2014 20th International Conference on Automation and Computing, Cranfield, UK, 12–13 September 2014; pp. 283–288.
190. Inderwildi, O.; Zhang, C.; Wang, X.; Kraft, M. The impact of intelligent cyber-physical systems on the decarbonization of energy. *Energy Environ. Sci.* **2020**, *13*, 744–771. [CrossRef]
191. Thekkilakattil, A.; Dodig-Crnkovic, G. Ethics aspects of embedded and cyber-physical systems. In Proceedings of the 2015 IEEE 39th Annual Computer Software and Applications Conference, Taichung, Taiwan, 1–5 July 2015; Volume 2, pp. 39–44.
192. Trentesaux, D.; Rault, R. Designing ethical cyber-physical industrial systems. *IFAC-PapersOnLine* **2017**, *50*, 14934–14939. [CrossRef]