

Review

A Survey on Internet of Things and Cloud Computing for Healthcare

L. Minh Dang, Md. Jalil Piran, Dongil Han, Kyungbok Min and Hyeonjoon Moon *

Department of Computer Science and Engineering, Sejong University, Seoul 143-747(05006), Korea

* Correspondence: hmoon@sejong.edu

Received: 10 June 2019; Accepted: 6 July 2019; Published: 9 July 2019



Abstract: The fast development of the Internet of Things (IoT) technology in recent years has supported connections of numerous smart things along with sensors and established seamless data exchange between them, so it leads to a stringy requirement for data analysis and data storage platform such as cloud computing and fog computing. Healthcare is one of the application domains in IoT that draws enormous interest from industry, the research community, and the public sector. The development of IoT and cloud computing is improving patient safety, staff satisfaction, and operational efficiency in the medical industry. This survey is conducted to analyze the latest IoT components, applications, and market trends of IoT in healthcare, as well as study current development in IoT and cloud computing-based healthcare applications since 2015. We also consider how promising technologies such as cloud computing, ambient assisted living, big data, and wearables are being applied in the healthcare industry and discover various IoT, e-health regulations and policies worldwide to determine how they assist the sustainable development of IoT and cloud computing in the healthcare industry. Moreover, an in-depth review of IoT privacy and security issues, including potential threats, attack types, and security setups from a healthcare viewpoint is conducted. Finally, this paper analyzes previous well-known security models to deal with security risks and provides trends, highlighted opportunities, and challenges for the IoT-based healthcare future development.

Keywords: IoT; healthcare; cloud computing; security; privacy; fog computing; communication; networking

1. Introduction

The Internet of Things (IoT) is undoubtedly one of the most exciting topics to the research community, public sector, and industry. While traditional internet facilitates communication between a number of limited devices and humans, IoT connects all sorts of connected “Things” into a comprehensive network of interrelated computing intelligence without the intervention of a human. The adoption of IoT and the development of wireless communication technologies allow patient’s health conditions being streamed to caregivers in real-time [1,2]. Furthermore, many available sensors and portable devices can measure specific human physiological parameters such as heart rate (HR), respiration rate (RR) and blood pressure (BP) through a single touch. Although it is still in the early development stage, businesses and industries have quickly adopted the power of IoT in their existing systems, and they have witnessed improvements in production as well as user experiences [3].

However, the integration of IoT technology in the healthcare brings several challenges, including data storage, data management, exchange of data between devices, security and privacy, and unified and ubiquitous access. One possible solution that can address these challenges is Cloud Computing technology. Figure 1 shows a typical healthcare system that integrates both IoT and cloud computing to provide the ability to access shared medical data and common infrastructure ubiquitously and

transparently, offering on-demand services, over the network, and performing operations that meet growing needs [4].

Cloud computing delivers computing services including servers, databases, networking, software, and data analytics over the internet to provide faster deployment, flexible resources, and economies of scale. Furthermore, the current shift from centralized paradigm (cloud computing) to decentralized paradigm (fog computing) [5] is taking the headline. Fog computing performs data analytics on edge devices, so it enables real-time processing, improves data privacy, and reduces costs. The rise of portable devices, artificial intelligence (AI) [6], and cloud computing ensures a firm foundation for the evolution of IoT in the healthcare sector to revolutionize every aspect of human lives. Interested readers are referred to IoT reviews carried out by [7–11] for more in-depth and more comprehensive knowledge about several aspects of IoT enabling technologies, its current development progress as well as major challenges that the research community has to solve. Furthermore, they can refer to [4,12] to gain insights about cloud and fog computing technologies, their typical application scenarios, various challenges that occur when implementing cloud and fog computing systems, and possible future work that need to be conducted.

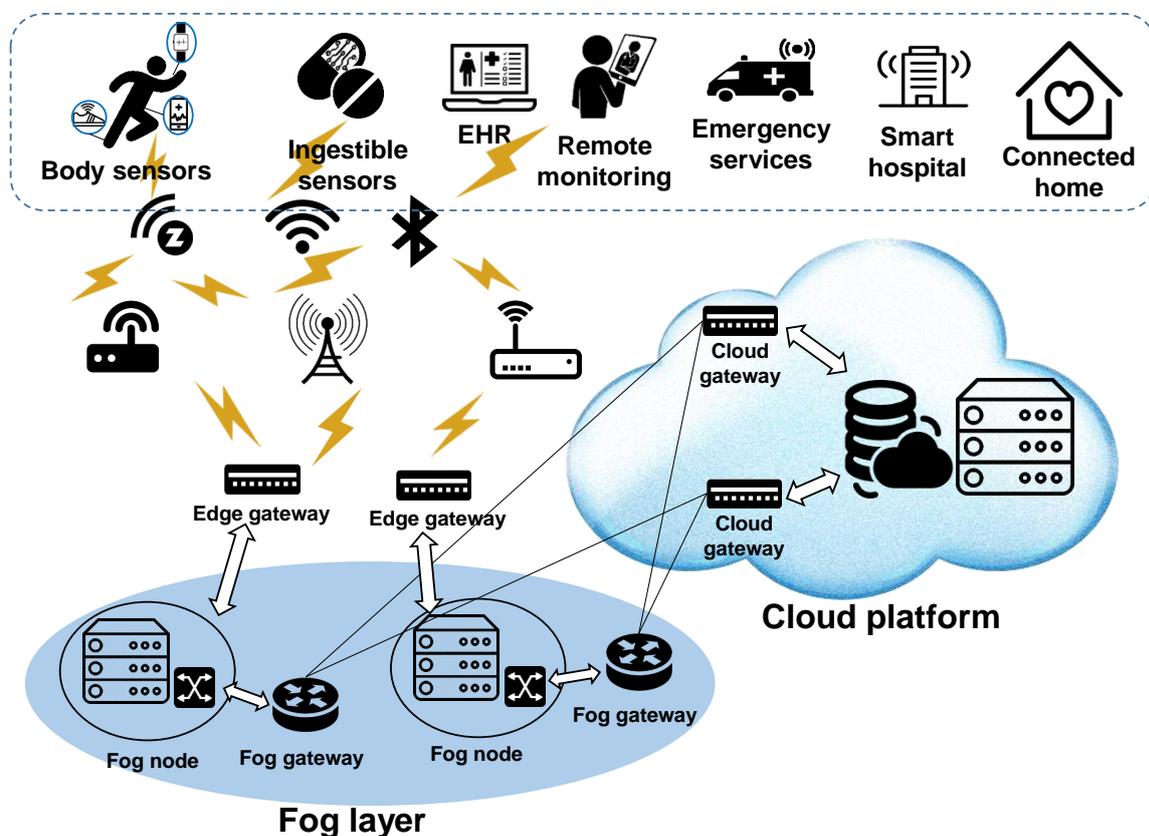


Figure 1. An overview of a typical IoT and cloud computing-based healthcare system.

IoT delivers proper solutions for various applications that cover all aspects of life such as smart cities [13], smart traffic management, waste management, structural health monitoring, security, emergency services, supply chain, retail, industrial management [14–17], and healthcare. According to a report by CISCO [18], by 2030, 500 billion devices will be connected, which is approximately equivalent to 58 smart devices per person on our planet. At the end of 2017, IoT market research carried out by Statista [19] revealed that global IoT market value will reach 8.9 trillion USD by 2020, and 7% of the total market value comes from the healthcare sector. Thanks to the integration of IoT and cloud computing into the healthcare sector, health professionals can provide faster, more efficient and better healthcare services, which thus lead to better patient experience. As a result, it brings better healthcare services, better patient experience, and less paperwork for health professionals.

Table 1 shows notable contributions from eight review papers which considered different aspects of IoT and cloud computing in healthcare. In 2015, a comprehensive IoT in healthcare survey was carried out by [20] which discussed several aspects of IoT in the healthcare such as architectures, services and applications; they also discussed several issues including security and standardization that require more research. However, it has already been four years since this paper was published. During four years, many technologies and state-of-the-art research have been proposed. Thus it is necessary to conduct a new survey to analyze and summarize them. Moreover, in recent years, cloud computing has developed significantly and healthcare applications based on cloud computing have increased significantly. As a result, it has become a fundamental element of IoT in the healthcare. Several research works [21–24] focused on reviewing different aspects of fog computing and fog applications for healthcare as well as addressing several issues that researchers need to overcome. On the other hand, the authors in [25] investigated previous architectures and applications of cloud computing in the healthcare and showed critical issues that need extensive work. From a different viewpoint, the authors in [26] concentrated on analyzing different types of sensors and standard communication techniques. In 2018, Farahani conducted an IoT in the healthcare survey regarding hardware and software [27]. Then, the authors investigated security issues in hardware and software and proposed proper solutions that need to be carried out to ensure the security of healthcare systems.

Each of the reviews dedicated to a particular aspect of IoT or cloud computing in the healthcare and the fact that the healthcare industry is still adopting the IoT and cloud computing leads to the promotion of several fundamental concepts, frameworks, and applications. At this stage, an in-depth review of previous research on the IoT and cloud computing in healthcare is essential for various groups including researchers, physicians, and stakeholders who are planning to integrate IoT and cloud computing into healthcare or carrying out further research.

1.1. Contributions

To address the mentioned limitations, in this paper, we conduct a comprehensive survey about IoT and cloud computing in healthcare. It covers several sections of IoT and cloud computing in the healthcare such as the standard IoT and cloud computing structure, standard platforms that facilitate healthcare applications to communicate to IoT and cloud computing backbone. We also discuss related concepts, applications, services, and challenges of integrating IoT and cloud computing in the healthcare. The main contributions of the study are described as follows:

- Present a comprehensive survey about IoT and cloud computing in the healthcare (From 2015 to present).
- Review IoT framework for the healthcare by discussing typologies, platforms, and structures.
- Survey cloud computing and especially the fog computing for healthcare, including standard architecture, remarkable fog-based healthcare applications.
- Discuss various concepts and existing applications in IoT and cloud computing in the healthcare.
- Describe healthcare latest industry trends and policies regarding IoT and cloud computing around the world.
- Discuss security issues of IoT and cloud computing in healthcare systems and summarize appropriate solutions.
- Show challenges and open research directions for the integration of IoT and cloud computing in healthcare.

1.2. Problem Statement

The remainder of the paper is divided into nine sections. In Section 1, we thoroughly survey previous reviews on IoT in healthcare and provide a list of contributions that these reviews mentioned, then notable contributions from our paper are presented. The proposed IoT framework for healthcare will be explained carefully in Section 2. In Section 3, we focus on cloud computing technology for

healthcare. In Section 4, various IoT healthcare new concepts and applications will be showed. Then, Section 5 discusses how IoT in healthcare applications are being applied in the industry. In Section 6, all the aspects of the IoT in healthcare security will be discussed. After that, Section 7 shows policies and strategies to trigger the development of IoT in healthcare from numerous developed countries, whereas Section 8 discusses several IoT in healthcare challenges and issues that need to be solved. Finally, in Section 9, we summarize and discuss future approaches.

Table 1. List of contributions from previous surveys on cloud computing and IoT in healthcare.

ID	Reference	Year	IoT	Cloud	Contributions
1	Mutlag et al. [21]	2019	✓	✓	<ul style="list-style-type: none"> Indicate three fundamental factors to effectively manage resources in cloud-based healthcare systems. Review some papers which used fog computing in the healthcare IoT systems. Show limitations of recent methods, systems, and frameworks.
2	Kumari et al. [22]	2018		✓	<ul style="list-style-type: none"> Address various opportunities and challenges on applying fog computing to healthcare. Introduce a three-layer healthcare architecture for real-time applications.
3	García et al. [23]	2018		✓	<ul style="list-style-type: none"> Propose a fog computing-based framework to accelerate the response to mobile patients. Apply proposed framework on a prototype (the response time is reduced by four times).
4	Farahani et al. [27]	2018	✓		<ul style="list-style-type: none"> Focus on recent IoT in e-health research. Introduce a systematic IoT in e-health ecosystem (hardware and software). Show challenges and future directions for IoT in e-health. List security issues in IoT devices and networks.
5	Ahmadi et al. [25]	2018	✓	✓	<ul style="list-style-type: none"> Describe some aspects of IoT architecture in healthcare. Investigate cloud-based architecture role for IoT in healthcare. Discuss critical IoT in healthcare issues and challenges.
6	Baker et al. [26]	2017	✓		<ul style="list-style-type: none"> Describe basic elements in an IoT in healthcare system. Concentrate on different types of sensors and communications methods. Introduce a framework that can be applied in various IoT in healthcare applications. Focus on reviewing cloud computing for data storage.
7	Kraemer et al. [24]	2017		✓	<ul style="list-style-type: none"> Complete a thorough survey on fog computing for healthcare. Categorize fog computing applications into use case classes. Analyze which network level that fog computing tasks can be used. Discuss in detail fundamental components in fog computing.

Table 1. Cont.

ID	Reference	Year	IoT	Cloud	Contributions
8	Islam et al. [20]	2015	✓	✓	<ul style="list-style-type: none"> • Review services and applications in IoT in healthcare systems. • Show how IoT in healthcare has been implemented in the medical industry. • Review security and privacy issues of IoT in healthcare frameworks. • Show several difficulties and future directions for IoT in healthcare.

2. IoT Framework for Healthcare

The IoT in healthcare framework (IoTHeF) is considered the most fundamental aspect of IoT in healthcare because it helps healthcare applications to completely utilize the IoT and cloud computing. The framework also provides protocols to support the communication and broadcast of raw medical signals from various sensors and smart devices to a network of fog nodes.

As shown in Figure 2, there are three essential components of IoTHeF, which include topology, structure, and platform. Each component serves a specific function in the IoT healthcare framework, all of which will be discussed in detail in the following sections. The readers are recommended to review proposed IoT architectures in [28,29] to gain insights into the IoT architectures for healthcare. The systems can collect data about patient health status through multiple sensors. After that, the collected data were transmitted to the remote server for analyzing, and the results were displayed in real time.

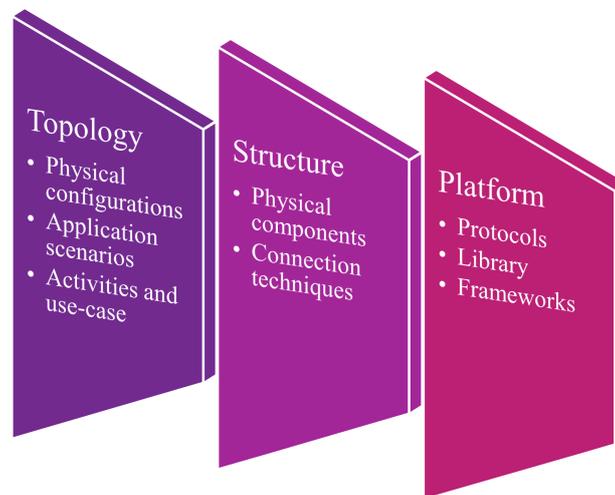


Figure 2. Three basic components and their main functions in the IoT framework for healthcare.

The IoTHeF topology handles the arrangement of general IoT components and outlines some standard setups for given application scenarios in the IoTHeF framework. Figure 3 presents a typical IoT and cloud computing in healthcare topology containing three main elements [30]. First of all, a publisher represents a network of connected sensors or hand-held devices in charge of recording patient’s vital signs, and continuously sending a considerable amount of raw information such as electrocardiogram (ECG), electromyography (EMG), body temperature, blood glucose (BG), and the volume of air inspired and expired by lungs to a broker. Next, the broker analyzes and stores processed data on the cloud. Finally, a subscriber, who directly monitors patients can access the data from any location and responds immediately when unexpected incidents happen. The IoTHeF framework

incorporates individual components into a hybrid computing grid where each component serves a specific purpose on IoT and cloud computing in the healthcare network.

Figure 4 illustrates a situation in which attached body sensors constantly collect the patient’s health condition and vital information. Next, data are sent to hand-held devices via an edge router where it will be analyzed and stored on a cloud computing platform for evaluation later. By analyzing the collected data, caregivers can monitor patients remotely and provide timely treatment when their health statuses reveal that they are in critical condition. This scenario is a typical application scenario for IoT in healthcare. In addition, the bottom part in Figure 4 shows two standard communication configurations which incorporate necessary network components to maintain the streaming of health data through an interconnection of multiple networks. As a result, it is possible for different healthcare systems to exchange information using a long-term evolution (LTE) network, worldwide interoperability for microwave access (WiMAX) [31–34].

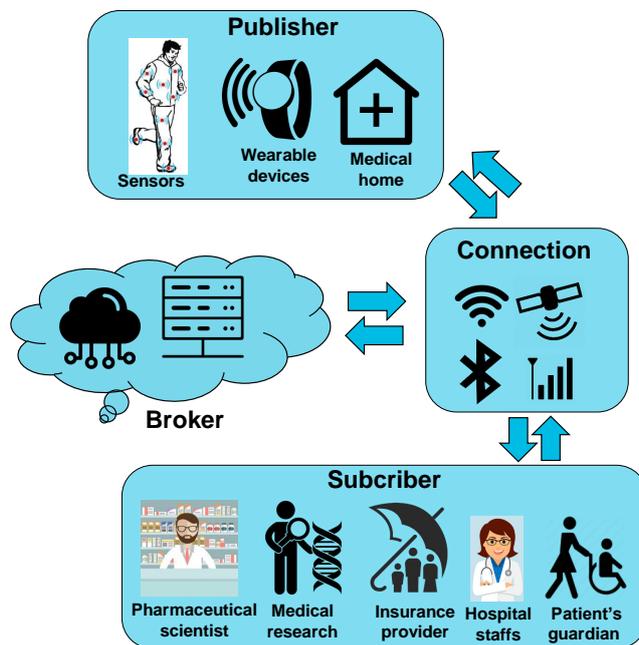


Figure 3. Typical topology for the IoT framework for healthcare which includes publisher, broker, subscriber and the connection technologies between them.

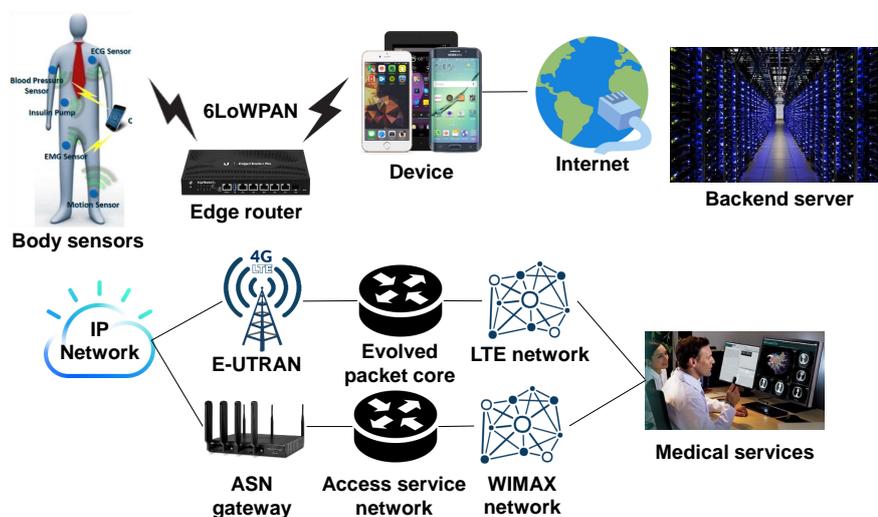


Figure 4. Topology for remote patient monitoring using body sensors (top part) with two standard communication techniques (bottom part).

When it comes to the implementation of a new IoT and cloud computing healthcare-based system, the first thing is to list all associated activities and use-case in the system. Because each disease requires complicated treatment procedures which involve various healthcare activities mostly based on health care provider's viewpoint. The introduction of associated activities and use-case have been mentioned in the context of the remote monitoring system [28], smart healthcare service [35], and IoTheF topology for pervasive patient health monitoring system based on cloud computing [36]. The mentioned healthcare systems can be viewed as standard local network topology systems with the ubiquity of internet connection. As indicated by [35,37], semantic data annotation using heterogeneous IoT devices and a set of medical rules must be defined in the topology of a semantic healthcare system.

2.1. IoTheF Structure

The IoTheF structure or architecture refers to the arrangement of physical IoT components, widely used communication techniques between smart devices and explains the crucial role of a gateway. A basic structure for integrating IoT and cloud computing into a smart health solution was shown in [1]. In this structure, many sensor nodes were used to monitor patients, gather data, and then all collected data were transmitted to a network of sink nodes. Each sink node was identifiable and accessible through IPv6. All nodes in the network were fixed, and sink nodes played the role of the gateway by connecting to local computers through serial ports. In this scenario, the gateway controlled access to the Internet by acting as a border router, and it also functioned as an IPv6 packet fragmentation management system in IPv6 over low-power wireless personal area networks (6LoWPAN). The sensor node was programmed to be both sender and receiver so that it can spread data created by neighbour nodes. In addition, a standardized internet engineering task force (IETF) routing protocol was applied to ensure data collection through multihop by efficiently transmitting the IPv6 data packet using a reliable radio link based on the IEEE 802.15.4 standard. Finally, to mine a massive volume of data, a big data back-end server was built to support data collection and data hosting. It can be deployed on the cloud or a remote data centre to store data permanently. Users can access, modify and query data through the Internet or prioritized channels dedicated to data processing and data analysis.

Figure 5 proposed by [38] shows an effective IoTheF structure which emphasizes the role of a gateway; it is a complete framework from using analogue devices and 6LoWPAN medical sensors to record and store biosignal, contextual and health metrics on the cloud. After that, collected data are analyzed on a remote system. Finally, the system shows visualized results to end users. The proposed model also contains a gateway that forwards health data from various sensors to the back-end server, a tunneling protocol which supports data transfer between a network employing the 6LoWPAN protocol and a network that uses Internet protocol version 4 (IPv4)/ Internet protocol version 6 (IPv6) protocol, and a socket that analyzes and displays patient's health metrics in real-time. Furthermore, the mentioned gateway also has several functions including local clinical data warehouse, local computing ability, and a notification system to maintain a high data transmission rate and improve the robustness of the system particularly at the time when the Internet is unavailable. A similar IoTheF structure can be seen in [33], which integrated several medical devices for remote health monitoring.

Wireless communication techniques for the IoTheF are separated into two major groups: short range and medium range. While short-range communication facilitates a transmission among objects within a medical body area network (MBAN), the medium-range communication is usually used to support communication between a base station and a central node of a MBAN. Each communication technique will be further discussed in the context of IoT and cloud computing-based healthcare systems.

2.1.1. Short-Range Communication Techniques

Short-range communication techniques are usually applied between device nodes in which data processing happens, especially gateway/controller and smart sensors. A signal can travel from a few centimetres to several meters. Even though these techniques can be applied for various types of

networks, we only focus on the development of a small MBAN containing a single central node and several sensors' nodes. Among short-range communication techniques, the most widely used ones are infrared, Bluetooth, and ZigBee. Important characteristics of the three techniques are described in Table 2. Based on these distinctive features, Bluetooth and Zigbee are commonly used in IoT and cloud computing for healthcare applications [39].

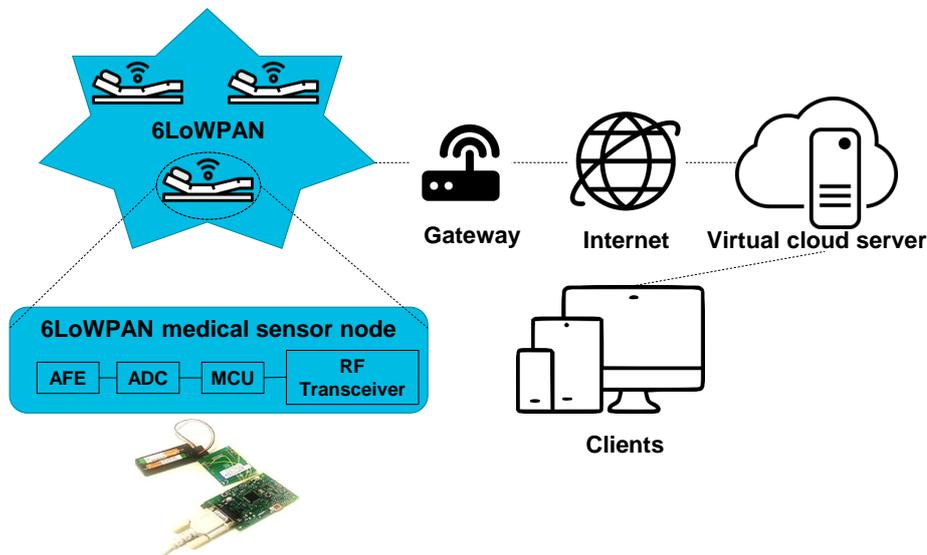


Figure 5. Common IoTHEF structure in a medical sensor network which includes smart healthcare gateways.

Table 2. Comparison between different characteristics of Bluetooth, ZigBee and Infrared short-range communication techniques.

Characteristics	Bluetooth	ZigBee	Infrared
Band	2.4 GHz	2.4 GHz	430 THz to 300 GHz
Range	150 m	10–100 m	Less than 1.5 m
Data rate	1 Mbps	20–250 Kbps	9.6–115.2 Kbps
Topology	Star	Mesh	Point-to-point
Security	Secure pairing 128-AES encryption	Shared network key Optional 128-AES encryption	Line-of-sight and very low bit error rate

2.1.2. Medium Range Communication Techniques

A low-power wide-area network (LPWAN) is a type of wireless communication over a wide area network, which is essential for IoT industrial applications. LPWAN range is remarkably longer than short-range communication techniques because it carries short bursts of data and can reach up to several kilometres at a low data rate and low-power consumption [40]. As a result, it is appropriate for IoT and cloud computing based healthcare applications such as remote patient monitoring and rehabilitation. Among the protocols of LPWAN, LoRaWAN and Sigfox are the most well-known standards.

Although the two standards are well-developed and broadly used in IoT and cloud computing based healthcare applications, they are confronted by rising competition from emerging standards. Many studies [39–43] have proved that the 6LoWPAN has the potential to become the basis of the IoT in healthcare. 6LoWPAN protocol stack complies with IPv6 standard and includes a small adaptation

layer (LoWPAN) to optimize IPv6. 6LoWPAN is compatible with the IEEE 802.15.4 standard, and it is particularly well-fitted to be applied in low data-rate and battery-powered applications. For IoT in the healthcare use case, wearable devices and sensors utilize 6LoWPAN to transmit data over the 802.15.4 standard. The 6LoWPAN protocol establishes the communication between 6LoWPAN devices and devices that use the IEEE 802.15.4 standard. Furthermore, it also supports communication with other internet protocols; e.g., devices using 6LoWPAN can send and receive signals via WiFi networks by applying a simple bridge. Other characteristics that prove the potential of the 6LoWPAN protocol are IPv6 based protocol; a node in the network operates in either secure mode or non-secure mode (the security is still in the development stage). Table 3 summarizes and compares separate characteristics of SigFox, LoRaWAN, and 6LoWPAN protocols, including frequency, channel, range, bandwidth, data rate, payload, channel coding, and security.

Table 3. Comparison between different characteristics of SigFox, LoRaWAN, and 6LoWPAN medium range communication techniques.

Characteristic	SigFox	LoRaWAN	6LoWPAN
Frequency	902 megahertz (US) 868 megahertz (Europe)	902–928 megahertz (North America) 863–870 megahertz or 434 megahertz (Europe) 779–787 megahertz (China)	2.4 gigahertz (Worldwide) 902–929 megahertz (North America) 868–868.6 megahertz (Europe)
Channel	360 channels with 40 reserved channels	80 channels (902–928 megahertz band) 10 channels (779–787 megahertz band and 863–870 megahertz band)	16 channels (2.4 gigahertz band) 10 channels (915 megahertz band) 1 channel for (868.3 megahertz band)
Bandwidth	100 hertz–1.2 kilohertz	125 kilohertz and 500 kilohertz (915 megahertz band) 125 kilohertz and 250 kilohertz (868 megahertz band and 780 megahertz band)	5 megahertz (2.4 gigahertz band) 2 megahertz (915 megahertz band) 600 kilohertz (868.3 megahertz band)
Range	10 to 50 kilometers	5 to 15 kilometers	10 to 100 meters
Data rate	980 bit/sec to 21.9 kbit/s (915 megahertz band)	100 to 600 bit/sec	250 kbit/s (2.4 gigahertz band) 40 kbit/s (915 megahertz band) 20 kbit/s (868.3 megahertz band)
Payload	Between 0 to 12 bytes	Between 19 to 250 byte	Header (6 bytes) and session data unit (127 bytes)
Channel coding	Ultra narrow band coding	Chirp spread spectrum (CSS)	Direct sequence spread spectrum (DSSS)
Security	No encryption mechanism	Two common protection keys: NwkSKey (128 bits), AppSKey (128 bits) NwkSKey ensures data integrity AppSKey provides data confidentiality	Handled at link layer which includes secure and non-secure mode

One of the weaknesses of the 6LoWPAN protocol is that it is incapable of supporting mobile IPv6 (MIPv6), which is a branch of IPv6 that supports mobility feature. Although the support of mobility is a crucial factor in healthcare applications, the default configuration of 6LoWPAN protocol leads to extreme packet delays and loss. Many approaches have been proposed to supplement the mobility capability to existing 6LoWPAN protocols. A new protocol, namely Proxy Mobile IPv6 (PMIPv6), provides a mechanism for mobile patient nodes to communicate with base networks was introduced in [44], this protocol reduced the handover latency, and the integrated piggyback

technique also decreased the signalling overhead. Another research proposed a framework for mobility management that performed two distinct modes, hard mode and soft mode [45]. In the hard mode, a device node in the network must suspend a connection before making a new connection). On the other hand, a device node makes a new connection before interrupting the current connection in the soft mode. In addition, to overcome the backward compatible issue, mRPL+ was used in the 6LoWPAN architecture; it is a mobility management framework in a 6LoWPAN network. Obtained experimental results showed that the ratio of data packets received by using the proposed framework and mRPL+ was almost 100%. In another approach, a lightweight framework to manage mobility protocol intra-MARIO was demonstrated [46]. The proposed framework used an adaptive detection module to identify when a mobile node was moving, a lightweight re-connection mechanism to create a seamless connection of mobile nodes during the change in position, and a multi-hop pointer forwarding scheme to track the location of mobile nodes continuously. Through several experiments, they concluded that, in comparison with previous mobility management frameworks, intra-MARIO significantly reduced handoff delay with low energy consumption, and it also minimized packet loss when a handoff happened. Finally, a seamless mobility handover concept (SMH) in the 6LoWPAN network was introduced in [47]. In the data link layer of the SMH, mobility handover was carried out, whereas the IPv6 based nodes automatically supported the routing process of control message protocol. However, one limitation of SMH was that joining operation between mobile nodes' permanent IP address and the temporary IP address was not conducted. A variety of experiments were carried out to verify the effectiveness of SMH, and the obtained results proved that SMH improved mobility and handoff management.

2.2. IoTheF Platform

IoTheF platform focuses on computing and network platforms; it is fed a huge volume of information created by wearable devices, multiple types of sensors, and it can perform real-time data analytics and responses instantly. IoTheF platform uses IoTheF topology to arrange IoT components and IoTheF structure to choose suitable communication techniques between IoT components.

The importance of a network platform is that it ensures that all sensors operate smoothly so users can interact with them easily. The IoTheF platform was named a common recognition and identification platform (CRIP) in [48]. The development of two prototypes based on the proposed platform demonstrated the practicability of combining regular IoT communication and identification; they also addressed some challenges, including device incorporation and potential security risks. Similarly, a platform focusing on privacy and security issues in medical education learning platform based on IoT and cloud computing, which consisted of two main processes [49], as shown in Figure 6. The first process referred to local storage and communication technologies including data perception (devices identification), data aggregation and preprocessing (data preprocessing and exchange of data), local security and access technologies (different measures to ensure the security and privacy of the locally stored patient data). The second process managed cloud storage and communication including cloud security (identification of user and cloud storage security), presentation (data encoding, data decoding, error handling), application and service (application delivery procedures), and business (service packages and the business policies). Moreover, the proposed framework also introduced some significant functions such as seamless data exchange between different modules, a smart gateway to minimize network traffic load, a fog computing based data storage to increase data sharing speed and security, the implementation of several layers to handle errors and security risks in both local and remote environments. These functions ensured that the framework provided the best security and privacy settings for patients' health data. By analyzing the presented platform [49], the data perception layer belongs to the publisher, the local security layer and cloud security layer represent the broker, and the application and service layer is the subscriber in the IoTheF topology. Furthermore, the access technologies layer, as well as the gateway, show the selection of communication techniques from the IoTheF structure for this platform.

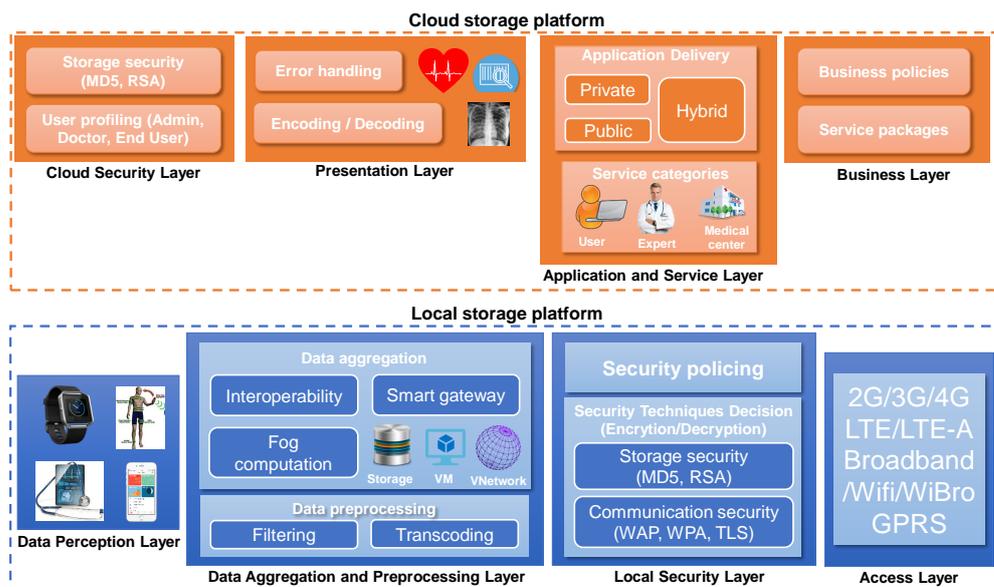


Figure 6. Common IoTheF platform including local storage and cloud storage platforms.

Three studies [50–52] have addressed several IoTheF platform issues such as interoperability, the difficulties that occur when integrating cloud computing in healthcare applications. Each study is exceptional in solving a specific issue. However, it failed to provide a generalized and comprehensive analysis of the IoTheF platform issues. As a result, in 2017, a semantic platform architecture which provided interoperability among heterogeneous IoT devices by using semantic annotation was introduced [37]. Authors also provided a shallow data annotation model and a standard data format and exchange protocol on the Web for semantic applications in the IoT network.

2.3. Discussion

IoT framework for healthcare, namely IoTheF, is a critical component in the development of IoT healthcare systems because it provides healthcare applications with the ability to fully utilize the IoT backbone and supports multiple communication protocols for smart devices.

We divided the IoTheF into typology, structure and platform to discuss important characteristics of the IoT framework for the healthcare. (1) We defined IoTheF topology as the arrangement of general IoT components and provided standard setups for given applications based on new research on this topic. (2) In IoTheF structure, we described the arrangement of physical IoT devices and standard communication technologies (short-range and medium-range communications). Furthermore, the critical role of the gateway in IoTheF framework has also analyzed. For medium-range communication, we concentrated on recent emerged 6LoWPAN technology by showing its advantages compared to standard communication techniques, and we also explained 6LoWPAN limitations as well as described research that worked on solving these limitations. (3) In IoTheF platform, we described computing and network platforms which is based on the foundation of IoTheF topology and IoTheF structure, surveyed relevant research on IoTheF platform and showed IoTheF platform challenges and solutions.

3. Cloud Computing for Healthcare

In recent years, the cloud computing paradigm has become one of the hottest topics in information technology. It has scalability, mobility and security benefits by providing on-demand computing resources (e.g., storage, services, networks, servers, applications, and hardware) to users. According to a research [53], cloud computing has recently emerged as a backbone of IoT healthcare systems. Another great advantage of cloud computing is the capability of sharing information among health professionals, caregivers, and patients in a more structured and organized way, thus minimizing the

risks of medical records lost [20]. As a result, healthcare services and applications have benefited from the development of technologies such as IoT and Cloud Computing [54].

A platform of an m-Health monitoring system based on a cloud computing technology which contained three main layers was proposed in [55]; the platform was presented in Figure 7.

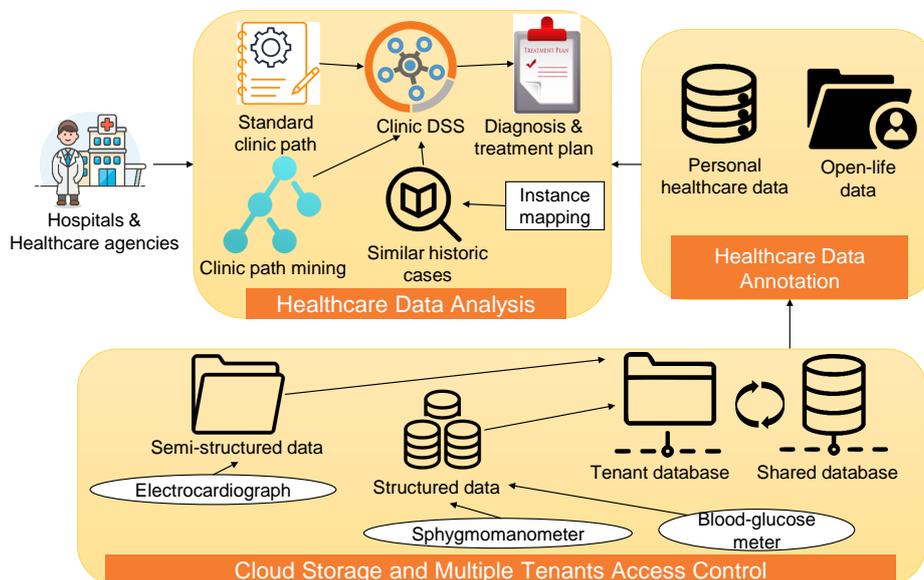


Figure 7. Functional platform of the cloud-computing-based m-Health monitoring system with three main layers' cloud storage and multiple tenants access control, healthcare data annotation, and healthcare data analysis.

- The Cloud Storage and Multiple Tenants Access Control Layer is the backbone of the platform, which receives healthcare data collected by sensors such as BG and sphygmomanometers in daily activities. The authors reduced the cost of storing and managing data by adopting the cloud framework. Moreover, a multiple tenant access control module between tenant database and shared databased is implemented to enhance the security and privacy of patient data.
- The Healthcare Data Annotation Layer solves data heterogeneity issue that is commonly happened during data processing. Because equipment varied by hospitals, generated data are often heterogeneous, which increases the complexity of automatic healthcare data sharing and comprehending between medical agencies. The authors proposed an open Linked Life Data (LLD) sets to annotate personal healthcare data and integrate dispersed data in a patient-centric pattern for the cloud application.
- The Healthcare Data Analysis Layer analyses healthcare data stored in the cloud to assist in clinical decision making because similar historical data are valuable assets to make a treatment plan for a similar illness case. As shown in Figure 7, mining algorithms are implemented to induce clinic paths from personal healthcare data. After that, a similarity calculation module is designed to compare patients' healthcare data with historical cases.

Each layer was specially designed to handle a predefined task, and it can be implemented to serve a variety of demands for healthcare using cloud platform and service-oriented architecture. This platform helped practitioners to observe and evaluate health conditions by transmitting raw sensors information from end-user to the cloud platform for processing and then displayed results to doctors [28,56,57].

However, the majority of the cloud data centres are geographically centralized and located far from end-users [58]. Thus, for applications that require immediate real-time feedback, like remote monitoring or telehealth, communication time between users and remote cloud servers cause significant issues such as high round-trip delay, network congestion, and other issues. As a result,

recent technological evolution, such as fog computing and big data, extend cloud computing ability by supporting highly scalable computing platforms [59].

CISCO has first introduced the fog computing concept as a solution to extend the computing power and storage capacity of the cloud to the network edge [60]. Fog computing is closer to devices and has a dense geographical distribution, so applications and services can be placed at the edge of the local network, which reduces bandwidth usage and latency. In other words, it brings the cloud closer to its users. Thus, it enables data to be collected and processed locally, reduces network latency and bandwidth usage.

Table 4 compares different characteristics of cloud and fog computing. Based on the comparison, fog computing shows that it is more suitable for IoT healthcare systems compare to cloud computing. Different from traditional IoT based healthcare systems, the fog-assisted system can improve various aspects of IoT based healthcare systems like scalability, energy awareness, mobility, and reliability [61–64].

Table 4. Comparison of several characteristics of cloud computing and fog computing.

Characteristics	Cloud Computing	Fog Computing
Node location	The internet	Local network edge
Number of node	Little	Large
Latency	High	Low
Delay	High	Low
Distance between devices and server	Multiple hops	Single hop
Location awareness	No	Yes
Distribution	Centralized	Distributed
Scalability	Supported (Dynamic adaptation to workload)	Limited (Fog is not as scalable as cloud)
Mobility support	Limited	Good
Real-time interaction	Supported	Supported
Data storage	Huge	Limit
Transmission	Device to cloud	Device to device
Data aggregation	At cloud	Partially and remaining to cloud
Security	No user-defined security (Carried out by cloud service providers)	User-defined security (Data is processed by a complex distributed system)

3.1. Fog Computing Architecture

Fog computing architecture is a promising topic in cloud computing research. Recently, a large number of architectures have been introduced for fog computing, and three tiers architecture is considered to be the predominant structure nowadays [65]. The basic fog computing architecture depicted in Figure 8 is split into the following three main layers:

1. Device layer: The device layer is the closest layer to the end-users/devices. It consists of several devices, such as sensors and smart devices. These devices are widely geographically distributed and are responsible for sensing the physical object and sending data to the upper layer for processing and storage.
2. Fog layer: The second layer is the fog layer located at the edge of the network, it contains a huge number of fog nodes, which commonly includes routers, gateways, access points,

and base stations. Fog nodes are responsible for performing tasks such as scheduling, storing, and managing distributed computation.

3. Cloud layer: The cloud layer is responsible for permanent storage and extensive computational analysis of data. Unlike traditional cloud architectures, in fog computing, the cloud layer is accessed in a periodical and controlled manner, leading to efficient utilization of all available resources.

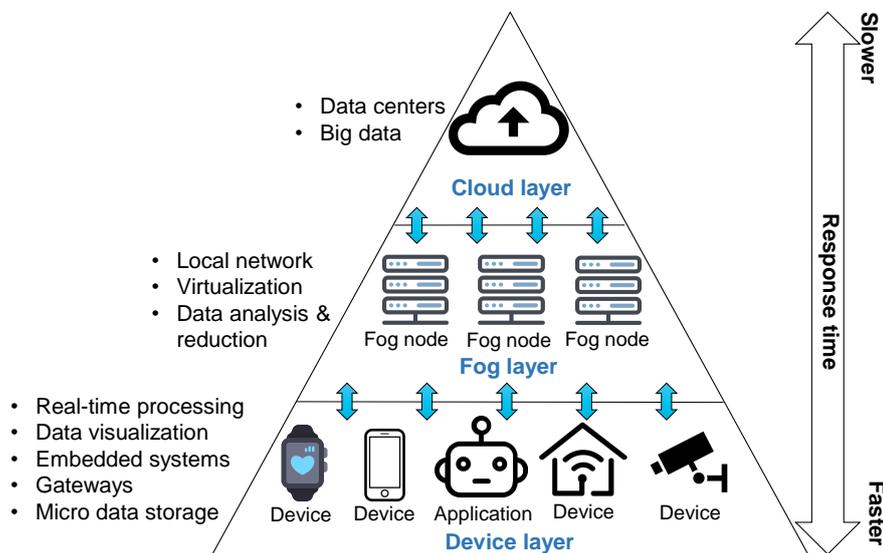


Figure 8. Illustration of fog computing architecture including device layer, fog layer, and cloud layer and their main attributes.

3.2. Fog Computing in the Healthcare

In 2017, a smart healthcare gateway for fog computing module was introduced [66]. More specifically, the authors concentrated on setting up a connection from household gateways to hospital gateways. Through various experiments, they proved that fog computing has a vital role in supporting the smart gateway. In another research work, Rahmani [34] analyzed the role of fog computing in implementing healthcare monitoring framework, and they proposed a mediator layer to receive raw information from sensor devices and then stored them on the cloud. Finally, a fog computing based early detection of chronic disease system was proposed to prove the effectiveness of adding the fog layer to the framework. In 2016, a healthcare framework which named HealthFog was presented [67]. In the proposed framework, fog computing technology was deployed to connect the user's layer to the cloud layer. They mostly focused on improving and solving the electronic medical record (EMR) privacy problems. Next, cloud-based security software was added to the HealthFog to strengthen system security. In addition, a new concept, namely cryptographic primitive, was proposed to improve the effectiveness of HealthFog. In the same year, Kim [68] introduced a prototype of IoT health monitoring application using fog computing. The proposed structure utilized edge computing's advantages for home and hospital automation system. In 2015, Gia improved existing fog computing systems by analyzing bio-signals on the fog server side to support real-time systems [32].

In recent years, healthcare applications are shifting from cloud computing to fog computing. Table 5 shows recent healthcare applications based on fog computing.

Table 5. Summary of the research field, dataset, results and main contributions from recent fog-based healthcare studies.

Ref	Year	Field	Dataset	Results	Contributions
[69]	2019	Smart health	Self	Efficient data sharing service with privacy preservation	<ul style="list-style-type: none"> • Implement a fog-enabled smart health to improve data sharing service. • Provide a privacy-preserving fog-assisted health data sharing case study.
[63]	2018		Dataset from other research	BBN classifier/93.6%	<ul style="list-style-type: none"> • Introduce a novel Fog-Cloud framework for healthcare services in smart office. • Propose a Severity Index to estimate the adverse effects of different activities on personal health. • Implement an application scenario for healthcare prediction and alert generation.
[70]	2018		Self	Reliable and faster processing speed	<ul style="list-style-type: none"> • A data processing system is proposed to improve network reliability and speed. • Introduce a self-adaptive filter to recollect missing or inaccurate data automatically. • Propose an RVNS queue to process preprocessed data.
[71]	2018		Self	J48 decision tree classifier/93.5%	<ul style="list-style-type: none"> • Design a fog assisted cloud-based healthcare system for early detection of the virus outbreak. • Generate alerts immediately on the user's mobile phone in the fog layer. • On the cloud layer, the virus outbreak is illustrated using temporal network analysis.
[34]	2018	Acute illnesses	Self	Enhance overall system efficiency	<ul style="list-style-type: none"> • Design smart e-Health gateway to provide several higher-level services. • Use fog computing to generate a Geo-distributed intermediary layer between sensor nodes and cloud. • Create a smart e-Health gateway prototype called UT-GATE with high-level features.
[61]	2019	Diabetes	UCI diabetes & UCI PAMAP2	J48Graft decision tree classifier/98.56%	<ul style="list-style-type: none"> • Propose a fog-based health framework to diagnose and remotely monitor diabetic patients in real-time. • Perform risk assessment of diabetes patients at regular intervals.
[62]	2018	Hypertension attack	Self	ANN classifier/95.21%	<ul style="list-style-type: none"> • Propose an IoT-fog-based healthcare system to continuous monitor patients. • Predict the risk level of hypertension attack of users remotely. • Data collected from patients were saved on the cloud and shared with domain experts.
[64]	2018	Healthcare system privacy	NA	Solutions for privacy issues	<ul style="list-style-type: none"> • Show research challenges in developing practical privacy-preserving analytics in healthcare systems. • Propose solutions to solve these challenges.
[72]	2018	Wearable healthcare monitoring system	NA	System is resilience against known attacks.	<ul style="list-style-type: none"> • Propose a cloud-based user authentication scheme for secure authentication of medical data. • Create a secret session key for future secure communications. • Conduct a detailed comparative analysis on the system's communication and computation costs.
[73]	2018	Mosquito-borne diseases	UCI Adult	FKNN classifier/95.9%	<ul style="list-style-type: none"> • Introduce a fog-based system to detect and classify different mosquito-borne diseases. • Implement Social Network Analysis to illustrate the outbreak of the mosquito-borne disease on the cloud layer.
[68]	2016	Smart homes and hospitals	NA	NA	<ul style="list-style-type: none"> • Introduce a cloud to fog U-healthcare monitoring system in smart homes and hospitals. • Investigate significant features of Fog computing and how it extends Cloud computing.

3.3. Discussion

Through this section, we explained in detail the cloud computing paradigm and primarily focused on fog computing architecture, which is a foundation for healthcare applications. We also compared several characteristics of cloud and fog computing and explained why fog computing is more suitable for healthcare applications. After that, a standard fog computing architecture which includes device layer, fog layer and cloud layer was described. Finally, we discussed fog computing in healthcare by summarizing recently published papers that apply fog computing in healthcare applications.

4. Healthcare Concepts and Applications

Before the dawn of IoT and cloud computing eras, physician-patient interactions were limited to in-person visits, telecommunications, and text communications. It was impossible for doctors to monitor patients' health condition remotely to make a timely treatment. However, recently, IoT and cloud computing based healthcare systems make real-time applications in the healthcare sector possible, unleash the full potential of IoT and cloud computing in the healthcare, and support physicians in delivering excellent healthcare services. IoT and cloud computing have increased patient engagement and satisfaction because communications between patients and doctors have become more accessible and more efficient. Furthermore, remote monitoring reduces the length of hospital stay and avoids hospital readmissions. As a result, these new technologies have significant impacts on reducing healthcare costs and improving treatment outcomes. IoT and cloud computing technologies are improving the healthcare industry by contributing to the evolution of a new array of IoT-connected medical devices and improving people interaction in healthcare systems. More and more IoT and cloud computing based healthcare applications have been developed to serve patients, families, physicians, hospitals and insurance companies.

We divide healthcare applications into two main groups to help readers gain a better understanding of this broad topic. The first group addresses concepts that arise during the convergence of IoT and cloud computing in the healthcare, whereas the second group mostly concentrates on dividing healthcare applications into two specific categories: single parameter and multiple parameters application. The single parameter application deals with an illness or a particular disease, while the multiple parameters application is used to handle over one disease or condition together as a whole. Figure 9 illustrates some concepts and trending application in the healthcare industry. The classification is extendable and can be easily altered by appending more concepts with distinctive characteristics or applications, including single- as well as multiple-parameter solutions.

4.1. Healthcare Concepts

IoT and cloud computing are revolutionizing the healthcare industry by bringing numerous concepts to the research community, and each concept supports a group of healthcare applications. However, it is hard to draw a general explanation for the concept of IoT and cloud computing in healthcare. This paper defines concepts as trending solutions that have the prospect to be a cornerstone for a list of applications and solutions. As healthcare systems are being developed, new concepts are constantly added. They will eventually become essential platforms for healthcare applications. The following sections highlight several fundamental concepts of IoT and cloud computing in the healthcare.

4.1.1. Ambient Assisted Living (AAL)

AAL appears as a sub-area of ambient intelligence. It is a relatively new IT trend that places smart objects in the surrounding environment to provide assistance and care for seniors to live independently. Recently, research related to AAL has increased significantly thanks to advancements in sensor technology, as well as the availability of smart healthcare gadgets. Furthermore, more and more AAL applications are applying cloud computing [74,75] to manage collected data from these

devices, analyzes and recognizes a person’s specific activity to allow real-time remote monitor and react to emergencies.

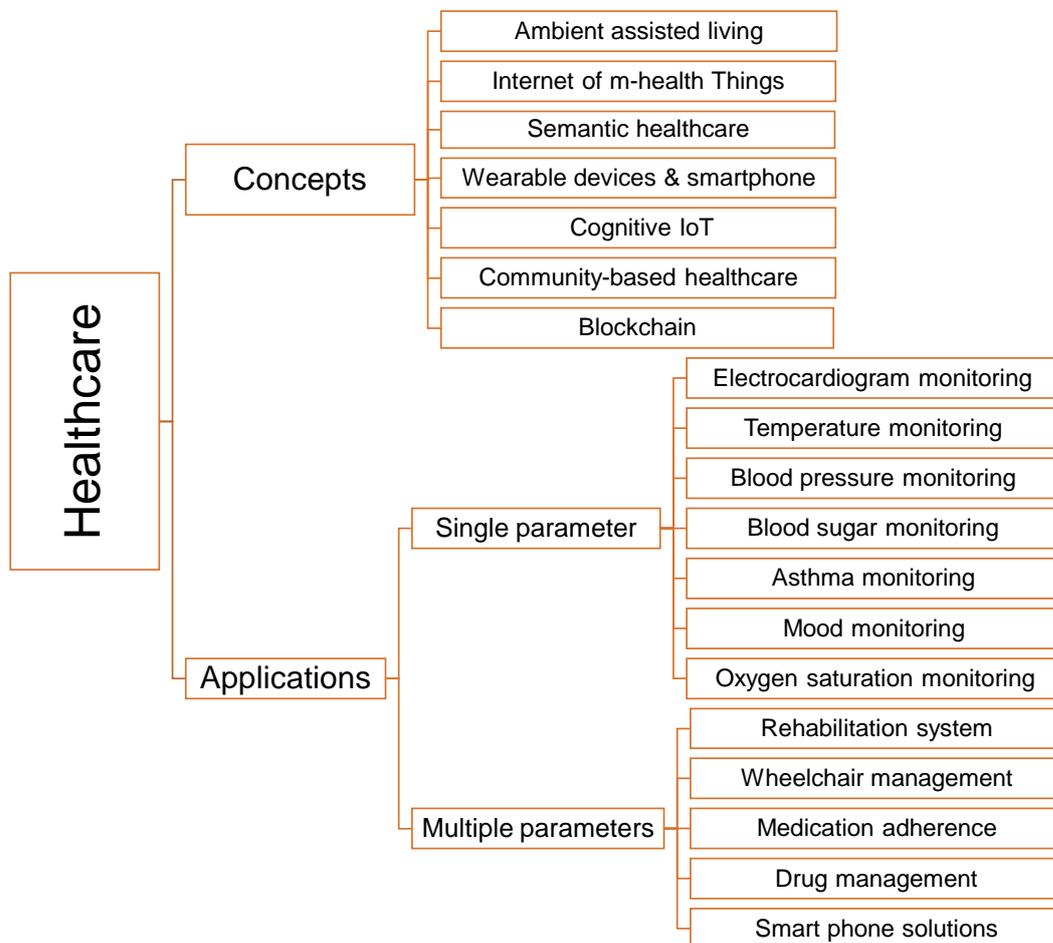


Figure 9. Classification of concepts, single parameter applications, and multiple parameters applications for IoT in healthcare.

Table 6 summaries general domains and typical sensors in recent studies about AAL. Three main domains in AAL are activity recognition, vital monitoring, and surrounding environment recognition. Among them, activity recognition interests a large number of researches as it is crucial to support the well-being of elders, and detect potential threats that can happen to seniors.

Table 6. List of ambient assisted living main domains and standard sensors that are used in each domain.

Domain	Types of Sensors	Main Study
Activity recognition	Force, button, ultrasonic, accelerometer, kinect	[74,76–80]
Vital monitoring	Heart rate, temperature, glucose meter, electromyography	[33,75,81]
Surrounding environment	Air temperature, moistness, carbon monoxide, carbon dioxide, glow	[82]

4.1.2. Internet of m-Health Things (mIoT)

In recent years, mIoT has been an active field in healthcare; it refers to the use of mobile computing, medical sensors, and cloud computing to monitor patient’s vitals in real time [83], and the utilization of communication technologies to forward data to a cloud computing framework. Data can be retrieved

by practitioners to observe, diagnose, and treat patients effectively and on time. As a result, it has the potential to become the foundation for inventive IoT and cloud computing in healthcare applications in the future since it provides fully connected and mobility functions. The challenge of ensuring system security and user's privacy for the m-health application was addressed by [29], where the authors proposed several ways to increase patient data confidentiality, including physical safeguards, technical safeguards, audit reports, technical policies, and network security. Recently, a platform for an m-Health health observing application based on cloud computing (Cloud-MHMS) was introduced [55]. The platform included many important layers; a multiple tenant access concept was introduced to secure data privacy in the data storage module. In the annotation module, a linked list was used to extend exchange EMR semantically. Finally, data mining and machine learning were performed to improve data analytic efficiently in the data analysis module.

4.1.3. Semantic Healthcare

In recent years, the application of semantics and ontologies in healthcare systems to store and manage large amounts of medical data has increased [37,56]. Putting semantics and ontologies on the top of the IoT allows semantic interoperability among multiple wearable devices in the healthcare domain.

For example, a semantic fog-based network model which stored and exchanged a large amount of soldiers health and weapons conditions between network components was proposed [56]. Through tactical and non-tactical operations, the system provided smooth communication between soldiers and control station. Furthermore, an IoT-based semantic healthcare framework supporting communication between heterogeneous IoT devices was introduced in [37]. The authors concentrated on designing a lightweight model for semantic annotation of data to make it semantically meaningful. Several papers have addressed semantic medical issues using IoT such as semantic modelling issue [35] and semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare [84].

4.1.4. Wearable Devices and Smart Phone

Wearable technology is a trending topic these days, and it is also a distinctive characteristic of IoT. In the context of healthcare, wearable gadgets reduce overall costs and bring numerous benefits to health professionals and patients. They can be anything from smart wristbands, watches, shoes, shirts, caps, necklaces, headbands and eyeglasses. Many sensors integrated into these smart devices facilitate the ability to gather user's health condition or surrounding environment and upload them on a database or fog layer for real-time processing. Moreover, these wearable devices are supported by smartphones which use their computing power to analyze or transmit collected data to a cloud computing-based framework for storing, processing, and analyzing the data. Finally, a health application on the smartphone is used to visualize analyzed data. In one recent study, an IoT in healthcare framework that included numerous wearable devices to gather and analyze sensors' bio-signal from time to time [85]. This framework is distinctive as it contained two or/and eight channel electrodes to evaluate ECG and EMG signals at 1 kHz fixed frequency, an analogue front-end (AFE) that complies with the IEEE 802.11 standard, a microcontroller used to transmit and process data, and a power management system. The prototype operated at 2.4 GHz, 3.3 V. The transceiver supported communication range between 20 m and 100 m with the transmission speed at 128 kB/s and a latency of 1.2 ms. The transceiver was combined with AES for encrypting data in real-time and had a high common-mode rejection ratio (CMRR).

4.1.5. Cognitive IoT (CIoT)

The impressive progress that sensor technology has made in recent years not only reduces sensors price significantly, but it also makes sensors more intelligent. As part of the current IoT new concepts, cognitive computing refers to a smart device that can mimic the human brain in solving problems. The CIoT application supports data analytic and reveals patterns hidden in vast volumes

of data. As a result, it improves the sensor's abilities in processing and adjusting to the surrounding environment automatically.

Taking into account the nature of IoT devices that continuously generate a large amount of health data, the CIoT becomes a practical solution. In a customized CIoT framework, it is a requirement that all sensors (body sensors or sensors placed in the environment) collaborate among themselves and with other smart gadgets to effectively observe the patient's health condition. The IoT and cloud computing for healthcare framework based on cognitive approach is smart enough to make appropriate decisions based on collected data and delivers necessary healthcare services on time.

Cognitive IoT healthcare research, which concentrates on processing and analyzing a huge volume of data, has been increasingly investigated recently. A great prospect of medical ontologies and semantics has earned tremendous attention from IoT-based healthcare application designers. The idea of a cognitive IoT framework using semantic data representation and message-oriented middleware was introduced [86]. In the structure, semantic publisher (data sources) sent personalized data over time to semantic subscribers (consumers) followed a particular subject. A semantic message broker was in charge of transmitting data from a publisher to a subscriber. As a result, to promote the interoperability, a semantic depiction for all the exchanged data was required. A more comprehensive framework that managed semantic health data was shown in [35]; it can (1) deduce valuable information from raw data sources and (2) combine them on the same topic. The proposed framework can perform inferences and generalization automatically. Thus, it encourages the data mining process and extends more data for the IoT in healthcare.

4.1.6. Community-Based Healthcare

Community-based healthcare concept introduces the establishment of a network which covers every part of a local community. It could be IoT and cloud computing in the healthcare framework that serves a public clinic, a residential suburb, or countryside. In a community-based healthcare framework, various networks can be linked to establish a collaborative network structure. Moreover, an exclusive utility, namely community health, is inevitable to serve aggregate practical demands as a whole. Philip in [87] showed an advanced IoT bio-fluid analyzer, an electronic reader based on Lora/Bluetooth technology for a bio-medical examining framework. They conducted several experiments to show the potential of long-range data transmission and an associated smartphone application to create a community-based healthcare examination platform for urinary tract infections (UTIs). The proposed prototype transmitted distance was from 1.1 km to 6 km with the reduction in the power density of an electromagnetic wave between 119 and 141 decibels. Finally, all data were uploaded to a cloud server for storage.

4.1.7. Blockchain

A critical problem that prevents connected healthcare (data sharing between different healthcare providers) is data fragmentation. In addition, strict security requirements and the issue of trust must be addressed to completely exploit the potential of healthcare components. Recently, the development of blockchain technology [88] offered a radical breakthrough to solve the data fragmentation problem. An outstanding benefit of blockchain is that it helps healthcare organizations bridge traditional data repositories and facilitates the secure sharing of sensitive medical data. Not only does blockchain technology increase transparency between patients and doctors, but it also ensures efficient collaboration between different healthcare providers and research organizations.

What makes blockchain stand out as a technology for secure and flexible data sharing is a combination of three factors. First, blockchain has an immutable "ledger" [89] that people can see, verify, and control. It is guaranteed that, once a record in the ledger is recorded, it cannot be changed. In addition, every transaction is verified according to predefined rules. Second, the blockchain is built as a distributed technology, which is simultaneously operated by multiple computers. This means that blockchain has no single failure point where digital assets or records were compromised or hacked.

Third, blockchain supports data exchange logic and agreement rules with a flexible mechanism of smart contracts. For example, a smart contract can be used to manage identity and specify different permissions for different EMRs stored on the blockchain. Thus, doctors only allowed to access EMR profile that they were assigned. There are many promising blockchain projects underway in the healthcare area that utilize the blockchain to manage EMR, pharmaceutical supply chain, medicine prescriptions, payment distribution, and clinical pathways. One example is a system which triggered a smart contract when a handshake between sensors and smart devices happened [90]. After that, all transactions were recorded on the blockchain. The proposed system supported medical interventions and real-time patient monitoring by automatically notifying responsible health professional when a patient is in desperate need of emergency services, and all events were also registered on the blockchain. As a result, it resolved various security vulnerabilities associated with the delivery of notifications and remote patient monitoring to all included parties. Another three-tier healthcare data storage architecture on a blockchain included health professionals, healthcare facilities, and inpatients [91]. Data inquiry has strictly followed the role of individuals in the blockchain. Thus, it ensured data privacy and security as well as provided a promising way to avoid many issues that have prevented providers, researchers, and patients from taking full advantage of connected healthcare.

4.2. IoT in Healthcare Applications

By practising the mentioned concepts, various healthcare applications have been introduced recently. It can be noted that concepts from previous sections are applied to implement real applications, while applications refer to end-to-end products that are written to serve end users. As a result, concepts are proposed by researchers, whereas healthcare applications are created by developers to serve patients and physicians.

This section discusses wearable technology, portable gadgets, sensors for healthcare, and the latest medical devices that have appeared recently. These technologies are considered an IoT breakthrough which leads to potential solutions for various healthcare issues. Among them, sensors contribute to the integration of IoT in healthcare. Currently, many sensors on the market can track a patient's vital information, and then directly transmit data to a network or through mobile devices. Sensors allow healthcare professionals to observe a patient's health condition in real-time and provide appropriate treatment. Furthermore, sensors can also be used to track the user's vital information when they work out or to track sleep quality. There are many types of medical sensors that evaluate BG, heart pulse, BP, arterial oxygen, and emotion tracking; they can notify patients or physicians in time if abnormalities occur. Thanks to the development in IoT technology, sensors achieve better performance, become cheaper and consume lesser energy. The following subsections show a diverse collection of healthcare applications based on IoT, and they discuss single as well as multiple parameters applications.

Based on existing IoT in healthcare research that applied on a specific disease, Table 7 is generated to show what sensors were applied in each research, and how did they transmit data.

Table 7. Type of sensors that are usually used in specific disease and detailed data transmission descriptions.

Disease/Condition	Sensors	IoT Roles/Connections
Diabetes [92,93]	Glucose sensor, contextual sensor, near infrared led	The sensor's output is sent to Android gateway for local storage and data pre-processing then they are sent to the cloud for analysis and notification to the responsible person (Doctors, caregivers) if abnormalities occur.
Asthma [94,95]	Pulse sensor, temperature sensor	Microcontroller board processes signals, and then the data is sent through a WiFi module to the cloud for storage via hypertext transfer protocol (HTTP).

Table 7. Cont.

Disease/Condition	Sensors	IoT Roles/Connections
Heart disease [28,96–103]	Optical heart rate sensor, BP sensor, ECG sensor	The data are transmitted to a microcontroller using a wireless transmitter, and then it is sent to the servers through an appropriate smartphone gateway.
Hyperthermia and hypothermia [104–106]	Thermopile infrared (IR) sensor, wearable thermometry	wireless body area network (WBAN) connects sensors through an appropriate gateway, the raw data are sent to the server through WiFi for storage and analyzing.
Tele-surgery [107]	Microelectromechanical sensors (Mems sensors), robot arms, microcontroller	The sensors values are fed to a microcontroller and transmitted to 2 connected Zigbee system in realtime without delay and data loss.
Ebola [108]	Lightweight body sensors, radio frequency identification (RFID) reader	The sensors' output is recorded by WBAN and is sent to mobile devices through Bluetooth connection, then finally the data is broadcast to the remote server instantly using WiFi or 4G network.
Wheelchair management [109,110]	Camera sensor, accelerometer sensor, force sensor	The controller integrated into the wheelchair process signals from sensors and realizes abnormality; the controller then sends data to the web server through an appropriate gateway.
Rehabilitation [111,112]	Force sensor, distance sensor, RFID	The controller integrated into the node processes signals and communicate with the remote system using a WiFi connection or through a smartphone gateway.
Medication non-compliance [111,112]	Force sensor, distance sensor, RFID	The controller integrated into the node processes signals and communicate with the remote system using a WiFi connection or through a smartphone gateway.
Neuromuscular diseases [113,114]	EMG sensors	The raw sensor data is sent to the controller; then, a signal classification model is performed to detect neuromuscular disorders. The classification results are sent to the cloud for storage.
Respiratory disease [115,116]	SpO2 sensor	The wearable devices recorded the sensor data then it connects to a wireless mesh network and sends data to the server through a personal computer connected to the internet.

4.2.1. ECG Monitoring

An ECG sensor records the electrical activity of a heart at rest, delivering information about HR and rhythm. The information is valuable in early prediction of a heart enlargement due to hypertension (high BP) or a heart attack (myocardial infarction). An ECG test is necessary if a patient is in a high-risk group of heart diseases such as high BP, and symptoms such as palpitations or chest pain. The integration of IoT in ECG monitoring has a high potential to warn users about heart rate abnormality, which is a vital sign of early heart disease detection. Thus, various studies [28,96–100] explicitly discussed ECG monitoring using IoT technology. It is worth noticing that in [117], the authors introduced an energy saving framework that performed ECG compression and QRS detector for wearable gadgets in real-time. Next, they proposed a mechanism to increase QRS complex detection productively and using less computing power. Another advantage of this framework is that it did not require multipliers. Moreover, in recent years, we have seen the emerging of smartwatches, and HR monitors are one of the most important features in smartwatches and fitness trackers now. Optical heart rate sensors [118,119] are suitable for producing information like on-the-spot readings or resting heart rate data, which is an essential indication about the current health state. They are also quite useful for monitoring HR data when people are working out.

4.2.2. Temperature Monitoring

Human body temperature is a crucial variable which allows general practitioners to diagnose a patient's health condition. For some illnesses (such as sepsis, and trauma), a change in core body temperature is an early warning sign. By measuring patients body temperature, doctors can gather illness trajectory for many diseases. A common approach in measuring the body temperature is a thermometer that is attached to body parts (rectum, mouth, ear, and vagina), but it is uncomfortable for patients and increases the chance of contracting infectious diseases. However, thanks to the development of IoT in healthcare recently, various replacements have been proposed. For example, an intelligent 3D printed hearable gadget equipped with an infrared sensor was demonstrated [106]; it can be comfortably worn on human ears to monitor ear temperature based on the eardrum. The device was perfectly incorporated with a wireless module and data processing circuits for data processing function. Through the smart earbud, they demonstrated how the ear temperature was precisely tracked despite environmental changes and user activities. The device also served as a hearing aid because it was equipped with a microphone and an amplifier. Some other studies summarized each stage in the development of a wearable core body temperature thermometry [104,105]. Working prototypes that followed the theory were developed. Experimental results proved that the thermometry captured variation accurately in core body temperature.

4.2.3. BP Monitoring

Blood pressure measurement is a standard procedure in the hospital. However, this mandatory measurement can put tremendous pressure on resources. As part of the move towards paperless EMR, many hospitals are looking to curb these cumbersome processes. The authors in [101] introduced a wearable cuffless gadget based on photosensors to monitor blood pressure. Recorded blood pressure information is stored on the cloud. By monitoring blood pressure from 60 subjects, they proved that the proposed gadget obtained accurate blood pressure data with no error in systolic and diastolic blood pressures. In another study, blood pressure monitoring framework based on deep learning which can monitor blood pressures constantly was demonstrated [102]. They also combined CNN with time-domain characteristic to evaluate systolic and diastolic blood pressures. Moreover, a prototype of a monitoring system that frequently evaluated blood pressure based on obtaining ECG and photoplethysmogram (PPG) from fingertips was introduced in [103]. Collected signals were transmitted to a micro-controller where blood pressure was computed. After that, results were shown locally and then sent to the cloud for storage.

4.2.4. BG Monitoring

It is no secret that diabetes is one of the biggest epidemics and costly diseases to manage in healthcare. It is a condition that happens when the BG remains high over a long period. There are three major types of diabetes, including type 1 diabetes (juvenile-onset diabetes), type 2 diabetes (non-insulin dependent diabetes), and gestational diabetes. As a result, based on distinctive characteristics of diabetes, three main tests that are usually conducted to identify diabetes and prediabetes including random plasma glucose test, oral glucose tolerance test, and fasting plasma glucose test [120]. Test results provide necessary proofs for diabetes diagnosis and treatment plan. A widely used method in drawing the blood sample for diabetes diagnosis is "Finger-pricking" followed by BG estimation using a BG meter.

Nevertheless, drawing blood from patients' fingertip is an unpleasant process. In addition, unsafe practices during finger-pricking such as contaminated equipment may expose a patient to the blood-borne disease. In the last few years, thanks to the integration of IoT in healthcare, wearable gadgets have been increasingly adopted for measuring BG levels because they are safer, more comfortable, and more convenient. For example, an innovative BG monitoring framework was introduced recently [92]; the authors chose a suitable sensor and designed a front-end interface to display the glucose level,

core body temperature and environmental data in real-time. Additionally, they developed a BG test tailored communication protocol which consumed energy efficiently. Finally, various experiments were conducted, and the results proved that the proposed framework included numerous structured design improvements for BG monitoring, as well as interface service such as push notification to inform doctors when patient's BG level was too low or too high. Another example is a compact optical sensor in conservative management of glucose level monitoring [93]. The proposed sensor circuit composed of an Infrared LED with 650–2500 nm wavelength to measure BG and a near-infrared photodiode that acquired light reflected from the human body. Obtained light signals were used to quickly and accurately compute the glucose level.

4.2.5. Asthma Monitoring

Asthma is a long-lasting illness that has an effect on airways and causes difficulty in breathing. If a patient suffers asthma, there is a swelling of air passages that lead to a temporary shrinking of airways (carrying oxygen to the lungs), which causes a series of asthma signs including coughing, wheezing, shortness of breath, and chest pain. Critical case results in hunched shoulders strained abdominal and neck muscles, and inability to talk.

In order to get an asthma attack under immediate control, handheld inhalers or nebulizers are commonly used. The most typical inhaler is a metered dose inhaler; when it is squeezed, a moderate amount of medicine is released as a spray. For example, an IoT asthma monitoring system which included a heart pulse sensor was introduced [94]. Then, data gathered from the sensor was sent wirelessly to a micro-controller in real-time and finally transferred to a remote server. In the server side, a database was deployed to manage the data. Hospital staff can access a web page to observe a live update of a patient health condition. In another research work, a customized temperature sensor was utilized to compute the respiratory rate [95]. Then, the respiratory rate values were showed in a web browser, which was very handy for doctors to monitor patients' health conditions from anywhere. Finally, an artificial intelligence system was conducted to automatically evaluate patient health record and reduce burdens for medical professionals.

4.2.6. Mood Monitoring

Mood tracking includes a set of psychological techniques to help individuals stay in healthy emotional states, and assist them with mental diseases, such as bipolar disorder and depression. Self-monitoring of emotion improves the user's understanding and proactive management of their mind. The ubiquity of smartphones and their apps has allowed them to support many health purposes. Maintaining a healthy lifestyle is a hot trend in smartphone application development. Self-tracking is one of the most important functions in health apps as it helps users continuously monitor their physical and mental status. An approach to track mood based on a set of predefined rules was introduced [121]. They collected data from ad hoc sensors and smart cities to prevent the frailty and mild cognitive impairment of senior people.

4.2.7. Oxygen Saturation Monitoring

Blood oxygen saturation is an important physiological parameter to monitor the cardiovascular system, and it is also an important measurement in healthcare and medical treatment. Non-invasive methods in oxygen saturation tracking solve issues that occur in conventional approaches and demonstrates the potential of real-time monitoring, which has exceptional advantages for remote monitoring. Recently, non-invasive tissue oximeter which could obtain HR information, oxygen saturation level, and pulse parameters was proposed [115,116]. After that, obtained data were transmitted to a remote server via GPRS/WiFi/Zigbee networks and processed by an expert decision-making system.

4.2.8. Rehabilitation System

Rehabilitation contains a set of procedures which help patients (who suffer or are diagnosed to suffer from a disability) to maintain and reach their maximum physical, mental and social abilities. A walker based physiotherapy system using orientation, ultrasound, and force sensors was proposed in [111]. The system contained three layers, including sensors, edge and cloud, and application layers. When the smart walker was used, it continuously evaluated movement metrics and sent them to the cloud. After that, data were analyzed, and results were updated on the website and mobile application. Moreover, an IoT based stroke rehabilitation system which contained a tiny-sized and low power IoT sensing device within a wearable armband was demonstrated [112]. The device measured, analyzed, and transmitted biopotential signals wirelessly to a robot hand created by a 3D printing machine. After that, a machine learning algorithm was implemented to interpret the signals and gave users the feedback of their muscle movements, whereas the robot hand assisted patients in adjusting their posture and walking pattern in real time.

4.2.9. Wheelchair Management

A wheelchair plays a crucial role in supporting disabled people not only physically but also psychologically. The electric wheelchair has been invented and implemented to make it easier for people with disabilities to become more independent in their daily activities rather than always depend on other people. However, it failed to support disabled people whose mobility was restricted because of brain damage. As a result, an intelligent wheelchair with a smarter and easier navigation system has been discussed recently. One example of wheelchair management is the creation of an IoT based steering system and a real-time obstacle avoidance method for a smart wheelchair [110]. The steering system was formed by recording real-time video, and image processing techniques were applied to examine the video to detect obstacles. Furthermore, the m-health concept was applied in a smart wheelchair development by using various sensors (infrared sensor and sensors from wearable devices) and cloud computing technology [109]. The system included software allowing the disabled to interact with the wheelchair easily through a mobile app that analyzed data from sensors, and then it visualized results for caregivers to monitor the disabled from a distance.

4.2.10. Medication Adherence

Medication non-adherence is arising at epidemic proportions causing progressive disease, complications, and even premature death. One of the most common motivations for intentional non-adherence is the price of drugs. Some people do not strictly abide by prescriptions from doctors, skip or take doses less regularly. Thus, in the context of IoT development in healthcare, active research is focusing on tracking patient's compliance to medication, as well as reducing the time a patient has to come to a hospital to take a prescription. An innovative medicine box to manage adherence to medication was demonstrated [122]. The system contained several sensors such as a glucometer, blood pressure, body temperature, and ECG connected to a Raspberry Pi 3 controller. All raw data were then transferred to the cloud for analyzing. The box contained three trays, and each tray carried drugs for a specific time of the day. Tray 1 contained the morning dose, tray two was used for the afternoon, and tray 3 was applied for the evening. Authors also developed an Android application to support the communication between a patient and the responsible doctor. Moreover, a smart medication compliance management system that used fuzzy logic to evaluate raw data gathered from temperature sensors [123]. The prototype provided a robust medication management system that treated the fever by constantly monitoring a patient's core body temperature in real time to automatically adjust doses and time between doses.

4.2.11. Drug Management

Drug management is an important area in the healthcare industry in which IoT technology is creating a positive impact by effectively solving high-cost problems in developing new drugs as well as storage and preservation of drugs. As a result, a growing list of startup companies and researchers are actively working in this field. Radio-frequency identification and IoT [124] were combined to manage the medicines in an intelligent drug store system. It included three main sections. In the first section, the authors showed how they set up the sensors, and an RFID device to efficiently sense the environment parameters. The second section described the flow of data and communication protocol from sensors to a Raspberry PI device. Finally, the third section defined all users' role for data accessing. On the other hand, an abstract system to solve sensitive temperature monitoring for drug storage by applying both RFID tags and sensors to adjust a suitable temperature for each type of drug accordingly in [125].

4.2.12. Smart Phone Solutions

The rapid development of mobile computing, which includes a variety of compact devices such as smartphones, tablets, and personal digital assistants (PDA), has significantly affected many domains, including healthcare. Until recently, doctors only used smartphone or tablets for tasks for which they needed complicated procedures to accomplish. Nowadays, smartphones include both communication and computing features in a small handheld device, which is accessible at any time. Besides plain text and voice features, the mobile device has become smarter and offered more cutting-edge technologies including video telephony, multimedia messaging service, web browsing, video recording, camera, an overwhelming volume of apps. Mobile devices have essentially become a handheld computer because they have advanced single-chip systems (SoC), larger RAM size, highly customized mobile operating system, large storage, larger screen size, and higher display resolution.

Clinical end-user programs or “apps have partly propelled widespread adoption of IoT in clinical practice”. Each app is specially programmed to serve a particular purpose. The emergence of IoT in healthcare has led to the release of many clinical apps for both professional and personal purposes. A systematic review on mobile healthcare application by categorizing each application to a particular class such as BG measurement, vital sign monitoring, and m-health applications by the authors in [126]. They also showed critical challenges and issues facing smartphone healthcare applications.

There are a huge number of apps available on IOS and Android app stores, and not all of them are useful. Thus, we apply some criteria to select appropriate apps in each category. The chart is used to search for the best apps in each category, and then we further filter out apps which have under three star reviews. Finally, by checking each app features, we decide which category the app should be put on. However, the method mentioned is limited by regional apps since each region will have its popular apps for each category. Thus, we also add more apps based on reviews from famous and trusted review articles by searching specific keywords such as “top apps for ...”, “best apps for ...”. Table 8 is generated to summarize and categorize outstanding healthcare apps. However, Table 8 only shows healthcare apps that are designed to be used by physicians, whereas apps which are created for patients and users will be introduced later in this section. There are five main categories in Table 8. Diagnostic apps are used to match patients' symptoms with an extensive medical database of symptoms so that they can recommend the most suitable remedy. Drug reference applications generally contain a full list of drug names, their descriptions, side effects, interactions, dosages, and characteristics. Education apps contain detailed instructions on drugs, video tutorials on various procedures and educational activities for medical students. Medical news apps refer to applications that provide the latest medical news worldwide. Telemedicine apps allow patients to receive remote healthcare services from doctors via phone or video without coming to hospital or clinic. Calculator applications provide various equations and formulas. Moreover, they support the calculation of frequently used parameters. Lastly, clinical communication applications provide a simple and effective communication interface between physicians.

In the previous section, we discussed healthcare apps for physicians. Next, in this section, Table 9 lists and categorizes widely used smartphone-based healthcare apps for end-to-end users with some information for each category (common apps and a short description of each category). Although apps are developed by developers worldwide, in a specific region, some apps are more popular than others; Table 9 shows numerous representative apps based on category, number of users, and the benefits they provide. Many other apps similar to those listed here can be found on the internet by interested readers.

Table 8. Classification of healthcare apps for academic purpose by category and a description for each category.

Category			Description
Diagnosis	PEPID, UpToDate, Prognosis Your Diagnosis, Diagnosis Medical App, Quick Medical Diagnosis & Treatment, InSimu Patient-Diagnose Virtual Clinical Cases, Ada-Your Health Guide, Doctor Diagnose Symptoms Check, Cardiac diagnosis, Eye Diagnosis, Self Diagnosis, VisualDx.	PPEPID, UpToDate, Prognosis Your Diagnosis, Heart Rate Plus Pulse Monitor, Differential Diagnosis Guide, 5 Minutes Clinical Consult, Ear Age Diagnosis, Emergency Central, Dem DX Diagnostic Reasoning, Diagnosaurus DDx, mRay.	Evidence-based clinical and drug information resources for point-of-care decision making.
Drug references	Epocrates, Drugs.com Medication Guide, KnowDrugs Drug Checking, Drug Dictionary Offline, Drug INFO, Drugs Classifications.	Epocrates, Drugs.com Medication Guide, Medicine Dictionary, Davis’s Drug Guide.	Mobile medical reference applications, look up drug information, identify pills.
Education	Medscape, Muscle Trigger Point, Visual DX, PEPID.	Medscape, 3D4Medical, Muscle Trigger Point, Visual DX, PEPID.	Show practical clinical sources, including detailed guidelines on drugs, videos tutorials, and educational exercises for students.
Medical news	MedPage, Medscape, Newsfusion, Internal Medicine News.	MedPage, Medscape, Newsfusion, Internal Medicine News, NEJM This Week.	health apps support the flow of information in the health industry, becoming a new digital tool to help complement traditional searches for health news.
Telemedicine	MDLIVE, LiveHealth Online Mobile, Express Care Virtual, Amwell, Lemonaid, I Online Doctor, Ask a Doctor, Doctor’s Circle, My Live Doctors, JustDoc Online Doctor, Carrydoctor, Personal Doctor, Halodoc, MySwaath-Doctor consultation, doctor appointment.	MDLIVE, LiveHealth Online Mobile, Express Care Virtual, Amwell, First Opinion, Doctor Pocket, Ask a Doctor, iCliniq, Ask Apollo, DocOnline, Continuous Care Health, JustAnswer, OkaDoc.	These applications make connecting with a doctor fast, easy, and convenient from anywhere at any time.
Medical calculator	MDCalc Medical Calculator, Medical Calculators, Calculate by QxMD, Caddy, MedicALC, Medical Formulas, Mediquestions Medical Calculator, IV Infusion Calculator, eGFR Calculators.	MDCalc Medical Calculator, Calculate by QxMD, MedicALC, Mediquestions Medical Calculator, IV Infusion Calculator.	Receive reliable clinical solutions fast and smoothly with fundamental input values.

Table 9. Classification of healthcare apps for normal purpose by category and a description for each category.

Category	Common Apps	Description
Workout	Fitbit, Freeletics, Sworkit, Nike+ Training Club, Daily Burn	<ul style="list-style-type: none"> • Keep a record of daily activities including steps, distance, calories burned and active minutes. • Monitor users daily activity using sensors from the smartphone. • Integrate AI model that analyze the collected data and give a suitable exercise during the training session. • Provides social network functionality to encourage people to achieve their goal.
Diet and nutrition	MyFitnessPal, FatSecret, YAZIO, Lose It!, MyPlate Calorie Tracker	<ul style="list-style-type: none"> • Support a huge database of food and nutrition. • Image recognition technology is usually used to recognize food automatically. • Apply AI to creates meal plans by monitoring calorie intake and daily step taken from embedded sensors from the smartphone.
Mental health	Calm, Headspace, Moodnotes, Moodpath, Pacifica	<ul style="list-style-type: none"> • The app can record users' emotions through the heart rate sensor and boost their mental state through the implementation of cognitive behavioural therapy. • Offer an AI pocket-sized mental balance chatbot which guides users through their hard times. • The AI is trained on the gathered data and automatically recommends relaxation exercises such as music, breathing, and relaxing sound.
Medical records	Medical records, Patient Medical Records & Appointments for Doctors, FollowMyHealth	<ul style="list-style-type: none"> • Logs appointments, keep medication records, communicate with healthcare providers, and more. • Offers data synchronizes to the cloud for safe storage. • Offers 24/7 access to users medical information and healthcare records anywhere.

Recently, healthcare is leading to development in the smartwatches that can be paired with smartphones to aid individuals in setting their exercise goal, keep track of their performance, and also monitor vital body signs. Currently, two big brands in the smartwatch market are Apple and Fitbit. Both of them have clear objectives to focus on the healthcare industry. Apple's wearable smartwatch includes various sensors that can notify users of abnormal heart rhythm. On the other hand, Fitbit is conducting clinical trials to get regulatory approval of its wearable devices used in assessing health statuses such as sleep disorder and abnormal heart rhythm. Thus, Apple and Fitbit both want to be the leader in the smart wearables industry by keeping upgrading their smart devices. The following section provides a more detailed discussion on current healthcare products on the market.

5. Latest Industry Trends in IoT and Cloud Computing in Healthcare

The rapid growth of IoT and cloud computing technologies and the increasing number of IoT and cloud computing based applications in healthcare have drawn much interest from researchers, healthcare stakeholders, and business owners. It can be noted that a large number of startup companies and corporations are actively contributing to the sustainable development of IoT and cloud computing in healthcare market by introducing new technologies as well as applying the technologies in prototypes and products.

We classify the IoT and cloud computing in the healthcare industry market into three main groups, including components, applications, and end-user. For the component category, the market is divided

into hardware, software, and services, whereas, in the application category, each healthcare application is grouped into either clinical operation, patient monitoring, drug development, or fitness. The market is divided into the end-user category by practitioners, patients, payers, laboratories, and governments.

Figure 10 shows the latest industry development in IoT and cloud computing that improve the healthcare services.

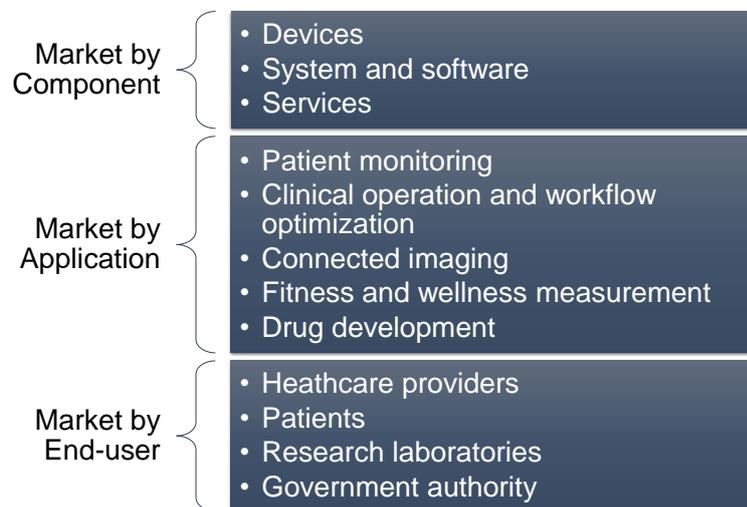


Figure 10. Latest industry trends by component, application and end-user which support the development of IoT and cloud computing in healthcare.

5.1. By Component

5.1.1. Hardware

Recently, the smartwatch has emerged as an essential wearable device which offered many disruptive technologies that have expanded the appeal of wearable devices. It had two remarkable functions, including fall detection and heart monitoring [127]. The watch automatically detects both backward and forward falls, and if the person lays immobile for a while, an emergency SOS call can be made. Furthermore, it can take an electrocardiogram, which enables users to monitor their heart for anomalies and test for atrial fibrillation, and can even export a PDF report and send to the physician. The headband is another example of wearable devices that has the potential to treat mental health. It delivers low energy waveforms to cautiously and pleasantly trigger nerves located on the user's head and face, allowing the body to relax or energize [128]. It can also be used to treat depression at home [129]. Through the gadget, doctors can review the treatment process and adjust the treatment process accordingly. Another application of a headband wearable is a neurotechnology pain relief gadget [130] that transmits neural pulses to the brain to alleviate chronic pain by stimulating the body's natural pain relievers. Because each person has a distinctive pain, based on a huge data collection, the AI model can provide customized treatments that are appropriate for each user. In recent years, wearable glasses were also been used to offer medical practitioners a remote service; they can use the devices during patient visits, and the recording data are transmitted to a remote server for storage and analytics [131]. Many wearable devices can be used on other parts of the body, such as the wearable body [132], which provide gentle vibrational reminders for posture whenever the user slouches. Track user posture hours, steps taken, distance travelled and calories burned by using the angle displacement, and the patented biomechanics monitoring sensors. Another kind of wearable device is the one that wraps around the ankle [133]. The sensors on the wearable can determine if the user is asleep or awake. By utilizing machine learning, it provides real-time insights into user sleep patterns.

Sensors have already been embedded in some gadgets which can measure gluten at home to prevent food allergies, gluten sensitivity and celiac disease [134], the sensor integrated into the gadget uses antibody-based chemistry to examine food samples to find specific proteins. Recently, a sleep tracking device [135], which integrates a sensor based on a technology called ballistocardiography (BCG) that monitors ballistic forces on the heart and the flow of blood, has also been introduced. Moreover, a smart thermometer integrated with a temperature sensor has also been developed. It records temperature continuously and notifies parents if the temperature is too high or increasing too quickly. The device tracks the temperature in real time, so it helps the patients monitor the effects of their treatment. Another device [136] uses advanced sensor technology to examine user oral health and notifies users of harmful oral bacteria and gives the user an accurate reading in a matter of seconds. The scores are compiled for the app to visualize how changes in the user's daily routine affect oral health.

In the last decade, flexible robotics device which is equipped with cameras and tools to manoeuvre into a patient's airways, into the far and narrow reaches of their lungs, giving doctors a direct view of what is inside. The system also provides computer-assisted visualization to doctors. Thus, it can guide doctors to a particular part of the lung that they need to evaluate. Health centres such as hospitals and clinics directly benefit from new technologies originated from integrating IoT into healthcare. In recent years, medical devices have gotten cheaper and smarter, and can they can speak to each other as the combination of IoT and healthcare is bringing a better experience for the patients as well as reducing the burdens for doctors [137]. Some other robots have also been developed to support nurses by doing administrative tasks [138], including automatically managing supply rooms and preparing medical equipment. The robot navigates the world using cameras and lidar, which is a remote sensing technology that measures distance using lasers. It features LED "eyes" and two arms capable of picking up light equipment. When a nurse addresses it, the robot moves its head in their direction and displays heart and rainbow symbols to convey pleasure. They can also autonomously deliver food and drugs and reduce time-consuming and mundane tasks for nurses [139]. Based on reflecting lasers around, the robot constructs a comprehensive map in 3D as an addition to the traditional map of the hospital and stores the 3D map in its memory. The robot moves around the hospital by starting at a single position and positions its location using geometry as it moves through the passageway or gets on an elevator.

5.1.2. Software

Regarding the software market, four major healthcare software topics that will become hot trends in the following years are shown below:

- **Multispeciality electronic health record (EHR) solutions** A multispecialty EHR brings many advantages for speciality practices expanding across many domains. It boosts the consistency and stops a patchwork approach when different EHR systems are integrated. The solution greatly reduces the extra time and cost of concatenating various groups of specialists. The multispeciality EHR solution in healthcare organizations brings higher efficiency in managing patient health record and serves various clinical requirements.
- **Patient portal and self-service software** Thanks to the integration of IoT and cloud computing in healthcare, patient portals are becoming the mainstream in the healthcare software market. It allows patients to interact and communicate online with responsible physicians, and the patient's medical records are available on the internet and can be accessed at any time. Besides the patient portal, self-service software is becoming smarter, easier to use, which will eventually bring tremendous benefits to patients. Patient Kiosk software is an interesting example of self-service software because it assists patients in the identification process, hospital registration, copay payment, and paperwork.
- **Blockchain solutions** The role of blockchain technology in healthcare is to provide a secure mechanism for storing and sharing of medical records on the blockchain; patients and medical

professionals have greater control over their information, and the sensitive data are securely protected from hackers. However, blockchain technology still needs more research and prototypes to achieve its full potential.

- **Enterprise software design** For years, physicians have been forced to use software that are confusing and uncomfortable. The biggest issue that leads to poor software design is the purchasing process of the enterprise. The lack of communication and market research in the developing process between developers and users.

Nevertheless, in 2019, products which bring better user experience at a lower price are expected to increase significantly. Healthcare administration systems are going to rely more on AI to enhance the overall performance of the system.

5.2. By Application

5.2.1. Patient Monitoring

In recent years, IoT and cloud computing technology have shown a crucial role in remote patient monitoring applications because the connected devices let healthcare providers and physicians observe patients remotely. This trend leads to fewer admissions to the hospital, more comfortable services, and operation cost reduction.

The main element of patient monitoring is various types of sensors and wearable devices. They assist healthcare professionals in observing and diagnosing patients vitals and symptoms without demanding them to show up at the doctor's office physically. By setting up appropriate components in the patient monitoring framework, it will become an early warning system for potential medical symptoms that could be life-threatening to the patient if left uncured. A smart contract based on the blockchain to manage sensors securely was implemented [90]. The proposed system used a blockchain based on the Ethereum protocol, and sensors in the blockchain interacted with smart contracts, then all events that happened on the blockchain were recorded. The framework allowed medical interventions and patient monitoring by informing and practitioners and patients in real time, whereas it also maintained all activities records securely. The adoption of blockchain in healthcare eliminated some security vulnerabilities in remote patient monitoring. In another research work, a fog layer is implemented at the gateway of a health monitoring framework because the system required accurate responding at a minimum delay [50]. They categorized the health condition into safe or unsafe in the fog layer. As a result, data processing and analyzing that are performed on the cloud were significantly reduced. In addition, the event triggering mechanism was deployed to automatically sent patients' vital signal to the cloud layer when patient health condition changed from safe to unsafe.

5.2.2. Telemedicine

An increasing requirement from a new generation of the tech-savvy population has pushed for rapid adoption of telemedicine because of its convenience, time-saving and intelligent features.

Telemedicine enables the remote delivery of healthcare service so patients can be treated remotely using telecommunications technology. The breakthrough in technology and healthcare innovation has substantially improved its usability and making it a crucial part of remote patient monitoring. Recently, thanks to the development of IoT and cloud computing, telemedicine technology will see even more enhancements that support the communication between doctors and patients across space and time. A good architecture for IoT and fog computing based telemedicine was introduced by [140]. They increased the communication link security and provided a reliable user authentication and privacy management mechanism. On the other hand, a new user-friendly graphical user interface (GUI) application that supported the health data visualization and can be applied in patients' remote monitoring [141].

5.2.3. Pharmaceutical Supply Chain Management

The increasing use of IoT connected devices for communication, tracking, and management of the pharmaceutical supply chain are improving the existing in-transit medication management. Advanced medication management brings many benefits to consumers and the pharmaceutical industry. Another benefit of applying IoT technology in the supply chain is that inventory is pulled by demand from the outlets instead of being pushed by the factory, which makes the supply chain more efficient. The evolution of IoT technologies, especially sensors, has boosted the sensor accuracy, power efficiency, and cost-effectiveness. As a result, more environment variables in the supply chain can be calculated accurately at little cost.

5.3. By Technology

5.3.1. Bluetooth

The spread of smart sensors, hand-held devices, and wearable devices requires a new wireless communication technology that is more efficient and consumes less power. As a result, In December 2016, the Bluetooth special interest group (SIG), the group which owns the Bluetooth standard, announced Bluetooth version 5.0. Bluetooth 5 offers the flexibility to make IoT solutions better because of twice the speed, four-fold improvement in range, and eight-fold better data capacity compared to the original Bluetooth. All the improvements and features of Bluetooth low energy focused on supporting applications where energy usage is critical, and data are sent irregularly. For example, a system that supported Bluetooth low energy (BLE) technology was proposed [142]; it guaranteed easy communication between IoT devices in a healthcare network where the gateway uses BLE technology. The system had an analysis module for the extraction of the variables needed during the data transmission. In addition, they also implemented a gateway selection technique that transferred connection detail to an optimum list of gateways, so the system reduced the overall communication latency.

5.3.2. Light Fidelity (LIFI)

A new wireless communication technology called LIFI was invented by Harald Haas [143]—a German scientist; it is wireless and supports communication through visible light instead of the radio wave. Some of the advantages of LIFI include high bandwidth, higher transmission rate, and it can operate in areas that are vulnerable to radio-frequency interference, such as aeroplanes or hospitals. Other potential areas that can exploit LIFI are petrochemical factories, power plants, and areas where a normal wireless communication method cannot work. The light direction can be easily redirected in the other direction, and it is also simple to confront interference problems in the LIFI network. Recently, a comprehensive survey on how the LIFI technology was used in previous projects and research was conducted, and the author also listed several LIFI products that were produced by leading companies and manufacturers in wireless communication technology [144]. Finally, they also proposed an IoT system that uses LIFI as a wireless communication technique.

5.3.3. Near Field Communications (NFC)

NFC is widely used for very short-range wireless communication, and it is similar to the infamous RFID technology. The limited range (a few inches) is applied for applications that require unique communication; the two devices that use NFC have to come very close to each other to trigger a transaction. It has become a crucial technology for specific human interaction transactions in the IoT network. It can be applied to send data between devices or to quickly establish a connection to other wireless communication technologies such as Wi-Fi handover or Bluetooth pairing. For example, an application of NFC technology in an intensive care unit was presented [145]; the framework was comfortable, required low setup cost, and increased the safety of the patient with the reduction of adverse events.

6. Security

6.1. Security Characteristics

- **Authentication** Authentication in the IoT network is complicated because it demands heterogeneous network authentication. Computing devices have to be recognized and validated in advance of entering the network. For the IoT network, each device has a unique identification key or a global unique identifier (UID).
- **Confidentiality** Confidentiality makes sure that medical information such as patient health record is protected from unauthorized users. In addition, all the confidential data must be stored safely and not be disclosed to unauthenticated identities.
- **Self-Healing** In case a node in an IoT network runs out of power and is broken, the remaining nodes must deliver the least security level.
- **Fault tolerance** If a crash happens in the network (e.g., a device failure, a software error), the system still can operate and support many security protocols.
- **Resilience** In case one or several points in the IoT network is damaged, the system prevents incoming attacks.
- **Data freshness** In a system that manages remote patient monitoring, the system has to use the latest data or information. Take an analytic of the heart functioning as an example; the system demands the most recent ECG information so it can provide the most accurate diagnostic.
- **Liability** For a healthcare system if any unexpected incident occurs, the system should be able to identify who will take responsibility.
- **Trust** In an IoT network, users or patients need to be assured that their private data will not be misused.

6.2. Security Challenges

- **Memory constraints** The memory of IoT devices is small, and most of the device's memory is used to store an embedded operating system. As a result, the system that uses IoT computing devices has limited memory to perform complex security protocols.
- **Speed of computation** Almost all IoT computing devices have low-power processors; the processor needs to perform multiple tasks including managing, sensing, analyzing, saving, and communicating with a limited power source. Therefore, force the processor to do the security procedure is a challenging issue.
- **Power consumption** Most IoT devices have low battery capacity. As a result, there is a mechanism that forces them to automatically enter the power saving mode to save power at sensors' idle time. Thus, it is difficult for IoT devices to perform security protocols all the time.
- **Scalability** There is a sharp rise in the number of computing devices in the IoT network. Thus, it is challenging to find the most suitable security algorithm for the growing number of devices in the IoT in the healthcare network.
- **Communication channel** IoT computing devices mostly participated in the network through multiple wireless communication protocols. As a result, it is challenging to find a standard security protocol that is suitable for various wireless communication protocols.
- **Security updates** The security framework needs to be updated frequently to minimize potential security breaches. However, automatic updates will also consume enormous power.

6.3. Threats and Attacks

Possible threats, vulnerabilities, and attacks aiming at the IoT are divided into three major groups by determining what the main target of the attack is.

6.3.1. Attack on Device (Type 1)

Thanks to the development of IoT, medical devices are becoming more efficient, cheaper, and smarter. However, they likely become a potential target because they are continually collecting data about their users so that hackers can exploit more valuable data. An attack in a medical device can lead to an unexpected functional failure or affects other medical devices in the same network, which can affect patient health. In the worst scenarios, it can even lead to human casualties. For example, a compromised closed-circuit television (CCTV) allows hackers to spy on a location without them knowing continuously. Although medical devices have to remain accurate all the time, hackers can attack one target to exploit confidential data, and the attack could lead to complete grid failure.

6.3.2. Attack on Communication Channel (Type 2)

Attackers can also intervene with the communication between medical devices by observing or revising messages. Because the nature of transmitted data is sensitive and confidential, consequences from an attack on communication protocol are particularly severe, as information could be intercepted, captured, and manipulated while being sent. These potential threats can endanger the faith in data and messages being sent and faith in the entire system.

6.3.3. Attack on Manufacturers and Cloud Providers (Type 3)

Hackers can also aim at IoT service providers, cloud service providers, and device manufacturers because the attack will cause critical loss to these parties. They are trusted to collect and handle a large amount of highly sensitive and confidential data; this data is also invaluable to IoT providers because, based on analyzing data, providers can come up with appropriate strategies, and figure out the future direction. Moreover, disrupting services also pose a massive threat as internal networks need to be in service all the time to serve the communication between devices. For example, an attack in a server that is responsible for releasing update patches could distribute malicious programs into all other devices.

Table 10 describes possible attacks on an IoT network and to which group it belongs. Moreover, we also add some references for each attack.

6.4. Security Model

Although IoT and cloud computing in healthcare systems are being developed and deployed continuously, they are not yet fully integrated. Hence, it will be challenging to prepare a security paradigm that prevents all potential flaws, threats, and attacks that can occur in IoT in the healthcare models. At any cost, security experts have to ensure that a proposed security solution for IoT and cloud computing in the healthcare system can cope with problems that can potentially occur during the system operations. Nevertheless, if a security scheme is proposed to deal with an anticipated event, the security experts must ensure that it can solve or at least mitigate that issue to reduce the damage it may cause to the entire system. To accomplish the previous description of an ideal security scheme, it should have a dynamic range of properties to cover as many unnoticed problems as possible. Suppose that we have an IoT in a smart grid where sensor nodes are connected; it also supports a security model that can identify and confront attacks on node integrity. Nevertheless, too many sensor nodes added to a network will make the system more vulnerable to any new types of attacks that can threaten the entire network integrity. Hence, the security model is used to be supposed to localize, eliminate or at least contain those attacks.

Table 10. Different types of attacks on an IoT for healthcare systems.

Type	Attacks	Description	Reference
1	Side-channel attack	Any attack that exploits information leaked from the deployment of a system. Power consumption, electromagnetic leaks, timing information, and even sound can reveal valuable information for hackers to attack the system.	[146,147]
2	Sniffing	Hackers take advantage of unsecured network communications to intercept data sent on a network. For network administrators, sniffers are very hard to identify since they do not intervene in the network traffic.	[2,148]
2	Radio frequency jamming	Attackers carry out this attack by intentionally jamming a target radio signal through the transmission of one or many radio signals that have similar frequency range.	[149,150]
3	Message Injection	It is a potential security vulnerability which happens when attackers attack or disrupt a network by deliberately injecting wrong messages.	[151]
2	Message Replication	Attackers conduct this attack by intercepting packets being transmitted on a network, replicating and forwarding them to other nodes on the network.	[152]
1	Node Destruction	When an IoT in healthcare network is under a node-destruction attack, attackers will try to reprogram or destroy as many nodes in the network as possible in order to cause the complete network failure.	[153]
3	Denial of service	A Denial-of-Service attack's main goal is to damage the network connection, which makes it unavailable to users. Attackers carried out this attack by sending a large request at the same time to the target network to flood its traffic or prevent sensors from entering idle state, so they run out of battery power quickly. This attack is easy and cheap to implement and cause serious problem to a sensor network.	[154,155]
1	Hello Flooding	Attackers use some devices and deceive the target sensors network that these devices are genuine, then through these fake nodes; attackers flood the network with several hello requests and break the security link between legitimate nodes in the target sensors network.	[156,157]
1	Black Hole Attack	During the pathfinding process, a malicious node under attackers control advertises an invalid path as a good path to the source node. When the source follows the path, including the attacker node, the traffic travels through the adversary node, and this node begins to drop the packets selectively or entirely.	[158,159]
1	Gray Hole Attack	This attack is a variant of the black hole attack; in grey hole attack, only one or two nodes in the network are affected whereas the whole network is affected in black hole attack.	[160,161]
1	Wormhole Attack	Different from the black hole attack, a routing protocol is the main target of wormhole attack in which a packet or individual bits of a packet is captured at one location, transfer to another location and then replayed at another location.	[162,163]
1	Sinkhole Attack	In this attack, a region of nodes will forward packets destined for a base station through an adversary node where attackers can capture all data. The malicious node can fool the network because it provides the fastest path to the base station.	[164]
1	Sybil Attack	Attackers take multiple fake identities and use the identities of the other nodes in order to take part in distributed algorithms such as the routing table. These fake identities are known as Sybil nodes.	[165,166]

As a result, by reviewing several studies on healthcare security model [2,10,167], Figure 11 is created to show the security trend for healthcare applications. In the security model, security specialists first analyze a healthcare framework to make a list of all known and unknown threats, vulnerabilities, and attacks that may occur when the framework operates. After that, an AI model is trained by adjusting a range of properties so it can eliminate or at least automatically find an appropriate approach to minimize the damage caused to the IoT and cloud computing in healthcare framework.

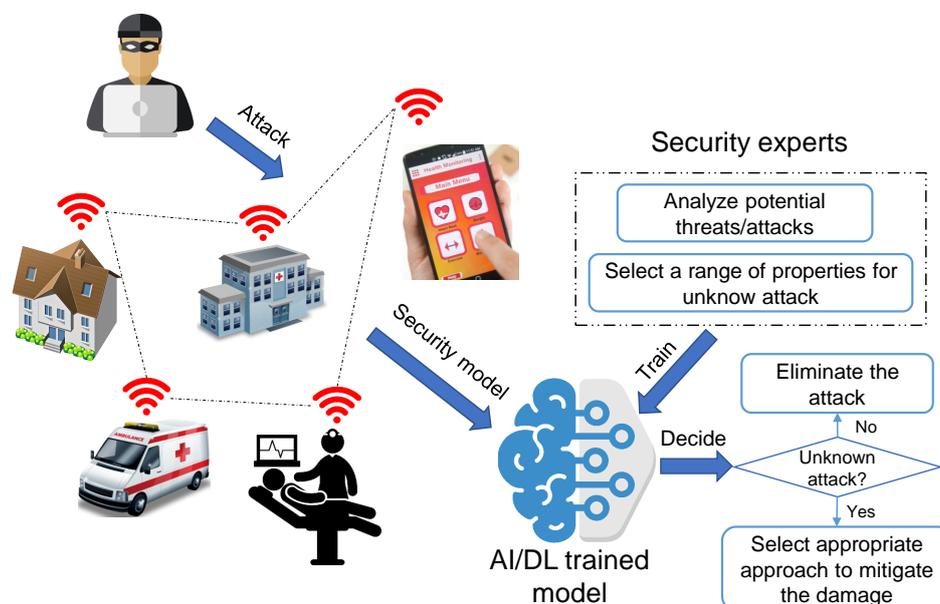


Figure 11. Smart security model for IoT in healthcare frameworks.

7. IoT and Cloud Computing in Healthcare Policies

Policies and development plans set by countries around the world are a vital element that drives the development of IoT and cloud computing. Although IoT and cloud computing-based healthcare applications have not been mentioned in existing policies, healthcare is likely the biggest winner from IoT and cloud computing development policy initiatives across the world. This section briefly discusses ongoing policies and plans on integrating IoT and cloud computing in healthcare from countries and international organisations across the world.

7.1. US

In 2017, the Department of Commerce published a paper [168] to find essential elements to cultivate the development of IoT and cloud computing and technologies surrounding it. Moreover, policies strategies to solve several security issues in the future were also discussed. U.S Department of defence issued a “Cloud computing security requirement guide” [169] to leverage cloud computing along with the security controls and requirements necessary for using cloud-based solutions. There is a section to show requirements for cloud-based healthcare applications.

At the beginning of 2018, a group of researchers [170] found that information regarding the locations and precise movements of army personnel using fitness trackers can be easily exploited. Later that year, the same privacy incident [171] happened on Polar—a popular fitness app as positions of the army personnel all over the world were exposed. As a result, the U.S. federal government has given more consideration on adjusting policies regarding the privacy issue of IoT devices. Thus, the U.S. Department of Defense declared a policy [172] to prohibit all Defense Department personnel from using geo-locatable features of digital devices and services while they are in secret locations.

7.2. China

China's authority is pursuing policies and strategies that boost the adoption of IoT and cloud computing in every aspect of life, including healthcare. Among them, 'Made in China 2025' strategy [173] is remarkable because its primary purpose is to improve technologies that support manufacturing, including IoT and cloud computing so China can be acknowledged as "a manufacturing super house" in the next decade. More recently, in 2018, China's National Health Commission released a Healthcare IoT and cloud computing white paper and eight new healthcare IoT standards [174] to promote the strategic plan for the integration of IoT and cloud computing in healthcare and attract investments. In China, IoT is considered a crucial strategic element to improve productivity and innovate existing technologies. China authority shows its interest in IoT technology by hosting the annual Inter-Ministerial Joint Conference [175]; the most recent conference addresses a detailed IoT development plan and discusses the fund used for IoT sustainable development.

7.3. Japan

Japan has been applying IoT and cloud computing in industry policies through the I-Japa strategy [176], which shows the government IoT development strategies for particular areas such as healthcare, education, and electronic government. The I-Japan also describes urgent issues that need to be solved to completely integrate IoT and cloud computing in every area. Moreover, the Japan government also released the smart Japan ICT strategy [177], which shows Japan vision in promoting cost savings and improved clinical outcomes through IoT and cloud computing. In August 2016, the Japanese National Center of Incident Readiness and Strategy for Cybersecurity (NISC) released a document called the General Framework for Secured IoT Systems [178]. The framework suggests that Japan will start seeking security even in noncritical infrastructure, including manufacturing, and pursuing a global multi-stakeholder approach to security in IoT. The framework is a follow up to Japan's Cybersecurity Strategy, which acknowledged the importance of sustainable economic development by IoT innovation and security for the first time as a Japanese national strategy. The strategy was released after Tokyo was selected to host the Summer Olympic Games in 2020 (Tokyo 2020) to show what Japan needs to do over the next three years to make Tokyo 2020 successful.

7.4. South Korea

South Korean government is planning to establish fourth industrial revolution infrastructure, abolish unnecessary regulations, assist in the growth of software firms and prevent adverse effects related to ICT [179]. The government's plans also include public data opening, development of integrated ICT services such as smart home and precision medicine, and establishment of infrastructure for 5G mobile communications, cloud computing and IoT networks. The government is planning to complete the establishment of dedicated IoT networks before the end of this year, launched commercial 10 Gbps Internet services in 2018, and launch 5G mobile services in 2019. According to the government, these measures for software-ICT combination are expected to create approximately 260,000 new jobs in the private sector. The government and the ministry also said that they would work on a platform for automobile-ICT combination as well so that smart car and self-driving car development can be accelerated and near-self-driving cars can be put to commercial use in 2020.

7.5. India

The Indian Authority is planning to build 100 smart cities [180], which could become a firm foundation for the fast development of IoT and cloud computing in India. Moreover, India implemented a Digital India Program of the Government [181], the main purpose of which is to turn India into a digital empowered society and knowledge economy which will also trigger the spread of IoT and cloud computing in every part of the country.

7.6. Russia

According to the analytical report by International Data Corporation (IDC) [182], the average annual market growth rate until 2020 will amount to 21.3%. By 2020, investment in the Russian IoT market will amount more than \$4 billion, and the market by that time will amount \$9 billion. The leaders of growth will become smart manufacturing, smart grid, smart agriculture and self-driving cars. The government has established a new standardisation [183] which will begin working towards establishing a single, open standard of data exchange for a network of connected devices, something which does not yet exist on the market.

7.7. Denmark

The Danish parliament approves a 'Digital Growth Strategy' in January 2018 [184], which includes 38 solid schemes that fortify and boost Denmark's position as an appealing country for investment to get full profits of new technologies such as IoT, cloud computing, big data, and artificial intelligence.

7.8. EU

In March 2015, the Alliance for the IoT Innovation [185] was launched by the European Commission to promote the creation of an innovative and industry-driven European Internet of Things ecosystem. It indicates the European Commission's intention to cooperate with all IoT stakeholders and actors towards the foundation of a competitive European IoT market and the creation of new business models. Today, the Alliance for IoT Innovation is the largest European IoT Association. In May 2015, the Digital Single Market Strategy [186] was approved, which involves factors that can drive Europe a step further in accelerating developments in IoT and cloud computing. In particular, the strategy emphasises the need to avoid fragmentation and to foster interoperability for IoT and cloud computing to reach its full potential.

8. IoT and Cloud Computing in Healthcare Challenges and Open Issues

IoT and cloud computing have been integrated into the healthcare which leads to changes in many aspects of the health industry. For instance, connected medical devices let the senior safely take care of themselves and reduce the burden for nursing homes. Moreover, IoT and cloud computing connect health professionals and specialists all over the world, and they can observe and consult patients remotely. Nevertheless, there are also several challenges that need to be addressed to integrate IoT and cloud computing in healthcare completely. The following subsections describe seven issues that prevent the development of IoT and cloud computing in healthcare; possible solutions for these issues are also discussed.

8.1. System Development Process

Accessibility and communication speed are two main points that encourage organisations and businesses to implement IoT and cloud computing in healthcare. However, research from Cisco [187] in 2017 unveiled that complete projects only occupied 26% of all the IoT and cloud computing in healthcare projects. On the other hand, 60% of projects faced difficulties at the proof-of-concept stage. By analysing all the projects, CISCO pointed out that forming partnerships with other partners was a significant point for a successful project. Companies have to be careful when they intend to implement IoT and cloud computing in healthcare projects. They might begin with small and specified projects that reflect patient needs or business objectives.

8.2. Resource Management

When three separate concepts (IoT, cloud computing and healthcare) are included in one system, the resources management process is the main concern [53]. For fog computing, the resource management process can be even more challenging due to the decrease in computing power and

available storage compared with cloud computing. When multiple IoT devices are included in the system and collected data are being transmitted and processed in the cloud computing layer, the systems must have the ability to reduce redundant data to prevent them from using all valuable resources. Another scenario that shows the importance of resource management in IoT and cloud computing for healthcare systems is that these systems usually involve a large number of users who share the same resources. Thus, resource management is critical to guarantee the smallest delay. As a result, when implementing an IoT and cloud computing in healthcare system, different factors that affect the resources allocation must be carefully analysed. Quality of service (QoS) is another important factor that is related to resource management because poor resource management will lead to bad QoS.

8.3. Interoperability, Standardisation and Regulatory Issues

In recent years, as the number of IoT devices rocketed, the standardisation concern has arisen. The standardisation issues are mentioned when IoT devices are applied to a broad range of disciplines that are controlled by different regulatory parties. In the case of IoT and cloud computing in healthcare, the complexity becomes more challenging due to the stringent regulations and medical standards. As a result, it is necessary that IoT devices manufacturers and different regulatory parties have to establish standard policies and rules to guarantee the standardisation.

8.4. Data Analysis

The growing number of sensors, smart devices and connected "things" indicate that a huge volume of data is being generated every day. Thus, it is challenging for IoT and cloud computing in healthcare systems to be able to analyse all of it and extract knowledge. There are three main challenges within the data analysis challenges, including data complexity and huge volumes of data.

8.4.1. Huge Volumes of Data

In recent years, a huge volume of data collected from sensors and wearable devices have caused concern in computing resources and the time-intensive process to analyse all of the data. Thus, it is essential for organisations to apply recently emerged technologies such as fog computing and big data to keep up with this massive influx of data.

8.4.2. Data Complexity

The complex nature of data collected from wearable devices and sensors is another difficulty. The complexity increases when the rate of data generated is rising. The implemented system must prepare for the data complexity challenge by focusing more on fog computing layers to increase the computing power, and leveraging the resources with efficient data preprocessing and data analysis algorithms.

8.5. Security and Privacy

Better processing power and availability of IoT devices and fog computing nodes in healthcare systems make them become more valuable targets of attackers. The development of these technologies also leads to the sharp rise of cyber attacks so that hackers can exploit a system and aim for the most precious data. The information the hackers gain from attacking IoT medical devices or fog computing nodes helps them successfully infiltrate the hospital network or making devices malfunction and affect patient care. However, a collaboration between providers, vendors and security experts can prevent cyber attacks by reinforcing standards and normalising secure protocols. Thus, facilities that want to utilise IoT and cloud computing in healthcare must be fully aware of existing vulnerabilities and threats and design a security model to protect networks and gadgets from potential cyber attacks.

The security and privacy issues have to be solved by considering the multi-layer structure as presented below:

8.5.1. Device Layer

A few examples of devices from the healthcare system are medical devices, connected sensors, fog nodes, gateways, and mobile devices that collect, analyse and transmit the data to the cloud. In order to prevent attacks at the device layer, security measures such as identity authentication, authorisation management, whitelisting, application sandboxing, secure booting, protection of data during the collection and transmission, fault tolerance, password encryption, and secure pairing protocols must be evaluated and implemented. Moreover, the nature of IoT devices (memory, processing power, battery capacity, network range, embedded operating systems) should also be considered when security algorithms are conducted.

8.5.2. Network Layer

The network layer is in charge of establishing suitable communication techniques between sensors, smart devices, fog nodes and cloud computing that use several network protocols (such as Wi-Fi, Bluetooth, ZigBee). This layer is the target of attacks, including Man-in-the-Middle attack, eavesdropping, sinkhole attack, and Sybil attack. The network layer can be protected by applying secured routing mechanisms and message integrity verification techniques as well as point to point encryption techniques.

8.5.3. Cloud and Fog Layers

The cloud and fog layers provide computing power and storage for data collected by the device layer. This layer is frequently attacked by Structured Query Language (SQL)

Injection, Denial-of-service (DoS) attack, sniffing attack, malicious code injection, cross-site scripting (XSS), brute-force attack, phishing attack, trojan horses, and viruses. Both the cloud service providers and businesses that implement IoT and cloud computing in healthcare systems have to take adequate and efficient approaches to protect their system from potential attacks.

8.6. Business Model

Outdated infrastructure is a challenge when organisations want to integrate IoT and cloud computing in healthcare. When hospitals wish to improve the infrastructure, they have difficulties in preparing the fund and training the staff about the functioning and usage of various IoT devices. Organisations and businesses must have a detailed plan that covers upgrade cost and implementation specifications.

8.7. Transition Process

Healthcare administrations integrate IoT and cloud computing in existing healthcare systems by replacing or adding medical devices and sensors into the existing device network. However, devices from different vendors have entirely different communication protocols. As a result, it is a challenge to ensure a smooth transition of these new devices. Thus, it is compulsory that manufacturers and vendors follow the same standard to guarantee that their devices support backward compatibility when they are deployed on an existing network of devices.

9. Conclusions

Administration, organisations and research communities all over the world are closely cooperating to ensure a seamless transformation that IoT and cloud computing bring to the healthcare industry. This research is useful for readers who are interested in learning different aspects of IoT and cloud computing in the healthcare.

It offers a complete IoT and cloud computing framework for healthcare that supports applications in utilising the IoT and cloud computing backbone and provides a platform to facilitate the transmission of medical data between medical devices and remote servers or cloud computing platforms. During the

integration process of IoT and cloud computing in healthcare, many concepts and applications are continuously appended, so this survey also briefly categorises and summarises them. Then, we also do a comprehensive survey on cloud computing, particularly fog computing, including standard architectures and existing research on fog computing in healthcare applications. After that, we group existing research and development process in the healthcare industry by components, applications, and end-user, and then significant achievements that prove the effectiveness of integrating IoT and cloud computing in healthcare were described. The paper also considers various threats, vulnerabilities, and attacks that need to be considered, and analyse and summarise relevant security models to prevent possible security risks. Policies from governments across the world that motivate the development of IoT and cloud computing in healthcare are also mentioned. Finally, many challenges that prevent the development of IoT and cloud computing in healthcare, such as data security, system development processes, and business models, are shown.

Author Contributions: Introduction and IoT framework for healthcare sections, L.M.D. and M.J.P.; Healthcare concepts and applications L.M.D., M.J.P.; Security and challenges, L.M.D. and D.H.; writing—original draft preparation, L.M.D.; writing—review and editing D.H.; visualization, K.M.; supervision, H.M.

Acknowledgments: This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT)(2019-0-00136, Development of AI-Convergence Technologies for Smart City Industry Productivity Innovation).

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

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
6LoWPAN	IPv6 over low-power wireless personal area networks
AAL	Ambient assisted living
AES	Advanced encryption standard
AFE	Analog front-end
AI	Artificial intelligence
BCG	Ballistocardiography
BG	Blood glucose/blood sugar
BLE	Bluetooth low energy
BP	Blood pressure
CCTV	Closed-circuit television
CIoT	Cognitive IoT
CMRR	Common-mode rejection ratio
ECG	Electrocardiogram
EMG	Electromyography
EMR	Electronic medical record
GUI	Graphical user interface
HR	Heart rate
HTTP	Hypertext transfer protocol
IETF	Internet engineering task force
IoTHeF	IoT framework for healthcare
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
IR	Infrared
IT	Information technology
LIFI	Light fidelity
LPWAN	Low-power wide-area network
LTE	Long-term evolution
MBAN	Medical body area network
mIoT	Internet of m-health things

MIPv6	mobile IPv6
NFC	Near field communications
PDA	Personal digital assistants
PPG	Photoplethysmogram
RFID	Radio frequency identification
RR	Respiration rate
SIG	Bluetooth special interest group
SOC	Single-chip systems
UID	Global unique identifier
UTI	Urinary tract infection
WBAN	Wireless body area network
WiMAX	Microwave access

References

1. Abidi, B.; Jilbab, A.; Haziti, M.E. Wireless sensor networks in biomedical: Wireless body area networks. In *Europe and MENA Cooperation Advances in Information and Communication Technologies*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 321–329.
2. Xu, Q.; Ren, P.; Song, H.; Du, Q. Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. *IEEE Access* **2016**, *4*, 2840–2853. [[CrossRef](#)]
3. Scuotto, V.; Ferraris, A.; Bresciani, S. Internet of Things: Applications and challenges in smart cities: A case study of IBM smart city projects. *Bus. Process Manag. J.* **2016**, *22*, 357–367. [[CrossRef](#)]
4. Stergiou, C.; Psannis, K.E.; Kim, B.G.; Gupta, B. Secure integration of IoT and cloud computing. *Future Gener. Comput. Syst.* **2018**, *78*, 964–975. [[CrossRef](#)]
5. Truong, H.L.; Dustdar, S. Principles for engineering IoT cloud systems. *IEEE Cloud Comput.* **2015**, *2*, 68–76. [[CrossRef](#)]
6. Minh, D.L.; Sadeghi-Niaraki, A.; Huy, H.D.; Min, K.; Moon, H. Deep learning approach for short-term stock trends prediction based on two-stream gated recurrent unit network. *IEEE Access* **2018**, *6*, 55392–55404. [[CrossRef](#)]
7. Paul, P.V.; Saraswathi, R. The Internet of Things: A comprehensive survey. In Proceedings of the 2017 International Conference on Computation of Power, Energy Information and Commuication (ICCPEIC), Melmaruvathur, India, 22–23 March 2017; pp. 421–426.
8. Chen, E.T. The Internet of Things: Opportunities, Issues, and Challenges. In *The Internet of Things in the Modern Business Environment*; IGI Global: Hershey, PA, USA, 2017; pp. 167–187.
9. Yaqoob, I.; Ahmed, E.; Hashem, I.A.T.; Ahmed, A.I.A.; Gani, A.; Imran, M.; Guizani, M. Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. *IEEE Wirel. Commun.* **2017**, *24*, 10–16. [[CrossRef](#)]
10. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [[CrossRef](#)]
11. Li, S.; Da Xu, L.; Zhao, S. 5G internet of things: A survey. *J. Ind. Inf. Integr.* **2018**, *10*, 1–9. [[CrossRef](#)]
12. 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*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 29–40.
13. Dang, L.M.; Hassan, S.I.; Im, S.; Moon, H. Face image manipulation detection based on a convolutional neural network. *Expert Syst. Appl.* **2019**, *129*, 156–168. [[CrossRef](#)]
14. Nguyen, T.N.; Thai, C.H.; Luu, A.T.; Nguyen-Xuan, H.; Lee, J. NURBS-based postbuckling analysis of functionally graded carbon nanotube-reinforced composite shells. *Comput. Methods Appl. Mech. Eng.* **2019**, *347*, 983–1003. [[CrossRef](#)]
15. Nguyen, T.N.; Thai, C.H.; Nguyen-Xuan, H.; Lee, J. NURBS-based analyses of functionally graded carbon nanotube-reinforced composite shells. *Compos. Struct.* **2018**, *203*, 349–360. [[CrossRef](#)]
16. Nguyen, T.N.; Lee, S.; Nguyen-Xuan, H.; Lee, J. A novel analysis-prediction approach for geometrically nonlinear problems using group method of data handling. *Comput. Methods Appl. Mech. Eng.* **2019**, *354*, 506–526. [[CrossRef](#)]

17. Dang, L.M.; Hassan, S.I.; Im, S.; Mehmood, I.; Moon, H. Utilizing text recognition for the defects extraction in sewers CCTV inspection videos. *Comput. Ind.* **2018**, *99*, 96–109. [CrossRef]
18. Internet of Things at a Glance. Available online: <https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf> (accessed on 23 February 2019).
19. Size of the Internet of Things Market Worldwide in 2014 and 2020, by Industry. Available online: <https://www.statista.com/statistics/512673/worldwide-internet-of-things-market/> (accessed on 24 February 2019).
20. Islam, S.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K.S. The internet of things for health care: A comprehensive survey. *IEEE Access* **2015**, *3*, 678–708. [CrossRef]
21. Mutlag, A.A.; Ghani, M.K.A.; Arunkumar, N.; Mohamed, M.A.; Mohd, O. Enabling technologies for fog computing in healthcare IoT systems. *Future Gener. Comput. Syst.* **2019**, *90*, 62–78. [CrossRef]
22. Kumari, A.; Tanwar, S.; Tyagi, S.; Kumar, N. Fog computing for Healthcare 4.0 environment: Opportunities and challenges. *Comput. Electr. Eng.* **2018**, *72*, 1–13. [CrossRef]
23. García-Valls, M.; Calva-Urrego, C.; García-Fornes, A. Accelerating smart eHealth services execution at the fog computing infrastructure. *Future Gener. Comput. Syst.* **2018**.10.1016/j.future.2018.07.001. [CrossRef]
24. Kraemer, F.A.; Braten, A.E.; Tamkittikhun, N.; Palma, D. Fog computing in healthcare—A review and discussion. *IEEE Access* **2017**, *5*, 9206–9222. [CrossRef]
25. Ahmadi, H.; Arji, G.; Shahmoradi, L.; Safdari, R.; Nilashi, M.; Alizadeh, M. The application of internet of things in healthcare: A systematic literature review and classification. *Univer. Access Inf. Soc.* **2018**, 1–33.10.1007/s10209-018-0618-4. [CrossRef]
26. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [CrossRef]
27. Farahani, B.; Firouzi, F.; Chang, V.; Badaroglu, M.; Constant, N.; Mankodiya, K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Gener. Comput. Syst.* **2018**, *78*, 659–676. [CrossRef]
28. Yang, Z.; Zhou, Q.; Lei, L.; Zheng, K.; Xiang, W. An IoT-cloud based wearable ECG monitoring system for smart healthcare. *J. Med. Syst.* **2016**, *40*, 286. [CrossRef]
29. Almotiri, S.H.; Khan, M.A.; Alghamdi, M.A. Mobile health (m-health) system in the context of IoT. In Proceedings of the IEEE International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 39–42.
30. Oryema, B.; Kim, H.S.; Li, W.; Park, J.T. Design and implementation of an interoperable messaging system for IoT healthcare services. In Proceedings of the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017; pp. 45–52.
31. Abideen, Z.U.; Shah, M.A. An IoT based robust healthcare model for continuous health monitoring. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017; pp. 1–6.
32. Gia, T.N.; Jiang, M.; Rahmani, A.M.; Westerlund, T.; Liljeberg, P.; Tenhunen, H. Fog computing in healthcare internet of things: A case study on ecg feature extraction. In Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), Liverpool, UK, 26–28 October 2015; pp. 356–363.
33. Rashed, A.; Ibrahim, A.; Adel, A.; Mourad, B.; Hatem, A.; Magdy, M.; Elgaml, N.; Khattab, A. Integrated IoT medical platform for remote healthcare and assisted living. In Proceedings of the 2017 Japan-Africa Conference on Electronics, Communications and Computers (JAC-ECC), Alexandria, Egypt, 18–20 December 2017; pp. 160–163.
34. 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]
35. Reda, R.; Piccinini, F.; Carbonaro, A. Semantic Modelling of Smart Healthcare Data. In *Proceedings of SAI Intelligent Systems Conference*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 399–411.
36. Abawajy, J.H.; Hassan, M.M. Federated internet of things and cloud computing pervasive patient health monitoring system. *IEEE Commun. Mag.* **2017**, *55*, 48–53. [CrossRef]
37. Jabbar, S.; Ullah, F.; Khalid, S.; Khan, M.; Han, K. Semantic interoperability in heterogeneous IoT infrastructure for healthcare. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 9731806. [CrossRef]

38. Gia, T.N.; Thanigaivelan, N.K.; Rahmani, A.M.; Westerlund, T.; Liljeberg, P.; Tenhunen, H. Customizing 6LoWPAN networks towards Internet-of-Things based ubiquitous healthcare systems. In Proceedings of the 2014 NORCHIP, Tampere, Finland, 27–28 October 2014; pp. 1–6.
39. Ronen, E.; Shamir, A.; Weingarten, A.O.; O’Flynn, C. IoT goes nuclear: Creating a ZigBee chain reaction. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017; pp. 195–212.
40. Al-Kashoash, H.; Kemp, A.H. Comparison of 6LoWPAN and LPWAN for the Internet of Things. *Aust. J. Electr. Electron. Eng.* **2016**, *13*, 268–274. [[CrossRef](#)]
41. Gomes, T.; Salgado, F.; Pinto, S.; Cabral, J.; Tavares, A. A 6LoWPAN accelerator for Internet of Things endpoint devices. *IEEE Internet Things J.* **2018**, *5*, 371–377. [[CrossRef](#)]
42. Lee, J.L.; Tyan, Y.Y.; Wen, M.H.; Wu, Y.W. Development of an IoT-based bridge safety monitoring system. In Proceedings of the 2017 International Conference on Applied System Innovation (ICASI), Sapporo, Japan, 13–17 May 2017; pp. 84–86.
43. Arndt, J.; Krause, F.; Wunderlich, R.; Heinen, S. Development of a 6LoWPAN sensor node for IoT based home automation networks. In Proceedings of the 2017 International Conference on Research and Education in Mechatronics (REM), Wolfenbuttel, Germany, 14–15 September 2017; pp. 1–4.
44. You, I.; Leu, F.Y. Comments on “SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks”. *IEEE Syst. J.* **2018**, *12*, 1038–1041. [[CrossRef](#)]
45. Fotouhi, H.; Moreira, D.; Alves, M.; Yomsi, P.M. mRPL+: A mobility management framework in RPL/6LoWPAN. *Comput. Commun.* **2017**, *104*, 34–54. [[CrossRef](#)]
46. Ha, M.; Kim, S.H.; Kim, D. Intra-MARIO: A Fast Mobility Management Protocol for 6LoWPAN. *IEEE Trans. Mob. Comput.* **2017**, *16*, 172–184. [[CrossRef](#)]
47. Xiaonan, W.; Hongbin, C. Research on seamless mobility handover for 6LoWPAN wireless sensor networks. *Telecommun. Syst.* **2016**, *61*, 141–157. [[CrossRef](#)]
48. Miranda, J.; Cabral, J.; Wagner, S.R.; Fischer Pedersen, C.; Ravelo, B.; Memon, M.; Mathiesen, M. An open platform for seamless sensor support in healthcare for the internet of things. *Sensors* **2016**, *16*, 2089. [[CrossRef](#)] [[PubMed](#)]
49. Ali, M.; Bilal, H.S.M.; Razzaq, M.A.; Khan, J.; Lee, S.; Idris, M.; Aazam, M.; Choi, T.; Han, S.C.; Kang, B.H. IoTFLiP: IoT-based flipped learning platform for medical education. *Digit. Commun. Netw.* **2017**, *3*, 188–194. [[CrossRef](#)]
50. Verma, P.; Sood, S.K.; Kalra, S. Cloud-centric IoT based student healthcare monitoring framework. *J. Ambient Intell. Humaniz. Comput.* **2018**, *9*, 1293–1309. [[CrossRef](#)]
51. Manashty, A.; Light, J.; Yadav, U. Healthcare event aggregation lab (HEAL), a knowledge sharing platform for anomaly detection and prediction. In Proceedings of the 2015 17th International Conference on E-health Networking, Application & Services (HealthCom), Boston, MA, USA, 14–17 October 2015; pp. 648–652.
52. Pace, P.; Aloï, G.; Gravina, R.; Fortino, G.; Larini, G.; Gulino, M. Towards interoperability of IoT-based health care platforms: The INTER-health use case. In Proceedings of the 11th EAI International Conference on Body Area Networks, Turin, Italy, 15–16 December 2016, pp. 12–18.
53. Sultan, N. Making use of cloud computing for healthcare provision: Opportunities and challenges. *Int. J. Inf. Manag.* **2014**, *34*, 177–184. [[CrossRef](#)]
54. Darwish, A.; Hassanien, A.E.; Elhoseny, M.; Sangaiah, A.K.; Muhammad, K. The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: Opportunities, challenges, and open problems. *J. Ambient Intell. Humaniz. Comput.* **2017**, 1–16. [[CrossRef](#)]
55. Xu, B.; Xu, L.; Cai, H.; Jiang, L.; Luo, Y.; Gu, Y. The design of an m-Health monitoring system based on a cloud computing platform. *Enterp. Inf. Syst.* **2017**, *11*, 17–36. [[CrossRef](#)]
56. Singh, D.; Tripathi, G.; Alberti, A.M.; Jara, A. Semantic edge computing and IoT architecture for military health services in battlefield. In Proceedings of the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017; pp. 185–190.
57. Yang, G.; Xie, L.; Mäntysalo, M.; Zhou, X.; Pang, Z.; Da Xu, L.; Kao-Walter, S.; Chen, Q.; Zheng, L.R. A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2180–2191. [[CrossRef](#)]
58. Corcoran, P.; Datta, S.K. Mobile-edge computing and the Internet of Things for consumers: Extending cloud computing and services to the edge of the network. *IEEE Consum. Electron. Mag.* **2016**, *5*, 73–74. [[CrossRef](#)]

59. Dastjerdi, A.V.; Buyya, R. Fog computing: Helping the Internet of Things realize its potential. *Computer* **2016**, *49*, 112–116. [[CrossRef](#)]
60. Solutions, C.F.C. *Unleash the Power of the Internet of Things*; Cisco Systems, Inc.: San Jose, CA, USA, 2015.
61. Devarajan, M.; Subramaniaswamy, V.; Vijayakumar, V.; Ravi, L. Fog-assisted personalized healthcare-support system for remote patients with diabetes. *J. Ambient Intell. Humaniz. Comput.* **2019**, 1–14. [[CrossRef](#)]
62. Sood, S.K.; Mahajan, I. IoT-Fog based Healthcare Framework to Identify and Control Hypertension Attack. *IEEE Internet Things J.* **2018**, *6*, 1920–1927. [[CrossRef](#)]
63. Bhatia, M.; Sood, S.K. Exploring temporal analytics in fog-cloud architecture for Smart Office HealthCare. *Mob. Netw. Appl.* **2018**, 1–19. [[CrossRef](#)]
64. Sharma, S.; Chen, K.; Sheth, A. Toward practical privacy-preserving analytics for iot and cloud-based healthcare systems. *IEEE Internet Comput.* **2018**, *22*, 42–51. [[CrossRef](#)]
65. Hu, P.; Dhelim, S.; Ning, H.; Qiu, T. Survey on fog computing: Architecture, key technologies, applications and open issues. *J. Netw. Comput. Appl.* **2017**, *98*, 27–42. [[CrossRef](#)]
66. Negash, B.; Gia, T.N.; Anzanpour, A.; Azimi, I.; Jiang, M.; Westerlund, T.; Rahmani, A.M.; Liljeberg, P.; Tenhunen, H. Leveraging fog computing for healthcare iot. In *Fog Computing in the Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 145–169.
67. Ahmad, M.; Amin, M.B.; Hussain, S.; Kang, B.H.; Cheong, T.; Lee, S. Health Fog: A novel framework for health and wellness applications. *J. Supercomput.* **2016**, *72*, 3677–3695. [[CrossRef](#)]
68. Nandyala, C.S.; Kim, H.K. 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](#)]
69. Tang, W.; Zhang, K.; Zhang, D.; Ren, J.; Zhang, Y.; Shen, X.S. Fog-Enabled Smart Health: Toward Cooperative and Secure Healthcare Service Provision. *IEEE Commun. Mag.* **2019**, *57*, 42–48. [[CrossRef](#)]
70. Wang, K.; Shao, Y.; Xie, L.; Wu, J.; Guo, S. Adaptive and Fault-tolerant Data Processing in Healthcare IoT Based on Fog Computing. *IEEE Trans. Netw. Sci. Eng.* **2018**. [[CrossRef](#)]
71. Sood, S.K.; Mahajan, I. A fog-based healthcare framework for chikungunya. *IEEE Internet Things J.* **2018**, *5*, 794–801. [[CrossRef](#)]
72. Srinivas, J.; Das, A.K.; Kumar, N.; Rodrigues, J. Cloud centric authentication for wearable healthcare monitoring system. *IEEE Trans. Depend. Secur. Comput.* **2018**. [[CrossRef](#)]
73. Vijayakumar, V.; Malathi, D.; Subramaniaswamy, V.; Saravanan, P.; Logesh, R. Fog computing-based intelligent healthcare system for the detection and prevention of mosquito-borne diseases. *Comput. Human Behav.* **2018**. [[CrossRef](#)]
74. Konstantinidis, E.I.; Antoniou, P.E.; Bamparopoulos, G.; Bamidis, P.D. A lightweight framework for transparent cross platform communication of controller data in ambient assisted living environments. *Inf. Sci.* **2015**, *300*, 124–139. [[CrossRef](#)]
75. De Venuto, D.; Annese, V.F.; Sangiovanni-Vincentelli, A.L. The ultimate IoT application: A cyber-physical system for ambient assisted living. In Proceedings of the 2016 IEEE International Symposium on Circuits and Systems (ISCAS), Montreal, QC, Canada, 22–25 May 2016; pp. 2042–2045.
76. Zgheib, R.; De Nicola, A.; Villani, M.L.; Conchon, E.; Bastide, R. A flexible architecture for cognitive sensing of activities in ambient assisted living. In Proceedings of the 2017 IEEE 26th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Poznan, Poland, 21–23 June 2017; pp. 284–289.
77. Corno, F.; De Russis, L.; Roffarello, A.M. A healthcare support system for assisted living facilities: An iot solution. In Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, 10–14 June 2016; Volume 1, pp. 344–352.
78. Tariq, M.; Majeed, H.; Beg, M.O.; Khan, F.A.; Derhab, A. Accurate detection of sitting posture activities in a secure IoT based assisted living environment. *Future Gener. Comput. Syst.* **2018**, *92*, 745–757. [[CrossRef](#)]
79. Rghioui, A.; Sendra, S.; Lloret, J.; Oumnad, A. Internet of things for measuring human activities in ambient assisted living and e-health. In *Network Protocols and Algorithms*; Macrothink Institute: Las Vegas, NV, USA, 2016; Volume 8, pp. 15–28.

80. Mainetti, L.; Manco, L.; Patrono, L.; Secco, A.; Sergi, I.; Vergallo, R. An ambient assisted living system for elderly assistance applications. In Proceedings of the 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 4–8 September 2016; pp. 1–6.
81. Konstantinidis, E.I.; Bamparopoulos, G.; Billis, A.; Bamidis, P.D. Internet of things for an age-friendly healthcare. *Stud. Health Technol. Inform.* **2015**, *587–591*. [[CrossRef](#)]
82. Marques, G.; Pitarma, R. An indoor monitoring system for ambient assisted living based on internet of things architecture. *Int. J. Environ. Res. Public Health* **2016**, *13*, 1152. [[CrossRef](#)]
83. Erdeniz, S.P.; Maglogiannis, I.; Menychtas, A.; Felfernig, A.; Tran, T.N.T. Recommender Systems for IoT Enabled m-Health Applications. In Proceedings of the IFIP International Conference on Artificial Intelligence Applications and Innovations, Rhodes, Greece, 25–27 May 2018; pp. 227–237.
84. Ullah, F.; Habib, M.A.; Farhan, M.; Khalid, S.; Durrani, M.Y.; Jabbar, S. Semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare. *Sustain. Cities Soc.* **2017**, *34*, 90–96. [[CrossRef](#)]
85. Kelati, A.; Dhaou, I.B.; Tenhunen, H. Biosignal Monitoring Platform Using Wearable IoT. In Proceedings of the 22st Conference of Open Innovations Association FRUCT, Petrozavodsk, Russia, 9–13 April 2018; p. 47.
86. Zgheib, R.; Conchon, E.; Bastide, R. Engineering IoT healthcare applications: Towards a semantic data driven sustainable architecture. In *eHealth 360*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 407–418.
87. Catherwood, P.A.; Steele, D.; Little, M.; McComb, S.; McLaughlin, J. A Community-Based IoT Personalized Wireless Healthcare Solution Trial. *IEEE J. Transl. Eng. Health Med.* **2018**, *6*, 1–13. [[CrossRef](#)] [[PubMed](#)]
88. Kumar, T.; Ramani, V.; Ahmad, I.; Braeken, A.; Harjula, E.; Ylianttila, M. Blockchain Utilization in Healthcare: Key Requirements and Challenges. In Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, Czech Republic, 17–20 September 2018; pp. 1–7.
89. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
90. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *J. Med. Syst.* **2018**, *42*, 130. [[CrossRef](#)]
91. Bhuiyan, M.Z.A.; Zaman, A.; Wang, T.; Wang, G.; Tao, H.; Hassan, M.M. Blockchain and Big Data to Transform the Healthcare. In Proceedings of the International Conference on Data Processing and Applications, Guangzhou, China, 12–14 May 2018; pp. 62–68.
92. Gia, T.N.; Ali, M.; Dhaou, I.B.; Rahmani, A.M.; Westerlund, T.; Liljeberg, P.; Tenhunen, H. IoT-based continuous glucose monitoring system: A feasibility study. *Procedia Comput. Sci.* **2017**, *109*, 327–334. [[CrossRef](#)]
93. Sunny, S.; Kumar, S.S. Optical based non invasive glucometer with IoT. In Proceedings of the 2018 International Conference on Power, Signals, Control and Computation (EPSCICON), Thrissur, India, 6–10 January 2018; pp. 1–3.
94. AL-Jaf, T.G.; Al-Hemiary, E.H. Internet of Things Based Cloud Smart Monitoring for Asthma Patient. In Proceedings of the 1st International Conference on Information Technology (ICoIT'17), Erbil, Iraq, 10 April 2017; p. 380.
95. Raji, A.; Devi, P.K.; Jeyaseeli, P.G.; Balaganesh, N. Respiratory monitoring system for asthma patients based on IoT. In Proceedings of the 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, India, 19 November 2016; pp. 1–6.
96. Satija, U.; Ramkumar, B.; Manikandan, M.S. Real-time signal quality-aware ECG telemetry system for IoT-based health care monitoring. *IEEE Internet Things J.* **2017**, *4*, 815–823. [[CrossRef](#)]
97. Beach, C.; Krachunov, S.; Pope, J.; Fafoutis, X.; Piechocki, R.J.; Craddock, I.; Casson, A.J. An ultra low power personalizable wrist worn ECG monitor integrated with IoT infrastructure. *IEEE Access* **2018**, *6*, 44010–44021. [[CrossRef](#)]
98. Soby, D.; Muruganandham, S.; Nallusamy, S.; Chakraborty, P. Wireless ECG Monitoring System using IoT based Signal Conditioning Module For Real Time Signal Acquisition. *Indian J. Public Health Res. Dev.* **2018**, *9*, 294–299. [[CrossRef](#)]

99. He, J.; Rong, J.; Sun, L.; Wang, H.; Zhang, Y.; Ma, J. D-ECG: A Dynamic Framework for Cardiac Arrhythmia Detection from IoT-Based ECGs. In Proceedings of the International Conference on Web Information Systems Engineering, Dubai, UAE, 12–15 November 2018; pp. 85–99.
100. Bansal, M.; Gandhi, B. IoT based smart health care system using CNT electrodes (for continuous ECG monitoring). In Proceedings of the 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 5–6 May 2017; pp. 1324–1329.
101. Xin, Q.; Wu, J. A novel wearable device for continuous, non-invasion blood pressure measurement. *Comput. Biol. Chem.* **2017**, *69*, 134–137. [[CrossRef](#)] [[PubMed](#)]
102. Chao, P.C.P.; Tu, T.Y. Using the Time-Domain Characterization for Estimation Continuous Blood Pressure via Neural Network Method. ASME 2017 Conference on Information Storage and Processing Systems collocated with the ASME 2017 Conference on Information Storage and Processing Systems, San Francisco, CA, USA, 29–30 August 2017; p. V001T02A003.
103. Dinh, A.; Luu, L.; Cao, T. Blood Pressure Measurement Using Finger ECG and Photoplethysmogram for IoT. In Proceedings of the International Conference on the Development of Biomedical Engineering in Vietnam, Ho Chi Minh, Vietnam, 27–29 June 2017; pp. 83–89.
104. Huang, M.; Tamura, T.; Tang, Z.; Chen, W.; Kanaya, S. A Wearable Thermometry for Core Body Temperature Measurement and Its Experimental Verification. *IEEE J. Biomed. Health Inform.* **2017**, *21*, 708–714. [[CrossRef](#)] [[PubMed](#)]
105. Li, Q.; Zhang, L.N.; Tao, X.M.; Ding, X. Review of flexible temperature sensing networks for wearable physiological monitoring. *Adv. Healthc. Mater.* **2017**, *6*, 1601371. [[CrossRef](#)] [[PubMed](#)]
106. Ota, H.; Chao, M.; Gao, Y.; Wu, E.; Tai, L.C.; Chen, K.; Matsuoka, Y.; Iwai, K.; Fahad, H.M.; Gao, W.; et al. 3d printed “earable” smart devices for real-time detection of core body temperature. *ACS Sens.* **2017**, *2*, 990–997. [[CrossRef](#)] [[PubMed](#)]
107. Shabana, N.; Velmathi, G. Advanced Tele-surgery with IoT Approach. In *Intelligent Embedded Systems*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 17–24.
108. Sareen, S.; Sood, S.K.; Gupta, S.K. IoT-based cloud framework to control Ebola virus outbreak. *J. Ambient Intell. Humaniz. Comput.* **2016**, *9*, 459–476. [[CrossRef](#)]
109. Ghorbel, A.; Bouguerra, S.; Amor, N.B.; Jallouli, M. Cloud based mobile application for remote control of intelligent wheelchair. In Proceedings of the 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018; pp. 1249–1254.
110. Lee, Y.K.; Lim, J.M.; Eu, K.S.; Goh, Y.H.; Tew, Y. Real time image processing based obstacle avoidance and navigation system for autonomous wheelchair application. In Proceedings of the Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Kuala Lumpur, Malaysia, 12–15 December 2017; pp. 380–385.
111. Nave, C.; Postolache, O. Smart Walker based IoT Physical Rehabilitation System. In Proceedings of the 2018 International Symposium in Sensing and Instrumentation in IoT Era (ISSI), Shanghai, China, 6–7 September 2018; pp. 1–6.
112. Yang, G.; Deng, J.; Pang, G.; Zhang, H.; Li, J.; Deng, B.; Pang, Z.; Xu, J.; Jiang, M.; Liljeborg, P.; et al. An IoT-Enabled Stroke Rehabilitation System Based on Smart Wearable Armband and Machine Learning. *IEEE J. Transl. Eng. Health Med.* **2018**, *6*, 1–10. [[CrossRef](#)]
113. Subhash, K.; Pournami, P.; Joseph, P.K. Census transform based feature extraction of EMG signals for neuromuscular disease classification. In Proceedings of the 2017 IEEE 15th Student Conference on Research and Development (SCoReD), Putrajaya, Malaysia, 13–14 December 2017; pp. 499–503.
114. Subasi, A.; Yaman, E.; Somaily, Y.; Alynabawi, H.A.; Alobaidi, F.; Altheibani, S. Automated EMG Signal Classification for Diagnosis of Neuromuscular Disorders Using DWT and Bagging. *Procedia Comput. Sci.* **2018**, *140*, 230–237. [[CrossRef](#)]
115. Fu, Y.; Liu, J. System design for wearable blood oxygen saturation and pulse measurement device. *Procedia Manuf.* **2015**, *3*, 1187–1194. [[CrossRef](#)]
116. Xie, Y.; Gao, Y.; Li, Y.; Lu, Y.; Li, W. Development of Wearable Pulse Oximeter Based on Internet of Things and Signal Processing Techniques. In Proceedings of the European Modelling Symposium (EMS), Manchester, UK, 20–21 November 2017; pp. 249–254.
117. Tekeste, T.; Saleh, H.; Mohammad, B.; Ismail, M. Ultra-Low Power QRS Detection and ECG Compression Architecture for IoT Healthcare Devices. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2018**, *66*, 669–679. [[CrossRef](#)]

118. Bathilde, J.B.; Then, Y.L.; Chameera, R.; Tay, F.S.; Zaidel, D.N.A. Continuous heart rate monitoring system as an IoT edge device. In Proceedings of the Sensors Applications Symposium (SAS), Seoul, Korea, 12–14 March 2018; pp. 1–6.
119. Krachunov, S.; Beach, C.; Casson, A.J.; Pope, J.; Fafoutis, X.; Piechocki, R.J.; Craddock, I. Energy efficient heart rate sensing using a painted electrode ECG wearable. In Proceedings of the Global Internet of Things Summit (GloTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–6.
120. Diabetes. Available online: <https://medlineplus.gov/lab-tests/blood-glucose-test> (accessed on 29 March 2019).
121. Capodieci, A.; Budner, P.; Eirich, J.; Gloor, P.; Mainetti, L. Dynamically Adapting the Environment for Elderly People Through Smartwatch-Based Mood Detection. In *Collaborative Innovation Networks*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 65–73.
122. Bharadwaj, S.A.; Yarravarapu, D.; Reddy, S.C.K.; Prudhvi, T.; Sandeep, K.; Reddy, O.S.D. Enhancing healthcare using m-care box (monitoring non-compliance of medication). In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), Palladam, India, 10–11 February 2017; pp. 352–356.
123. Medina, J.; Espinilla, M.; García-Fernández, Á.; Martínez, L. Intelligent multi-dose medication controller for fever: From wearable devices to remote dispensers. *Comput. Electr. Eng.* **2018**, *65*, 400–412. [CrossRef]
124. Gupta, K.; Rakesh, N.; Faujdar, N.; Kumari, M.; Kingler, P.; Matam, R. IOT Based Automation and Solution for Medical Drug Storage: Smart Drug Store. In Proceedings of the 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 11–12 January 2018; pp. 497–502.
125. Monteleone, S.; Sampaio, M.; Maia, R.F. A novel deployment of smart Cold Chain system using 2G-RFID-Sys temperature monitoring in medicine Cold Chain based on Internet of Things. In Proceedings of the 2017 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Bari, Italy, 18–20 September 2017; pp. 205–210.
126. Baig, M.M.; GholamHosseini, H.; Connolly, M.J. Mobile healthcare applications: System design review, critical issues and challenges. *Australas. Phys. Eng. Sci. Med.* **2015**, *38*, 23–38. [CrossRef] [PubMed]
127. Watch Series 4, A. Apple Watch Series 4. Available online: <https://www.apple.com/lae/apple-watch-series-4> (accessed on 23 February 2019).
128. Thync. Available online: <https://www.thync.com/> (accessed on 23 February 2019).
129. Ybrain. Available online: <http://www.ybrain.com> (accessed on 23 February 2019).
130. Quell. Available online: <https://www.quellrelief.com> (accessed on 23 February 2019).
131. Augmedix. Available online: <https://www.augmedix.com/> (accessed on 23 February 2019).
132. Lumo. Available online: <https://support.lumobodytech.com/hc/en-us> (accessed on 23 February 2019).
133. Sprouting. Available online: <http://misscharmsie.com/?p=19716> (accessed on 23 February 2019).
134. Nima Sensor. Available online: <https://nimasensor.com> (accessed on 23 February 2019).
135. Beddits Sleep Monitor. Available online: <https://www.beddit.com> (accessed on 23 February 2019).
136. Breathometer. Available online: <https://www.breathometer.com> (accessed on 23 February 2019).
137. AURIS. Available online: <https://www.aurishealth.com> (accessed on 23 February 2019).
138. Moxi. Available online: <http://diligentrobots.com/moxi/> (accessed on 23 February 2019).
139. Tugrobot. Available online: <https://aethon.com/> (accessed on 23 February 2019).
140. Albalawi, U.; Joshi, S. Secure and trusted telemedicine in Internet of Things IoT. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 30–34.
141. Galletta, A.; Carnevale, L.; Bramanti, A.; Fazio, M. An innovative methodology for Big Data Visualization for telemedicine. *IEEE Trans. Ind. Inform.* **2018**, *15*, 490–497. [CrossRef]
142. Hussain, S.R.; Mehnaz, S.; Nirjon, S.; Bertino, E. Secure Seamless Bluetooth Low Energy Connection Migration for Unmodified IoT Devices. *IEEE Trans. Mob. Comput.* **2018**, *17*, 927–944. [CrossRef]
143. Dimitrov, S.; Haas, H. *Principles of LED Light Communications: Towards Networked Li-Fi*; Cambridge University Press: Cambridge, UK, 2015.
144. Albraheem, L.I.; Alhudaithy, L.H.; Aljaser, A.A.; Aldhafian, M.R.; Bahliwah, G.M. Toward Designing a Li-Fi-Based Hierarchical IoT Architecture. *IEEE Access* **2018**, *6*, 40811–40825. [CrossRef]
145. Martínez Pérez, M.; Dafonte, C.; Gómez, Á. Traceability in Patient Healthcare through the Integration of RFID Technology in an ICU in a Hospital. *Sensors* **2018**, *18*, 1627. [CrossRef] [PubMed]

146. Kim, Y.; Lee, W.S.; Raghunathan, V.; Jha, N.K.; Raghunathan, A. Vibration-based secure side channel for medical devices. In Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, 7–11 June 2015; p. 32.
147. Al Alkeem, E.; Yeun, C.Y.; Zemerly, M.J. Security and privacy framework for ubiquitous healthcare IoT devices. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 70–75.
148. Gope, P.; Hwang, T. BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sens. J.* **2016**, *16*, 1368–1376. [[CrossRef](#)]
149. Salameh, H.B.; Almajali, S.; Ayyash, M.; Elgala, H. Securing delay-sensitive cognitive radio IoT communications under reactive jamming attacks: Spectrum assignment perspective. In Proceedings of the 2018 Fifth International Conference on Software Defined Systems (SDS), Barcelona, Spain, 23–26 April 2018; pp. 20–24.
150. Namvar, N.; Saad, W.; Bahadori, N.; Kelley, B. Jamming in the internet of things: A game-theoretic perspective. In Proceedings of the Global Communications Conference (GLOBECOM), 2016 IEEE, Washington, DC, USA, 4–8 December 2016; pp. 1–6.
151. Abdallah, A.; Shen, X.S. Efficient prevention technique for false data injection attack in smart grid. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–6.
152. Amah, T.; Kamat, M.; Bakar, K.; Rahman, S.; Mohammed, M.; Abali, A.; Moreira, W.; Oliveira-Jr, A. The Impact of Message Replication on the Performance of Opportunistic Networks for Sensed Data Collection. *Information* **2017**, *8*, 143. [[CrossRef](#)]
153. Singh, S.P.; Sharma, S. Secure clustering protocols in wireless sensor networks. *J. Wirel. Sens. Netw.* **2016**, *3*, 1–10.
154. Adat, V.; Dahiya, A.; Gupta, B. Economic incentive based solution against distributed denial of service attacks for IoT customers. In Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 12–14 January 2018; pp. 1–5.
155. Chen, Q.; Chen, H.; Cai, Y.; Zhang, Y.; Huang, X. Denial of Service Attack on IoT System. In Proceedings of the 2018 9th International Conference on Information Technology in Medicine and Education (ITME), Hangzhou, China, 19–21 October 2018; pp. 755–758.
156. Gill, R.K.; Sachdeva, M. Detection of hello flood attack on LEACH in wireless sensor networks. In *Next-Generation Networks*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 377–387.
157. Bhatia, T.; Verma, A.; Sharma, G.; Bala, S. A Novel Defense Scheme against Flooding Attack in Mobile Adhoc Networks. *Recent Patents Eng.* **2018**, *12*, 15–22. [[CrossRef](#)]
158. Mohammad, S.N.; Singh, R.; Dey, A.; Ahmad, S.J. ESMBCRT: Enhance Security to MANETs Against Black Hole Attack Using MCR Technique. In *Innovations in Electronics and Communication Engineering*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 319–326.
159. Kumar, V.; Kumar, R. An adaptive approach for detection of blackhole attack in mobile ad hoc network. *Procedia Comput. Sci.* **2015**, *48*, 472–479. [[CrossRef](#)]
160. Gurung, S.; Chauhan, S. A novel approach for mitigating gray hole attack in MANET. *Wirel. Netw.* **2018**, *24*, 565–579. [[CrossRef](#)]
161. Schweitzer, N.; Stulman, A.; Margalit, R.D.; Shabtai, A. Contradiction based gray-hole attack minimization for ad hoc networks. *IEEE Trans. Mob. Comput.* **2017**, *16*, 2174–2183. [[CrossRef](#)]
162. Pongle, P.; Chavan, G. Real time intrusion and wormhole attack detection in internet of things. *Int. J. Comput. Appl.* **2015**, *121*, 1–9. [[CrossRef](#)]
163. Giri, D.; Borah, S.; Pradhan, R. Approaches and Measures to Detect Wormhole Attack in Wireless Sensor Networks: A Survey. In *Advances in Communication, Devices and Networking*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 855–864.
164. Cervantes, C.; Poplade, D.; Nogueira, M.; Santos, A. Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, 11–15 May 2015; pp. 606–611.
165. Mishra, A.K.; Tripathy, A.K.; Puthal, D.; Yang, L.T. Analytical model for Sybil attack phases in internet of things. *IEEE Internet Things J.* **2019**, *6*, 379–387. [[CrossRef](#)]

166. Jamshidi, M.; Zangeneh, E.; Esnaashari, M.; Darwesh, A.M.; Meybodi, M.R. A Novel Model of Sybil Attack in Cluster-Based Wireless Sensor Networks and Propose a Distributed Algorithm to Defend It. *Wirel. Pers. Commun.* **2019**, *105*, 145–173. [CrossRef]
167. Thota, C.; Sundarasekar, R.; Manogaran, G.; Varatharajan, R.; Priyan, M. Centralized fog computing security platform for IoT and cloud in healthcare system. In *Fog Computing: Breakthroughs in Research and Practice*; IGI Global: Hershey, PA, USA, 2018; pp. 365–378.
168. Fostering the Advancement of the Internet of Things. Available online: https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf (accessed on 29 March 2019).
169. CLOUD COMPUTING SECURITY REQUIREMENTS GUIDE. Available online: https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf (accessed on 29 March 2019).
170. Track the Movements of Fitness Tracker-Wearing Military Personnel. Available online: <https://dod.defense.gov/News/Article/Article/1594486/new-dod-policy-prohibits-gps-enabled-devices-in-deployed-settings/> (accessed on 29 March 2019).
171. Polar Fitness Suspends Its Global Activity Map after Privacy Concerns. Available online: <https://www.theverge.com/2018/7/8/17546224/polar-flow-smart-fitness-company-privacy-tracking-security> (accessed on 29 March 2019).
172. USBan. Available online: <https://dod.defense.gov/News/Article/Article/1594486/new-dod-policy-prohibits-gps-enabled-devices-in-deployed-settings/> (accessed on 29 March 2019).
173. Made in China 2025. Available online: <http://isdpeu/content/uploads/2018/06/Made-in-China-Backgrounder.pdf> (accessed on 29 March 2019).
174. China IoT in Healthcare White Paper. Available online: <http://global.chinadaily.com.cn/a/201809/14/WS5b9bb789a31033b4f465629c.html> (accessed on 29 March 2019).
175. EU-China Joint White Paper on the Internet of Things. Available online: <http://www.eglobalmark.com/wp-content/uploads/2016/06/2016-01-EU-China-Joint-White-Paper-on-IoT.pdf> (accessed on 29 March 2019).
176. i-Japan Strategy 2015. Available online: https://japan.kantei.go.jp/policy/it/i-JapanStrategy2015_full.pdf (accessed on 29 March 2019).
177. Smart Japan ICT Strategy. Available online: https://japan.kantei.go.jp/policy/it/i-JapanStrategy2015_full.pdf (accessed on 29 March 2019).
178. General Framework for Secured IoT Systems. Available online: https://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf (accessed on 29 March 2019).
179. Master Plan for Building the Internet of Things. Available online: http://www.iotkorea.or.kr/2013_kor/uploadFiles/board/KOREA-%20IoT%28Internet%20of%20Things%29%20Master%20Plan%20-%202014.pdf (accessed on 29 March 2019).
180. Allocation of Rs. 7060 Crores for Smart Cities. Available online: <https://www.thehindu.com/business/budget/rs-7060-crore-for-100-smart-cities/article6198022.ece> (accessed on 29 March 2019).
181. Digital India Program of the Government. Available online: <https://www.digitalindia.gov.in/> (accessed on 29 March 2019).
182. Russia Internet-of-Things Market 2018–2022 Forecast . Available online: <https://www.idc.com/getdoc.jsp?containerId=CEMA43447018> (accessed on 29 March 2019).
183. Russian Internet of Things Market . Available online: <https://iot.ru/upload/Russia%20Internet%20of%20Things%20market.pdf> (accessed on 29 March 2019).
184. Digital Growth Strategy. Available online: https://eng.em.dk/media/10566/digital-growth-strategy-report_uk_web-2.pdf (accessed on 29 March 2019).
185. Alliance for Internet of Things Innovation. Available online: <https://aioti.eu/> (accessed on 29 March 2019).
186. Digital Single Market Strategy. Available online: https://ec.europa.eu/commission/priorities/digital-single-market_en (accessed on 29 March 2019).
187. Cisco Survey IoT Projects. Available online: <https://newsroom.cisco.com/press-release-content?articleId=1847422> (accessed on 29 March 2019).

