


Review

# Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review

Chanapha Butpheng <sup>1</sup>, Kuo-Hui Yeh <sup>1,2,\*</sup>  and Hu Xiong <sup>3</sup>

<sup>1</sup> Department of Information Management, National Dong Hwa University, Hualien 97401, Taiwan; 810532009@gms.ndhu.edu.tw

<sup>2</sup> Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung 804, Taiwan

<sup>3</sup> School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China; xionghu@uestc.edu.cn

\* Correspondence: khyeh@gms.ndhu.edu.tw; Tel.: +886-3-8903117

Received: 2 June 2020; Accepted: 7 July 2020; Published: 17 July 2020



**Abstract:** When the Internet and other interconnected networks are used in a health system, it is referred to as “e-Health.” In this paper, we examined research studies from 2017–2020 to explore the utilization of intelligent techniques in health and its evolution over time, particularly the integration of Internet of Things (IoT) devices and cloud computing. E-Health is defined as “the ability to seek, find, understand and appraise health information derived from electronic sources and acquired knowledge to properly solve or treat health problems. As a repository for health information as well as e-Health analysis, the Internet has the potential to protect consumers from harm and empower them to participate fully in informed health-related decision-making. Most importantly, high levels of e-Health integration mitigate the risk of encountering unreliable information on the Internet. Various research perspectives related to security and privacy within IoT-cloud-based e-Health systems are examined, with an emphasis on the opportunities, benefits and challenges of the implementation such systems. The combination of IoT-based e-Health systems integrated with intelligent systems such as cloud computing that provide smart objectives and applications is a promising future trend.

**Keywords:** security; privacy; internet of things (IoT); cloud; e-Health

## 1. Innovation in e-Health Technology

Technological changes have allowed advanced solutions to be implemented to enhance the quality of human life. Researchers studying the evolution of technology have identified and evaluated health information from these sources to gain knowledge and solve health-related problems. Thus, the development of integrated healthcare technology has the possibility to enhance efficiency and improve patient outcomes at every level of the healthcare system. The development of new electronic-Health (e-Health) application systems can solve certain problems germane to traditional healthcare systems via robust patient safety controls, ubiquitous data access, remote inpatient monitoring, immediate clinical interventions and decentralized electronic-healthcare records. These systems can manage health information and patient data, enhance patient quality of life, increase collaboration, improve patient outcomes, decrease costs and increase the overall efficiency of e-healthcare services. In addition, Eysenbach [1] described e-Health as a hi-tech industry that represents the convergence of the Internet, networking and healthcare and greatly benefits the system’s users and stakeholders. E-health is an emerging field at the intersection of medical informatics, public health and Internet health services that embrace and drive the worldwide development of new technology to solve deep-seated problems, drive down costs and improve patient care. At the same time, the evolution of the Internet of Things (IoT) is the driving force for the creation of myriad smart services

that provide access to shared/configurable resources, such as computers, cloud computing/storage, network-connected devices, software, systems and other resources. Thus, models, devices and systems connected to the IoT have become ubiquitous. Moreover, the widespread adoption of IoT has coincided with the development of interrelated communication technologies, such as computing intelligence for healthcare, business, industry, operational systems and so on. The efficient and safe implementation of health information technologies, services and overarching e-Health systems requires exceedingly efficient and robust security systems to make such implementation viable. The ubiquity of IoT systems has driven research and development of IoT technology, including diverse architectures for use in health networks. Linking networks, devices, applications and services to the IoT allows e-Health systems to share related information using the latest technology.

IoT and cloud computing are emerging revolutionary technologies that complement each other's capabilities when integrated as flexible, scalable and efficient patient healthcare systems. The combination provides benefits including ease of implementation compared to conventional networks, enhanced information security during communication, quick access to records and energy savings over traditional modalities. IoT-cloud-based e-Health systems can significantly improve healthcare services and promote continuous systematic innovation. In IoT-cloud-based e-Health systems, underlying IoT networks enable communication between users, services and servers, with medical data stored in the cloud.

With new developments in cloud computing continuing to push beyond the status quo, however, various security threats to communicated or stored information must be considered. Pasha and Shah [2] developed a framework for IoT-based smart health systems used as an e-Health system, focusing on interoperability, different technology standards, communication protocols and system requirements in its design. The relevant protocols and standards utilized web technologies, communication protocols and hardware design. Their framework was proved secure by confidence experiments that showed the interoperability between different IoT devices, standards and protocols in an e-Health system could be achieved and used simultaneously in the Internet environment. Rahmani et al. [3] proposed the concept of Fog computing in a healthcare IoT system as a smart e-Health system to implement a distributed intermediary layer of intelligence between sensor nodes and the Cloud. They capitalized on the ubiquity of existing healthcare systems to alleviate the burden on sensors, networks and remote healthcare centers, thereby solving mobility, energy efficiency, scalability and reliability issues. The successful implementation of their e-Health system is a gateway called UT-Gate that provides higher-level features such as an IoT-based Early Warning Score (EWS) health monitoring system with enhanced overall system intelligence, efficiency, performance, interoperability, security and reliability. Robinson et al. [4] designed a system integrating smart IoT devices to allow access to patient data via the internet using cloud computing. By facilitating the acquisition and accumulation of data needed to monitor patient health, physicians were better able to solve their health problems in timely fashion. Using cloud computing, Islam et al. [5] designed a four-step architecture for e-Health systems comprised of devices, data aggregation and processing, data storage and data analysis. They described applications where the system would be useful, related technologies necessary to make it work and attendant benefits and limitations. Shewale et al. [6] proposed IoT-based body sensor network technology utilizing lightweight wireless sensor nodes with IoT built-in to sending and receiving data via cloud computing. They consider privacy and security protocols to secure the healthcare system and ensure patient data remains confidential. Selvaraj et al. [7] analyzed the growing integration of IoT devices and cloud computing in e-Health systems and outlined relevant challenges, opportunities and limitations. They pointed out authentication are crucial to IoT-cloud-based e-Health system security and proposed an authentication scheme to secure IoT-cloud-based e-Health systems with superior performance and convenience protocols. Kaur et al. [8] summarized the advantages of cloud hosting services and concluded that IoT-cloud-based applications add great value to startups by increasing flexibility, expandability and reducing cost by virtue of a pay-as-you-use structure. Whereas, IoT-based systems and cloud computing systems were once discrete, they have gradually

been combined into a codependent system that can execute highly specialized tasks and process massive quantities of data efficiently. Similarly, Dang et al. [9] presented a survey on IoT and Cloud computing for healthcare. They presented survey cloud computing for healthcare and indicated various concepts application in IoT and cloud computing for healthcare. Moreover, they described the healthcare industry trends and policies regarding IoT and cloud computing around the world. The most common problems with combined IoT-cloud-based systems are high latency and bandwidth requirement to transmit and receive data between IoT devices and cloud servers. Consequently, security challenges are inherent to the integration of IoT-based and cloud computing in e-Health systems. Chattopadhyay et al. [10] presented a framework for IoT-based healthcare systems and introduced a secure communication process. Their model has three different kinds of communication channels: from the biometric sensor nodes (the edge sensors) to the internal processing unit (IPU), from the IPU to the gateway (router) and from the gateway to the cloud. Nandyala and Kim [11] examined IoT-cloud technologies in the form of embedded devices, sensors, and actuators to generate big data, compute it, and provide storage for it using cloud computing. They showed how data can be analyzed and shared in real-time using network-connected IoT devices and cloud computing resources to implement healthcare monitoring systems in homes, hospitals, and other locations. Maksimović [12] analyzed the benefits of implementing cloud and fog computing in IoT-based e-Health systems and showed IoT is a positive influence on all aspects of healthcare. Specifically, the presentation of the processing and analytical capabilities are used to illustrate how principles of cloud and fog computing can be used to deal with patient data in healthcare settings. Yeh [13] presented a secure IoT-based Healthcare system with body sensor networks. He introduced a secure IoT-based healthcare system that operates through body sensor networks and indicated system efficiency and robustness of transmission within IoT-based communication networks. Similarly, Deelip and Sankpal [14] presented IoT-based Smart and secure healthcare system analysis and data comparison by using body sensor networks technology. They indicated the security and privacy of patients is a very essential protection provision in body sensor networks healthcare system. To ensure the privacy of the data transmission system is secured for the healthcare system. As aforementioned above voluminous research [1–14] therefore been devoted to mitigating risks related to privacy, integrity, trust, or information authentication.

IoT-cloud-based e-Health system studies have designed efficient security protocols to provide comprehensive frameworks with critically important software elements to ensure accurate and secure transmission of data between devices. In addition to security and privacy, IoT-cloud-based e-Health systems must also be designed with efficiency in mind, such that any volume of data can be analyzed and transmitted easily and without added delay from implemented solutions. The bulk of critical privacy and security elements for IoT-cloud-based e-Health systems involve data confidentiality [2–4,10,13,14], data integrity [4,6,10,13], service availability [10–12,14], accountability [6,10,13], authentication [4,12,13], access control [3,5,9,10,13,14] and non-repudiation [4,7,13,14]. Although several works have studied the security and privacy issues of IoT-cloud-based e-Health systems with various integrated implementations, the security and privacy for IoT-cloud-based e-Health systems warrant closer scrutiny. Of particular concern are insecure techniques for e-Health systems that may lead to the breach of healthcare record confidentiality if hackers or a man-in-the-middle attack (MITM) can gain full access to patient accounts. Devising a secure technique for IoT-cloud-based e-Health systems can overcome this threat to patients, physicians, and other stakeholders.

### *1.1. Innovative e-Health Concepts*

Innovative e-Health systems are revolutionizing health by empowering users as new applications and protocols that were not possible a decade ago are developed. It is difficult to define innovative e-Health systems because new concepts that are constantly being developed will eventually become the new cornerstones of modern health systems such as presented in Ambarkar and Sheokar [15] analyzed and compared research the concept of IoT systems and healthcare IoT systems by investigating the security measures incorporated in the healthcare IoT system. The investigation leads to the conclusion

that the security provided for the healthcare IoT systems by analyzing various architecture and further discusses the potential IoT systems enhance the healthcare system. Farahani et al. [16] presented the benefits of adopting IoT healthcare which the technologies can improve diagnostics in a variety of applications. IoT-enabled devices will help physicians with the information to create data-driven treatment plans, significantly improving the chance of a successful recovery. Abouelmehdi et al. [17] presented big data to drive e-Health systems, knowledge discovery, aspects, and personal health management. They indicated true potential IoT-based e-Health systems and healthcare field including the advantages and disadvantages of privacy and security technologies in the context of big healthcare data. Similarly, Connor et al. [18] indicated usability of IoT within the smart health domain and presented the privacy concepts can be integrated for IoT smart healthcare. They proposed a practical application IoT-based can assist with addressing healthcare problems. Hathaliya and Tanwar [19] presented an exhaustive literature review and analysis on security and privacy issues in Healthcare 4.0. They explored the blockchain-based solution for security and privacy issues in Healthcare 4.0. Then they showed the advantages of security and privacy techniques used, tools, frameworks in Healthcare 4.0. Similarly, Aceto et al. [20] introduced Industry 4.0 and highlighted the relevant to healthcare 4.0. They presented the application scenarios of healthcare 4.0, how to adopt Industry 4.0 technologies to healthcare 4.0. To provide the main benefits, services, technologies in relation to healthcare.

The following is a list of fundamental concepts of innovative e-Health systems:

- Ambient Assisted Living (AAL): the placement of smart objects within an assisted living environment that care for and assist seniors to live more independently. AAL applications also collect, manage, and analyze patient activity to allow remote monitors to react quickly to emergencies and accurately investigate allegations of mistreatment [1,6,8,15,18].
  - Internet of Health Things (IoHT): smart devices with integrated mobile and cloud computing capabilities used in the medical field to monitor patient data in real-time. Collected data can be analyzed immediately and used to diagnose and treat patients quickly and effectively. However, such systems are still vulnerable to security attacks and privacy leaks, which many researchers have tried to identify and rectify [1,2,4,10,16,19,20].
  - Wearable Devices: a distinctive sub-category of IoT devices, such as smart wristbands, watches, shoes, shirts, caps, necklaces, headbands and eyeglasses with integrated sensors and microcontrollers. Most of these devices operate on the fixed IEEE 802.11 standard frequency [5,14].
- Blockchain: a system in which a record of actions is maintained across several computers linked in a peer-to-peer network. Use of blockchain technology in health systems can increase transparency between patients and doctors, ensure efficient collaboration between health organizations using smart contracts and resist failure and data fragmentation with its decentralized and distributed architecture as used in Ray et al. [21] presented blockchain technologies for IoT-based healthcare that are being heavily exploited and used in many domains. They presented consensus algorithms and platforms in IoT-based e-healthcare. They showed how their key features of the IoT and blockchain can be leveraged to support healthcare services. However, blockchains are inherently highly vulnerable to attack because of their transparency.

IoT-cloud-based e-Health system implementations are highly variable and can be tailored to meet the needs of specific e-Health system providers. Therefore, e-Health system providers offer many different types of IoT and cloud computing services to allow functionality like continuous monitoring, preventive care, patient satisfaction tracking and AI-driven diagnosis. Each of these services constitutes a potential privacy leak that must be considered when implementing privacy protection measures within a given system. Growing awareness among end-users has made them more cautious than ever about the privacy of their medical data. For example, if a patient suffering from an embarrassing health condition had their confidential information leaked or disseminated on social media, it would be difficult to maintain their trust in the health service provider, not to mention extremely difficult for

the provider to rectify the situation such indicated in Nazir et al. [22] presented IoT for healthcare by using effects of mobile computing. They used a systematic literature review protocol and showed how mobile computing can assist IoT application in healthcare. The IoT in healthcare system can bring privacy and security in health IoT devices. Similarly, method used in Semantha et al. [23] analyzed the contemporary based on a systematic literature review to examine privacy by design frameworks in-depth targeted at the healthcare sector and identify the key limitations in the healthcare section. They propose their viable for the future research and development direction for healthcare. Wu et al. [24] established a model based on mobile health for IoT system in social networks. The model is applied to a social network which user can used the model through APP in IoT for diagnosis and treatment. The model can modify the control variable, provide the most effective for hospitals. Khatoon et al. [25] presented a survey on application of IoT in healthcare. IoT for healthcare services can enhance the reliability and quality to the patients. The IoT in healthcare consists of sensor enabled smart devices that accurately data for analysis and actions.

However, the implementation of IoT-cloud-based e-Health systems can be used in different situations. For example, presented in Tuli et al. [26] presented an ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and Fog computing environments. To provide efficient computation services to heart patients and other user requiring in real-time results. Cloud based computation model is required to deliver healthcare and latency sensitive high accuracy results. Gupta et al. [27] proposed an IoT-based smart sole shoe to detect the health of foot ulcer. They designed of IoT-based system to be used in healthcare for detection of diabetic foot ulcer by divided into four section works. The model will monitor the health of diabetic foot ulcer patient and will send alerts if found any abnormality. Elmisey et al. [28] presented a new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services. They collected and processed of the health data from various IoT-based healthcare devices by utilized cloud healthcare services. The integration is to achieve patient privacy which can control the usage of their health data.

The security and privacy measures previously discussed can be implemented in almost any situation. In IoT-cloud-based e-Health systems, the following technologies are among the most commonly integrated ones:

- **Wireless Sensor Network (WSN):** a flexible, scalable, dynamic, cost-effective ad-hoc network of analog or digital devices and nodes that communicate using secure radio signals. They enable providers to monitor their patients in real-time. The communication of WSNs secured via hardware and software can act as an adversary to sense and challenge the individual wireless signals transmitting data to determine authenticity [2,19,22,24–26].
- **Body Sensor Network (BSN):** a collection of sensors connected to the body of a patient that transmits data wirelessly to system nodes for later analysis. The patient's data is collected by the sensors, then transferred to the nodes using commonly accepted routing and switching protocols such as LoWPAN, multi-hub routing and so forth. [5,14,22,25].
- **Radio Frequency Identification (RFID):** a low-cost system of physical tags that continually transmit information over very low radio frequencies and the accompanying readers. RFID provides automatic identification and easy monitoring/tracking. RFID readers identify the tags, collect, process and transfer the data to designated servers. RFID tags are usually attached to the patient to collect physical health system parameters or are used in inventory systems to track medication and other miscellaneous hospital supplies and equipment. RFID has a protracted lifespan as the tags do not require power to operate as used in Fan et al. [29] presented lightweight RFID protocol for medical privacy protection in IoT. The application of RFID system to the medical system can effectively solve the problem of medical privacy. RFID can collect useful information and conduct data exchange and processing with back-end server through the reader.
- **Remote Patient Monitoring (RPM):** a system that utilizes flexible wireless or web-based services to monitor patients without physical contact. RPMs are used in conjunction with WSNs, BSNs and

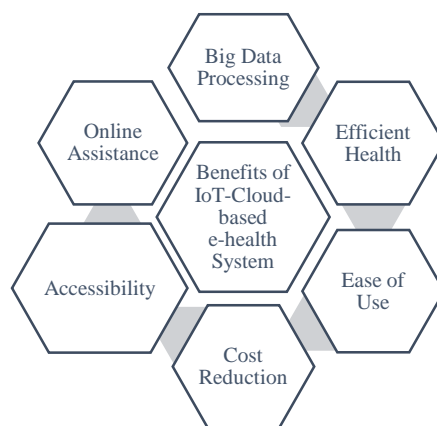


various IoT devices. RPMs are commonly used for patients that are discharged from the ICU and shifted to a general ward, patients at high risk for complications or patients with special needs [13,26–28] and more presented in Shirley et al. [30] combined the IoT and cloud computing to develop a framework for healthcare applications where the patients, patient's family members, doctors, nurses, attenders, technicians, or health center that everyone can share data and service on the a single platform. The system has improved the performance, increased efficiency, and maximized resource utilization. Khader et al. [31] provide a competent and structure approach to handle service deliverance aspects of healthcare in terms of mobile health and remote patient monitoring. IoT generates of data that can be processed using cloud computing. Swaroop et al. [32] presented and designed a real-time health monitoring system which can store a patient's basic health parameters. The data can be made available to a medical practitioner as an alert. They health monitoring system enhance healthcare delivery by communicating multiplexed data over internet. Additionally, Wilt et al. [33] presented e-Health services like online diagnostic testing, help to increase efficiency in work processes and decrease the workload. They examined the general practitioners' attitude towards and adopting of e-Health in general and online diagnostic testing in specific primary care.

As mentioned above, the flexibility, adaptability and resilience of IoT-cloud-based e-Health systems give rise to numerous advantages:

- All-encompassing: IoT-cloud-based e-Health systems are customizable enough to satisfy stakeholders' needs when used in virtually all fields, including remote monitoring, patient diagnosis, medication tracking, adverse drug interaction detection, safety monitoring and so on. [6,20,21,33].
- Big Data Processing and Analytics: IoT-cloud-based e-Health systems can effectively process, analyze and manipulate vast quantities of multi-modal, multiscale, distributed, heterogeneous data collected by IoT devices connected to networks [1,7,8,12,16,19,21–23,30].
- Lifetime Monitoring: IoT-cloud-based e-Health systems can effectively collect, store, track and process patient data from the past, present and predicted future. This can greatly improve patient outcomes and make targeted preventative treatment more feasible and effective [18,20,24,32].
- Ease of Use: IoT-cloud-based e-Health systems are easily adopted by users as they only require clicks on wearable devices, simple input interactions using smartphone applications or simply wearing sensors and allowing the systems to collect data automatically [1,4,8,16,19,21,22,24,25].
- Cost Reduction: IoT-cloud-based e-Health systems can integrate diverse technologies to increase efficiency, decrease waste and drive down costs. Moreover, they can scale up or down quickly based on demand and they allow health systems to pay-as-they use [3,16,18,22,25–27].
- Increased Physician Involvement: in IoT-cloud-based e-Health systems physicians can obtain patient health data in real-time and remotely. This enables them to monitor more patients wearing sensors, improve outcomes and even engage in telemedicine under certain circumstances [1,8,18–20,22,25,29,32].
- Accessibility and Availability: in IoT-cloud-based e-Health systems patients, caregivers and healthcare professionals can access e-Health data or services anytime, anywhere by using cloud computing servers or web servers [1,4,8,19,22,28,32].
- Online Assistance: IoT-cloud-based e-Health systems enable anytime, anywhere, real-time communication and assistance [8,19,22,25,26,28,29].
- Efficient Health Resource Management: IoT-cloud-based e-Health systems guarantee patients have access to their data so they can learn about their health status. They also allow physicians to monitor patient health effectively and efficiently and control the allocation and use of health resources precisely [1,3,4,8,16,18–22,24,25,30].

The aforementioned benefits of IoT-cloud-based e-Health systems are illustrated in Figure 1.



**Figure 1.** The benefits of Internet of Things (IoT)-cloud-based e-Health systems.

### 1.2. How IoT and Cloud Computing Can Be Integrated with e-Health Systems

The Internet of Things (IoT) and cloud computing are emerging revolutionizing technologies that can be integrated to complement each other's capabilities and competencies. The integration between IoT and cloud computing is known as the Cloud of Things (CoT). CoT comprises intelligently connected humans, machines, devices, objects, systems and applications communicating with each other via the internet. The implementation of cloud computing and IoT technology in e-Health systems leads to improved patient outcomes thanks to streamlined health diagnostics and treatments, provides convenience and reduces costs without loss of redundancy. The integration and utilization of IoT with cloud computing technologies for e-Health systems is convenient because users can access services via cloud servers anytime, anywhere and in any environment. These numerous advantages mean security and privacy problems are often overlooked in a trade-off for convenience and efficiency. Each IoT device is discrete, has its core functionality and purpose and gathers private data. Cloud computing technology integrates IoT devices and stores and processes the data in a distributed private network of cloud servers in e-Health systems. Cloud computing enables authorized users to authenticate themselves and securely access data from anywhere via robust authentication. Kang et al. [34] provided a novel approach and solution IoT-based which can interact with technologies such as mobile health, cloud computing, big data, and smart environments. The result from their experiments to reduce bandwidth and battery resources with hear rate have accuracy of data transmitted after inference by up to 99%. Wang et al. [35] presented technological advancement of IoT devices can be combined with cloud computing. Their framework is evaluated quantitatively reduce the medical data retrieval latency and cost compared with the existing solution. Yamin [36] provide an overview the importance IoT-based and benefits of IT and how data management can be contributed to the medical science. field. The medical data collected from different institutions can be mined and analyzed by using big data via internet. Mohammed and Meri [37] presented utilizing the new trend technologies in healthcare sector. The alternative way for patients' health records and improved the healthcare quality. They provided the overview of IoT technology in healthcare can be emerging and connecting via smart devices or objects with capabilities of collecting and sharing in various types such as people to machine (P2M), people to people (P2P), or machine to machine (M2M).

Additionally, the use of cryptanalysis in the authentication process can confirm if the protocol is protected against all possible security threats. Thus, IoT-based technology and cloud computing in e-Health systems requires careful consideration of security, privacy, reliability and trust [6–37] because it uses communications technology to connect devices or machines. Connections may take the form of device to machine (D2M) as used in References [21,36], object-to-object (O2O) as used in References [28,37], machine to machine (M2M) as used in References [26,32], patient to doctor (P2D) and patient to machine (P2M) as used in References [13,32]. Cha et al. [38] attempted to facilitate access and transmission for IoT device services and applications and explicate the vulnerabilities of system

architecture. They conducted a comprehensive review of potential security/privacy threats and the corresponding technologies necessary to mitigate them. Zhou et al. [39] described alternative key security and privacy properties such as authentication against invalid data access, anonymity and intractability and resistance to spoofing attacks to secure IoT-based systems with cloud computing. These properties are indispensable for guaranteeing security and privacy in IoT-based e-Health systems.

IoT-based systems represent a watershed in the e-Health industry because they allow for off-site remote monitoring. Mohanty and Das [40] presented an IoT health service model for hospitals to monitor patients and connected devices remotely, using a cloud-connected device. The model implements a scope that can read barcode sensors that capture and process user authentication credentials. The proposed system sensor is wireless and is used inside a specifically designed smart room to monitor babies as part of an integrated wireless sensor network. Muzammal et al. [41] studied the possibility of implementing cloud and fog computing and found improved cloud computing to be capable of efficiently processing and analyzing data for IoT-driven e-Health systems in which IoT devices are embedded with electronics, software, sensors and network connectivity which allows them to sense, collect and exchange information in the environment or among each other. The data are processed, analyzed and transmitted via the internet, wireless, remote control. System parameters ensure real-time feedback is available to users or physicians to facilitate further medical analysis or treatments. Iman et al. [42] combined IoT and cloud technologies in a flexible, scalable and efficient remote patient healthcare monitoring system using wireless technologies for an e-Health system. Physicians use IoT-cloud for checking patient records and making diagnoses while the patients use it to monitoring their health improvement. Tyagi et al. [43] proposed a wearable IoT-based remote patient monitoring system with cloud computing to collect patient data. The monitoring devices are tiny patches that adhere to the skin, clothes, shoes and so forth and data are uploaded or downloaded from the devices via transmission systems. The cloud application's back end will save the patient's medical records and stored data to share with physicians on demand by the patients. Nandyala and Kim [11] proposed a U-healthcare monitoring system for machine-to-machine (M2M) interaction, data collection, data processing and conveying control commands to the actuators. Networked sensors capture patients' data, which can be augmented with information such as body temperature and blood pressure. The sensors and actuators are essentially medical equipment that connects with the network to transfer data to cloud computing. Focusing on a healthcare management system for hospitals in India, Thakare and Kumbhar [44] analyzed the potential for combining IoT and cloud computing services with artificial intelligence (AI) to collect data for diagnosis or treatment of diseases, monitor patients remotely and store and process data. Similarly, Khan [45] utilized IoT technology in a healthcare system to collect sensor values for heart disease diagnosis and prediction. He proposed an IoT-based framework to evaluate heart disease by using a modified deep convolutional neural network (MDCNN) as a wearable smartwatch device attached to the patient, which monitors blood pressure. Comparison of the proposed network with MDCNN and results of logistic regression demonstrated the superiority of the proposed system's 98.2% accuracy rate.

Table 1 summarizes how IoT and cloud computing can be integrated with e-Health systems. However, the integration and implementation of these distinctive systems are neither perfect nor easy. As with any new technology, myriad challenges remain in relation to open issues for IoT-cloud-based e-Health systems, as shown in Table 1 as well.



**Table 1.** The integration and utilization of IoT and cloud computing for e-Health systems.

Implementation	Benefits	How to Integrate and Utilize in e-Health Systems	Open Issues
IoT-based	<ul style="list-style-type: none"> <li>Enhanced electromedical devices.</li> <li>Interoperability and evolvability.</li> </ul>	<ul style="list-style-type: none"> <li>Internally embedded [2,3,5,6,21,22,35].</li> <li>Wearable technologies [3,4,6,9,10,17–19,24,26,36,37,39,41].</li> <li>Remote patient monitoring [2–4,10,11,17–19,21,26,27,35,36].</li> </ul>	<ul style="list-style-type: none"> <li>Energy constraints.</li> <li>Security.</li> <li>Scalability.</li> </ul>
Cloud Computing	<ul style="list-style-type: none"> <li>Infrastructure for high-level functions.</li> <li>Paradigmatic model for offering services to patients or healthcare operators.</li> </ul>	<ul style="list-style-type: none"> <li>Access Control for users [3–6,9,10,13,16,18,19,25,26,32,33,38].</li> <li>Patient Privacy protection [4,9,14,19,24,35,36,41,44,45].</li> <li>Security communications and security protocols [3,4,6,9,15,16,35–37,40–43,45]</li> <li>Reliability and Trust [3,6,18,19,21,42,43,45]</li> </ul>	<ul style="list-style-type: none"> <li>Performance monitoring.</li> <li>Obscurity of the infrastructure.</li> <li>Data privacy.</li> <li>Infrastructure availability.</li> </ul>

### 1.3. The Organization of This Study

In this paper, we summarize the major contributions to e-Health systems from implementing robust IoT-based and cloud computing techniques. Additionally, we provide critical system requirements for IoT-cloud-based e-Health systems and investigate existing possible security and privacy solutions. The remainder of this paper is organized as follows: Section 2 introduces challenges in innovative IoT-cloud-based e-Health applications, while Section 3 presents the central considerations of security, privacy and system requirements in IoT-based e-Health systems with cloud computing. This same section also provides an overview of the current system requirements, from a technical point of view, in the context of security and privacy in IoT-cloud-based e-Health systems. Section 4 proposes existing security and privacy related solutions for IoT-cloud-based e-Health systems. Section 5 discusses the research studies selected for analysis published between 2017–2020. Lastly, the conclusions and recommendations for future development and research into IoT-cloud-based e-Health systems are presented in Section 6.

## 2. Challenges in IoT-Cloud-Based e-Health Innovations

IoT systems facilitate the connection of both small and large systems, using the internet to communicate. Users must be fully confident in the security of IoT devices/systems due to related concerns about data privacy. IoT systems are inherently vulnerable to outside attack or manipulation because IoT devices use conventional networks to connect virtually everything wirelessly. While researchers strive to find viable solutions to security and privacy issues, these two aspects are usually researched in isolation, as discrete variables. We believe, however, that security and privacy breakthroughs will only be accomplished if the variables are merged and researched as a unified system, with an emphasis on Confidentiality, Integrity and Availability (CIA). Some security threats in IoT-based systems are attacks by spoofing, eavesdropping, jamming, crypto-attack, wormhole attack and so forth. The security requirements of IoT-based systems are dependent on the characteristics of the environment in which the system is implemented, and the devices required for users' specific applications. Researchers such as [2,7,9,10,15,16,23,25,33,36,40] have designed custom security and privacy architectures for specific IoT applications and presented security requirements for IoT-based systems utilizing standard CIA with additional custom security variables, such as authentications that are all assessed and challenged by classical security risk analysis. For instance, a smart home system used to control home appliance functions was presented by Nagaraja [46]. Such a system must

incorporate strong security to prevent attacks, particularly on wireless communications between the IoT-based appliances. Novel architecture for IoT-based home automation was proposed to protect prevent any attacks on wireless communication, including man in the middle attack (MITM). Recently, Li et al. [47] presented an algorithm for IoT-based systems that can secure all transmissions and manage resources within a heterogeneous network. The algorithm uses lightweight encryption and resource management architecture to increase system performance, efficiency and accuracy. A study by Amin et al. [48] evaluated and compared new protocols against the protocols that they are intended to replace. A protocol evaluation system can measure and compare parameters such as performance, resource usage and security treat robustness, as used in References [42,43]. Fan et al. [29] applied an RFID system to a medical system to solve the problem of privacy. RFID tags embedded in the system collect information and conduct data exchange and processing with the back-end server through the reader. They also presented a lightweight mutual authentication scheme for use in a medical context based on a novel protocol. The scheme consumes fewer computing resources to meet the security requirements such as anonymity, attack resistance, synchronization and so on. This scheme bolsters the efficiency of the medical system and can protect private patient data securely. Deebak and Turjman [49] designed the implemented with selected sensor monitor nodes in ad hoc sensor network to improve secure data transmission between IoT devices and cloud computing. To offer flexible routing, monitoring security protocol with multi-variant tuples using symmetric key. The mechanism allows the ad hoc sensor network to escalate the secure data transmission. Sharma and Singh [50] presented an overview of WSN. The WSN architecture applications in different fields and overview of the security aspect on routing in WSN. They provided an analysis of various security protocols in opportunistic routing. The standards can be defined as the protocol and functions used by sensor nodes to interface different kind of networks. Moreover, Garcia et al. [51] integrated IoT and WSN technologies that can be applied in the development of these systems. They presented a survey to summarize the current smart irrigation system by using IoT-based irrigation system regarding water quantity and quality, soil, and weather conditions. They indicated the utilization nodes and wireless technologies are practice for the implementation of sensor-based irrigation system. Therefore, IoT-based and cloud computing is the best implementation in widely varying fields.

IoT and cloud computing have been combined and integrated into e-Health systems all over the world. This has caused overarching changes in operating principles, medical device protocols, privacy and security and health systems. IoT-cloud-based systems make remote health systems feasible for the first time in history. Doctors can now observe, diagnose, consult and prescribe remotely, without ever having to meet the patient physically. Nevertheless, there are several challenges that need to be considered and addressed for the integration of IoT-cloud-based e-Health systems to be successful. The collecting and exchanging of health information have become challenging due to the increasing demand for health services, as well. The following issues and challenges related to IoT-cloud-based e-Health systems have been identified from the literature.

### 2.1. Resource Management

- Resource Management: the separate concepts of IoT, cloud computing, health systems and all associated resources are combined into one heterogeneous system. Therefore, resource management is critical to consolidate resources, eliminate redundancy, increase efficiency and reduce system lag when an IoT-cloud-based e-Health system is implemented. The resource management system must be perpetually optimized to realize continued efficiency gains and/or prevent degradation of efficiency [7,15,18,29,38].
- Address shortage: the storage of health information in cloud computing or other related technologies allow patients and other users to monitor healthcare and access and utilize health information at any time and place. While choices can be made about managing stored information online, users have legitimate concerns about storing their personal information on the Internet. In addition, collected data must be managed in compliance with standard formats and protocols

in order for them to be retrieved and used by other healthcare providers. However, a common standard protocol for data is yet to be conceived [42,43,48]. Furthermore, patients should be allowed to access their own data and be given the right to dispose of these data freely, while ensuring that their information is secured [5,9,11,14,33,39,47].

- **Compatibility:** compatibility refers to potential adopters perceiving innovations as consistent with their values, previous experiences and needs. Physicians' expectations for e-Health systems utilizing IoT technologies and cloud computing should be compatible with the exigencies of their work, including the need to motivate patients and other stakeholders to adopt and learn how to use such technology [1,20,26,27,30–32].
- **Integrated patient data:** this challenge refers to the combination of patient data that are obtained from IoT-cloud-based e-Health systems for sharing healthcare information. The unification of patient data provides excellent opportunities for long-term care, improving care quality and analyzing and monitoring care service delivery and patient health outcomes [3,7,18,21,24,30,35,36].

## 2.2. System Components

- **System capability:** IoT-cloud-based e-Health systems used in hospitals, clinics or other sites should be effective and sustainable. System capacity limitations could result in the failure to implement technological improvements and the need to upgrade to improve capability. This may stem from the delayed development of a standard in a compliance program or system. The overlapping of functions among the needs of several areas reduces the need for information exchange [3,5,7,9,20–22,26,28,35,41,48].
- **Interoperability and Standardization:** the difficulty of standardizing heterogeneous systems makes interoperability difficult as well. The various components of heterogeneous IoT-cloud-based e-Health systems use different hardware, software, operating systems, I/O methods and so on, which increases complexity and raises interoperability issues. Therefore, standards must be established to reduce interoperability complexity and make integration easy [3,13,14,20,21,26,41,47–49].
- **Data Analysis:** a fully integrated IoT-cloud-based e-Health system has thousands of connected smart sensors that are perpetually collecting and communicating a huge quantity of data. Thus, for IoT-cloud-based e-Health systems to be able to analyze all the data, the data processing infrastructure must grow proportionally to the quantity of data collected [7,9,15,18,29,38,40,45].
- **Transition Process:** e-Health integrates IoT-cloud-based systems into existing health systems by replacing or adding sensors, medical devices and operating protocols. The integration of new equipment and procedures is rarely smooth. It must be done deliberately over time and all relevant personnel must receive appropriate training. Additionally, all new devices and protocols must have backward compatibility with the system being replaced or modified [25,31,42,43,48].

## 2.3. Security and Privacy

- **Security and Privacy:** facilities that utilize IoT-cloud-based e-Health systems must be fully cognizant of inherent vulnerabilities and threats and actively design security and privacy architectures to protect networks. Security and privacy issues must be identified and addressed proactively and all vulnerabilities and threat vectors must be considered for each system layer. Due to security and privacy concerns [17,19,38,39,47], many physicians and healthcare providers prefer to store patient records on computers or local systems that are not connected to the Internet. Medical record exchange requires the development of infrastructures to allow physicians to exchange clinical data while guarding patient data security [15–17,23,25,42,43,45].
- **Privacy awareness:** privacy awareness measures can be deployed in a specific system to inform the public about privacy risks or raise awareness. The privacy and security warnings attempt to create awareness of potential privacy risks. Privacy awareness systems and services are increasingly

required to comply with established frameworks laws, regulations, ethical requirements and industry-specific operational standards. For example, Abstract Personal Data Lifecycle models (APDLs) facilitate the traceability of personal data (see more detail in Section 4) [23,28,29,38,44]. In addition, Diamantopoulou et al. [52] proposed the patterns expert knowledge and provided predefined solutions for satisfaction of different typed of privacy concerns. The pattern presented are used as a component of an existing privacy aware system design methodology. Perera et al. [53] evaluated how a set of privacy guideline can be used to effectively improve the IoT application design. They integrated the method for applying to privacy by design framework and IoT applications. Their method is uniquely designed to address IoT challenges and significant difference from existing privacy by design frameworks.

### 3. Security, Privacy and System Requirements for IoT-Cloud-Based e-Health Systems

In this section, we provide an overview of technical system requirements related to privacy and security in IoT-cloud-based e-Health systems, including identity, authentications and authorizations. By examining each aspect and independently identifying vulnerabilities, systems can be designed that can reduce the chances of attack and of private data being leaked. Privacy has various types, states, clusters, categories and dimensions, including information privacy. This section discusses ongoing plans to integrate IoT-based and cloud computing-based systems for use in e-Health systems. This research is still in its infancy, since most e-Health applications have only emerged in recent years. The following is a summary of general security and privacy concerns in IoT-cloud-based e-Health systems:

- All data must be gathered, processed and used fairly in accordance with the law [16–18].
- All data must not be used without an adequate level of security and privacy protection [17,18,23].
- All IoT devices connected to a given network must be able to transmit and receive data through the network without compromising data accuracy or integrity [11,24,31,33,36].
- All devices must be designed to provide comprehensive security against certain attacks, unauthorized access to the system and unauthorized use or adulteration of data [10,14,15,19,20,22,24,30,31,33].
- Clearly Defined Data Protocols: protocols involving data collection, transmission, authorized uses, authorized users and informed consent must be clearly defined in simple language. This will improve patient trust and specifically outline all responsibilities related to patient data so that accountability can be traced easily [1,3,4,7–9,13,14,26,27,30].

When deciding what minimum security requirements are required to secure data in an e-Health system, it is also necessary consider what the least possible security, privacy and system requirements should be as well. The following are what we consider to be the security, privacy and system requirements to ensure patient trust when providing their data to e-Health systems.

#### 3.1. Security Requirements for IoT-Cloud-Based e-Health Systems

In order to propagate the use of IoT-cloud-based e-Health systems successfully, Bhattacharjya et al. [54] identified data protection, data integrity, confidentiality, authentication, encryption and access accountability as fundamental security functions. In an investigation on security and privacy in IoT-based systems, Srinivas et al. [55] showed the chance of individuals' private data being leaked could be reduced by utilizing a database that provides identification services and authentication. Other related research has been dedicated to the authentication architecture used to secure IoT-based cloud computing systems used for smart innovation, technology development, environment simulations and various educational applications [44,47,48]. In addition, Kalyani and Chaudhari [56] presented an efficient approach for enhancing security in IoT-based by using the optimum authentication key. The enhances IoT security authentication by utilizing cryptographic-based methodologies to secure IoT sensitive data with the help of optima homomorphic encryption with high dependability. During

encryption the key authentication and optimal key is selected by using step size fire optimization algorithm. Yu et al. [57] provided a secure authentication and key agreement scheme for IoT-based cloud computing environment. The cooperating with cloud computing, IoT-based can provide more efficient and practical services. To implement effective access control and secure communication in IoT-based cloud computing environment and identity authentication should be secured. Garg and Diksha [58] classic wireless IoT application scenarios along with associated models of safety and privacy assault. They present security and confidentiality in wireless IoT requires data privacy, safety, assault robustness, and self-maintenance. The data information is used in wireless IoT for excellent reason, danger emerge as attackers seek to take advantage. Jimenez et al. [59] adopted wireless body area networks (WBAN) IoT along with cloud computing systems has led to the development of new methodologies to monitor and treat patients. The adoption of the new technologies comes with several challenges in terms of performance and security. Considering that, WBAN can be wearable or implanted under the skin, and the overall concept leads to cybersecurity.

In general, the security of an IoT-cloud-based e-Health system can be assessed by using classical security and risk analysis measures, such as CIA and others. Based on our literature review, we can summarize security as having the following elements:

- Confidentiality: ensures that exchanges between a sender and receiver are protected against any malicious or unauthorized misuse. Confidentiality needs to be guaranteed for the entire communication network, including the transmissions between various IoT devices and cloud computing to e-Health systems [2,3,15,24,44,51,56].
- Data Integrity: ensures that the content exchanged between a sender and receiver is protected against any manipulation from malicious or unauthorized users without the receiver being able to track the manipulation. In an IoT-cloud-based system, an integrity check can be carried out at each node involved in the exchange between the sender and receiver [3,24,42,51,53,59].
- Availability: ensures that malicious or unauthorized users are incapable of disrupting or harmfully affecting communication or the quality of service provided by the IoT-cloud-based system's communication network [3,4,7,8,13,17,33,47,54,56].
- Access Control: controlling and restricting user access to protected information by evaluating, deciding and enforcing access [3,6,9,13,18,25,26,32,46,53].
- Anonymization: use of anonymous authentication protocols to preserve privacy and security [2,8,9,14,42,56].
- Authentication: verifying and validating user credentials [5,12,15,17,23,24,27,35,54,57].
- Resistance Attraction: avoiding or preventing attacks from unauthorized users [7,14,42,44].

Next, we show the individual researchers who have either defined or researched each of the defined security elements (see Table 2).

**Table 2.** Security requirements.

Security Function	Description	References
Access Control.	To restrict or limit user access.	[3,6,9,13,18,25,26,32,46,53,55].
Anonymization.	To preserve privacy.	[2,8,9,14,42,56].
Authenticity.	To verify and validate user credentials.	[5,12–15,17,23,24,27,35,54].
Confidentiality.	To prevent/limit user access to preserve privacy.	[2,3,15,24,44,51,56].
Data Integrity.	To prevent unauthorized modification of data.	[3,24,42,51,53,56,59].
Resistance attraction.	To avoid/prevent attacks from unauthorized users.	[7,14,42,44,50–52,54].

### 3.2. Privacy Requirements for IoT-Cloud-Based e-Health Systems

Patient privacy must be actively considered throughout the entire data lifecycle. *Who* can access or view personal, financial or confidential data is determined by internal privacy policies. For example,



GDPR (General Data Protection Regulation) [18,23,28,29,45] is a collection of several data protection laws adopted by many governments around the world (see details in Section 4). The most important factor related to privacy in a health system is the protection of personal data. Data privacy protection is defined as the process by which personal data is safeguarded from unauthorized or unintended use, manipulation or disclosure. The safeguarding of data is accomplished using a variety of methods, including cloud computing, data anonymization, data change tracking and utilizing big data analysis to identify suspicious actions. Privacy protection measures are highly varied and must be tailored to the specific needs of each health system provider, since e-Health system providers offer many different types of services, such as continuous monitoring, preventive care, patient satisfaction tracking and AI-driven diagnosis. Each of these services entails a potential privacy leak that must be considered when implementing privacy protection measures within a given system as used in Wong and Mulligan [60] contributed to broaden perspectives on the potential role for design within privacy by design (PbD) research and practitioner community. PbD should engage with the variety of purposes for which design can be enrolled for privacy. They identify design approaches the foreground social values and use design to explore and defined data privacy problems. Avinash [61] presented the implementing privacy by design through privacy impact assessments. The PbD through the GDPR which become a fundamental principle to be implemented as virtual online privacy under GDPR. One of such requirements in data protection business and technological system. Alshammari [62] investigated various methods for PbD that can address privacy issues in the design process. The investigation how to adapt model key aspects of privacy principle in legal frameworks and standards. The development of a privacy risk model can define the main factors that have impacts on privacy risks along with conceptual relationships. Nwachkwu [63] contributed to the advancement of PbD from a conceptual framework for an engineering technique. The requirement of PbD can start in a system development life cycle instead of adding privacy features at the tail end of development. Also, Morales-Trujillo et al. [64] determined the existing research addresses the PbD approach which has been applied in software development endeavors. A systematic mapping study to identify primary PbD practices or technologies are used in software development. The indication of good PbD related practices and tasks should be more prescriptive requirements, specifications, standards, best practices, and operational performance. Manasrah and Shannaq [65] surveys the data privacy preserving over the cloud through analyzing and discussing the various privacy-preserving methods. They proposed the privacy of the user's data. The pros and cons of the surveyed approaches are drawn in comparison with each other. The results are consolidated and the issues to be addressed in the future are concluded for the advancements in cloud data privacy preserving. Yin et al. [66] proposed a location privacy protection method that satisfying differential privacy constraint to protect location data privacy and maximize the utility of data and algorithm in industry IoT. The combination of utility with privacy and build a multilevel location information model is used to select data according to the tree node accessing frequency. The theoretical analysis and their experiment result can achieve significant improvement in terms of security and privacy.

The end-users are becoming more aware of and cautious about the privacy of their medical data. For example, if someone with an embarrassing disease had their information leaked or disseminated on social media, it would be difficult for the end-user to continue trusting the provider and extremely difficult for the provider to rectify the situation. Privacy is especially important for IoT-cloud-based e-Health systems. Users of various IoT devices must have trust in both the devices themselves and in the underlying technologies, to collect, tag, manage and preserve their data safely. Privacy can be preserved through proper access control, robust utilization of protocols/checklists and integration of broader privacy regulations. Trust, privacy and security of IoT-cloud-based e-Health systems can be strengthened through the integration of PbD [16,23,25,43,54,58–60] and all the following elements into the core system architecture:

- **Data Lifecycle Protection:** Data lifecycle protection involves security measures that are essential to privacy from start to finish. This ensures all data are securely retained and then securely destroyed

at the end of the process. To secure the lifecycle management of information end-to-end, the data lifecycle needs to be improved to effectively manage archiving, transport and deletion of data [15,23,43,45,51,54,58,60].

- Full Functionality: Full functionality seeks to accommodate all legitimate interests and objectives in positive-sum, “win-win” configurations, thereby making trade-offs between privacy and security unnecessary. It possible and far more desirable to protect both privacy and security without compromising the main goals/purpose of the target systems [15,16,25,43,45,53,59,60].
- Proactivity: In contrast to reactive measures, proactive ones anticipate and prevent threats to sensitive private data before they materialize. The aim is to prevent privacy threats from happening rather than reacting to privacy breaches once they have occurred [16,25,45,53,59,61].
- Location Privacy Protection: Big data networks make it necessary to construct location information for data. To prevent the loss, leaking or disclosure of location data related to individual users, effective privacy strategies are required [15,17,23,58,61,66].
- Privacy as the Default Setting: Privacy means ensuring that personal data are protected in all situations automatically. This means even if an individual does nothing, their privacy remains intact. In other words, no action is required on the part of the individual to protect their privacy, as it is built into the system by default [17,25,45,52,60]. This is in contrast to traditional systems, in which the transformation and protection of data are done through direct human intervention.
- Privacy Embedded Design: By embedding it into the design and IoT architecture of systems, privacy becomes an integral core function [23,43,51,54,60].
- Robustness: Ensuring strong security measures are in place to protect privacy and ensure a secure data lifecycle for IT systems [43,45,51,53].
- Visibility and Transparency: Privacy includes seeking to assure all stakeholders that all technologies, operations and objectives, are subject to independent verification. The operations should remain visible and transparent to users and providers alike, to maintain their trust. Transparency and visibility ensure all actions including the collection, analysis, accessing, modification, transportation and dissemination of personal data are recorded continually and remain available to all users and providers for accountability purposes [16,23,25,52,59].

Next, we show the individual researchers who have studied each of the defined PbD elements in Table 3.

**Table 3.** The Privacy by Design requirements.

Functional Privacy	Description	References
Data Lifecycle.	To protect privacy and security while managing, archiving and transforming data.	[15,23,43,45,51,54,58].
Full Functionality.	To protect both privacy and security without compromise.	[15,16,25,43,45,53,59,60].
Proactive.	To prevent privacy threats rather than react to them.	[16,25,45,53,59,61].
Privacy as the Default Setting.	To ensure built-in automatic protection.	[17,25,45,52,60].
Location of Privacy Protection.	To protect location data from loss, leak or disclosure.	[15,17,23,60,66].
Privacy Embedded.	To ensure privacy protection is embedded in system design.	[23,43,51,54,58].
Robustness.	To ensure strong security measures.	[43,45,51,53,61].
Visibility and Transparency.	To remain visible, transparent and accountable.	[16,23,25,52,59].

Furthermore, Tamò-Larrieux [67] presented privacy protection into context of IoT environment and elaborates on RFID. To identify objects and monitor smart energy architectures, which measure and communicate energy data, and smart wearable devices that are used to track health and fitness data of users. Patil et al. [68] they investigated privacy preserving is a major issue in such things due to cloud services. They showed how IoT works with cloud computing of privacy issues. The privacy preservation can eliminate person to machine interaction and makes system smart with device-to-device interaction, privacy of this interaction is still not completely guaranteed. The results of this work surely intercalate new concept in an area of cloud security and IoT, which would provide future research directions. Tewari and Gupta [69] analyzed the cross-layer heterogeneous integration issues and security issues of IoT. They presented the security, privacy, and trust of different layer in IoT framework. IoT is built on the basis of internet and contained three layers: perception layer, transportation layer, and application layer. The integration of IoT with other technologies such as cloud computing requires a lot of issues to be addressed including privacy are the major concerns the development of IoT-based. Abba et al. [70] focused on security and privacy consideration by analyzing potential challenges and risks that need to be resolved. The achievement of IoT-based and cloud computing architecture have been investigated in terms of privacy and security in Cloud of Things. They indicated the preserving data privacy in IoT-cloud-based is a critical concern. Similarly, Sahmin and Gharsellaoui [71] gave insights into the problems of security and privacy of the cloud computing and IoT-based concepts especially confidentiality issue. The intrusions and vulnerabilities should be more recurrent due to the system complexity and difficulty to control each access attempt. They presented risk factors and solutions regarding these technologies are current trends. Altam and Wills [72] provided a discussion of IoT security, privacy, safety, and ethics by providing an overview of IoT systems. The architecture IoT security, privacy requirements and best practices to protect IoT devices. The IoT privacy is a highlighting various IoT privacy threats and solution to preserve the privacy of IoT devices.

Privacy and Security are routinely presented as the same thing by many researchers because of their conceptual and methodological similarities. However, to ensure the protection of data privacy, data privacy must be clearly defined. This is to avoid the misconception that security aims to protect and control data, whereas privacy aims to make appropriate decisions about the collection, processing and dissemination of personal data, all of which are governed by laws, regulations, social norms, economics, policies or contracts. From a data privacy protection perspective, security is a means of ensuring privacy by *enforcing* decisions but not *making* them per se. Cavoukian [73] showed how this principle could be integrated into engineering design perspectives. The methodology is described and introduced in two case studies; the first aims to represent the processing of personal data in risk analysis and compliance checking. The second aims to identify and systematically assess potential privacy risks in contextual and comprehensive privacy protection so that PbD and security can be utilized in various fields.

Methodologically, both privacy and security need to integrate some risk management processes. The integration of security risk assessments has the potential to reduce the loss of CIA within an IT system. The privacy risk assessments help address the potential loss of anonymity, pseudonymity, unobservability, undetectability, unlinkability, intervenability and transparency. Both privacy and security must comply with international standards for risk management processes and frameworks in order to be widely adopted. Data privacy is also a foundational concept that is concerned with protecting user data. One of the requirements of data privacy is data protection through design as known as PbD which is a key element in safeguarding privacy in many technological and information systems (IS). Axon et al. [74] shed light on the gaps in PbD implementation by using privacy impact assessments to identify shortcomings specifically. They indicated PbD is requirement in cybersecurity application of blockchain and in safety requirement. The requirements that have as much to do with safety as it does with security. The safety is related to availability of confidentiality and usage context of an IoT services. Kubo et al. [75] showed the statistical system could proceed in adapting PbD with

bring an example from high level self-assessment of a statistical organization. They proofing how statistical organization can cooperate and support how to build trust required by adopting PbD.

Another matter of concern that must not be overlooked is that despite all the research into both security and privacy, no system is invulnerable. In other words, even a system that incorporates all the aforementioned elements can still be vulnerable. Therefore, we can conclude that privacy and security should be continually researched and improved over time. Table 4 further illustrates the key differences and characteristics of security and privacy challenges as experimental conclusions.

**Table 4.** Security and privacy characteristics open challenges.

Security Challenges	Privacy Challenges
Security addresses the CIA in the IT system.	Privacy addresses user information.
Encryption and decryption algorithms are used in security.	Third-party/outside users cannot use data without permission.
Provide data confidentiality.	Preserve data confidentiality.
Create confidence in data.	Decide if, what, how and with whom information is shared.

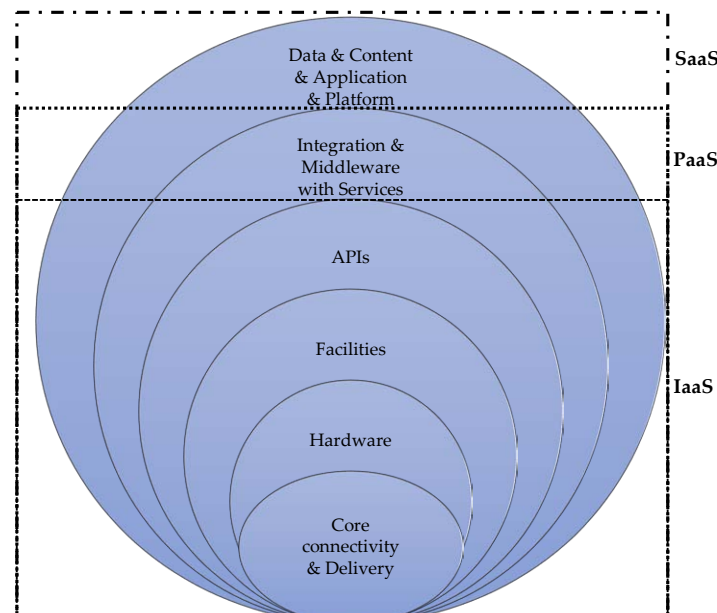
### 3.3. System Requirements for IoT-Cloud-Based e-Health Systems

The integration of IoT with cloud computing technologies has made life more convenient in recent years. People can utilize IoT services via cloud servers anytime, anywhere and in any environment. Cloud computing enables authorized users to authenticate themselves and securely access data from anywhere in the world using robust authentication protocols. Additionally, the use of cryptanalysis in the authentication process can confirm if the protocol is protected against all possible security threats. Securely accessing data on a private cloud server via an internet client would be impossible without the use of authorization protocols. Therefore, authentication protocols are crucial to the security of IoT-cloud-based systems, as mentioned by Yu et al. [55]. These researchers found a symmetric key cryptography authentication scheme to secure IoT-cloud-based systems had better performance than conventional authentication protocols. The scheme used asymmetric key cryptography that balanced security and performance and an authentication protocol that utilized smartcards. Ragib et al. [76] proposed a lightweight, highly localized architecture for IoT-cloud-based systems. This system gives users the flexibility to use any localized computing hardware that is idle to process data and to supplement it with cloud-based servers when necessary. Users can have complete flexibility and control of their application configurations, as demonstrated by Chamandeeep [77], who concluded that IoT-cloud-based applications and hosting services add great value to startups by increasing flexibility, expandability and reducing cost because of their pay-as-you-use structure. Three discrete service models were presented by Sehgal et al. [78] to demonstrate they could be used in the three types of cloud computing; software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). Other related studies [30,31,39,43,48,63,64,68–70] compared three different cloud computing service models and summarized the differences between them. These researchers noted that what was referred to as multitenancy was simply resource sharing and that resource sharing in a private cloud was far more secure than in a public cloud. They concluded that the security risk inherent with resource sharing in public clouds was the most significant variable limiting the expansion of cloud computing. Despite the fact that applications of cloud computing are nearly limitless, we briefly summarize the most common functions of cloud computing services, based on our literature review, as follows (Figure 2):

1. Software as a Service (SaaS) provides application access so users can execute the application in their virtual machine or server. The application is focused on end-users of the Cloud. For example, Google.com is serving Docs and Gmail [6,25,32,38,47,53,60,64,69].
2. Platform as a Service (PaaS) provides the auto scaling, memory, storage and elastic servers. The services can be a new virtual machine for load balancing with minimal administrative

overhead, such as Google's Apps Engine, Amazon Web services, Microsoft's Azure and so forth. These Cloud Service Providers (CSPs) have the capability to support different operating systems on the physical server [6,18,26,33,38,50,53,61,65].

3. Infrastructure as a Service (IaaS) provides direct access to virtualized or containerized hardware. This service makes specified CPUs, memory and storage available over the network [6,26,33,50,61,65].



**Figure 2.** The functions of APIs, SaaS, PaaS, and IaaS services.

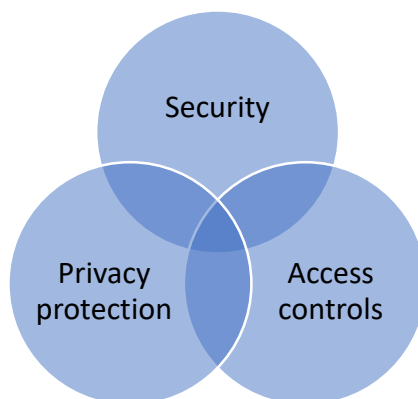
Robust security and privacy measures are essential for the future expansion and sustainability of the cloud computing industry. The most effective security and privacy measure for cloud computing is strict access control as used in Kaliya and Hussain [79,80] presented framework for privacy preservation in IoT through classification and access control mechanism. They indicated security and privacy of user data is a serious issue in IoT that classifies data into a structural format based on its and user and access control lists are created. Then, Caiza, et al. [81] addressed data privacy protection concerns that can conform to GDPR guidelines. They pointed out reusable elements for the systematic design of privacy are a friendly information system. They used privacy by design and GDPR to ensure solutions that focused on remote health systems and mobile health applications. Ensuring that only authorized users with predetermined privileges can access the system can reduce the chance of attacks from within and without. Moreover, it can help ensure data integrity, transfer, and recovery. Overall, cloud computing security concerns fall into three major the categories. These classifications are as follows:

- Access Control: the ability to access a computer system can be controlled at a hardware level by using a special access device such as a USB thumb drive with a built-in security/authentication key. Access control can also be addressed at the operating system level [6,18,26,33,50,61,65,71,79,80].
- Secure Communications: encryption that utilizes robust algorithms is required to secure system communications. Communication encryption can be deployed at the hardware level to secure I/O ports, at the operating system level to ensure data integrity and authentication of access signatures or at the application level to encrypt routine functions [18,25,32,38,47,60,64,69].
- Privacy Protection: routine integrity checks, security breach checks and limiting the availability of data to authorized users are the most common measures to ensure data privacy [6,25,33,50,61,65,81].

Additionally, security solutions in cloud computing can be implemented on multiple system levels, depending on the necessary functions of a given system. Multifunction, multilevel and



high-security operations all need customized security solutions for specific applications, such as the implementation of access control, secure communication and privacy protection. Each of these three security measures can be implemented independently or together to create a more robust overarching protection architecture, as shown in Figure 3.



**Figure 3.** Measures for robust cloud computing.

Cloud computing security threats to information to be communicated or stored could be related to privacy, integrity, trust or information authentication. Since the security and privacy of patient health information is a priority, many of the keys that can handle health information have policies and security to protect patient health information, including protecting personal private medical records, data integrity and managing data to defend it from outside hackers and attacks.

Healthcare industry trends involving IoT and Cloud Computing in e-Health systems can be classify into three main market groups: components, applications and end-users. The component category can be further subdivided into hardware, software and services. In the second category, applications can be grouped into clinical operations, patient monitoring and drug development. The end-user category involves healthcare practitioners, patients, financial backers, laboratories and governments. The e-Health systems can utilize IoT-based and cloud computing to monitor health information such as patients' heart rate and body temperature and to effectively diagnose health status, including identifying disease risk and severity. E-Health systems integrate diverse hardware instruments, such as thermometers, through software components and allow structured and seamless end-to-end integration of Cloud computing for fast and accurate delivery of results. The other system requirements of IoT-Cloud-based e-Health systems corresponding to these components are as follows:

- **Secure Transmission:** This ensures data can be transmitted both internally and externally without malicious or unauthorized users intercepting or harmfully affecting the transmission. The security of transmitted data can be achieved using appropriate cryptographic mechanisms to encrypt transmissions [43,64,67].
- **Secure Protocols:** These are used to improve security and ensure computer network communications are secured. The application of encryption technology to data not only increases the security and stability of network data storage but also enhances the security of information [2,17,19,42,43,45].
- **Secure Communication:** This is provided by technical cryptosystems and includes ensuring confidentiality and authenticity. Communications security is achieved by the application of measures designed to protect transmissions from interception and exploitation by using cryptanalysis [13,17,19,46,51,58,64,65].
- **Data encryption:** This involves preventing unauthorized access and protecting data throughout its lifecycle by encoding all data. Encryption is used to avoid the exposure of raw uncodified data from breaches, packet sniffing and physical theft of storage devices [9,14,39,47].

Stepien et al., [82] provided a way of establishing a secure connection between cloud servers and devices. The secure connection and data transfer may involve authentication, cryptographic protocols, and other techniques to prevent many kinds of attacks. The connection between IoT devices and cloud computing involves potential security leaks. Hu et al. [83] presented technology to ensure the identity consistency of humans in physical space and cyber space. IoT and cloud computing improve processing capacity and save bandwidth. Their authentication and session key agreement scheme, data encryption scheme, and data integrity checking scheme are implemented a prototype system to evaluated the influence of security scheme on the system performance. Any possible solutions must provide robust security and privacy while meeting IoT-cloud-based e-Health system requirements. The quest to devise such solutions drives the development of a variety of custom applications and architectures, such as those used in References [6,26,27,35,38]. Figure 4 is a Venn diagram model for the combination IoT-cloud-based e-Health systems.

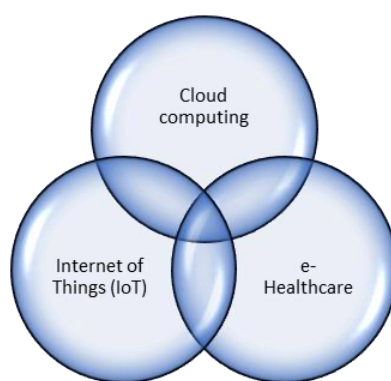


Figure 4. The IoT-cloud-based e-Health systems model.

#### 4. Security and Privacy Solutions for IoT-Cloud-Based e-Health Systems

This section presents the existing security and privacy solutions for robust IoT-cloud-based e-Health systems. Such systems will revolutionize healthcare in terms of investment, security, privacy, reliability and trust. For instance, IoT in health framework systems are used in References [2,3,30,37] to demonstrate the possibility of IoT-based e-Health systems. Moreover, researchers [2–5,11–14,17,18,26–28,32–34,37] have also touted the benefits of merging IoT-based and cloud computing systems in the health field. The functionality of IoT devices used in e-Health systems does not necessarily guarantee privacy or security. Various investigations and research studies have therefore been done to identify and define constituent elements of IoT-cloud-based e-Health systems and address the critical issues related to architecture, system models, applications, communication protocols and security protocols. A similar study [43,48,70] focused on security, privacy and trust in different layers in the IoT framework, analyzing security problems at each layer, as well as cross-layer heterogeneous integration and security issues. The authors pointed out that IoT network security should be addressed by the communication protocols used at each layer, rather than by applying external security models. The primary security design requirements are to ensure confidentiality, integrity, authentication, and anonymity. This can be accomplished with the help of the modes, access control functions and time-synchronization present in IEEE 802.15.4. Stergiou et al. [84,85] proposed a new system for cloud computing integrated with IoT as a based scenario for big data. To establish an architecture relaying on the security of the network to improve the security issues. A solution proposed is installing a security between cloud server and internet with the aim to eliminate the privacy and security issues. The interaction and cooperation between things and objects communicate through the wireless networks in order to fulfil their objective. Paranjothi et al. [86] presented a scheme for intelligent personal health devices integrated with IoT networks and pointed out security, privacy and trust are the major challenges in this domain. In addition, service and cloud computing, dependability,

reliability, context awareness, multimodal intelligence and secure healthcare are emerging areas. The strategy of using aggregation techniques is a promising way to provide synergism in these contexts.

Despite the diligent efforts of researchers, more work must be dedicated to solving the privacy and security issues of IoT-cloud-based e-Health systems to ensure continued growth. This includes further identifying vulnerabilities and creating viable countermeasures to increase the security and privacy of the whole system. In the following, we summarize the various contributions related to the privacy and security of IoT-cloud-based e-Health systems published in academic books and journals between 2017–2020. The contributions are summarized in Table 5.

**Table 5.** The security and privacy solutions in IoT-cloud-based e-Health systems.

Ref.	Privacy & Security	e-Health	IoT	Cloud Computing	Contributions
[7] (2020)	×	✓	✓	✓	Utilized IoT services of the health system with remote patient monitoring medical sensors by using Cloud computing.
[8] (2020)	×	✓	✓	×	Presented application of IoT healthcare technologies with four-step architecture.
[9] (2020)	✓	✓	✓	✓	Presented security analysis of IoT-based health architecture applications and integrated Cloud computing.
[11] (2020)	✓	✓	✓	×	Proposed IoT-based health architecture systems and investigated security measures in the health IoT system.
[12] (2020)	✓	✓	✓	✓	Presented IoT Healthcare application from hospital-centric to patient-centric with considering key services and collaborative security and privacy.
[13] (2020)	✓	✓	✓	✓	Presented automatic IoT building blocks for the exchange of information between devices and integrated cloud computing.
[14] (2020)	✓	✓	✓	×	Utilized IoT BSN technologies in the healthcare system with system security and patient privacy.
[17] (2020)	×	✓	✓	✓	Proved advantage of cloud hosting service adds value to IoT by reducing cost structure for healthcare.
[18] (2020)	×	✓	✓	✓	Survey on how to adopt healthcare 4.0 technologies and provide an analysis of benefits and novel challenges.
[21] (2020)	✓	✓	✓	×	Proposed various wearable techniques with sensing, storage, computation and transmission capabilities for heart disease prediction.
[22] (2020)	✓	✓	✓	×	Presented blockchain technologies used in IoT-based e-healthcare.
[23] (2020)	✓	✓	✓	×	Analyzed various privacy frameworks and identify key systematic requirements in the health system sector.
[26] (2020)	×	✓	✓	✓	Proposed remote patient health monitoring in Smart Home by using IoT-cloud-based technique.
[27] (2020)	×	✓	✓	✓	Proposed remote patient health monitoring in Smart Home by using fog computing.
[30] (2020)	×	✓	✓	✓	Presented GPs used in e-Health services online and examined GPs diagnostic testing in e-Health.
[33] (2020)	✓	×	✓	✓	Integrated IoT and cloud computing and presented authentication, key agreement schemes, asymmetric cryptography with automated security verification (ProVerif).
[38] (2020)	✓	✓	✓	✓	Presented a conceptual framework for IoT-based healthcare systems using cloud computing.

Table 5. Cont.

Ref.	Privacy & Security	e-Health	IoT	Cloud Computing	Contributions
[39] (2020)	✓	✓	✓	×	Proposed a secure routing patient monitoring protocol using Two-Fish (TF) symmetry and designed the authentication, encryption.
[40] (2020)	×	✓	✓	✓	Proposed multisensory fusion to work with medical data obtained from BSNs in fog/cloud computing environment.
[55] (2020)	×	✓	✓	✓	Studied various aspects of IoT architecture to convert real scenarios in hospitals in India.
[3] (2019)	✓	✓	✓	×	Presented a secure framework for an IoT-based healthcare system by using wearable.
[4] (2019)	✓	✓	✓	×	Proposed a framework for IoT-based health system (IoMT) by using wearable biosensors and IoT devices and utilized cryptosystem security in the smart sensors.
[6] (2019)	✓	✓	✓	✓	Analyzed and surveyed trends of using IoT and cloud computing in the healthcare system.
[19] (2019)	✓	✓	✓	×	Proposed systematic mobile computing to assist IoT application in the healthcare system.
[20] (2019)	✓	✓	✓	✓	Presented IoT applications in healthcare to bring privacy and security to mobile device computing.
[28] (2019)	×	✓	✓	×	The proposed remote patient monitoring system enhanced health system delivery using multiplexed data modes.
[36] (2019)	×	✓	✓	×	Provided utilizing IoT technology in healthcare.
[37] (2019)	✓	✓	✓	✓	Proposed a secure IoT e-Health architecture based on Blockchain technology and using fog/cloud computing
[42] (2019)	✓	×	✓	×	Presented security for IoT wireless sensor networks that can help healthcare systems.
[2] (2018)	×	✓	✓	✓	Provided and developed a framework for IoT-based smart health system focusing on interoperability, standards and protocols by using gateway web technology.
[3] (2018)	✓	✓	✓	✓	Presented a prototype Smart e-Health gateway (UT-Gate) by forming sensor nodes and the clouds.
[34] (2018)	×	✓	✓	×	Presented a survey on the role of the IT system in healthcare management, hospitals and the healthcare industry.
[43] (2018)	✓	✓	✓	×	Presented a new lightweight RFID scheme used in the medical context.
[15] (2017)	✓	✓	×	×	Presented the security and privacy issues in big data that can apply to the healthcare industry.
[16] (2017)	✓	✓	✓	×	Proposed privacy requirements associated with GDPR and considered IoT-based data collection and data sharing for Smart Healthcare.
[25] (2017)	✓	✓	✓	✓	Presented a new computing environment for privacy protection in IoHT-cloud health services
[31] (2017)	✓	✓	✓	×	Provided a novel solution to reduce data transactions in sensors in a medical healthcare system.
[35] (2017)	×	✓	✓	✓	Analyzed and improved cloud computing issues in IoT-based e-Health systems.

Traditional IoT architecture is comprised of three basic layers: the perception layer, the network layer and the application layer. However, many researchers have experimented with various alternative IoT architectures. Ferrandez-Pastor et al. [87] identified four discrete layers of IoT: edge layer, web services layer, data storage layer and the Human-Machine Interface (HMI) layer. Sinha et al. [88] proposed a prototype three-layer smart traffic monitoring system that is designed to relieve congestion

and manage traffic lights. Alaba et al. [89] proposed another three-layer IoT architecture comprised of an application layer, perception layer and network layer. Baldassarre et al. [90] present integration security and privacy in software development. IoT architecture that incorporates a network layer to communicate data collected from the receiving layer through either the internet or a mobile network. Brian [91] presented the method that can be used to mitigate the cyber security threats by IoT developer and operator. The complex threat environment that IoT system operate within and provide guidance for implementing cyber security measure across the core architectural element of IoT system. Maninder et al. [92] investigated the architecture, applications, and challenges in the implementation of digital twin with IoT capabilities. Some of the major research areas like big data and cloud, data fusion, and security in digital twins have been explored. AI facilitates the development of new models and technology systems in the domain of intelligent manufacturing. Al-Emran et al. [93] presented a highlight the recent progress of IoT applications in education and provide various opportunities and challenges for future trials. They summarized the prospects of adopting IoT in education, medical education and training, vocational education and training, Green IoT in education, and wearable technologies in education. It is concluded that the adoption of IoT and its applications in developing countries is still in its early stages and further research is highly encouraged such adopted and presented in Chiu et al. [94] experimental wearable IoT and built an authentication system based on brainwave reactions to a chain of events. Brainwaves, as external signals of a functioning brain, provide a glimpse into how we think and react. They indicated the action or event could be linked back to its corresponding brainwave reaction. Hosseinian-Far et al. [95] showed cloud computing can be emerged to address and improve the quantity and quality of data that can collect and analyze from multiple sources and devices. Cloud computing has also revolutionized the software paradigm by changing into a service-oriented paradigm where cloud resources and software are offered as a service. Similarly, Zhou et al. [96] integrated IoT and cloud computing for secure data retrieval and robust access control on large-scale IoT networks. However, it does not have a best practice for simultaneously deploying IoT and cloud computing with robust security. They presented a novel authentication scheme for IoT-based architectures combined with cloud servers. To pursue the best efficiency, lightweight crypto-modules, such as one-way hash function and exclusive-or operation, are adopted in our authentication scheme. Wang et al. [97] combined IoT and cloud computing which not only enhances the IoT's capability but also expands the scope of its applications. They a novel architecture that integrates a trust evaluation mechanism and service template with a balance dynamics based on cloud and edge computing. Their architecture, the edge network and the edge platform are designed in such a way as to reduce resource consumption and ensure the extensibility of trust evaluation mechanism. Fu et al. [98] design a flexible and economic framework to solve the problems by integrating the fog computing and cloud computing. Based on the time latency requirements, the collected data are processed and stored by the edge server or the cloud server. The results illustrate that the framework can greatly improve the efficiency and security of data storage and retrieval in IoT.

Likewise, the IoT application can be integrated in various applications such as Yeh et al. [99,100] introduce a secure transaction scheme with certificateless cryptographic primitives for mobile payments. Their scheme takes advantage of the merits of Android Pay and a refined certificateless signature cryptosystem to simultaneously deliver transaction security and achieve payment efficiency in practice. Their performance evaluation shows the practicability transaction scheme, as the total computation cost is acceptable for a common Internet of Things (IoT)-based testbed. Shojafar and Sookhak [101] introduced novel techniques to merge the benefits of the cloud computing and makes it applicable in highly volatile IoT devices. For the highly virtualized platform, the processing of data and applications execution is emerging as an option of choice with handle an increasing number of interconnected devices and an evolving demand of the IoT. The significant scientific advances on their research that can be made through both in-depth theoretical analyzes and integration of data from related real-world experimental studies. Sadique et al. [102] presented the connected smart objects. The connected IoT objects can be able to communicate with each other between different networks of their locations,



network providers, and manufacturers. They used software-defined networking (SDN) approach in IoT, due to its flexibility and easy adaptability with any network. However, it will not be possible for the devices to freely move within the networks if do not have a common identity solution. Arasteh et al. [103] developed digital technologies, smart cities with different electronic IoT devices. They survey described and provided a comprehensive on the concepts of smart cities and on their motivations and applications. IoT technologies for smart cities and the main components and features of a smart city. According to literature review and many researchers have studied IoT technology will affect the various aspects of citizens' life like health, security, and data privacy. On the other hand, it can play an important role regarding to the policy; GDPR and required infrastructure. IoT will help to provide more efficient, economic and secure operation of the system based on different aspects, considerations, reliability levels, trust, etc.

Based on our literature review of previous research, we can present an architecture for a five-layer privacy and security solution for IoT-cloud-based e-Health systems. The five layers are as follows:

1. Things Layer/Device Layer: This layer is where all devices can perform their specific functions such as detection, monitoring, controls and actions and it is the bridge connects information collection and the control network. It transmits information from the lowest layer to the higher layers of the IoT architecture. The connections to physical devices such as sensors, wireless, monitors, controls and so forth can be either direct or indirect.
  - Security Goals: This layer is designed to prevent attacks including physical, identity spoofing, whitelisting, sandboxing, secure booting, sniffing, as malicious attacks seen in References [2,3,13,14,19,26,35,38,39,47,64,76,87,90,99,100].
2. Communication/Service Layer: This layer allows different devices to interconnect with each other over a central network to collect and share data across local devices. The transmission in the form of sending and receiving signals between the layers uses various protocols such as mobile/wireless networks, Bluetooth, wired serial protocols and so forth. Some processing capabilities can also be incorporated into the layer to suit the needs of users, such as signal and identity authentication.
  - Security Goals: Secure communication against sniffing and adulteration, as used in References [13,17,19,46,51,58,64,65,74,84,92,103].
3. Network Layer: This layer is where IoT services and devices can connect to or be operated by cloud computing servers operating off-site. This connection is made via physical hardware devices such as switches, gateways, routers and broadband internet. Moreover, this layer provides secure network transmission and constitutes an access environment for the perception layer. The network layer ensures that reliable response mechanisms, storage and analytic resources can be accessed and utilized by users, things or services.
  - Security Goals: Secure routing and switching data traffic from attacks such as man in the middle, sniffing, spoofing and DoS, as used in References [2,17,19,42,43,45,82,86,92].
4. Cloud Layer: This layer provides internet-based distributed computing that can process, store and monitor data collected by the device layer. Cloud computing services enable the use of IoT devices in the health system because of the ability to process massive quantities of data, near-instant scalability and low cost. Moreover, Cloud computing affords users data resources for computation, bandwidth, storage and services on a pay-per-use basis.
  - Security Goals: Protection of stored and processed data against unauthorized user access, adulteration and attacks such as injections, sniffing, cross-site scripting (XSS), phishing and viruses/malware, as used in References [18,25,32,38,47,60,64,69,96–98,101].
5. Application Server Layer: This layer is where users directly interact with the IoT-cloud-based e-Health system. Users can receive alarms, visualize gathered data in real-time,

manually/automatically react to emergent situations and so on. This layer is responsible for providing application-specific services to the user. It defines the various applications in which IoT can be deployed, such as smart homes, smart cities, and e-Health systems.

- Security Goals: Protect against attacks such as blating, bribery of information and malicious code, as used in References [7,9,15,18,29,38,40,56,60,99,100,103].
6. Cross Security Layer: This layer is where the system performs its security, including CIA (see in Section 2). In this layer, we consider system requirements for the physical layer through application layers such as security protocols, security transmission, secure communication between layers and data encryption, to prevent unauthorized access to the systems and protect all data throughout its life cycle by codifying it. Furthermore, the encryption of communication, accountability tracking, data anonymization and so forth takes place here.
- Security Goals: authentication, protection against malicious code, data integrity, identity protocol, man in the middleware, sniffing and spoofing, fake information and adulteration, black-box and sand-box, as presented in References [2,9,13,14,39,42,43,46,51,58,64,65,74].
7. Cross Privacy Layer: in this layer, patient privacy is actively considered throughout the entire data lifecycle and who can access or view personal, financial or confidential data is determined by internal privacy policies including privacy requirements (see Section 2 for details). Data privacy is a primitive's unique and secure identities for the queries and responses in conjunction with usage/access rights policies. The users normally can control their encrypted data to safeguard the security and privacy of the outsourced data. However, considering the various types of privacy data that can be stored in the cloud and the users' demand for data safety, preserving the data privacy in Cloud computing applications becomes even more challenging.
- Security Goals: Privacy protection, full functionality, data lifecycle, reliability, trust, proactivity and identification, as presented in References [15,16,23,25,43,45,51,54,59,60,65,68,71,72].

Based on our literature review of past research studies, we can present our architecture solution in the form of five-layer security and privacy for IoT-cloud-based e-Health systems. The five layers are illustrated in Figure 5, below.

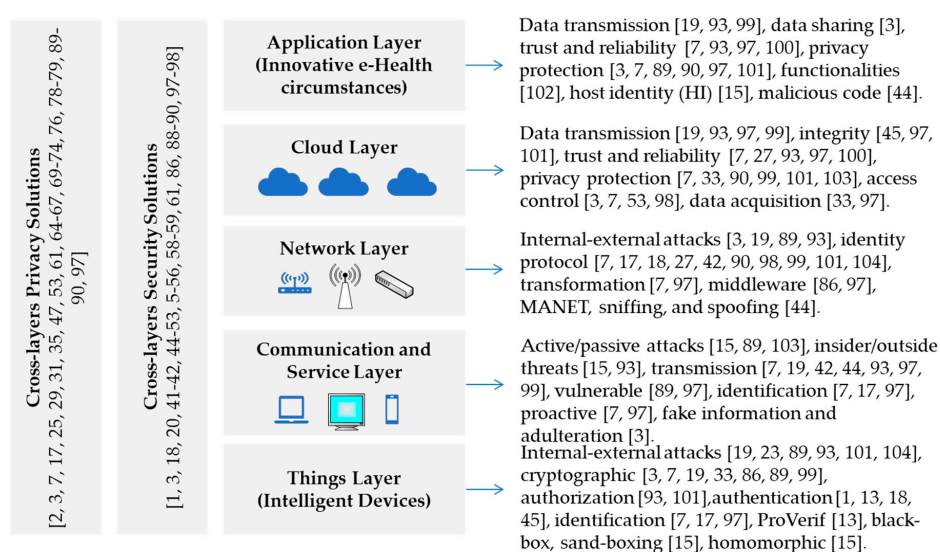


Figure 5. Security and privacy solutions for IoT-cloud-based e-Health systems.

## 5. Discussion and Limitations

IoT-cloud-based e-Health systems are groundbreaking technology that can be integrated into virtually any application. Many governments and fortune-500 companies are either researching this technology or actively integrating and developing it. Although there are many diverse opinions about the effects of climate change, companies and governments are attempting to abate their negative contributions by becoming more sustainable. To this end, they are turning to IoT-cloud-based e-Health systems to reduce waste, increase efficiency, reduce reliance on carbon-based power and adopt sustainable practices while maintaining and even growing, their operations. However, integrating and implementing these two distinctive systems is far from perfect or easy. As with any new technology, there myriad challenges must be overcome. The following is a summary of the challenges unique to the integration and implementation of IoT-cloud-based computing in e-Health systems.

### 5.1. Privacy in IoT-Cloud-Based e-Health Systems

Data privacy has been defined several different ways, reflecting divergent perspectives. For example some researchers [15–17,23,25,43,45,51,52,54,58–62,65,68,70–82] have focused on data privacy in terms confidential data protection and provided a legal framework with built-in privacy standards, including PbD. Semantha et al. [23] analyzed the contemporary PbD frameworks in the health systems to identify the key limitations. The integration of PbD can be incorporated into the General Data Protection Regulation (GDPR), which is supported by the European Parliament and Council of the European Union (EU) to unify data protection laws for all data citizens. Moreover, PbD can be used to create a new framework, as shown in References [23,72,75,80]. Data privacy is a foundational concept that is concerned with protecting user data. One of the requirements of data privacy is data protection through design. That is a key element in safeguarding privacy in many technological and information systems (IS) and IT systems. Therefore, in this paper, we focus on privacy and security schemes that consider the challenges of both GDPR and PbD, as well as other frameworks.

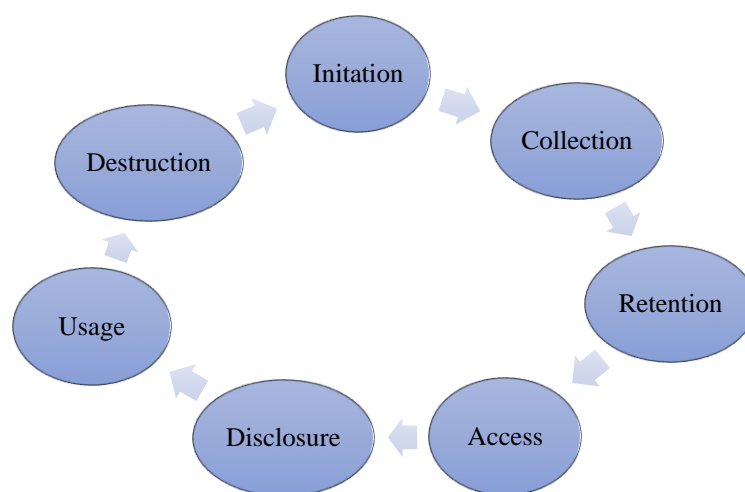
The EU's GDPR attempts to protect all personal data through strict regulations. To simplify the regulatory environment, controllers and processors of personal data must implement appropriate technical and organizational measures to comply with the required data protection principles. Data controllers must design information systems with data privacy as a fundamental concern. All processing must fall within one of six legally defined categories specified in the GDPR in order to remain compliant with the law. These categories are consent [16,43,45,59,70,75,79,81], contract [15,25,45,62,81,82], public task [15,23,25,43,58,81], vital interest [15,23], legitimate interest [43] or legal requirement [17,52,54,65,70,77,79,82]. Many researchers have acknowledged the importance of the GDPR. Kubo et al. [80], created a system of engineering standards that incorporated elements of GDPR and PbD. This system was widely adopted in both the private and public sectors. They showed by statistics that “the PbD should become a default standard” for the engineering field. Caiza et al. [81] addressed issues relating to how data privacy protection can conform to GDPR guidelines. They pointed out reusable elements for the systematic design of privacy characterize a user-friendly information system and used PbD and GDPR to provide solutions focused on remote health systems and mobile health applications. Nwachukwu [63] presented evidence that PbD and EU GDPR can reduce the occurrence of improper use of personal data. He pointed out what kind of methods have been proposed in PbD and EU GDPR in research driven by the need to make privacy compliance possible with the EU GDPR by design standardization.

Abstract personal data lifecycle models (APDL) [15,77,85] are a representation of personal data in the form of lifecycle stages with associated activities and involved actors. APDL facilitates the traceability of personal data. Various security and privacy approaches in Sahmin [71] could mitigate risk factors, protect data from attacks and guarantee the CIA of data. That research describes an abstract personal data lifecycle model for PbD that greatly increased awareness of the PbD framework. Big data processing techniques can be utilized to minimize the security and privacy vulnerabilities in health systems, as demonstrated by Abouelmehdi et al. [15]. Moreover, patterns that encapsulate expert

knowledge and provide predefined solutions to different types of privacy threats were presented in a study by Diamantopoulou et al. [52], who showed the theory of PbD has many limitations, depending on how and where it is implemented. They suggested that data privacy concerns should be classified by reference to the specific activities that may lead to privacy violations and then further subdivided into categories according to shared characteristics. Controlling access to personal data is the cornerstone of developing strong privacy with the goal of mitigating the potential risk arising from the inappropriate collection, processing and dissemination of personal data under the data subject's control. There are various key aspects of privacy awareness solutions that we can summarize as follows:

- Initiation: Represents complete processing during the processing of personal data [58,65,68,70].
- Collection: Represents the acts of gathering personal and assigning data values [58,59,68,70,71].
- Retention: Represents the acts of organizing, structuring, storing and retaining personal data values for operational, compliance or recovery purposes [59,61,65,73,85].
- Access: Represents the acts of specifying, retrieving or consulting personal data [59,60,68,72].
- Disclosure: Represents the acts of disseminating, making available or transmitting personal data for external use by third parties [60,65,72,74,78,80,85].
- Usage: Represents the acts of using, altering, adapting, refining or aligning of personal data [58,62,68,81].
- Destruction: Represents the acts of erasing, destroying, redacting or disposing of personal data [62,70,82,85].

We can present these key aspects of privacy awareness visually as shown in Figure 6.



**Figure 6.** Privacy awareness cycle.

## 5.2. Context Awareness

Only a complete and detailed picture of a particular patient's situation enables an IoT-cloud-based e-Health system to determine his or her actual need for assistance appropriately. In IoT-cloud-based e-Health systems, data must be accurately interpreted in order to obtain a reasonable [1,15–17,20,22,23,25,30], all-inclusive understanding of contextual data based on a patient's condition [1,20,25,30] or on the requirements of a caregiver or health provider [1,15,16,20,22,31]. Providing context-awareness in IoT-cloud-based e-Health systems is challenging due to the issues of data acquisition [16,25] and data analysis methods [23,29,31], including presentation of context-based services and information. For instance, when designing context-aware monitoring systems, it is important to consider reasoning, interpretation and observation of the patient's condition from multiple perspectives, including behavioral and physiological ones [26–28]. A system also has to consider all appropriate contextual dimensions, including human activities, objects, location, time,

frequency and attitude. As well, all available historical data such as health documentation of disease, diagnoses, treatment plans and daily behavior must be taken into account.

### 5.3. Security in IoT-Cloud-Based e-Health Systems

In this paper, we consider security and privacy in IoT-cloud-based e-Health systems that manage medical data and can actively increase the quality of patient health through integrated storage, tracking, compilation, collection and dissemination of both personal and health information. Therefore, we examine a multitude of different approaches to security that all work together to ensure an effective, secure and private health system for all. The various privacy threat vectors and challenges and their related countermeasures have been studied by Perera et al. [53], who evaluated the utility of using a PbD framework in IoT applications. They designed a privacy awareness scheme for IoT applications by considering PbD, EU GDPR and risk awareness for personal data. The approach used in Hu et al. [83] utilized data integrity checking to solve issues of confidentiality and availability of data. In addition, they presented a security and privacy preservation scheme based on face identification. Patil et al. [52] presented enhanced privacy preservation by using secure anonymization in an IoT-based system and used it as a Smart home. They outlined the advantages and disadvantages of privacy in IoT-cloud-based e-Health systems and analyzed the contemporary PbD framework. IoT systems are comprised of devices that are located in a certain environment and perform multiple activities such as detection, monitoring, control and actions. The devices must have interfaces that allow their connection with other devices to transmit necessary information. The protocols used in different communications must work together in the same IoT system communication channels, such as the ones from the IPU to the gateway (router) and from the gateway to cloud computing. The data transmission on these channels must be secured to guarantee data integrity, manage data and codify it to defend it from unauthorized users, hackers and so forth. What follows is a summary of other major security concerns for IoT-Cloud-based e-Health systems:

- **Cryptographic security:** Communications security from the provision of technical cryptosystems includes ensuring confidentiality and authenticity. Cryptanalysis is the method for obtaining the encrypted information without access to the key normally required by crack encryption algorithms or implementations, as described in more detail in References [42,54,58,62,67].
- **Transmission security (TRANSEC):** Communications security from the application of measures designed to protect transmissions from interception and exploitation by using cryptanalysis. Cryptanalysis is the use of an analytical information system to breach a cryptographic security system and gain access to the contents of the encrypted message, even if the cryptographic key is unknown. In cryptography, the key determines the functional output of a cryptographic algorithm as a specific key or authentication code for the transformation of plaintext into ciphertext and vice versa, for decryption algorithms. Keys are generated to be used with a given suite of algorithms we called a cryptosystem. Encryption algorithms use the same key for both encryption and decryption. We call these symmetric key algorithms (e.g., AES, DES, Twofish, etc.) On the other hand, an asymmetric key algorithm (e.g., RSA, DSA, etc.) uses a pair of keys, a public key for encryption or verification and a private one for decryption, as described in more detail in References [42,56,64,92].
- **Physical security:** Communications security resulting from all physical measures. Physical security describes security measures designed to deny unauthorized access to facilities and resources and to protect personnel from damage or harm. Physical security involves the use of multiple layers of interdependent systems including surveillance, access control, perimeter intrusion detection, deterrent systems and other systems. Physical security systems for protected facilities deter potential intruders, detect intrusions and trigger appropriate incident responses, as described in more detail in References [25,31,48,92,96].



#### 5.4. Challenges and Open Issues for IoT-Cloud-Based e-Health Systems

The most common problem with IoT-cloud-based e-Health systems is high latency and bandwidth requirements for transmitting and receiving data between the IoT devices and the cloud servers. Security challenges germane to the integration of IoT-based and cloud computing systems are as follows:

- **Heterogeneity:** The variety of manufacturers, devices, operating systems, platforms, servers, services, features and so forth is virtually limitless. This routinely causes compatibility issues or monopolistic/oligopolistic systems where users are locked into one provider's product/service stack [6,18,25,32,38,47,60,64,69,88,96].
- **Performance:** Every user requires custom applications for their specific needs based on their goals, location, business type and so forth. Sometimes the needs are easy to satisfy, whereas sometimes this is not the case. Depending on circumstances, either IoT or cloud computing may be better for specific workflows. However, synergistic benefits like more flexibility and efficiency result from their combination in an IoT-cloud-based system [6,18,26,33,39,51,64,69].
- **Reliability:** Generally speaking, a mechanism that is less complicated and is comprised of fewer parts is more reliable than a complex mechanism with many parts. Therefore, IoT and cloud computing systems are inherently more reliable when used independently. If they are combined into an IoT-cloud-based system, great effort must be taken to ensure the reliability of their operation [18,25,26,33,38,39,50,51,60,64,69,92].
- **Big Data:** Depending on its complexity and quantity, the efficient transportation, storage, access and processing of very large quantities of data might not be easily achievable without a combination IoT-cloud-based system [7,15,18,38,60,87].
- **Monitoring:** To supervise a cloud computing system and detect any problems or inefficiencies, constant monitoring of resource allocation, infrastructure failures and security breaches/threats is essential. Therefore, IoT-cloud-based systems will inherit this need for continuous monitoring [13,26,27,32,69].

Most researchers have designated the security of IoT systems as the most serious challenge to overcome to increase the rate of IoT device utilization. IoT systems facilitate the connection of both small and large systems together and use the internet to communicate. Overcoming the security challenges inherent in IoT systems should therefore be a fundamental priority of IoT applications. The users need to be fully confident in the security of IoT devices/systems that relate to concerns such as data privacy. IoT systems are inherently vulnerable to outside attack or manipulation because the IoT devices use conventional networks to connect virtually everything wirelessly. Researchers are still trying to find viable solutions for many security and privacy issues; however, security and privacy aspects are usually researched in isolation as discrete variables. We believe the greatest security and privacy gains will only be accomplished if the variables are merged and researched as a unified system, with an emphasis on the CIA. The security requirements of IoT-based systems are dependent on the characteristics of the environment where a given system is implemented, as well as the devices required for the user's specific applications. Many researchers [15,17,51,59,62] have designed custom security and privacy architectures for specific IoT applications in studies that presented security requirements for IoT-based systems that utilized standard CIA in conjunction with additional custom security variables, such as authentication and assessed and challenged their proposed schemes using classical security risk analysis methods.

IoT and cloud computing have been combined and integrated into e-Health systems in use all over the world. This has caused overarching changes in operating principles, medical device protocols, privacy and security requirements and protocols and health systems themselves. IoT-cloud-based systems make remote health systems feasible for the first time in history. Doctors can now observe, diagnose, consult and prescribe remotely, without ever having to meet patients face-to-face. Nevertheless, there are several challenges that need to be considered and addressed for the integration of IoT-cloud-based e-Health systems.

## 6. Conclusions and Future Work

We reviewed recent literature to clearly identify the overarching features and characteristics of IoT-cloud-based e-Health systems and the motivations driving their use. In this paper, we explored the utilization of computers in health systems and its evolution over time, particularly the integration of the IoT devices and cloud computing. We also presented an overview of privacy and security issues in IoT-cloud-based e-Health systems and performed a comparative analysis of major privacy and security issues, definitions, categories, solutions and architectures used in IoT-cloud-based e-Health systems. Every application of an IoT-cloud-based e-Health system is unique and requires custom privacy and security solutions and architectures that will protect it from harm without interfering with the mission and operations of the system itself. The combination of IoT-based systems with intelligent cloud computing systems to enhance the capabilities of smart objects, smart health systems, smart remote monitoring and associated applications is one of the most interesting future trends in technology. The rapid advancements made in IoT technology are changing lives by connecting limitless devices. Moreover, e-Health applications utilizing IoT-cloud-based systems are more efficient, offer the advantage of lower cost and have better patient outcomes than any health systems in the past. However, privacy and security have never been as vulnerable as they are now, with countless devices transmitting and receiving vast quantities of data wirelessly. Therefore, researchers must continue to develop and improve upon existing privacy and security solutions for IoT-cloud-based e-Health systems, such as automatic identification schemes, watermarking, fingerprint verification schemes and active smart monitoring. Additionally, research should be conducted on the feasibility of hardening physical facilities and devices against attacks as well. Lastly, concerns about climate change and environmental health have become seemingly ubiquitous. Therefore, future research must be done to find new ways to make IoT-cloud-based e-Health systems more sustainable, such as developing devices with a longer useful life, manufacturing devices from recycled or repurposed materials or increasing power efficiency. Moreover, achieving effective solutions should focus more on the scalability of big data for healthcare problems by the simulation of diverse privacy and security approaches.

**Author Contributions:** Conceptualization: C.B. and K.-H.Y.; methodology: C.B. and K.-H.Y.; investigation: C.B.; writing—original draft preparation: C.B.; writing—review and editing: C.B. and K.-H.Y.; supervision: K.-H.Y.; project administration: K.-H.Y. and H.X.; funding acquisition: K.-H.Y. and H.X. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by the Ministry of Science and Technology, Taiwan, under Grants MOST 109-2218-E-011-007, MOST 109-2221-E-259-011-MY2, MOST 109-2221-E-011-109-MY2, MOST 109-2634-F-259-001, and MOST 108-2911-I-259-502.

**Acknowledgments:** The authors would like to thank the anonymous reviewers for their valuable comments and feedback which was extremely helpful in improving the quality of the paper.

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

## References

1. Eysenbach, G. What is e-health? *J. Med. Internet Res.* **2001**, *3*, e20. [[CrossRef](#)] [[PubMed](#)]
2. Pasha, M.; Shah, S.M.W. Framework for E-Health Systems in IoT-Based Environments. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 1–12. [[CrossRef](#)]
3. Rahmani, A.M.; Gia, T.N.; Negash, B.; Anzanpour, A.; Azimi, I.; Jiang, M.; Liljeberg, P. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Gener. Comput. Syst.* **2018**, *78*, 641–658. [[CrossRef](#)]
4. Robinson, Y.H.; Presskila, X.A.; Lawrence, T.S. Utilization of Internet of Things in Health Care Information System. In *Internet of Things and Big Data Applications. Intelligent Systems Reference Library*; Balas, V., Solanki, V., Kumar, R., Eds.; Springer: Cham, Switzerland, 2020; Volume 180, pp. 35–46.
5. Islam, M.S.; Humaira, F.; Nur, F.N. Healthcare Applications in IoT. *Global. J. Med Res. B Pharma Drug Discov. Toxicol. Med.* **2020**, *20*, 1–3. [[CrossRef](#)]

6. Shewale, A.D.; Sankpal, S.V. IOT & Raspberry Pi based Smart and Secure Health Care System using BSN. *Int. J. Res. Appl. Sci. Eng. Technol.* **2020**, *8*, 506–510.
7. Selvaraj, S.; Sundaravaradhan, S. Challenges and opportunities in IoT healthcare systems: A systematic review. *SN Appl. Sci.* **2020**, *2*, 139. [[CrossRef](#)]
8. Kaur, H.; Atif, M.; Chauhan, R. An Internet of Healthcare Thing (IoHT) based Healthcare Monitoring System. In *Advances in Intelligent Computing and Communication, Lecture Notes in Networks and Systems*; Mohanty, M.N., Das, S., Eds.; Springer Nature: Singapore, 2020; Volume 109, pp. 475–482.
9. Dang, L.M.; Piran, M.J.; Han, D.; Min, K.; Moon, H. A Survey on Internet of Things and Cloud Computing for Healthcare. *Electronics* **2019**, *8*, 768. [[CrossRef](#)]
10. Chattopadhyay, A.K.; Nag, A.; Ghosh, D.; Chanda, K. A Secure Framework for IoT-Based Healthcare System. In Proceedings of the International Ethical Hacking Conference 2018, Kolkata, India, 5 October 2018; *Advances in Intelligent System and Computing*. Chakraborty, M., Chakrabarti, S., Balas, E.V., Mandal, J.K., Eds.; Springer Nature: Singapore, 2019; Volume 811, pp. 383–393.
11. Nandyala, C.S.; Kim, H. From Cloud to Fog and IoT-Based Real-Time U-Healthcare Monitoring for Smart Homes and Hospitals. *Int. J. Smart Home* **2016**, *10*, 187–196. [[CrossRef](#)]
12. Maksimović, M. Improving computing issues in the Internet of Things driven e-health systems. In Proceedings of the International Conference for Young Researchers in Informatics, Mathematics, and Engineering, Kaunas, Lithuania, 1 April 2017; Volume 1852, pp. 14–17.
13. Yeh, K.H. A Secure IoT-Based Healthcare System with Body Sensor Networks. *IEEE Access* **2016**, *4*, 10288–10299. [[CrossRef](#)]
14. Deelip, S.A.; Sankpal, S.V. IOT based Smart and Secure Health Care System Analysis & Data Comparison. *Int. J. Res. Appl. Sci. Eng. Technol.* **2020**, *8*, 394–398.
15. Sanjay, S.; Shekokar, N. Toward Smart and Secure IoT Based Healthcare System. In *Internet of Things, Smart Computing and Technology: A Roadmap Ahead, Studies in Systems, Decision and Control*; Dey, N., Mahalle, P.N., Shafi, P.M., Kimabahune, V.V., Hassanien, A.E., Eds.; Springer Nature AG: Cham, Switzerland, 2020; Volume 266, pp. 283–303.
16. Farahani, B.; Firouzi, F.; Charkabarty, K. Healthcare IoT. In *Intelligent Internet of Thing, From Device to Fog and Cloud*; Firouzi, F., Charkabarty, K., Nassif, S., Eds.; Springer Nature AG: Cham, Switzerland, 2020; pp. 515–537.
17. Abouelmehdi, K.; Beni-Hssane, A.; Khaloufi, H.; Saadi, M. Big data security and privacy in healthcare A Review. *Procedia Comput. Sci.* **2017**, *113*, 73–80. [[CrossRef](#)]
18. Connor, Y.O.; Rowan, W.; Lynch, L.; Heavin, C. Privacy by design informed consent and internet of things for smart health. *Procedia Comput. Sci.* **2017**, *113*, 653–658.
19. Hathaliya, J.J.; Tanwar, S. An exhaustive survey on security and privacy issues in Healthcare 4.0. *Comput. Commun.* **2020**, *153*, 311–335. [[CrossRef](#)]
20. Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. *J. Ind. Inf. Integr.* **2020**, *18*, 100–129. [[CrossRef](#)]
21. Ray, P.; Dash, D.; Salah, K.; Kumar, N. Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. *IEEE Syst. J.* **2020**, *2020*, 1–10. [[CrossRef](#)]
22. Nazir, S.; Ali, Y.; Ullah, N.; García-Magariño, I. Internet of Things for Healthcare Using Effects of Mobile Computing: A Systematic Literature Review. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 1–20. [[CrossRef](#)]
23. Samantha, F.H.; Azam, S.; Yeo, K.C.; Shanmugam, B. A Systematic Literature Review on Privacy by Design in the Healthcare Sector. *Electronics* **2020**, *9*, 452. [[CrossRef](#)]
24. Wu, J.; Tian, X.; Tan, Y. Hospital evaluation mechanism based on mobile health for IoT system in social networks. *Comput. Biol. Med.* **2019**, *109*, 138–147. [[CrossRef](#)]
25. Khatoon, N.; Roy, S.; Pranav, P. A survey on Applications of Internet of Things in Healthcare. In *Internet of Things and Big Data Applications. Intelligent Systems*; Khatoon, N., Roy, S., Pranav, P., Eds.; Springer Nature: Cham, Switzerland, 2020; Volume 180, pp. 89–106.
26. Tuli, S.; Basumatary, N.; Singh-Gill, S.; Kahani, M.; Chand-Arya, R.; Wander, G.; Buyya, R. HealthFog: An ensemble deep learning-based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. *Future Gener. Comput. Syst.* **2020**, *104*, 187–200. [[CrossRef](#)]

27. Gupta, P.; Pandey, A.; Akshita, P.; Sharma, A. IoT based Healthcare Kit for Diabetic foot Ulcer. In Proceedings of the ICRIC 2019, Jammu, India, 8–9 March 2019; Lecture Notes in Electrical Engineering. Singh, P.K., Kar, A.K., Singh, Y., Kolekar, M.H., Tanwar, S., Eds.; Springer Nature: Cham, Switzerland, 2019; Volume 597, pp. 15–22.
28. Elmisery, A.M.; Rho, S.; Aborizka, M. A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services. *Clust. Comput.* **2017**, *22*, 1611–1638. [[CrossRef](#)]
29. Fan, K.; Jiang, W.; Li, H.; Yang, Y. Lightweight RFID Protocol for Medical Privacy Protection in IoT. *IEEE Trans. Ind. Inform.* **2018**, *14*, 1656–1665. [[CrossRef](#)]
30. Shirley, M.A.J.; A, M.C.; Phil, M.; Ed, M. A cloud IoT based smart patient health monitoring system. *Adalya J.* **2020**, *9*, 963–968.
31. Khader, A.H.A.; Subasri, K. Fog Assisted-IoT Enabled Patient Health monitoring. *Adalya J.* **2020**, *9*, 525–530.
32. Swaroop, K.N.; Chandu, K.; Gorreputu, R.; Deb, S. A health monitoring system for vital signs using IoT. *Internet Things* **2019**, *5*, 116–129. [[CrossRef](#)]
33. Wilt, T.; Versluis, A.; Goedhart, A.; Talboom-Kamp, E.; van Delft, S. General practitioners' attitude towards the use of eHealth and online testing in primary care. *Clin. eHealth* **2020**, *3*, 16–22. [[CrossRef](#)]
34. Kang, J.J.; Larkin, H. Intelligent personal health devices converged with IoT networks. *J. Mob. Multimed.* **2017**, *12*, 197–212.
35. Wang, X.; Cai, S. Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud. *Future Gener. Comput. Syst.* **2020**, *112*, 320–329. [[CrossRef](#)]
36. Yamin, M. IT applications in healthcare management: A survey. *Int. J. Inf. Technol.* **2018**, *10*, 503–509. [[CrossRef](#)]
37. Mohammed, D.; Meri, A. IoT Service Utilization in Healthcare. In *Internet of Things (IoT) for Automated and Smart Applications*; Ismail, Y., Ed.; IntechOpen: London, UK, 2019; pp. 1–27.
38. Cha, S.; Hsu, T.; Xiang, Y.; Yeh, K. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet Things J.* **2019**, *6*, 2159–2187. [[CrossRef](#)]
39. Zhou, J.; Cao, Z.; Dong, X.; Vasilakos, A.V. Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions. *IEEE Commun. Mag.* **2017**, *55*, 26–33. [[CrossRef](#)]
40. Mohanty, M.N.; Das, S. Advances in Intelligent Computing and Communication. In *Lecture Notes in Networks and Systems Proceeding of ICAC 2019*; Springer Nature Singapore Pte Ltd.: Singapore, 2020.
41. Muzammal, M.; Talat, R.; Sodhro, A.H.; Pirbhulal, S. A multi-sensor data fusion enabled ensemble approach for medical data from body sensor networks. *Inf. Fusion* **2020**, *53*, 155–164. [[CrossRef](#)]
42. Iman, A.; Madi, A.A.; Addaim, A. Proposed Architecture of e-health IoT. *IEEE* **2019**, *19*, 1–7.
43. Tyagi, S.; Agarwal, A.; Maheshwari, P. A conceptual Framework for IoT-based healthcare system using Cloud computing. In Proceedings of the International Conference-Cloud System and Big data Engineering, Noida, India, 14–15 January 2016.
44. Thakare, V.; Kumbhar, M. Internet of Things (IoT) in Hospitals of India A Literature Review and Research Direction. *UGC Care List. J.* **2020**, *68*, 132–137.
45. Khan, M.A. An IoT Framework for Heart Disease Prediction Based on MDCNN Classifier. *IEEE Access* **2020**, *8*, 34717–34727. [[CrossRef](#)]
46. Nagaraja, G.S.; Srinath, S. Security Architecture for IoT-Based Home Automation. In *Smart Intelligent Computing and Applications: Smart Innovation System and Technologies*; Satapathy, S.C., Bhateja, V., Das, S., Eds.; Springer Nature: Singapore, 2020; Volume 159, pp. 57–65.
47. Li, D.; Zhongsheng, W.; Xiaodong, W.; Dong, W. Security information transmission algorithms for IoT based on cloud computing. *Comput. Commun.* **2020**, *155*, 32–39.
48. Amin, R.; Kumar, N.; Biswas, G.P.; Iqbal, R.; Chang, V. A lightweight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. *Future Gener. Comput. Syst.* **2018**, *78*, 1005–1019. [[CrossRef](#)]
49. Deebak, B.D.; Al-Turjman, F. A hybrid secure routing, and monitoring mechanism in IoT-based networks. *Ad Hoc Netw.* **2020**, *97*, 102022.
50. Sharma, A.; Singh, Y. On Security of Opportunistic Routing Protocol in Wireless Sensor Networks. In Proceedings of the ICRIC 2019, Jammu, India, 8–9 March 2019; Lecture Notes in Electrical Engineering. Singh, P.K., Kar, A.K., Singh, Y., Kolekar, M.H., Tanwar, S., Eds.; Springer Nature: Cham, Switzerland, 2019; Volume 597, pp. 407–419.

51. Garcia, L.; Parra, L.; Jimenez, J.M.; Lloret, J.; Lorenz, P. IoT-Based Smart Irrigation Systems: An Overview on the Recent Trends on Sensors and IoT Systems for Irrigation in Precision Agriculture. *Sensors* **2020**, *20*, 1042. [[CrossRef](#)] [[PubMed](#)]
52. Diamantopoulou, V.; Argyropoulos, N.; Kalloniatis, C.; Gritzalis, S. Supporting the design of privacy-aware business processes via privacy process patterns. In Proceedings of the 2017 11th International Conference on Research Challenges in Information Science (RCIS), Brighton, UK, 10–12 May 2017; pp. 187–198. [[CrossRef](#)]
53. Perera, C.; Barhamgi, M.; Bandara, A.K.; Ajmal, M.; Price, B.; Nuseibeh, B. Designing privacy-aware internet of things applications. *Inf. Sci.* **2019**, *512*, 238–257. [[CrossRef](#)]
54. Bhattacharjya, A.; Zhong, X.; Wang, J.; Li, X. Present Scenario of IoT Projects with Security Aspects Focused. In *Internet of Things: Digital Twin Technology, Communications, Computing, and Smart Cities*; Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H., Eds.; Springer Nature AG: Cham, Switzerland, 2019; pp. 95–123.
55. Srinivas, T.A.S.; Somula, R.; Govinda, K. Privacy and Security in Aadhaar. In *Smart Intelligent Computing and Applications, Smart Innovation System, and Technologies*; Satapathy, S.C., Bhateja, V., Das, S., Eds.; Springer Nature: Singapore, 2020; Volume 159, pp. 405–410.
56. Kalyani, G.; Chaudhari, S. An efficient approach h for enhancing security in the Internet of Things using the optimum authentication key. *Int. J. Comput. Appl.* **2019**, *42*, 306–314. [[CrossRef](#)]
57. Yu, Y.; Hu, L.; Chu, J. A Secure Authentication and Key Agreement Scheme for IoT-Based Cloud Computing Environment. *Symmetry* **2020**, *12*, 150. [[CrossRef](#)]
58. Garg, A.; Diksha, N.M. A security, and Confidentiality survey in wireless Internet of Things (IoT). In *Internet of Things and Big Data Applications: Recent Advances and Challenges*; Balas, V., Solanki, V., Kumar, R., Eds.; Springer Nature: Cham, Switzerland, 2020; Volume 180, pp. 65–88.
59. Jimenez, J.I.; Jahankhani, H.; Kendzierskyj, S. Healthcare in the cyberspace: Medical Cyber-Physical System and Digital Twin Challenges. Digital Twin Technologies, and Smart cities. In *Internet of Things (Technology communication Computing)*; Springer Nature AG: Cham, Switzerland, 2020; pp. 79–92.
60. Wong, R.Y.; Mulligan, D.K. Bringing Design to the Privacy Table: Broadening “Design” in “Privacy by Design” Through the lens of HCI. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Scotland, UK, 4–9 May 2019.
61. Avinash, F.A. Implementing Privacy by Design through Privacy Impact Assessments. Master’s Degree Programmed in Law and Information Society. In *Faculty of Law and Information Society*; University of Turku: Turku, Finland, 21 May 2019.
62. Alshammari, M. A Principled Approach for Engineering Privacy by Design. Ph.D. Thesis, University of Oxford, Oxford, UK, 2019; p. 304.
63. Nwachukwu, O.J. *Privacy by Design. Master’s Degree of Science in Telematics: Communication Networks and Networked in Telematics-Communication Networks*; Norwegian University of Science and Technology: Trondheim, Norway, July 2017.
64. Morales-Trujillo, M.E.; Matla-Cruz, E.O.; Alberto, G.; Mireles, G.; Piattini, M. Privacy by design in software engineering a systematic mapping study. In Proceedings of the Conference in Computer Science and Software Engineering Department (CibSE), Bogota, Colombia, 23–27 April 2018; pp. 1–14.
65. Manasrah, A.M.; Shannaq, M.A.; Nasir, M.A. An Investigation Study of Privacy-Preserving in Cloud Computing Environment. In *Handbook of Computer Networks and Cyber Security 2020*; Springer Nature AG: Cham, Switzerland, 2020; Chapter 2, pp. 43–61.
66. Yin, C.; Xi, J.; Sun, R.; Wang, J. Location Privacy Protection Based on Differential Privacy Strategy for Big Data in Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2017**, *14*, 3628–3636. [[CrossRef](#)]
67. Tamò-Larrieux, A. Privacy Protection in an Internet of Things Environment. In *Designing for Privacy and its Legal Framework, Law, Governance and Technology Series*; Springer Nature: Cham, Switzerland, 2018; pp. 45–72.
68. Patil, S.; Joshi, S.; Patil, D. Enhanced Privacy Preservation using Anonymization in IoT-Enabled Smart Homes. In *Smart Intelligent Computing and Applications, Smart Innovation System, and Technologies*; Springer Nature: Singapore, 2020.
69. Tewari, A.; Gupta, B.B. Security, privacy, and trust of different layers in the Internet-of-Things (IoTs) framework. *Future Gener. Comput. Syst.* **2020**, *108*, 909–920. [[CrossRef](#)]



70. Abba, A.A.; Ngangmo, O.K.; Titouna, C.; Thiare, O.; Mohamadou, A.; Gueroui, A.M. Enabling Privacy and Security in Cloud of Things: Architecture, applications, security & privacy challenges. *Appl. Comput. Inform.* **2019**, *169*, 1–13. [[CrossRef](#)]
71. Sahmin, S.; Gharsellaoui, H. Privacy and Security in Internet-based Computing—Cloud Computing, Internet of Things, Cloud of Things: A review. *Procedia Comput. Sci.* **2017**, *112*, 1516–1522. [[CrossRef](#)]
72. Altam, H.F.; Wills, G. IoT Security, Privacy, Safety, and Ethics. In *Digital Twin Technologies and Smart Cities: Internet of Things (Technology Communication Computing)*; Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H., Eds.; Springer: Cham, Switzerland, 2019; pp. 123–149.
73. Cavoukian, A. Privacy-by-design. In *The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*; Information & Privacy Commissioner: Creation of a Global Privacy Standard, November; Information and Privacy Commissioner of Ontario: Ontario, ON, Canada, 2019; pp. 1–12.
74. Axon, L.; Goldsmith, M.; Creese, S. Privacy requirements in Cybersecurity applications of blockchain: Safety requirements in the Internet of Things. *Adv. Comput.* **2018**, *111*, 229–278.
75. Kubo, B.; Sahk, A.; Berendsen, V.; Saluveer, E. Privacy by design in statistics: Should it become a default/standard. *Stat. J. IAOS* **2019**, *35*, 623–631. [[CrossRef](#)]
76. Ragib, H.; Hossain, M.M.; Khan, R. Aura: An IoT Based Cloud Infrastructure for Localized Mobile Computation Outsourcing. In Proceedings of the 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, San Francisco, CA, USA, 30 March–3 April 2015; pp. 183–188.
77. Chamandeep, K. The Cloud Computing and Internet of Things (IoT). *Int. J. Sci. Res. Sci. Eng. Technol.* **2020**, *7*, 19–22.
78. Sehgal, N.; Bhatt, P.P.; Acken, J.M. (Eds.) Cloud Computing and Information Security. In *Cloud Computing with Security*; Springer Nature Switzerland AG: Cham, Switzerland, 2020; pp. 111–141.
79. Kaliya, N.; Hussain, M. Framework for privacy preservation in IoT through classification and access control mechanisms. In Proceedings of the 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, India, 7–9 April 2017; pp. 430–434. [[CrossRef](#)]
80. Hussain, M.; Kaliya, M. An Improvised Framework for privacy preservation in IoT. *Int. J. Inf. Secur. Priv.* **2018**, *12*, 46–63. [[CrossRef](#)]
81. Caiza, J.C.; Martin, Y.; Guaman, D.S.; del Alamo, J.M.; Yelmo, J.C. Reusable Elements for the Systematic Design of Privacy-Friendly Information Systems: A Mapping Study. *IEEE Access* **2019**, *7*, 66512–66535. [[CrossRef](#)]
82. Stepien, K.; Ponsizewska-Maranda, A.; Maranda, W. Securing connection and data transfer between devices and IoT cloud service. In *Integrating Research and Practice in Software Engineering: Studies in Computation Intelligence*; Springer Nature Switzerland AG: Cham, Switzerland, 2020; pp. 83–96.
83. Hu, P.; Ning, H.; Qiu, T.; Song, H.; Wang, Y.; Yao, X. Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in the Internet of Things. *IEEE Internet Things J.* **2017**, *4*, 1143–1155. [[CrossRef](#)]
84. Stergiou, C.; Psannnis, K.E.; Gupta, B.B.; Ishibashi, Y. Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT. *Sustain. Comput. Inform. Syst.* **2018**, *19*, 174–184.
85. Stergiou, C.; Psannnis, K.E.; Kim, B.; Gupta, B. Secure integration of IoT, and Cloud Computing. *Future Gener. Comput. Syst.* **2018**, *78*, 964–975. [[CrossRef](#)]
86. Paranjothi, A.; Khan, M.S.; Nijim, M. Survey on Three Components of Mobile Cloud Computing: Offloading, Distribution, and Privacy. *J. Comput. Commun.* **2017**, *5*, 1–31. [[CrossRef](#)]
87. Ferrandez-pastor, F.J.; Garciachamizo, J.M.; Nietohidalgo, M.; Morapascual, J.; Moramartinez, J. Developing Ubiquitous Sensor Network Platform Using Internet of Things: Application in Precision Agriculture. *Sensors* **2016**, *16*, 1141. [[CrossRef](#)]
88. Sinha, D.; Babu, R.; Patan, R.; Jiao, P.; Barri, K.; Alavi, A.H. Internet of things-based fog and cloud computing technology for smart traffic monitoring. *Internet Things Eng. Cyber Phys. Hum. Syst.* **2020**, 100175. [[CrossRef](#)]
89. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [[CrossRef](#)]
90. Baldassarre, M.T.; Barletta, V.S.; Caivano, D.; Scalera, M. Integrating security and privacy in software development. *Softw. Qual. J.* **2020**, 1–32. [[CrossRef](#)]
91. Brian, R. *IoT Cyber Security, in Intelligent Internet of Thing*; Firouzi, F., Chakrabarty, K., Nassif, S., Eds.; Springer Nature: Cham, Switzerland, 2020; pp. 473–513.

92. Kaur, M.J.; Mishra, V.P.; Maheshwari, P. The Convergence of Digital Twin, IoT, and Machine Learning: Transforming Data into Action. In *Digital Twin Technologies and Smart Cities: Internet of Things (Technology Communication Computing)*; Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H., Eds.; Springer: Cham, Switzerland, 2019; pp. 3–19.
93. Al-Emran, M.; Malik, S.I.; Al-Kabi, M.N. A Survey of Internet of Things (IoT) in Education: Opportunities and Challenges. In *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*; Hassanien, A.E., Bhatnagar, R., Khalifa, N.E.M., Taha, M.H.N., Eds.; Springer Nature AG: Cham, Switzerland, 2020; pp. 197–209.
94. Chiu, W.; Su, C.; Fan, C.; Chen, C.; Yeh, K. Authentication with What You See and Remember in the Internet of Things. *Symmetry* **2018**, *10*, 537. [[CrossRef](#)]
95. Hosseinian-Far, A.; Ramachandran, M.; Slack, C.L. Emerging Trends in Cloud Computing, Big Data, Fog Computing, IoT and Smart Living. In *Technology for Smart Futures*; Dastbaz, M., Arabia, H., Akhgar, B., Eds.; 2018; pp. 29–40.
96. Zhou, L.; Li, X.; Yeh, K.; Su, C.; Chiu, W. Lightweight IoT-based authentication scheme in cloud computing circumstance. *Future Gener. Comput. Syst.* **2019**, *91*, 244–251. [[CrossRef](#)]
97. Wang, T.; Zhang, G.; Liu, A.; Bhuiyan, M.Z.A.; Jin, Q. A Secure IoT Service Architecture with an Efficient Balance Dynamics Based on Cloud and Edge Computing. *IEEE Internet Things J.* **2019**, *6*, 4831–4843. [[CrossRef](#)]
98. Fu, J.; Liu, Y.; Chao, H.; Bhargava, B.K.; Zhang, Z. Secure Data Storage, and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4519–4528. [[CrossRef](#)]
99. Yeh, K.H. A Secure Transaction Scheme with Certificateless Cryptographic Primitives for IoT-Based Mobile Payments. *IEEE Syst. J.* **2017**, *12*, 2027–2038. [[CrossRef](#)]
100. Yeh, K.H.; Su, C.; Choo, K.R.; Chiu, W. A Novel Certificateless Signature Scheme for Smart Objects in the Internet-of-Things. *Sensors* **2017**, *17*, 1001. [[CrossRef](#)]
101. Shojafar, M.; Sookhak, M. Internet of everything, networks, applications, and computing systems (IoENACS). *Int. J. Comput. Appl.* **2019**, *42*, 213–215. [[CrossRef](#)]
102. Sadique, K.M.; Rahmani, R.; Johannesson, P. Identity Management in the Internet of Things: A Software-Defined Networking Approach. In Proceedings of the 2nd International Conference on Communication, Devices and Cloud computing, Lecture Notes in Electrical Engineering, Haldia, India, 14–15 March 2020; Springer Nature: Singapore, 2020; pp. 495–504.
103. Arasteh, H.; Hosseinnerzhad, V.; Loia, V.; Tommasetti, A.; Troisi, O.; Shafie-Khah, M.; Siano, P. IoT-based Smart Cities: A Survey. *IEEE Xplore* **2016**. [[CrossRef](#)]



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).