







Review

Towards Secure and Intelligent Internet of Health Things: A Survey of Enabling Technologies and Applications

Umar Zaman ¹, Imran ^{2,*}, Faisal Mehmood ³, Naeem Iqbal ⁴, Jungsuk Kim ^{2,*}
and Muhammad Ibrahim ⁵

¹ AIPSCom Convergence Lab, Department of Research and Innovation, SCIREP Institute of Scientific Research and Entrepreneurship, Islamabad 46000, Pakistan; umarzaman2010@gmail.com

² Department of Biomedical Engineering, Gachon University, 191 Hambakmoe-ro, Incheon 21936, Korea

³ Department of I.T Convergence Engineering, Gachon University, Sujeong-gu, Seongnam-si 461-701, Korea; faisal89@gachon.ac.kr

⁴ Department of Computer Engineering, Jeju National University, Jeju 63243, Korea; naeemiqbal@jejunu.ac.kr

⁵ Department of Information Technology, University of Haripur, Haripur 22620, Pakistan; ibrahimmayar@uoh.edu.pk

* Correspondence: imranj@gachon.ac.kr (I.); jungsuk@gachon.ac.kr (J.K.)

Abstract: With the growth of computing and communication technologies, the information processing paradigm of the healthcare environment is evolving. The patient information is stored electronically, making it convenient to store and retrieve patient information remotely when needed. However, evolving the healthcare systems into smart healthcare environments comes with challenges and additional pressures. Internet of Things (IoT) connects things, such as computing devices, through wired or wireless mediums to form a network. There are numerous security vulnerabilities and risks in the existing IoT-based systems due to the lack of intrinsic security technologies. For example, patient medical data, data privacy, data sharing, and convenience are considered imperative for collecting and storing electronic health records (EHR). However, the traditional IoT-based EHR systems cannot deal with these paradigms because of inconsistent security policies and data access structures. Blockchain (BC) technology is a decentralized and distributed ledger that comes in handy in storing patient data and encountering data integrity and confidentiality challenges. Therefore, it is a viable solution for addressing existing IoT data security and privacy challenges. BC paves a tremendous path to revolutionize traditional IoT systems by enhancing data security, privacy, and transparency. The scientific community has shown a variety of healthcare applications based on artificial intelligence (AI) that improve health diagnosis and monitoring practices. Moreover, technology companies and startups are revolutionizing healthcare with AI and related technologies. This study illustrates the implication of integrated technologies based on BC, IoT, and AI to meet growing healthcare challenges. This research study examines the integration of BC technology with IoT and analyzes the advancements of these innovative paradigms in the healthcare sector. In addition, our research study presents a detailed survey on enabling technologies for the futuristic, intelligent, and secure internet of health things (IoHT). Furthermore, this study comprehensively studies the peculiarities of the IoHT environment and the security, performance, and progression of the enabling technologies. First, the research gaps are identified by mapping security and performance benefits inferred by the BC technologies. Secondly, practical issues related to the integration process of BC and IoT devices are discussed. Third, the healthcare applications integrating IoT, BC, and ML in healthcare environments are discussed. Finally, the research gaps, future directions, and limitations of the enabling technologies are discussed.

Keywords: blockchain; IoT; healthcare; machine learning; IoHT; convergence



Citation: Zaman, U.; Imran; Mehmood, F.; Iqbal, N.; Kim, J.; Ibrahim, M. Towards Secure and Intelligent Internet of Health Things: A Survey of Enabling Technologies and Applications. *Electronics* **2022**, *11*, 1893. <https://doi.org/10.3390/electronics11121893>

Academic Editor: Federico Alimenti

Received: 25 April 2022

Accepted: 11 June 2022

Published: 16 June 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the growth of healthcare technologies, the information processing paradigm of the healthcare environment is evolving, and data are stored electronically. Healthcare is the most important field that needs attention to restructure with today's advanced solutions from science and technology to reduce pressure due to the growing population and to provide quality treatment. The information and communication technologies (ICTs) from the 1990s responded to such needs and improved the access, quality of virtually any process, and the efficiency related to healthcare [1]. However, the term e-health, assigned as an ICTs application to health care, has gained public and private funding and research efforts [2]. The advancement in technology and e-health is growing day by day, leading to changes in the characterization and specification of terms. The current one is Industry 4.0 (I4.0). However, the government is committed to promoting technology culture and legal frameworks. The German government used the term I4.0 once in November 2011 to define its high-tech strategy, "Industry4.0". Thus, technologies are associated, but a development plan includes enterprise management aspects, regulatory framework, and training. Technically, this is also called the fourth industrial revolution-based cyber-physical system (CPS), which relies on groups of technologies. The indication of fast technological growth associated with the world governmental struggles concludes that I4.0 effectively influences the healthcare sector that moves e-health towards Healthcare 4.0 [3,4].

The scientific community has published many research articles on IoT, ML, and BC in regard to e-health, supply chain, agriculture, smart cities, and smart home [5,6]. State-of-the-art works published on BC technology implementation and applications with the Internet of Energy (IoE) provide readers with future ideas [7]. Many BC smart contract applications are explained for energy management, such as automated data exchange trading on a secure peer-to-peer network and energy transactions. In the literature, BC applications in smart grids have been summarized with technical details, implementation, and challenges [8]. A detailed literature review explains the use of BC in smart agriculture and suggests how to use BC-based security in smart farming, explores the drawbacks in existing research, and presents future research directions in artificial intelligence [9]. Due to the capacity of innovative services for different applications, such as academics, researchers, and entrepreneurs, especially in telehealth, IoT has become popular [10,11]. In IoT, without human interaction, communication processes, sensing, and processing are controlled automatically in a physical network formed by heterogeneous devices and objects [12]. It can connect different devices on the network, such as a vehicle, household appliances, and other electronic devices, making human life more intelligent. Real-time identification, monitoring, event triggers, and location are all achieved by using an IoT-based system. The IoT applications can be categorized into two categories. The first category includes smart cities [13], crowdsensing [14], industrial automation [15], traffic monitoring [16], and power administration [17]. The second category includes IoT applications with business intelligence and predictive analytics. These applications refer to remodeling business operations commuted to commercial procedures, such as banking, insurance, and provision enhancement of healthcare [18]. In addition, the anticipation of more than 27 billion connected devices by 2025 is the arrival of smart cities, smart homes, and other intelligent machines [19]. In the literature, various technologies, such as cyber-physical systems (CPS), wireless sensor networks (WSNs), and machine-to-machine (M2M), have been developed and considered necessary elements for IoT. At the same time, security concerns arise in IoT with standard IP protocol that needs to be secure against security attacks. Similarly, IoT architecture and enabling technologies [20] highlighted and described various issues related to security in IoT systems [21]. Therefore, the IoT systems need to be restructured fundamentally to devastate these problems [22].

Initially, BC was considered a financial transaction protocol in Bitcoin. Then, the security features, such as fault tolerance, identities (IDs), and decentralization security, convinced analysts and researchers to use it as a solution to the security issues of IT. BC is the one proper technology that supports a distributed and secure ecosystem for IT [23]. It

is a distributed ledger as all the blocks are chained together. It can save information from billions of computing devices [24]. BC refers to a decentralized, tamperproof, transactional database that stores and processes information securely across a wide range of network nodes [25]. BC has grown as a breakthrough technology known as a distributed transaction ledger (DTL) that solves privacy, scalability, and security issues. The distributed ledger nature of BC removes the trust of the participating parties due to immutable features. BC development is essential for eliminating trust in a traditional system, such as online intermediaries, and for removing the need for trust among entities. Participants in BC are directed to the authority of technological techniques rather than a centralized organization that can be unreliable. However, trust in BC-based systems is not eliminated but indirectly reduces the need for trust by increasing confidence among participants. Trust can be achieved in BC because of its technical arrangements, and anyone can predict the outcome theoretically, specifically in open-source software in which the code is open. The higher the predictability of software, the greater the belief and the lower the need for trust in that technical system's operators or developers. The open Bitcoin protocol allows any participant to study and know that the new Bitcoin is produced at a particular speed of one block per 10 min when a miner wins a PoW without trusting any third party. Therefore, BC technology assures participants no need to be relied on by any third party, or no one can pretend to be trusted [26].

Challenges in IoT connectivity are sharing data with stakeholders, which requires connectivity with extensive storage, computing, and networking resources. However, its capability is limited to connecting IoT with BC technology to provide new opportunities to implement business applications and services in many domains [27]. Big data handling on BC requires copying the complete distributed ledger stored by every participant in BC. Every node appends a newly confirmed block to its local ledger broadcasted to a peer-to-peer network. Several issues are solved by this decentralized storage structure, such as efficiency and removing trust from the third party during load put on the participant's node by the management of IoT data on centralized BC [28]. For example, suppose a thousand participants exchange 2 MB of data per year. In that case, the BC node will need 730 GB of data, thus posing a storage challenge when IoT device stores data in BC infrastructure [29,30]. Transparency and privacy challenges can be better explained in some applications like finance, such as transparency in transactions. Moreover, BC ensures transparency and privacy in applications, such as e-health. However, transparency may be affected when storing and accessing IoT data from IoT systems. Moreover, regulatory challenges caused by BC features are promising security solutions for different IoT applications [31]. These features are decentralization, immutability, anonymity, and automation. For example, data cannot be deleted or modified once published by the immutability feature in DTL on a peer-to-peer network [32].

Some advantages of BC implementation with IoT include solving a single point of failure issue, increasing fault tolerance, and ensuring end-to-end communication without a centralized server's involvement. A single point of failure is an issue that affects reliability and high availability in any system [33]. In addition, data integrity and user identity can be verified very easily by participants [34]. Furthermore, to ensure traceability and accountability, BC stores data and event logs in an immutable way. BC solves many issues related to IoT, but it has many challenges, such as high computation costs and delays, which restricts storage and power capabilities [35,36]. Power, performance, and security trade-offs are essential because BC technology-based applications are slowed down due to the high computational power needed to run BC algorithms on limited-resource devices [37]. A comparison of energy consumed by Bitcoin in Ireland with domestic power consumption is made, which IoT devices cannot undertake [38]. The Bitcoin network consumes more energy than several nations, including Austria and Colombia. Moreover, the central algorithm can increase performance by increasing the number of confirmed blocks per second while processing IoT data by BC suggested by many researchers [39]. Improving performance and lowering power consumption can be achieved by eliminating proof of

work (PoW) [40]. Still, PoW protects from Sybil attacks and malicious attacks and makes the blocks immutable to make the BC process secure and efficient, which is the ultimate goal. Throughput and concurrency are also an issue; devices in IoT concurrently generate a stream of data [41]. Throughput is limited in BC due to its consensus mechanisms and cryptographic security protocol. A large amount of bandwidth for new blocks in the BC is required to improve throughput [42,43]. Thus, increasing throughput in BC is challenging to meet the need for frequent transactions in IoT systems. A bottleneck of an IoT-based advanced computing paradigm is that it generates a vast amount of data that results in a poor quality of service (QoS) [44].

Healthcare systems are transforming into smart healthcare environments with the advancement of computing and communication technologies. This encourages practitioners and researchers in the field of ICTs to implement their expertise to address the requirements of the health sector. Moreover, interdisciplinary researchers in the field of information systems and healthcare automation systems research new ideas productively and efficiently, constituting the IoHT evolution. However, smart health adopts ICT-based healthcare solutions with different expectations. It is important to note that the paradigm defined here as IoHT has a different meaning. It can be defined as information technology for intelligent health management in medical services. Like I4.0 revolutionized the manufacturing sector, IoT is revolutionizing e-health and its whole ecosystem. With technological progress, it is difficult for operators and stakeholders to keep pace because of the fundamental multidisciplinary nature of IoHT. Although several studies present I4.0 either at a technology base or as single ICT applications in the healthcare sector, there is no notable contribution in the field of intelligent and secure health care [45]. IoHT lies in the field of research that raises the use of biosensors, wearables, and other medical devices to improve patient data management in hospitals, decrease hospitalization times, and enhance patient healthcare delivery. However, the use of IoHT in hospitals raises many challenges; therefore, any technology that deals with healthcare must focus on privacy, security, safety, and trust, which needs to be identified as the basis for developing IoHT systems.

In this paper, we have systematically investigated the literature for the scope and purpose of our article. First, the background of IoT with detailed architecture, benefits, risks, and security requirements is discussed. Second, the background of BC is discussed with basic concepts of BC applications. Moreover, BC viability is discussed as a sustainable solution for enhancing the security and transparency of IoT applications, such as IoT-based health monitoring. Lastly, the convergence application of BC, IoT, and machine learning (ML) for secure internet of health things (IoHT) is discussed. For this purpose, we searched and selected articles related to the following keywords: IoT, BC, e-health, IoT security, ML, deep learning, AI-based IoT, BC-based health monitoring, e-health, Internet of Things, healthcare IoT, and ML for health monitoring. First, as selection criteria, we searched and selected articles from journals indexed by the web of science. Then, an excel-based database was created from the searched papers, and a query was applied to the database's list of papers selected from 2016 until 2022 (IC2). A total of 384 articles were searched, out of which 102 were collected from IEEEXplore, 71 from ScienceDirect, 59 from Springer Link, 41 from MDPI, 26 from ACM Digital Library, and 85 articles from other sources.

Moreover, after scanning the abstracts, these articles were thoroughly read and considered based on the English language (IC3). Another selection criterion was health-related papers based on IoT, BC, healthcare, e-health, and ML (IC4). The articles were excluded based on the type of the research study, such as a systematic review or literature survey (EC1). In addition, articles not focused on IoT were subjects for exclusion (EC2). Other exclusion criteria included were articles that are not mainly focused on healthcare applications (EC3). Relevancy was another criterion, for instance, articles that are not relevant to BC, IoT, ML, and DL (EC4). This study aims to answer the following research questions:

- What is IoT and its application in healthcare?
- What is BC and the applications of BC in healthcare systems?

- What is ML, and how can ML applications enhance pervasive computing-based healthcare systems?
- What are the convergence trends of IoT and BC for healthcare applications?
- What is the applicability of ML in IoT-based systems?
- What are the challenges of developing integrated healthcare platforms based on IoT, BC, and ML?

This research study was conducted to find answers to the above research questions. First, we provide a brief literature review to aid in readers' understanding of the background of IoT, BC, and convergence of IoT, BC, and ML for the internet of health care applications. Second, we summarize the contributions more relevant to healthcare. Finally, the main challenges and solutions for intelligent and secured IoT-based health monitoring applications with main benefits are discussed. A summary of the comparative analysis of this study with existing survey papers is presented in Table 1.

Table 1. Comparison of this study with existing survey papers.

S.No	Study	Publication Year	BC	ML & AI	IoT	Remote Patient Monitoring	Access Management	Healthcare Challenges & Related Solutions	Solutions for Secure and Intelligent IoHT
1	Shailaja et al. [46]	2018	No	Yes	No	No	No	No	No
2	Panarello et al. [47]	2018	Yes	Yes	Yes	No	No	Yes	No
3	Faust et al. [48]	2018	No	Yes	Yes	No	No	No	No
4	Kuo et al. [49]	2019	Yes	No	No	No	No	No	No
5	Ahmadi et al. [50]	2019	No	No	Yes	Yes	No	No	No
6	Aggarwal et al. [51]	2019	Yes	No	Yes	Yes	Yes	Yes	No
7	Andoni et al. [52]	2019	Yes	Yes	No	No	No	No	No
8	Naser et al. [53]	2019	Yes	No	Yes	No	Yes	Yes	No
9	Wang et al. [54]	2019	No	Yes	Yes	No	No	Yes	No
10	Qadri et al. [55]	2020	Yes	Yes	Yes	No	Partial	Yes	No
11	Qayyum et al. [56]	2020	No	Yes	No	Yes	No	No	No
12	Karthick et al. [57]	2020	No	No	Yes	Yes	No	Yes	Yes
13	Hosseinzadeh et al. [58]	2021	No	Yes	Yes	Yes	No	No	No
14	Uddin et al. [34]	2021	Yes	Yes	Yes	Yes	Yes	No	No
15	Yaqoob et al. [59]	2021	Yes	No	Yes	Yes	Yes	Partial	No
16	Mostafa et al. [60]	2021	No	yes	yes	Yes	No	No	Yes
16	Proposed survey	2022	Yes	Yes	Yes	Yes	Yes	Yes	Yes

The significance of this study is explained by the research questions and the comparison of our study with recent surveys and review studies. Our survey is based on the applications of IoT, BC, and ML in healthcare. Nevertheless, we attempted to survey the studies for futuristic secure, and intelligent internet of healthcare things. The overview of key contributions of this survey paper is as follows:

- This study presents a detailed background of IoT and BC to understand the core of IoT and BC for healthcare applications.
- This study presents the requirements of IoT in healthcare applications.
- This study provides trust and security solutions based on BC for IoT-based healthcare applications, such as remote health monitoring in smart hospitals.
- This study presents the background of IoHT and its enabling technologies.

- This study also highlights BC and ML-based solutions to address the current issues and challenges of secure and intelligent IoHT.
- Lastly, this study presents the limitations of the enabling technologies and research challenges and directions.

The rest of the paper is organized as follows. Section 2 presents the background of IoT, and Section 3 presents the background of BC. Section 4 presents enabling technologies for secure IoT-based healthcare applications. The convergence of BC, IoT, and ML for secure and intelligent healthcare applications is also discussed in Section 4. Section 5 presents the research gap and optimistic solutions for the future research directions in the IoHT. Finally, the conclusion of the study is presented in Section 6.

2. IoT Background

In this section, a brief background of IoT is discussed, including IoT architecture, the difference between current IoT and traditional networks, the security needs and performance of IoT systems, and the threat and intrusion detection environment. The scientific community presented many applications of IoT in daily life [61]. Today, the scope of the interaction of end devices and networking technologies from IoT applications' internal composition is broadened. Two essential features associated with IoT are heterogeneity and decentralization. Decentralization property is critical in the case of analyzing a large amount of data from hundreds of IoT devices, such as in the case of smart cities. Data collection from IoT devices and recording and analyzing such data are decentralized. Furthermore, decentralized algorithms can improve the IoT network's scalability and capacities. For instance, decentralized computation and clustering algorithms were implemented in wireless sensor networks (WSN) [62]. The increase in the rate of IoT devices in IoT networks is growing continuously due to the growing demand for IoT frameworks.

2.1. IoT Architectures Initiatives

IoT products lack standardization, due to which the world cannot agree on a specific IoT reference model [63–65]. The five-layered models contain the perception layer, services management or middleware layer, application layer, and business layers. The object abstraction layer works similarly to the network layers implemented in all other models. However, the function of this layer includes transferring and receiving data from devices in the next layer from the middleware or service management layer using different communication protocols. These communication protocols include RFID, 3G/4G, Wi-Fi, Bluetooth low energy (BLE), infrared, and ZigBee, to name a few. Management to control access to data provides an interface to business for data analysis, and service delivery to users is performed by the application layer. However, a four-layered architecture shows the difference between perception and physical layers. The business layer manages services and activities, such as business models and extensive data analysis for decision-making [66,67]. The physical layer has smart appliances in the network settings, such as smart objects of power supplies. Collecting sensor data is the responsibility of the perception layer, while the transfer of data among devices is done in the network layer. Finally, the application layer delivers service and provides a platform for data analysis.

The three-layered architecture model presented by Khari et al. can be compared to the previously discussed IoT architecture containing the sensor, network, and application layer. The functionality of each layer is the same as in the previous two models. However, the functionality of the layers is approximately similar. Another four-layered architecture consists of the sensing, networking, cloud, and application layer. The cloud computing layer was replaced by the service management or middleware layer in the previous architectures. Data analytics and storage capacity are better when the cloud servers have more computing power, thus performing better data analytics on massive heterogeneous data from IoT devices. In addition, the interoperability aspect is affected by proprietary protocols used in the middleware services. Another issue caused by middleware is disguising the differences in network protocols and operating systems. Moreover, middleware services among

incompatible protocols of subsystems suffer from time delay and memory overhead, while the cloud servers ensure the communication for heterogeneous systems flawlessly. Table 2 presents IoT architecture initiatives.

Table 2. IoT architecture initiatives.

S.No	Architecture	Description
1	SAM [68]	Proprietary DIY IoT platform with offline access and cloud support
2	IEEE Project P2413 [69]	Allows compatibility among heterogeneous frameworks
3	IoT-A [70]	Architecture Reference Model (ARM) for the inter-working of IoT platforms
4	iCore [71]	An IoT platform handling the heterogeneity and facilitating user-level management
5	TRESCIMO [72]	Smart City M2M Connections Test-beds
6	Glue.thing [73]	Proprietary DIY based IoT platform
7	FIWARE [74]	Software development in IoT using APIs
8	Node-red [75]	Web-based flow editor, open source IoT platform
9	Dweet.IO [76]	Open source middle-ware simply shares data using web-based RESTful API based on the IoT platform
10	Particle.IO [77]	Exclusive middle-ware based fully-integrated IoT platform
11	COMPOSE [78]	An Open Market in a collaborative fashion to allocate things at your service
12	IoTDM [79]	Middle-ware that act as M2M's information broker
13	OneM2M [80]	Handle the vertical heterogeneity, vertical applications connectivity

2.2. Benefits and Risks of IoT Adoption

The realization of IoT in healthcare still needs an understanding of its impact on different industries in terms of risk analysis. The impact on organizations means effects on data generated from IoT networks. In ref. [81], the authors presented three main characteristics of IoT, which are “Big,” “Open,” and “Linked.” Compared to the previous conventional techniques, extensive amounts of data with high quality and enhanced accuracy, diversity, and timeliness generates data referred to as big data. When the data are prepared for a specific aim and can be used for several other purposes to achieve different goals, it defines the open characteristic of IoT. IoT combining data from multiple sources with traditional sources defines the linked characteristics. Different sensors can be installed with regulations and public safety and considerations of diversity in IoT technology to ensure compliance. Moreover, smart governance and teamwork result from big data analytics based on secure and accurate data provided by IoT applications among collaborating agencies. In ref. [82], researchers noted that IoT in the asset management domain is also progressing to observe the health and quality of industrial assets. A person's privacy can be impacted by data leaks, such as asking about health conditions and personal financial status, etc. To prevent misuse of resources, it is crucial to prevent unauthorized access [83]. However, to uncover unforeseen sights, big data can be used. Therefore, to convert big data into practical information, the duality of IoT can be sighted in changes to industries, which is essential. However, standard data storage architecture is not accepted universally, nor is the quality of data clear. At the same time, the adoption of IoT has high costs and risks due to a reduction in return investment [84].

The data are made available by the IoT data feature for general open use. Advantages of making information open to the public include ensuring organization transparency, improving business processes, and reducing waste. Citizens and businesses can be empowered by enabling consumer services through better information gain. However, as IoT provides flexibility in business value delivery, better decision making, and service efficiency, the industries need to observe the situation in real-time. IoT allows other devices to use publicly published data on the IoT network while publishing and sharing information. A mature set of protocols is needed to guarantee the accessibility of data. Furthermore, search locality, scalability, and real-time processing are substantial barriers to IoT adoption

due to the mechanism of the current search that relies on remote information sharing and fails to provide local entity search efficiency. Technical and regulatory barriers are security, data sharing, and ownership. Reducing labor costs and empowering the community by providing consumer self-service are the advantages of using the linked feature of IoT. In addition, linking data from several sources can also develop consumer trust and detect fraud. Eventually, the organization can use insights gained from linking data from various sources to communicate effectively, support additional service revenues, and create new opportunities for interaction.

Furthermore, the insights collected from the processed big data can enhance efficiency, effectiveness, and compliance [85]. However, the collected data are from different sources due to diverse IoT applications. Furthermore, the user of these data is also different, and linked data use a different technique for processing these data. This feature complicates the design of IoT architecture. Furthermore, due to its challenging policies and lack of guidelines, achieving benefits from IoT adoption can be difficult. Due to this difficulty, limited education, training institutes, shortage of skilled staff, and new organization processes are needed [86].

2.3. Requirements of IoT in Healthcare Applications

First, the related security prerequisites must be resolved before estimating the potential security threats in the IoT healthcare system. Security prerequisites for IoT were studied and determined by researchers [87–89]. A few major security requirements for IoT are listed below:

2.3.1. Confidentiality

Confidentiality focuses on information hiding from unauthorized users and can be described using two steps. The first step is to ensure that unauthorized users do not access confidential data. The second step is to protect the proprietary data, and confidentiality should be guaranteed. Encryption schemes, asymmetric and symmetric, can contribute toward ensuring data confidentiality.

2.3.2. Integrity

Integrity ensures that unauthorized users cannot change or alter the data within IoT nodes. Integrity comprised by the most launched attack is the man-in-the-middle attack [90], which modifies data by intercepting its path before it is passed to its original receiver.

2.3.3. Authenticity

Authenticity guarantees that the origin of the information and transactions is authentic. The individuals involved in the operation must be the ones they claim to be. Authenticity contributes to preserving the authenticity of data through cryptographic digital signatures [91].

2.3.4. Non-Repudiation

Events or tasks that occurred and cannot be denied later are the responsibility of non-repudiation. Generally, the user's ownership cannot be refused by the users after performing a send or receive operation.

2.3.5. Authorization

The authority to perform some operation assigned to any user is the responsibility of the authorization. Therefore, the data and other network services to authorized users should be available all the time. Data and computational power resources must be available whenever a service requires them. Furthermore, all components need to work correctly, such as computation systems needed to analyze data, the IoT nodes responsible for the communication links, and data capture [92,93].

2.4. Security Challenges in IoT-Based Healthcare Systems

In IoT systems, security is a high priority due to different types of interactions in a virtual and physical world. In addition to addressing traditional networking attacks, the deployed IoT protocols need to provide secure communications [94,95]. The list of most significant security challenges in IoT systems is given below:

2.4.1. Data Volume

Critical and confidential data generated by different IoT applications, such as smart hospitals, and smart homes, cause security risks.

2.4.2. Privacy Protection

Sensitive data inside IoT nodes must not be linkable and traceable and must be protected to be identifiable. Moreover, data are processed in today's interconnected world, sent, and collected by large enterprises using multiple IoT devices, raising privacy concerns.

2.4.3. Resource Limitations

Even security protocols are not supported by these devices, such as asymmetric key encryption or other advanced privacy-preserving techniques, and the reason for this is limited computation power and memory [96].

2.4.4. Scalability

An efficient technique for security and confidentiality needs to be carried out through the IoT network because an IoT system involves many network nodes. Heterogeneity means the connectivity of IoT devices with different identities, release versions, and technical interfaces to perform different functions. Therefore, IoT needs to handle different devices and situations and connect among heterogeneous networks and things [97].

2.4.5. Interoperability

In an IoT system, security should not restrict the operational capabilities of IoT nodes. Many issues are caused by interoperability, such as difficulty developing cross-domain IoT applications, non-interoperable device implementation in heterogeneous systems, and user satisfaction.

2.4.6. Autonomous Control

The configuration is needed from users in conventional data systems. However, the setting must be developed autonomously in the end devices in the IoT network. Moreover, in IoT systems, end devices are tiny to secure, such as fixed devices that can be easily destroyed by natural disasters or sensors or mobile phones that can be stolen [98].

2.5. Security and Intrusion Attacks in IoT Systems

With the increase in the number of devices in IoT systems, the increase in vulnerabilities causes security attacks in IoT. For example, if it leaks, data encryption and access control enable attackers to launch attacks, such as eavesdropping and traffic analysis [99–101].

2.5.1. End Device Attacks

One thing that affects confidential data, such as certificates and keys, is that the attacker physically stops devices and controls them. At the same time, malicious users pretend to be authentic, orchestrating other attacks by providing the seized information [102].

2.5.2. Communication Channel Attacks

In some cases, if the communication channels are not encrypted, the attacker tries to intercept the communication and gain access to confidential data. Sometimes they try to interfere with or jam wireless channels by transmitting noisy or corrupt signals.

2.5.3. Network Protocol Attacks

Many attacks, such as blackhole attacks, Sybil attacks, wormhole attacks, denial of service (DoS) attacks, and reply attacks, are caused by vulnerabilities in network protocol. Therefore, these attacks would degrade the performance and precision of protocols [103].

2.5.4. Sensory Data Attacks

In the IoT system, ad hoc protocols are used for communication. Messages in the system are transferred hop by hop until they reach a destination, allowing attackers to modify data, which characterizes the process by which attackers modify data and broadcast it to other hosts [104]. Attackers transfer data with an authentic identity called data infusion or corrupt data. In a DoS attack on an IoT system, the system's resources are consumed so that they will not be available to the users on request [105]. However, these attacks consume many resources, such as energy reserves of sensory nodes and network lifespan mitigation, and paralyze entire networks [106].

2.5.5. Software Attacks

Mutating and controlling the entire system by using software loopholes is called a software attack. Malicious scripts, worms, or viruses are base of these attacks. Intrusion detection systems in the traditional security protocols are used to prevent such attacks [107].

3. Background of BC

BC is the technology behind the virtual Bitcoin cryptocurrency developed by Satoshi Nakamoto in 2008, and it can be defined as a decentralized, transparent ledger on a peer-to-peer network that contains data units called transactions. A collection of transactions is called a block. In a distributed ledger, a BC is created with all confirmed blocks, and each block is linked to the previous block using the cryptographic hash code of the block [108]. In BC, every participant on a peer-to-peer network can approve and verify the behavior and transaction of other participants. This infrastructure is resistant to tampering and reduces the vulnerability of a single point of failure. A consensus mechanism principle imposes a mutual agreement and strict rules among network nodes. The network authorities do not regulate it. Therefore, a BC ledger is available to all members, and the consensus mechanism refers to a process in BC to synchronize the decentralized ledger across all nodes.

The number of consecutive blocks connected to form a chain of blocks is termed BC, and the first block is called genesis. Each block in the chain is connected to the previous block with a hash code, and each block contains timestamp, nonce, and transaction history. The central concept is decentralization [109–112] and security in BC, where each node is a device that stores data securely. The BC system ensures security for each transaction made. Satoshi Nakamoto et al. stated that BC is not based on the third-party Bitcoin, with the first block created in January 2009. The timeframe between 2009 to 2013, referred to as BC 1.0, represents Bitcoin, and the next two years as BC 2.0, where smart contracts and cryptocurrency helped improve the financial area. During this duration, bitcoin-based trading and currency exchange existed, where investment in BC started from \$93 million to \$550 million in two years from 2013 [113] and grew to \$2.3 billion in 2021. Overall, BC is composed of three core parts, the block, chain, and network. A block stores information that is immutable once stored, and it cannot be modified until all other blocks validate and verify it, while the size and period depend on the type of BC. A *chain* is a function that involves the formation of a chain by linking a list of blocks leading to BC. BC blocks are considered nodes, and connected nodes form a network. Routes are considered nodes in a conventional network.

Two types of users can interact with BC, namely the reader and writer. The reader is a passive participant and can only analyze record contents and validate BC. On the other hand, the writer is an active participant who can participate in the transaction process to extend the chain by using the consensus protocol [114,115]. Thus, three categories of BC are based on the permission given to the users for interaction with a ledger. A user

can access the main chain in the consensus protocol allowed by the public BC without restrictions as a reader or writer. Mining is mainly based on incentives. Therefore, the public ledger cost is higher than a private ledger. Furthermore, the time to complete a transaction is longer in public BC than in private because of less connectivity in nodes [116]. Some examples of public BC are Bitcoin, Zerocash, and Ethereum [117]. In a private BC, the number of nodes is limited; they can be identified, and to selected miner nodes, only participation in the transaction is available. Compared to the public BC, a private BC is more confidential in terms of user information, and the user only has access to the data linked with him. As a result, transaction throughput is greater because committing transactions is less, and the transaction speed is faster [118]. Examples are multichain [119] and Quorum [120]. Consortium BC developed the aim for when the specific industry faces difficulties in scaling the effect of cooperation. It is a hybrid of private and public BC and is closer to private [121]. Moreover, it is decentralized and under the supervision of a particular group [122]. A multi-party consensus exists in which only predetermined nodes can authenticate all of the operations. A node can establish its instructions, modify account balances, and modify or delete erroneous transactions if all nodes agree and consortium BC execution is weak against malicious nodes due to its centralized feature. Table 3 presents a summary of the known types of BC.

Table 3. Summary of known types of BC.

S.No	BC Types	Description
1	Public BC	The transaction is open to the public for verification Open source public can read code
2	Private BC	Only trusted parties can participate, validate and verify a transaction
3	Consortium BC	Semi-private, which users of different organizations control Second largest open source enterprise BC
4	Enterprise Ethereum BC	Use for general purpose Facilitates smart contracts and distributed apps dApps Open-source
5	Enterprise Hyperledger Fabric	Permissioned distributed ledger developed by the Linux Foundation-hosted Hyperledger consortium To interact with Hyperledger Fabric Network, clients use SKD or REST API
6	Public Permissioned BC	Bridges the gap between the public permission-less network Examples are C3's Corda, Fabric Hyperledger Permissioned BC
7	Private Permissioned BC	Only selected participants can join the BC
8	Customized BC Customized Public/Private BC	Developers uses programming language such as Go language, C++, java, python, etc. to analyze their application performance
9	Enterprise Permission BC	Enterprise-level BC such as Hyperledger Fabric Permission needed for participation
10	Cloud BC	BC operated by third-party clouds such as AWS

3.1. Basics of BC Technology

Several research articles organize BC into different layers [123,124]. This section will discuss BC's five layers' core properties, such as security, integrity, and immutability. Figure 1 presents the layered architecture of blockchain.

3.1.1. The Data Layer

This layer manages the hash function, digital signature, blocks, and Merkle tree.

BC has a fundamental part called blocks, where the genesis block is the first block in the chain connected with other confirmed blocks, and each block in the chain has information called transactions. One information field belonging to a block is the hashtag of its previous block used to create a link between them. A typical block has two parts, namely transaction records and a header. Any modification to the block is impossible because all confirmed blocks in the chain can be traced back. Figure 2 presents the block structure of BC.

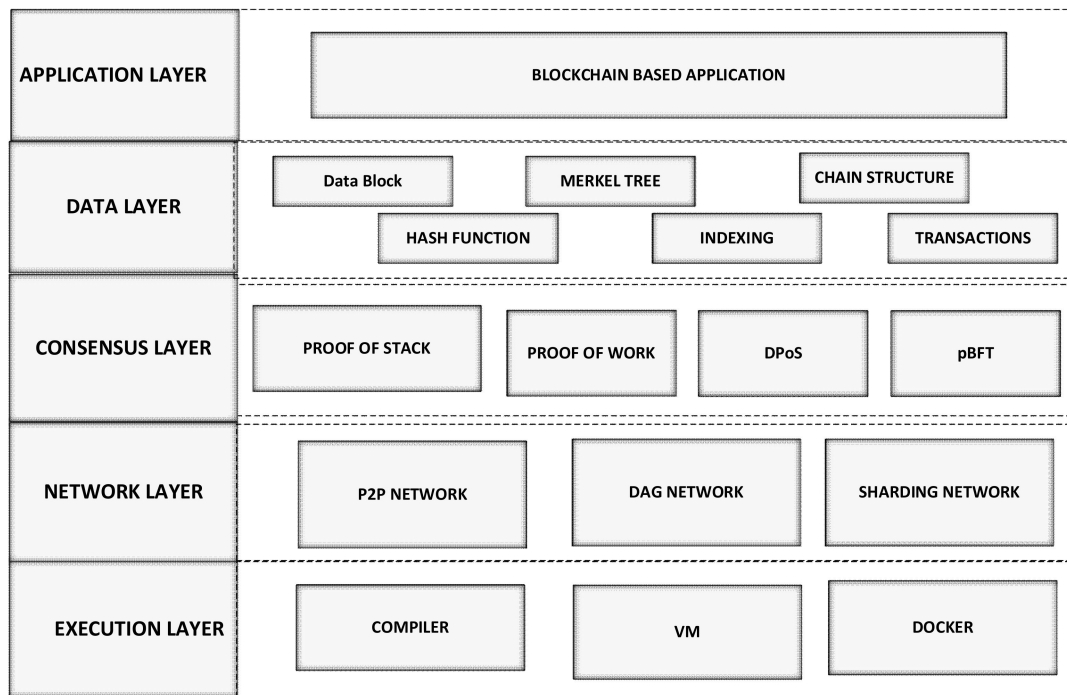


Figure 1. The layered architecture of BC.

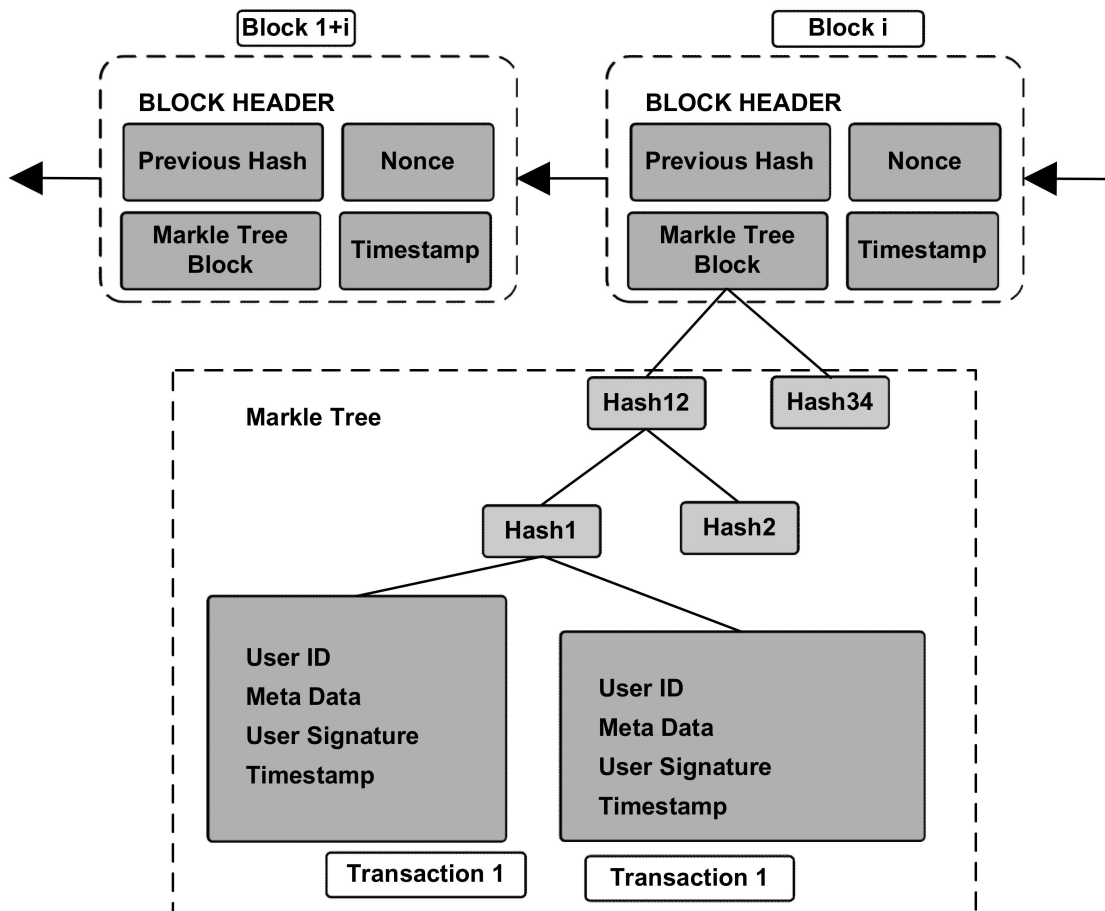


Figure 2. Block structure of BC.

Merkle tree checks and summarizes the content of large datasets securely and efficiently in binary tree structure form. Each node of the network keeps a complete copy of all transactions that the user has never committed on the BC if the transaction into Merkle trees is not packed [125]. Moreover, the Merkle tree of all transactions, generating a digital fingerprint to summarize transactions within a block, enables users to check if a transaction is included or not in a block. One field in the block's header contains the Merkle tree root that was generated while making the block. In essence, the Merkle tree or root hash involves continuously hashing node pairs until only one hash is left. The hash of the previous hash is in a non-leaf node, while the hash of transaction data is inside a leaf node. To ensure trust transactions and associated data are signed with the user's private key, they can securely exchange digital currencies or smart contracts. For authentication, the block header generally includes a hash of the previous block. The nonce uses the consensus mechanism, which generates a hash value. The time at which a block is created is known as a timestamp.

To authenticate and ensure the integrity of digital content, a digital signature (DS) can be used [126]. DS uses public-key cryptography (PKI), which uses the public and private keys as a pair but asymmetrically (not identical). The pair of keys can be shared with authorized entities that do not disclose the private key to anyone. The pair of keys can encrypt a message.

3.1.2. The Application Layer

Smart contracts, chain code, and dApps are inside the application layer of BC and are further divided into sub-layers, i.e., the presentation and execution layers. The user interface, APIs, and scripts belong to the presentation layer, while chain code, smart contract, and other underlying rules are part of the execution layer. The presentation and execution layers work together, i.e., the presentation layer informs the execution layer to execute transactions. Examples are Hyperledger Fabric receiving instructions in chain code and smart contracts in Ethereum Virtual Machine. The components of the application layer are discussed below.

3.1.3. Smart Contract

Smart contract [127], developed in the Ethereum runtime solidity language, is a bytecode produced by the compiler and is run faster on EVM. The network is isolated from the code executed on EVM, and after deploying on EMV bytecode, the smart contract is assigned a unique address. A smart contract is business logic in several functions that run when a transaction against those functions is issued. For example, a state change in a decentralized ledger results in a transaction related to a smart contract.

3.1.4. Chaincode

The chain code of Hyperledger Fabric groups several smart contracts and deploy them in the BC business network. For example, an insurance application in a chain code can group multiple smart contracts such as claim, processing, liability, etc. Furthermore, the chain code defines the schema of the ledger's data based on the consensus that initiates it. Finally, the chain code further governs packaging, deployment, and response to queries for ledger data. The chain code is run on a secure docker container, and unlike EVM in Hyperledger, the chain code is developed in many languages, such as Java, Go, and Node.js, on peer nodes. The client applications use REST API or SDK to access the chain code. According to his policy, it is initiated for a specific channel endorsed by an administrator.

3.1.5. dApps

A web application that runs on top of distributed BC technologies, such as Bitcoin, Ethereum, and Hyperledger Fabric, can interact with BC using the chain code or a smart contract known as dApp. dApp is not controlled by a single entity like a conventional app once installed on the BC network.

3.2. Performance Metrics of BC Application

Nowadays, many BC-based applications are being developed, and it is essential to evaluate performance and success for several use cases. Therefore, a comprehensive survey was conducted by Jamil et al. to assess BC performance parameters, metrics, and tools [128]. Figure 3 presents performance metrics and parameters for assessing BC-leveraged IOT applications and decentralized transaction ledgers (DTLs).

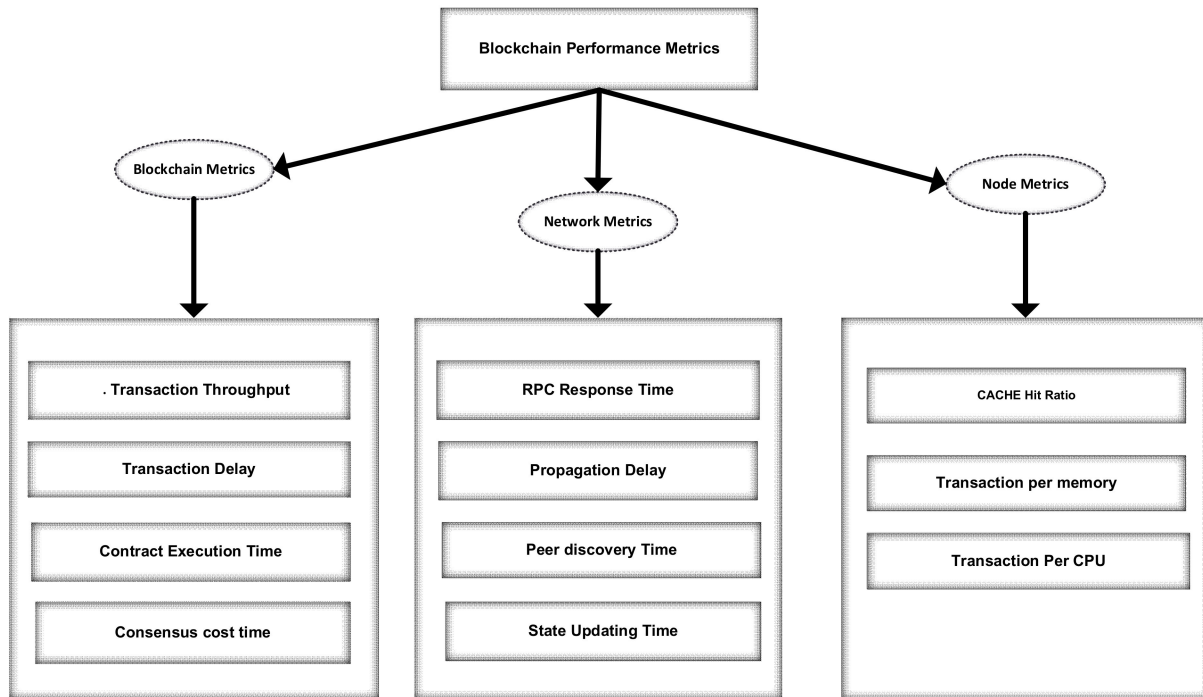


Figure 3. Performance metrics used for BC applications evaluation.

Transactions are timestamped and checked before inserting into a cryptographically protected block, using a hash technique by BC. Immutability is achieved with a chain of connected blocks so that each block header has a hash value containing metadata of the previous block [129].

4. Enabling Technologies for Secured IoHT

In 1999, the concept of IoT developed in the interconnected global network for the first time. Through wireless communication, sensing, and information processing technologies, which interacted with each other using their processing and communication capabilities, the smart object was autonomously contained in the IoT core. These concepts developed in recent years from sensing environmental data that provide applications, as well as services for communications, analytics, and exchange of information [130]. Different interpretation contexts are used for IoT depending on the application context, such as user-centric, things-centric, semantic, and internet-centric [131].

4.1. IoHT

IoT can be explicitly applied to healthcare, such as monitoring vital signs in the hospital ward. The IoHT consists of connected objects with the potential to transfer and process data to enhance patient health. This patient-centric representation comprises four different layers, described below.

4.1.1. Acquisition

Smart health objects, such as medical devices and wearables, are used with communication technologies, such as Bluetooth and Wi-Fi to collect data associated with vital signs or other physiological situations.

4.1.2. Storage

Cloud computing stores collected data that is profoundly interoperable and scalable, given its fundamental characteristics, including on-demand self-service, broad network access, resource pooling to attend to scalable demand, rapid elasticity, and metering capability. Another essential characteristic is a PHR with semantic interoperability using patient information registration.

4.1.3. Processing

Intelligent algorithms are based on ML techniques instead of traditional heuristic approaches that deal with patient data analysis. Advanced data fusion and predictive analytics are expected to better infer patient health deterioration, optimizing resources.

4.1.4. Presentation

Results generated from the combination of previous layers can be used to take the form of alerts, graphs, actions, and charts. In addition, de-identified data can be combined from different PHRs within a particular context to obtain epidemiological views [132].

Figure 4 presents the perspective architecture of intelligent and secured IoHT. The application of IoT to health assistance is still outset, but it has the potential to raise the quality of life, enhance user experience, and decrease the cost of the resources [133]. IoHT, from a healthcare provider’s view, can lessen service downtime, recognize the best time for refining supplies, and allot insufficient resources efficiently [134].

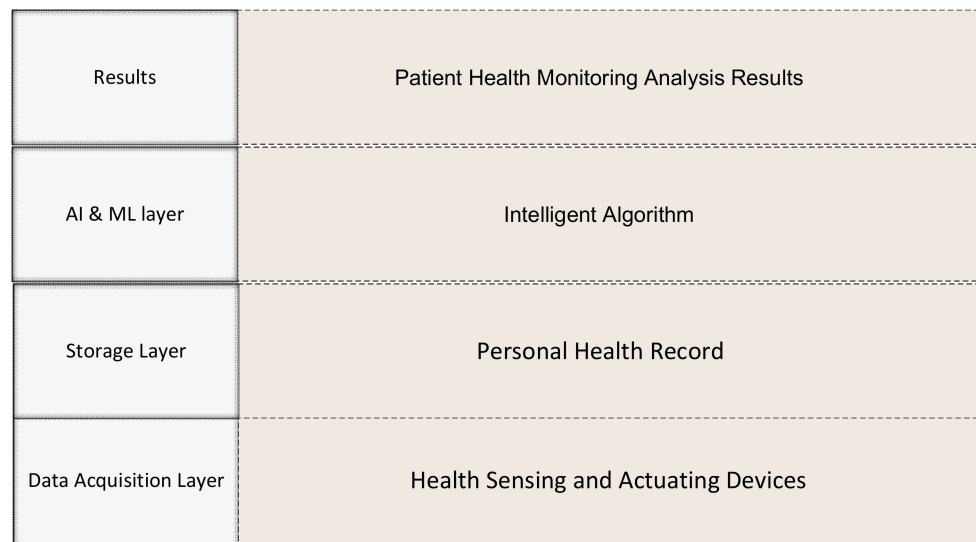


Figure 4. The perspective architecture of intelligent and secured IoHT.

Nurses can assess the level of pain or consciousness by using manual sphygmomanometers and stethoscopes, or by conducting questionnaires or manually collecting vital signs. Thus, IoHT can help achieve PCC and patient-related data using smartphones or tablets and reduce errors in registering vital signs and elapsed time instead of conventional manual annotation [135].

Another option is wearable technology, which can be used to collect vital signs [136]. One trend regarding smart health objects interconnection is to shift from manufacturing standards to using IP-based protocols, such as the IPv6 over 6LoWPAN [137]. For example,

Aung et al. introduced a solution to assess pain using sensors, including an accelerator and location sensor for activity evaluation, audio analysis of speech, and facial expression identification based on image processing that uses self-reported data [138]. Many commercial applications for pain evaluation exist for mobile devices, as highlighted by the authors. Similarly, for assessing the level of consciousness, Aung and colleagues used image processing to evaluate eye movement for assessing verbal responses and used an accelerometer to help determine motor responses. From an IoHT viewpoint [139,140], possibilities are presented in the literature for monitoring blood pressure, body temperature, heart rate, respiratory rate, and oxygen saturation. In addition, to monitor the urine output of critical patients, a device was suggested by Otero and colleagues. Various proposals employ sensors or other medical devices that communicate via RFID, NFC, or Bluetooth to a smartphone and further transmit this information to a middleware, typically inside a fog or cloud computing infrastructure. Figure 5 presents the healthcare applications of IoHT.

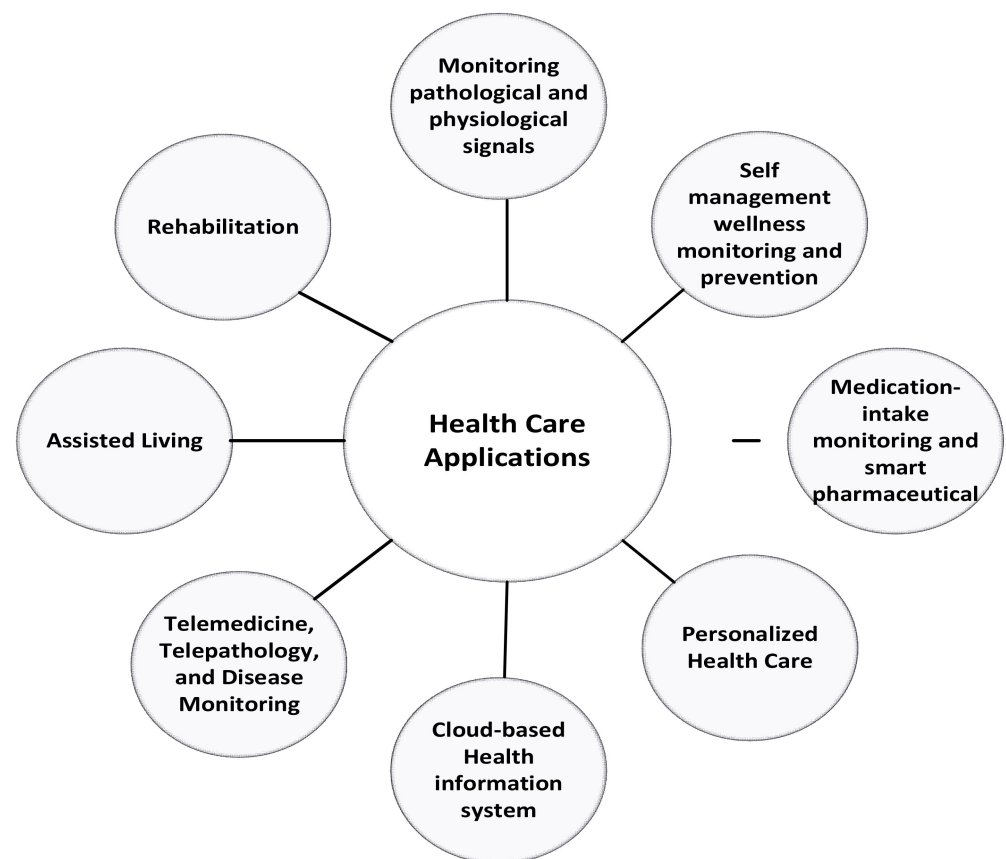


Figure 5. Healthcare applications of IoHT.

4.2. IoT-based Healthcare Applications

4.2.1. Monitoring Physiological and Pathological Signals

A framework resulting from the IoT paradigm with a combination of mobile communication technologies subsidizes applications for monitoring, such as the generation of statistical information and health records related to a health condition that can replace conventional hospital information systems [141–148]. Furthermore, this automated system lowers the risk of errors compared to manual intervention [149]. The system for remote monitoring of patients consists of three main components [150]:

- Collecting movement and physiological data by data collection and sensing hardware;
- Relaying data to the remote center using communication hardware and software;
- Extracting clinically relevant information from movement and physiological data using data analysis techniques.

Sensors adopted by applications can be either in-body or on-body [151]. In addition, the adoption of high-level environmental and medical sensors [152], such as gyroscopes, humidity sensors, accelerometers, temperature, glucose, gas, blood pressure, and ECG, enables continuous monitoring of a patient's physical and physiological conditions. Furthermore, these data are transmitted by IoT devices to remote data centers provided by cloud computing [153–155], where processing is scalable, services are highly available, and storage is infinite. However, this approach's reliable network connection for processing, remote storage, and retrieval of medical records imposes further network connectivity challenges and traffic [156]. Indeed, among the applicative scenarios, 5G brought health monitoring to the list of ultra-reliable communication requirements [157,158]. Others have mitigated these challenges to enhance the health-monitoring system by using fog computing at smart gateways, distributed storage, notification services, and embedded data mining at the edge of the network to alleviate inflicted challenges by adopting remote access cloud services [159]. Furthermore, fog computing plays an essential role in latency-sensitive applications of augmented reality; for instance, EEG-based brain-computer interfaces are leveraged by pervasive brain monitoring applications [160] or cognitive assistance systems [161]. In addition, medical devices implanted in human bodies to restore and enhance human functions are expected by fog-based architectures. These include deep brain stimulation and the heart muscle stimulation system [162].

4.2.2. Self-Management, Wellness Monitoring, and Prevention

Healthcare 4.0 highly advises a solution of self-management, which is very important. Big data allows implementing a shift from cure to restraint [163], one of the characteristics a P4 medicine proposes [164]. Researchers are designing an intelligent system rather than a simple function that temporarily indicates measured and stored data but provides valuable feedback to people. For instance, these solutions can implement algorithms that help stop diseases by designing health interventions for health behavior changes and addressing modifiable risk factors. In addition, chronic diseases, such as diabetes and obesity, are examples of self-management for healthcare where the system needs to provide fitness plan programs [165] and suggestions for empowering and educating nutritional habits [166,167].

4.2.3. Medication Intake Monitoring and Smart Pharmaceuticals

In the elderly, noncompliance with medication is expected, and medication monitoring identifies related issues, an essential tool for clinicians to manage the disease. Therefore, in the design of the early prototype, RFID and sensor networks were to be used for the elderly. In addition, many mobile apps have medication intake tracking, scheduled reminders, and prescription reminders that reduce unfavorable consequences and achieve effectiveness. Wearable, intelligent, and integrated IoT connectivity devices are advanced solutions [168]. In this context, smart pharmaceuticals can be defined as electronic packages and delivery systems for communication to a remote system allowed by internet communication that can analyze, compile, and store the data [169].

4.2.4. Personalized Healthcare

All user-centric plans belong to personalized healthcare, such as making patient-specific decisions [170,171]. Data collection from multiple sources is essential because the analysis of these related data facilitates health and social care decision-making and delivery. Typical sources of I4.0 vision, such as defibrillator vests, fall detectors, and implantable insulin pumps, are wearable therapy delivery devices or sensors. These sources are considered under the P4 medicine paradigm to profoundly highlight its reliance on the genetic information of each individual [172–174]. Indeed, understanding the biology of each individual comprehensively impacts diagnosis, pharmacogenomics, predisposition, prognosis, predisposition, and surveillance [175]. Therefore, big data needs to implement personalized healthcare for both individuals and populations [176].

4.2.5. Telepathology, Telemedicine, and Disease Monitoring

In 1980, the first practical telepathology endeavored while integrating video imaging. Moreover, the seminal availability of broadband communication and robotic microscopy was envisioned as the supporting infrastructure for telepathology services [177]. That resulted in how ICTs to support telepathology, disease monitoring applications, and telemedicine [178]. The available studies can be classified into two classes: the generic frameworks' applicability use cases and the concentration of works on diabetes, cancer detection, cardiovascular diseases, Parkinson's, and Alzheimer's. Thus, these monitoring systems can adopt and feed informed treatments and large-scale studies tailored to specific individuals' results. Furthermore, video cameras integrated into the operating room are expected in the future, seeing that it opens the door for open surgery and avoids the physical presence of consultants, as well as allowing an unlimited number of observers to watch the surgical procedure. Telesurgery is another application of this scenario in which the surgeon in his cockpit is physically isolated from the operating room [179].

4.2.6. Assisted Living

The increasing aging population raises many issues and challenges for the world population. The need for better nutrition and healthcare is concerned with increasing the cost for elderly patients monitored with chronic health conditions [180]. The idea of aging in place has been proposed to allow patients to remain in the home and avoid hospitalization; this is called an enhanced living environment. Remotely monitoring patients is required for safety and for facilitating the implementation of clinical medications. To better connect older people without moving, robotic and telepresence video conferencing solutions have been suggested [181]. To measure disabilities and health conditions, parameters that can be used are heartbeat rate, blood pressure, accelerometer data, and wearable sensors. Thus, WBAN technologies are most important for assisted-living facilities. To create an ambient-assisted living, WBAN was used with ambient sensors, where parameters for a living environment can be discerned using artificial intelligence techniques, such as automated learning. In case of emergency, healthcare centers can be alerted if usual activities are detected [182], while in less urgent emergencies, medical engagement is proposed [183]. Fog and cloud technologies provide the on-demand infrastructure that collects patient data in real-time and processes it all, creating pervasive healthcare that is supportive [184].

4.2.7. Rehabilitation

Home-based rehabilitation with assisted living is expected to bring patients a better quality of life and significant cost savings for the healthcare system. WBAN technologies are a primary tool that detects and follows humans' associated movements with rehabilitation practice. Unlike generic assisted living solutions, there are many requirements and specific constraints in home-based rehabilitation. Solutions associated with home-based rehabilitation are real-time patient feedback, multi-sensor data fusion, and virtual reality integration [185,186]. The role of WBANs in home-based rehabilitation is associated with biofeedback. Users provide feedback with data from measuring a physiological activity, enabling them to control their physiological activities to improve their health performance [187,188].

4.3. Convergence Applications of IoT and BC

BC-based IoT applications were discussed in the literature, with a detailed analysis of the essential aspects of the development of BC-based IoT applications and their current challenges [189–193]. For instance, Imran et al. highlighted the advantages and challenges of implementing BC into IoT applications. The surveys, as mentioned earlier, were extended by analyzing the improvements and challenges of BC-based IoT applications, studying different existing BC-based IoT platforms, and evaluating their performances. Contrary to that, BC technologies can manage challenges associated with IoT. In addition, data structure and consensus protocol enhancement that can fulfill the BC-based IoT application

requirements alongside manipulating their challenges were discussed. Few studies have reviewed the security specifications to develop BC-based IoT and IIoT solutions and explored how the implementation of BC with its intrinsic properties can enhance better security in IoT and IIoT applications. Finally, performance benefits of BC technologies and BC-based IoT applications against IoT requirements were collected, highlighting practical issues that result from the implementation of BC in IoT [194–199].

In this section, we discuss the scientific community's perspective of BC-based solutions and objectives for meeting the challenges of IoHT that were discussed in the earlier section on the IoT background. Decentralization is a salient feature of BC that solves a single-point-of-failure problem in IoT [200]. In addition, as the data are put into the blocks of a peer-to-peer network, the BC system opposes malicious attacks and technological malfunction. Therefore, the availability or security is not endangered even if any node goes offline, while old databases use multiple servers and are highly prone to cyber-attacks and technological failure. BC is more secure and reliable from many perspectives [201]. The transaction is encrypted and linked to the previous transaction as approved. Information is put on a network of computers rather than a single server, stopping attackers from jeopardizing transaction data. Public and private key infrastructure is used to further strengthen security. Authentication of assets, fraud prevention, historical data transactions to assist, and tracking goods in a complex supply chain are easier in BC than in a conventional ledger. Transactions history is transparent on the BC network as all transaction histories to all participants are available on the distributed network. Every node keeps an identical copy rather than in a conventional system in which each node keeps individual copies. In addition, a consensus process is used, which means all nodes agree to approve modifications, and all users have equal rights to link, track, and verify a transaction, which results in accuracy, robustness, and transparency. The immutability feature in BC is a prominent feature that protects data from alteration [202]. Therefore, BC uses immutable hash chains and digital signatures to archive data transactions and events in a preserved, authenticity-guaranteed manner. BC reduces operating costs by requiring no third parties and infrastructure deployment that guarantees business operations [203]. Transactions are timestamped and checked before inserting into a cryptographically protected block using a hash technique by BC. Immutability is achieved with a chain of connected blocks so that each block header has a hash value containing metadata of the previous block.

The IoT connects objects, goods, and individuals that allow data capture from embedded processors, actuators, and sensors to centralized or cloud servers. IoT analytic tools employ these data to contribute to new services and develop new business ideas. However, the privacy and security of the IoT ecosystem is a paramount concern that, on a large scale, affects its deployment, and it is vulnerable to security, such as malicious attacks, distributed denial of service (DDoS), and ransomware attacks. Figure 6 depicts the convergence applications of BC and IoT in a smart healthcare environment. Ensuring and securing the trust of data shared between heterogeneous IoT devices met by the common BC assures data immutability. Therefore, BC with decentralized architecture provides a feasible solution for IoT systems.

BC can be used as an auditable log of events, security, and TxS as per the type of IoT application, and the smart contract [204] can control and monitor access rights to the sensor or user, set policies, and execute many actions on predefined conditions. An issue related to bandwidth appeared in BC due to a complete replication mechanism where every node stores copies of all the blocks [205]. Moreover, the quality of the decentralized consensus process shows that BC nodes exchange BC-related information to join the process of consensus, validate TXs, and create new blocks [206]. Bitcoin-derived BC protocol uses a gossip protocol to broadcast all state modifications to the distributed ledger to all the nodes joining the consensus process. Bitcoin BC is permissionless and public. Anyone can participate and join the consensus process. Thus, the node with the smallest available bandwidth will become the network bottleneck. Moreover, with the increase in BC size, bandwidth, computing power, and storage requirements are required for participants who

join the consensus process. Hence, the issue of centralization occurs if some nodes cannot process BC.

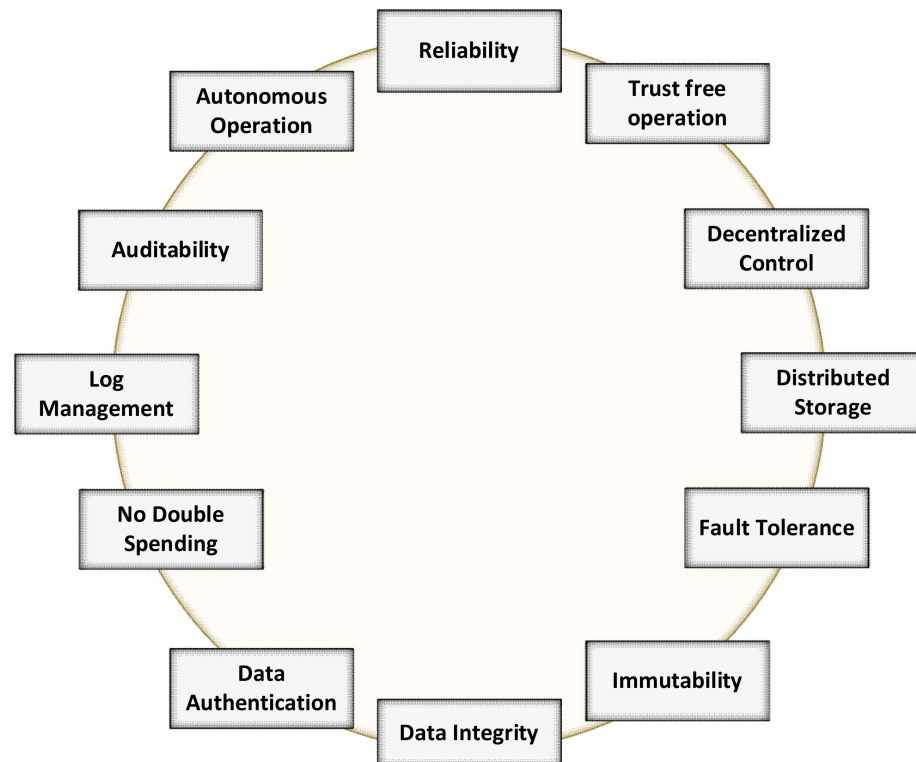


Figure 6. Integrated healthcare applications of BC and IoT.

E-health framework-related state-of-the-art works are reviewed in this section. E-health allows and offers medical benefits and hospital services to people to avail their health services fast. Using BC in e-health can address critical privacy and security issues and make e-health decentralized [207–209]. Research studies have used technologies such as BC, IoT, cloud, and fog to share data, manage storage, and secure networks. Using these technologies is the researchers' primary purpose. Some of the applications use patented blockchains developed for their appropriate requirements rather than open-source blockchains similar to Ethereum and Hyperledger.

BC technology solved some issues of healthcare systems inherent in traditional client-server data management systems, such as data stewardship, data privacy, and single point of failure. MeDShare, a BC-based system, proposed to solve such problems as data sharing among medical custodians by implementing access control and smart contracts to trace the data behavior and revoke access from the offenders in case of permission violations. In ref. [210], the authors implemented BC to simplify patient-centric operability in healthcare. A parallel healthcare system (PHR) based on AI, computational experiments, and parallel execution, relies on consortium BC to connect patients, health bureaus, and hospitals to enable data sharing, careful inspection, and review of medical records [211]. Private BC and smart-contract-based protected health information systems proposed by Griggs et al. achieve secure medical records storage by defining granular access rules. The GuardHealth framework provides data sharing based on consortium BC to maintain authentication, confidentiality, and efficient data preservation [212]. A summary of the convergence applications of healthcare based on IoT and BC is given in Table 4.

Table 4. Summary of convergence applications of IoT and BC for healthcare.

Application	Contributions	Year—References
BC for Healthcare	“GuardHealth” framework based on consortium BC for secure data sharing	2020—Wang et al. [212]
	MeDShare for effective data sharing among medical caregivers	2017—Xia et al. [209]
	Patients direct clinical examination by using IoT-enabled medical devices	2020—Celesti et al. [213]
	Using BC technology simplifies patient-centric interoperability in healthcare	2018—Gordon et al. [210]
	The framework used to implement BC in EHRs	2019—Shahnaz et al. [214]
	Consortium BC is used to connect patients and health centers and enable healthcare audibility, share data, and review medical records	2018—Wang et al. [211]
	Patient pivotal healthcare system for data management	2019—Omar et al. [211]
	By utilizing Smart contracts and BC to maintain PHI	2018—Griggs et al. [215]

In the current e-health system, most patients do not have access to their EMR system, and the patients that have access do not want a duplicate of their medical data or unnecessary tests. Patients are enabled by BC to fully control and access their medical records, which impacts efficiency and costs in healthcare and solves the issues for remote patients that access their data from outside by providing authorization and integrity of data.

4.3.1. Hospital and Drug Management

A cloud-driven model that uses front-end technologies, such as HTML and JavaScript, is based on a BC-based vital sign monitoring platform developed by Jamil et al. that helps patients in hospitals equipped with wearable sensors to transfer vital signs to nodes on BC networks [216].

Product-centered services are provided by BC using REST API, which is triggered by web clients or IoT devices.

The system ensures patient vital sign information confidentiality and consistency with data and a hosted BC ledger. Vital sign transactions are stored in a couch database installed on the nodes in the P2P network of BC. Hyperledger Caliper is used to evaluate system performance [217] in terms of several matrices, such as transaction latency (TL), transaction read latency (TRL), read throughput (RT), and transaction read throughput (TRT). The cloud of federated hospitals is connected with an e-health system by using Ethereum BC to make a telemedical laboratory, and the proposed healthcare system is only described while performance analysis is not performed to measure the feasibility of a system. In healthcare, patients are forced to perform tests and purchase medicine from clinics that physicians prefer due to inappropriate regulations and national policies. In addition, patients’ health data and medical tests are mainly controlled by physicians who do not allow patients and irrelevant persons to access them. Therefore, the patients perform those tests outside twice. To overcome this issue, a composite system for concocting multimedia generated from IoT healthcare based on BC has two types of nodes, executing nodes and miner nodes, and NS2 is used for simulation [218].

BC can track and secure the entire drug distribution process in the supply chain to avoid diluted drugs. In a drug delivery system, BC records every transaction generated in the drug production process in a permissioned BC, which archives traceability and transparency and avoids drug dilution, thus allowing authorities to trust the method. A cloud-based framework combined with BC and IoT connects a data-sharing platform with a data management system by decentralizing the mobile BC network. Still, scalability and communication cost were not examined; however, privacy and integrity are guaranteed. Researchers have tremendous interest in making data storage stable and secure using BC

technologies in healthcare. Still, few countries, such as Peru and Estonia, used BC for managing health data. A private health management system based on BC was introduced in Peru. The system used the cloud services of Amazon to control the medical supply chain and ensure security between clients, sales managers, and manufacturers. The drawback of the system is the lack of consideration for the confidentiality of the data [219].

4.3.2. Privacy Preservation in E-Health

In e-health, it is essential to preserve privacy between patient and physician to achieve quality treatment, avoid embarrassment, and tackle economic damage [220]. BC-based IoT e-health was designed to ensure the confidentiality of healthcare providers and patients [221]. The IoT network and cloud storage are integrated for privacy preservation. In BC, indexing the records is used to secure medical records, while a smart contract is used to secure electronic medical records (EMR) [222]. A privacy-preserved cloud health data platform was proposed by Uddin et al. to encrypt health records based on the BC smart contract and store them in the BC ledger on a cloud, while data confidentiality is solved by encrypting it into BC, which enhances the transparency and security of data storage on the cloud [223]. The drawback of this model is that the comparison of smart contracts and traditional techniques are not made for the performance evaluation.

Similarly, a related study presented by Tariq et al. developed a cloud-based BC EHR platform that timestamps data before storing it in BC, increasing the traceability and validity of medical records. However, the system's weakness is that a smart contract has not been implemented to manage data storage. In addition, the BC ledger is transparent to all entities, and before writing the contents of the block, miners verify it first. Therefore, it is a significant threat to patients' privacy in the e-health system. The BC peer-to-peer network is restructured using attribute-based encryption to classify BC nodes for cluster head miners based on their roles and attribute authorities in the BC network. As a result, IoT devices and cluster heads are connected to collect IoT data in the BC network and perform computation-intensive operations, while an attribute authority (AA) provides nurses, doctors, and other professionals related to health acts as a miner that decrypts data. Table 5 summarizes IoHT applications based on integrating IoT, ML, and BC, along with challenges and solutions.

Table 5. Summary of IoHT applications based on IoT, ML, and BC.

Pillars	Challenges	Solutions/Benefits
IoT	Scalability [149,151,224] Energy constraints [20] Security [224–226]	Interoperability, evolvability thanks to open communication standards [151] Enhanced electromedical devices based on closed-loop design and predictive maintenance [19]
Big Data	The opacity of analytics [227,228] Extreme heterogeneity [229]	New insights and actionable information from new data sources [230] Natural transformation of descriptive research into predictive and prescriptive one [231]
Cloud/Fog Computing	Infrastructure availability [45] Performance monitoring Data privacy [45] The opacity of the infrastructure	Paradigmatic model for an offering of services to patients or healthcare operators themselves Infrastructure for high-level functions such as data analysis and information systems [232]

4.3.3. mHealth Based on BC

Mobile devices in IoT enhance how patients engage in the treatment process using a patient app, secure text messaging, and telemedicine. Many researchers [233,234] secure mobile apps using BC to capture data safely from the wearable sensors of patients and deliver health services fast. mHealth is a mobile app based on JavaScript object notation (JSON) as the primary language. mHealth is based on BC to secure health data by modifying

the collected data from wearable sensors. The BC used is a private BC developed using Hyperledger Fabric [235]. mHealth does not adapt to security issues not examined between mobile apps and sensors.

4.3.4. Access Control in E-Health

An essential issue in e-health is security, which can cause the endangerment of patients' privacy by maliciously changing diagnostic data [236]. Access control is a security feature that ensures that only authorized users, groups, or organizations with correct privileges can access health services in an organization. Various techniques presented in the literature solve issues related to access controls and authentication in the BC e-health system [237–239].

The BC ledger was used to store access policies of medical records using many algorithms in the patient-centric framework that defined access policies [240]. In addition, tools such as Composer, Hyperledger Caliper, Hyperledger Fabric, Docker, and Wireshark were used to check performance in terms of latency and throughput.

Attribute-based encryption (ABE) and Ethereum BC used an interplanetary file system (IPFS) combined with decentralized cloud architecture to form decentralized storage. In addition, an access control management system based on a smart contract was used to handle keyword searches and improve the privacy of the framework and quality of service (QoS). However, delays arising from ABE, data security, and access control approach are drawbacks that are not analyzed.

A framework named HPA is a health prescription framework privileged for medical IoT devices provided with the security access token (SAT), representing that the IoT device is authenticated and can request services from the system [241]. Although performance analysis was not performed, the model is conceptually based on OpenID. Privacy laws in Europe, such as the drafted DGPR health regulations, enforce service providers to provide a report on the request of users and provide all the data in a readable format on a computer [242]. A conceptual e-health framework based on cloud and BC technology efficiently shares health data with authorized users and complies with regulations, such as GDPR [243]. The technological solution of BC can solve current storage methods, such as conventional cloud IoT-enabled healthcare systems and electronic health records (EHR) for health data that is sensitive to data attacks, to be more secure and effective. On-chain storage is another method to store records, but it is costly to insert a block on-chain [244]. This method is also not technologically or financially feasible. Off-chain is another technique with a hash code, a piece of tiny data stored in the BC ledger while the data are stored in conventional repositories. A conceptual model was presented for sharing personal health data continuously using BC-based decentralized cloud storage [245]. Off-chain in traditional cloud storage stores encrypted health datasets, while BC stores hash values to decrease storage load in the BC framework. Data sharing in e-health is based on BC.

BC has decentralization and manipulation resistance characteristics that resolve patient privacy issues effectively [246]. BC and smart contracts, used by MeDShare, are used to transmit data amongst untrusted cloud services providers (CSP), trace data access behavior of users, and identify breaches in data. Without confidentiality of data, BC-based CSPs facilitate such auditing without jeopardizing it. Access control of confidential data is an issue in cloud-based data processing that can solve user authentication for transferring data in the cloud layer. For instance, a secure cryptographic approach ensures efficient access control [247].

Usually, physicians who have medication and care expertise for a particular disease need cross-border medical experience from many worldwide medical practitioners. BC can play an essential role in facilitating global knowledge exchange for medical care, treatment, and personal diagnosis. Artificial intelligence and parallel execution are adopted for precision medical care and treatment in a hybrid healthcare system [248]. Descriptive intelligence or artificial healthcare systems simulate and model doctor and patient dynamic and static characteristics. The phase in which various disease scenarios assess the

applicability of an appropriate therapeutic regimen in AHS by computational experiments implementation is called predictive intelligence. Furthermore, specialists endorsed a list of the final regimen in both the current health care system and AHS to provide prescriptive intelligence. The system includes hospitals, healthcare institutions, patients, health officials, medical researchers, and BC-powered smart contracts to enable electronic health records (EHRs) to be inspected and reciprocated and is based on consortium BC.

BC-based decentralized data security techniques were introduced, including healthcare providers, patients, overlay networks, smart contracts, and cloud servers [249]. First, cloud storage stores medical records in block form connected to BC and stores its hash values, which facilitates the tracking of all changes in the cloud data, and a dual encryption technique is used to secure data. However, the drawback is that the simulations on the proposed security technique have not been performed. Second, Medchain is a platform for sharing medical records with BC P2P and typical P2P networks. Whereas the BC network stores session, data, and fingerprints operations, such as immutable data digests, the regular P2P network stores sessions and not mutable data [250]. A BC-based medical sharing system collects medical summaries by provincial hospitals from EMRs of regional hospitals [251]. A block contains medical data provided by local hospitals and then transfers data to the consensus nodes. Thus, verifying and validating blocks and initiating queries is the role of hospitals.

4.3.5. E-Health Based on BC Smart Contract

With the development of BC, a smart contract is one of the most demanded technologies due to its automated nature. Computer programming encodes rules and agreements stored in a public ledger running automatically when a related event occurs on the BC without a third party. For example, accessing medical records and permission management systems are based on the timed smart contract [252]. By implementing suitable user policies, computations on the EMRs can be monitored by introducing an agreement in the research control transactions. Furthermore, an incentive-based mining process was introduced to eradicate the need for a digital currency where nodes with low ratings create the block.

In contrast, nodes with higher ratings approve the blocks on the BC network that ensure consistency. Ethereum BC was used to carry out experiments, while the drawbacks of the system are the security and privacy of health data, which were not addressed. The healthcare professionals and patients used remote patient monitoring systems based on BC to provide wearable sensors and other medical service licenses [253]. In addition, the emergency alert system triggers an alert to inform consumers and healthcare professionals that they are remotely monitoring patients. Remix, an open-source web environment, was used for debugging, implementing, and testing their smart contract. Ethereum and smart-contract-based data retrieval have no security and privacy.

The BC-based medical platform protects the management of EMRs of different hospital departments, working by using smart contracts to store record logs, health data, and access to medical data of varying health organization's regulations [254]. The framework was tested on a network of hospitals to show systems' performance in terms of effectiveness, efficiency, and real-time validation. In addition, Hyperledger was used to develop a smart contract. A forensic-enabled framework for a medical device based on BC technology uses smart contacts for fine-grained authorization techniques [255]. Smart contracts define policies to ensure the confidentiality and integrity of transaction logs, while the PoS consensus technique validates BC transactions. API is used to query data by clinicians, healthcare professionals, patients, and researchers from a database at any given time. BC was used in the traditional biomedical database to ensure integrity and non-repudiation in retrieving information. The system was implemented in Ethereum BC using the Solidity language. The system has three primary parts:

- To record all user queries in the BC, a smart contract between the user interface and database is needed.
- An interface is used for communicating with the biomedical interface.

- The front-end interface is used to make health-based queries by third parties on lightweight BC.

Researchers have presented different ideas to enhance current BC technology. Currently, it requires much computational power due to its mathematical principles, such as the Merkel Hash tree, cryptographic key systems, and PoW [256].

Healthcare architecture based on lightweight BC is geographically divided into different roles in which the cluster head, called the head BC manager (HBM), is responsible for handling transactions and making a block. To avoid a fork, it maintains a single copy of the ledger for its members [257]. However, it cannot guarantee the tamperproof feature of the ledger, but it can reduce communication and computational delay. The system simulation was done in NS3, while the performance was compared to Bitcoin BC. BC-based healthcare improved power consumption using lightweight cryptographic techniques, such as the Ring Signature and the ARX, to improve privacy [258]. For instance, IoBHealth systems based on IoT, eHealthcare, and BC can access and manage EHR data securely, robustly, and effectively. A graphical user interface was implemented to visualize dashboards and display data of the network users. Furthermore, remote patient monitoring based on advanced, scalable BC used the GHOSTDAG protocol that examines each transaction as a node rather than a single large chain of blocks [259].

The integration of BC with wearable sensors and its challenges are addressed by many entities, such as cloud storage, smart contracts, BC networks, health providers, and patients with wearable IoT devices provided for healthcare achievements [260]. A node with high computational power in the BC algorithm is selected as a cluster head among the hierarchical topology of the network for a group of nodes to check and process blocks as representative of its members. A proof of familiarity (PoF) is a novel consensus technique for executing the e-health BC that requires collaborative medical decision-making to provide medical services to a patient [261]. A cured patient experience is asked of a new patient, giving him similar symptoms and disease. The medical opinion from many physicians, the strategic policies from insurance providers, and a favorable joint medical decision are developed from collecting these parties' feedback. On-chain is used to store findings and hash of the medical data, while off-chain is used to store medical data. The disadvantage of this study is the lack of practical implementation to study the feasibility [262].

4.4. Convergence Applications of IoT, BC, and ML

In the context of health informatics, big data means dealing with structured and unstructured data, real-time imaging, data generated from IoHT devices, and point-of-care-diagnostic devices [263]. In addition, social media and environmental factors can be considered essential sources of health information [264]. Big data analysis uses intelligent algorithms to process massive vital signs to identify risks and take corrective decisions to avoid risks. Researchers who report big data analysis applications demonstrate the importance of this field of study.

The ML-based approach that deals with data-driven models have three phases, data acquisition and preprocessing extraction of features, selection, and learning [265,266]. Data acquisition is obtained through IoHT devices and any device with registration and synchronization abilities in the hospitals. Before selecting and extracting features, data are preprocessed. Classifier or regressor algorithms then use the extracted features to map the relationship between the collected data and the venture of health degeneration [267]. Finally, in the case of the deep learning technique, features are selected using an algorithm rather than the manual feature selection approach used recently.

Various ML approaches are used in the literature to integrate vital signs. A support vector machine (SVM) is one of them. It creates a risk score in a multimodal way where the data are collected at the admission time and the remainder of the admission time [81static]. Another method that gained attraction is the decision tree that classifies the diseases. Furthermore, neural networks (NNs) combined with other artificial intelligence approaches have been used in medical-related research. A set of widely used techniques

are based on the long-short-term memory (LSTM) recurrent neural network (RNN) for pattern recognition in the EHR data [268]. In addition, gated recurrent units (GRU) is a new RNN mechanism used to create a deep model [269].

The deep learning technique consists of many NNs with several hidden layers and neurons [270]. A massive quantity of neurons covers a lot of raw data, while the chance of cascading different layers allows for higher abstraction and bypassing manual intervention [271]. The methodology that has a vital role in health informatics is the convolutional neural network (CNN) [272]. Many studies about CNN concentrate on medical images, while some up-to-date work uses it for vital sign analysis [273].

IoT allows providers to utilize assets to reduce costs and provide new revenue opportunities that impact patient care. In addition, IoT can maintain individual well-being and alter and improve health care delivery [274]. As a result, many IoT applications have been developed for healthcare services based on the DL technique, including dietary assessment, disease prediction, and elderly care.

4.4.1. Elderly Care

Recently, in the United Kingdom, the number of older people above 75 years has reached 2376 [154]. Thus, living alone in homes increased, and it is difficult for the elderly to take care of themselves. However, these people cannot take care of themselves to maintain a healthy lifestyle. Therefore, ML-based solutions have been introduced to monitor patients' positions and activities. For instance, a DL-based model called fall detection was used to analyze the smart home environment for some posture detection. The system triggers an alarm when it detects a human falling and helps fallen people get support from others fast [275]. DL uses RBF and DBN models to classify the posture of the human body with 86% accuracy. DL classifier is trained with the extracted human body position data with threshold values of different body positions. For example, if a body position threshold of a person resting on the floor is more than the defined threshold, the person is considered to have fallen.

In another work [276], CNN detects human falls by extracting images from a video sequence to learn the human body fall characteristics, showing 99.98% correctness in real-time. Using CNN for human fall detection in the fog computing environment, using smart device training, data were collected and fed to a model to extract relevant features from the collected data and detect the fall [277]. A vision-based tracking technique using the CNN model was presented by Adhikari et al. [278]. In contrast, others have used time-sequential mobile data with a recurrent network to accurately and quickly detect falls. The fall detection system used embedded software based on RNN within wearable devices to detect the falls of users and inform the monitoring system by notification through a wireless network, which achieves 98% accuracy [279]. Another android application, named SmartFall, collects data from wearable smartwatch users connected to a smartphone where the application is installed [280]. The RNN model is used for real-time detection with low latency and high privacy, as the computation on a smartphone is directly executed. The feature can be extracted from camera depth, and it notifies the family by triggering an alarm when a human fall is detected. The proposed system's fall detection accuracy is 93%.

Moreover, another fall detection system was developed by implementing LSTM and CNN combined, named the "ConvLSTM" model. Integrated LSTM and 3D CNN techniques demonstrated 100% accuracy for fall detection. During the preprocessing, features are extracted from the temporal sequence in each video. Many DL models were used for disease prediction based on analyzing health data and treatment history. For example, the CNN model was used for disease prediction of a patient with ductal carcinoma [281]. The model extracts deep features from digital mammograms and is pretrained on non-medical images. A CNN model was adopted in the healthcare system to identify the early disease of Parkinson's and the problem with the nervous system that affects human movement using image analysis and classification [282]. A CNN model with 12 layers was used to identify the cardiovascular disease and detect the disease from breast arterial calcification (BAC)

and mammograms, which is the method of detection to identify abnormal heartbeats [283]. Similarly, the RNN model, which uses GRU and LSTM models applied to the dataset, contains the sound of the heart that can identify abnormal heartbeats.

4.4.2. Dietary Assessment

An automatic system for dietary assessment is needed to solve the obesity problem. A CNN-based system for image recognition was developed to use mobile devices to capture food images and analyze them to estimate dietary intake [284]. The UEC-256 dataset gives 81.5%, and the Food-101 dataset shows an accuracy of 73.9%. Another food recognition system based on a CNN model was developed to classify food images using a mobile system based on the real-time data collected from the IoT [285].

A summary of smart healthcare applications developed and leveraged for IoHT is presented in Table 6.

Table 6. Summary of Smart Healthcare Applications based on ML in IoHT.

Scenario/Use Cases	IoT Based Application	Input Datasets	DL Models	Infrastructures
Smart Healthcare	Dietary assessment	UEC-100/UEC-256/Food-101 datasets [286]	CNN	Edge computing
		UEC-256/UEC-100 datasets [285]	CNN	
	Elderly care	SisFall dataset [279]	RNN	Cloud computing
		Sports-1M/Cameras fall/FDD/URFD datasets [287]	3D CNN + LSTM	Cloud computing
		Authors create their data [275] [288]	DBN + RBM CNN + LSTM	Cloud computing Cloud computing
		URFD dataset [276]	CNN	Cloud computing
		NTU RGB-D dataset [289]	LSTM	Cloud computing
		URFD dataset [277]	CNN	Fog computing
		Smartwatch, Notch, and Farseeing datasets [280]	RNN	Edge computing
		Coco dataset [278]	CNN	Cloud computing
Disease prediction	HandPD dataset [290]	CNN	Cloud computing	
	PhysioNet/Cardiology Challenge dataset [291]	RNN	Cloud computing	
	ImageNet dataset [281]	CNN	Cloud computing	
	Authors use 840 digital mammograms images collected from medical systems [283]	CNN	Cloud computing	

5. Future Research Directions and Relative Demerits of Existing Solutions

Issues in developing secured IoHT include interoperability, security vulnerability, lack of data analysis and transmission, and the absence of IT and OT convergence. However, the biggest issue to be solved is a security vulnerability. Connected computing devices in the information network share information directly with the cloud and therefore cause security threats and attacks. Distributed Denial of Service attacks based on IoT has shown their power to threaten business [292]. BC is a perfect solution for IIoT security. A BC platform for IIoT with deployed smart contracts enabled the development of various distributed applications for manufacturing using a decentralized, trustless, peer-to-peer network for IIoT applications.

Autonomous algorithms on smart gateway have been adopted with BC in IoT networks. Smart gateway is used as BC nodes to implement BC networks with low-energy IoT devices, facilitating an event-based messaging system and proof of concept to access BC networks using resource constraint IoT devices. Two issues are related to using IoT devices with BC: connectivity issues, which are resolved by the researchers, while the other issue is related to power and bandwidth consumption needed for BC and is not solved in the

literature. A privacy-preserving IoT framework developed using a BC-connected gateway uses the BC network to manage privacy as the underlying infrastructure [293]. The BC gateway cannot address user privacy but can track and secure user privacy preferences. However, proposals are conceptual and need to enhance IoT e-health data management and the BC algorithm. Figure 7 presents the body area sensors network with BC.

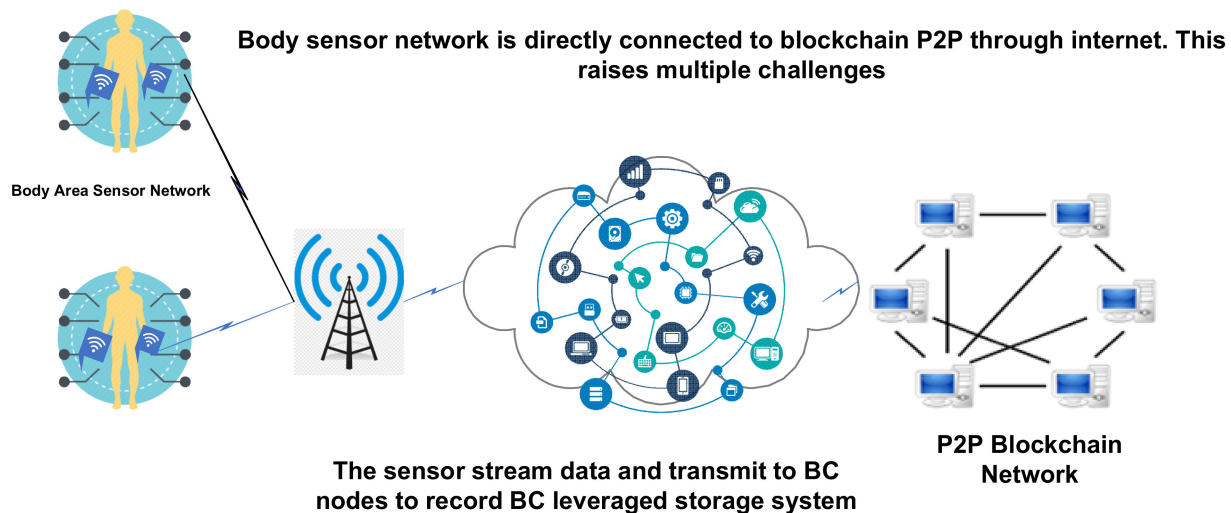


Figure 7. Body area sensors network with BC.

BC technology has been used by BC gateway to track and secure the privacy preference of users, but it cannot address user privacy concerns. However, proposals are conceptual and still considered to improve IoT e-health data management and the BC algorithm. For a hacker, health data are easy and fruitful targets, and researchers are the reason to misuse the storage and secure transmission of protected health information (PHI). Some research proposals used smart contracts and smart agents as a smart gateway to implement BC in a body area sensor network (BASN) to build a secure e-health system, for instance, the wireless body area sensor (WBAN). However, research about IoT, e-health, and BC regarding privacy and security of end devices related to patients, storage management of health data, and mining management for BC has very little knowledge to cover this gap. Similarly, the e-health framework was implemented for the patient agent-assisted end-to-end decentralized BC [294].

5.1. Integration Challenges and Solutions

- The sensor's streaming rate is higher than that of a miner that can process blocks in BC, particularly in Bitcoin;
- Patient's privacy is at stake as miner nodes process plain text data;
- Sensors cannot enforce access control and perform data encryption due to their limited processing and memory capacities;
- Different kinds of medical data require extra security, privacy, and QoS. In addition, sensors or miners cannot determine health data repositories because the choice of storage is subjective.

Generally, IoT is beginning in healthcare with many smart objects connected, despite many issues with communication technologies and smart objects. Energy is the central issue, and research is needed on energy conservation, energy harvesting, and usage to design and develop zero-entropy systems. Due to potentially drastic escalation, architecture scalability is an issue among the main concerns. In addition, organizations in hierarchical subdomains would profit from manageability and performance—BANs deployment and adoption record-specific design problems.

As IoT systems cannot fulfill functional design requirements and afford privacy and security risks, security solutions for IoT design are needed. Currently, there are unreliable security solutions to heterogeneous and extensive networks. For example, there is a need for secure and effective architecture to process data from health monitoring sensors, which generate a large amount of data. A cybersecurity framework presented by Obaidat et al. covers platform boundaries and the abstraction layer of heterogeneous systems. Furthermore, connected devices, such as wearables, are more vulnerable to security risks and need extra security. Devices with limited resources need lightweight algorithms to secure data management systems. Problems with cloud storage are that it hides the entire infrastructure, allows the customer to manage operations related to cloud resources, and provides economies of scale-grade prices [295]; these are the desired properties that limit the performance when required.

Network performance, the efficiency of communication protocol [296,297], and computing performance are the barriers that are still present. On the other hand, cloud technologies in the literature report are scalable, and scalability is the primary concern. Furthermore, adopting a public-cloud network increases researchers' focus on performance [298,299]. According to the discussion above, data-intensive applications need different stakeholders to work on service performance, manage, and troubleshoot [300]. Furthermore, as billions of small devices need to be configured, fog intensifies scalability issues, requiring a decentralized and scalable management system to be tested. Other issues are flexibility, power and efficiency, reliability, safety, availability, and maintainability. However, using third-party hardware for the cloud and fog applications raises concerns about data privacy [301]. Providers that store sensitive information in their infrastructure encounter issues that often lose control over data due to low confidence in the provider [302]. An identity management architecture proposed by Sánchez-Guerrero et al. enables patient-controlled partial disclosure of her to selected recipients. The system provides solutions to problems using external services rather than in-house solutions. Unlike the previous solutions, the proposed system does not require advanced security [303,304]. Moreover, these services increase availability that provides uninterrupted services with minimum downtime [305]. Among its characteristics, a significant challenge for Healthcare 4.0 is the formats, heterogeneity of sources, and attributes of data. Jirkovsky et al. concentrated on semantic heterogeneity and introduced a framework to encourage interoperability.

There are many advantages IIoT carries, such as the closed-loop design [306]. Patient feedback from physicians about product effectiveness and usability, health operators, and a patient can be returned to the design phase. The designers can better realize how the products can be improved and utilized by collecting these data. Predictive maintenance, the ability to continuously collect data, enables IoT devices to predict and maintain fault before failure occurs to provide the opportunity to avoid downtime of the machine. In addition, new service lines are used by manufacturers, allowing them to continuously monitor and maintain services through devices so that the service can be constantly improved. Electro-medical device communication systems have reliability and robustness requirements and are often tightly bound to jitter and latency. The continuous development and broad adoption of open standards for protocol design with constraints, such as IEEE 802.15.6 and IEEE 802.15.4, means that a type of non-mutually exclusive solutions will be possible, improving interoperability in components and devices from different vendors. In the IT world, the interoperability and pervasiveness of the TCP/IP communication stack have presented the adoption of wireless local area networks (Wi-Fi). Furthermore, real-world testing and their interconnection to the internet are growing from small offices or home offices to much more demanding industrial procedures [307].

The big data technique satisfies the selection of a value from the previously incomprehensible data. Operators can examine their processes in the healthcare sector by looking for new opportunities in consecutively and extensively collected data. Understanding big data procedures gives valuable in-time information. Furthermore, medical researchers can use big data technologies to transform descriptive research questions into predictive ones to

reach the authoritarian ones. Table 7 summarizes the convergence challenges and solutions of BC in IoHT.

Table 7. Convergence challenges and solutions of BC in IoHT.

Challenges	Solutions
Handling Big Data	The off-chain technique is used to overcome big data issues in an IoT system by many researchers using it in an IoT system by integrating BC storage with cloud storage.
Data Concurrency and Throughput Challenge	This issue is resolved by using the sharding technique by a researcher in which the peer-to-peer network of BC is divided into different groups. Members of that sharding handle the transactions because authentication and processing of transactions are generated here in the sharding.
Connectivity Challenges	Multi-access edge computing (MEC) is used in literature to host a side-chain for solving connectivity issues. The side-chain is used to connect IoT devices with the main chain.
Trust	BlockBDM is a technique used to handle IoT big data management trust and security issues.
Privacy	The privacy issues can be solved by using Ring signature BC, which is encrypted technology commonly used.
Single Point of Failure	The peer-to-peer architecture of BC technology can solve a single point of failure issue in IoT.

5.2. Technical Limitations of BC

Implementation of BC in IoT has many challenges that need to be identified in terms of security and privacy, scalability, and computational cost [308].

Due to some bottlenecks, there is poor scalability with limited throughput, efficiency, and high computational cost in current BC. The rapid increase in block time reduces overall system performance. In addition, the ledger will become notably large if all transactions are stored in BC [309]. Big data generated by complex systems, such as smart healthcare in smart cities, leads to complications in data processing based on the BC environment. Therefore, the realization of BC as an alternative solution to the current systems for large IoT systems is a viable issue [310]. For example, in their study, Wood et al. stated that transaction is the computational cost of BC [311]. Transaction processing combines several steps that consume high computing power, such as heavy security, mining, validating, and storing it across multiple participants. In addition, there is some consensus process that also needs an amount of energy, such as PoW, PoS, and pBFT.

6. Conclusions

Healthcare environments are revolutionized using the advancements in computing and communication technologies. This support and encourage medical practitioners and researchers to implement their expertise to handle new ideas productively and efficiently to improve the health diagnosis and monitoring of patients. IoHT lies in the field of research that raises the use of biosensors, wearables, and other medical devices to improve patient data management in hospitals, decrease hospitalization times, and enhance patient healthcare delivery. However, the realization of IoHT has many challenges, such as privacy, security, safety, and trust. BC technology revolutionized the existing IoT-based healthcare applications by integrating the promising features for data protection and sharing in a distributed fashion. Studies show that BC aims to enhance the traditional IoT-based healthcare applications to provide a safe and transparent environment for patients and healthcare practitioners. Industrial revolution technologies for the health sector include fog and cloud computing, IoT, and big data analytics. The traditional IoT-based EHR systems cannot deal with these paradigms because of inconsistent security policies and data access structures. BC comes in handy in storing patient data and encountering data integrity and confidentiality challenges. Therefore, it is a viable solution for addressing existing IoT data security and privacy challenges. The scientific community has shown a variety of healthcare applications based on ML to improve health diagnosis and monitoring practices. This study aimed to present a comprehensive survey to illustrate the implication of integrated

technologies based on BC, IoT, and AI to meet growing healthcare challenges. First, this research study examined the background of enabling technologies such as IoT, BC, and ML to leverage these innovative paradigms in the healthcare sector. Second, we presented a detailed survey on enabling technologies for intelligent and secure internet of health things. Third, the peculiarities of the IoHT environment and the security, performance, and progression of the enabling technologies were discussed. Lastly, we discussed the research gaps, future directions, and limitations of the enabling technologies.

In future work, we aim to develop and propose an architecture for BC-based secure and intelligent IoT architecture for patient health monitoring based on predictive and optimization techniques to enhance the performance efficiency of healthcare systems. This BC-enabled IoT-based patient health monitoring system will revolutionize the health sector by integrating unique capabilities to enhance data privacy, security, transparency, and accountability. In addition, it will consider a viable and robust solution to revolutionize the health sector by providing a distributed, decentralized, and secured environment for both patients and health practitioners.

Author Contributions: I. and J.K. conceived the idea for this paper, designed the methodology, and assisted in write-up of the paper. U.Z. Write the original article and assisted in the design and paper write-up. F.M., N.I. and M.I. assisted in review and editing. I. and J.K. supervised and proofread this study. All authors have read and agreed to the published version of the manuscript.

Funding: This study was supported by the National Research Foundation of Korea grant (NRF-2022R1A2C1012037).

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

References

1. Qayyum, F.; Afzal, T. Worldwide Knowledge Dissemination in Chemistry. *J. Intell. Pervasive Soft Comput.* **2022**, *1*. Available online: <https://scirep.institute/journals/index.php/jipsc/article/view/4> (accessed on 24 April 2022).
2. Germanakos, G.P.; Mourlas, C.; Samaras, G. A Mobile Agent Approach for Ubiquitous and Personalized Ehealth Information Systems. In Proceedings of the Workshop on ‘Personalization for e-Health’ of the 10th International Conference on User Modeling (UM 2005), Edinburgh, Scotland, UK, 24–29 July 2005; Available online: <https://cgi.csc.liv.ac.uk/~floriana/UM05-eHealth/Germanakos.pdf> (accessed on 24 April 2022).
3. Imran, Qayyum, F.; Kim, D.-H.; Bong, S.-J.; Chi, S.-Y.; Choi, Y.-H. A Survey of Datasets, Preprocessing, Modeling Mechanisms, and Simulation Tools Based on AI for Material Analysis and Discovery. *Materials* **2022**, *15*, 1428. [[CrossRef](#)] [[PubMed](#)]
4. Imran; Iqbal, N.; Kim, D.H. IoT Task Management Mechanism Based on Predictive Optimization for Efficient Energy Consumption in Smart Residential Buildings. *Energy Build.* **2022**, *257*, 111762. [[CrossRef](#)]
5. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A Survey on Privacy Protection in Blockchain System. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58. [[CrossRef](#)]
6. Zhu, Q.; Loke, S.W.; Trujillo-Rasua, R.; Jiang, F.; Xiang, Y. Applications of Distributed Ledger Technologies to the Internet of Things: A Survey. *ACM Comput. Surv.* **2019**, *52*, 1–34. [[CrossRef](#)]
7. Miglani, A.; Kumar, N.; Chamola, V.; Zeadally, S. Blockchain for Internet of Energy Management: Review, Solutions, and Challenges. *Comput. Commun.* **2020**, *151*, 395–418. [[CrossRef](#)]
8. Alladi, T.; Chamola, V.; Parizi, R.M.; Choo, K.-K.R. Blockchain Applications for Industry 4.0 and Industrial IoT: A Review. *IEEE Access* **2019**, *7*, 176935–176951. [[CrossRef](#)]
9. Vangala, A.; Das, A.K.; Kumar, N.; Alazab, M. Smart Secure Sensing for IoT-Based Agriculture: Blockchain Perspective. *IEEE Sens. J.* **2020**, *21*, 17591–17607. [[CrossRef](#)]
10. Marwah, K.; Hajati, F. A Survey on Internet of Things in Telehealth. In Proceedings of the Complex, Intelligent and Software Intensive Systems, Asan, Korea, 1–3 July 2021; Barolli, L., Yim, K., Enokido, T., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 235–248.
11. Borthakur, D.; Dubey, H.; Constant, N.; Mahler, L.; Mankodiya, K. Smart Fog: Fog Computing Framework for Unsupervised Clustering Analytics in Wearable Internet of Things. In Proceedings of the 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Montreal, QC, Canada, 14–16 November 2017; pp. 472–476.
12. Fortino, G.; Savaglio, C.; Palau, C.E.; de Puga, J.S.; Ganzha, M.; Paprzycki, M.; Montesinos, M.; Liotta, A.; Llop, M. Towards Multi-Layer Interoperability of Heterogeneous IoT Platforms: The INTER-IoT Approach. In *Integration, Interconnection, and Interoperability of IoT Systems*; Gravina, R., Palau, C.E., Manso, M., Liotta, A., Fortino, G., Eds.; Internet of Things; Springer International Publishing: Cham, Switzerland, 2018; pp. 199–232. ISBN 978-3-319-61300-0.
13. Bhushan, B.; Khamparia, A.; Sagayam, K.M.; Sharma, S.K.; Ahad, M.A.; Debnath, N.C. Blockchain for Smart Cities: A Review of Architectures, Integration Trends and Future Research Directions. *Sustain. Cities Soc.* **2020**, *61*, 102360. [[CrossRef](#)]

14. Luo, T.; Huang, J.; Kanhere, S.S.; Zhang, J.; Das, S.K. Improving IoT Data Quality in Mobile Crowd Sensing: A Cross Validation Approach. *IEEE Internet Things J.* **2019**, *6*, 5651–5664. [[CrossRef](#)]
15. Hassan, M.M.; Gumaei, A.; Huda, S.; Almogren, A. Increasing the Trustworthiness in the Industrial IoT Networks Through a Reliable Cyberattack Detection Model. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6154–6162. [[CrossRef](#)]
16. Yamada, Y.; Shinkuma, R.; Iwai, T.; Onishi, T.; Nobukiyo, T.; Satoda, K. Temporal Traffic Smoothing for IoT Traffic in Mobile Networks. *Comput. Netw.* **2018**, *146*, 115–124. [[CrossRef](#)]
17. Radhakrishnan, G.; Gopalakrishnan, V. Applications of Internet of Things (IOT) to Improve the Stability of a Grid Connected Power System Using Interline Power Flow Controller. *Microprocess. Microsyst.* **2020**, *76*, 103038. [[CrossRef](#)]
18. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of Threats to the Internet of Things. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1636–1675. [[CrossRef](#)]
19. Ahmad, S.; Jamil, F.; Iqbal, N.; Kim, D. Optimal Route Recommendation for Waste Carrier Vehicles for Efficient Waste Collection: A Step Forward Towards Sustainable Cities. *IEEE Access* **2020**, *8*, 77875–77887. [[CrossRef](#)]
20. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT Security: Challenges and Solution Using Machine Learning, Artificial Intelligence and Blockchain Technology. *Internet Things* **2020**, *11*, 100227. [[CrossRef](#)]
21. Iqbal, N.; Khan, A.-N.; Imran, A.; Rizwan, A.; Qayyum, F.; Malik, S.; Ahmad, R.; Kim, D.-H. Enhanced Time-Constraint Aware Tasks Scheduling Mechanism Based on Predictive Optimization for Efficient Load Balancing in Smart Manufacturing. *J. Manuf. Syst.* **2022**, *64*, 19–39. [[CrossRef](#)]
22. Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 616–644. [[CrossRef](#)]
23. Bhushan, B.; Sahoo, C.; Sinha, P.; Khamparia, A. Unification of Blockchain and Internet of Things (BIoT): Requirements, Working Model, Challenges and Future Directions. *Wirel. Netw.* **2021**, *27*, 55–90. [[CrossRef](#)]
24. Huh, S.; Cho, S.; Kim, S. Managing IoT Devices Using Blockchain Platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea, 19–22 February 2017; pp. 464–467.
25. Si, H.; Sun, C.; Li, Y.; Qiao, H.; Shi, L. IoT Information Sharing Security Mechanism Based on Blockchain Technology. *Future Gener. Comput. Syst.* **2019**, *101*, 1028–1040. [[CrossRef](#)]
26. De Filippi, P.; Mannan, M.; Reijers, W. Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance. *Technol. Soc.* **2020**, *62*, 101284. [[CrossRef](#)]
27. Tariq, N.; Qamar, A.; Asim, M.; Khan, F.A. Blockchain and Smart Healthcare Security: A Survey. *Procedia Comput. Sci.* **2020**, *175*, 615–620. [[CrossRef](#)]
28. Karafiloski, E.; Mishev, A. Blockchain Solutions for Big Data Challenges: A Literature Review. In Proceedings of the IEEE EUROCON 2017—17th International Conference on Smart Technologies, Ohrid, Macedonia, 6–8 July 2017; pp. 763–768.
29. Iqbal, N.; Jamil, F.; Ahmad, S.; Kim, D. A Novel Blockchain-Based Integrity and Reliable Veterinary Clinic Information Management System Using Predictive Analytics for Provisioning of Quality Health Services. *IEEE Access* **2021**, *9*, 8069–8098. [[CrossRef](#)]
30. Rehman, M.; Javaid, N.; Awais, M.; Imran, M.; Naseer, N. Cloud Based Secure Service Providing for IoTs Using Blockchain. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–7.
31. Srivastava, G.; Parizi, R.M.; Dehghantanha, A. The Future of Blockchain Technology in Healthcare Internet of Things Security. In *Blockchain Cybersecurity, Trust and Privacy*; Choo, K.-K.R., Dehghantanha, A., Parizi, R.M., Eds.; Advances in Information Security; Springer International Publishing: Cham, Switzerland, 2020; pp. 161–184. ISBN 978-3-030-38181-3.
32. Atlam, H.F.; Wills, G.B. Chapter One—Technical Aspects of Blockchain and IoT. In *Advances in Computers*; Kim, S., Deka, G.C., Zhang, P., Eds.; Role of Blockchain Technology in IoT Applications; Elsevier: Amsterdam, The Netherlands, 2019; Volume 115, pp. 1–39.
33. Agrawal, R.; Verma, P.; Sonanis, R.; Goel, U.; De, A.; Kondaveeti, S.A.; Shekhar, S. Continuous Security in IoT Using Blockchain. In Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, Canada, 15–20 April 2018; pp. 6423–6427.
34. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions. *Blockchain Res. Appl.* **2021**, *2*, 100006. [[CrossRef](#)]
35. Lamba, A.; Singh, S.; Balvinder, S.; Dutta, N.; Rela, S. *Mitigating IoT Security and Privacy Challenges Using Distributed Ledger Based Blockchain (DL-BC) Technology*; Social Science Research Network: Rochester, NY, USA, 2017.
36. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On Blockchain and Its Integration with IoT. Challenges and Opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [[CrossRef](#)]
37. O'Donoghue, O.; Vazirani, A.A.; Brindley, D.; Meinert, E. Design Choices and Trade-Offs in Health Care Blockchain Implementations: Systematic Review. *J. Med. Internet Res.* **2019**, *21*, e12426. [[CrossRef](#)]
38. de Vries, A. Bitcoin's Growing Energy Problem. *Joule* **2018**, *2*, 801–805. [[CrossRef](#)]
39. Kim, S.-K.; Huh, J.-H. A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective. *Energies* **2018**, *11*, 1973. [[CrossRef](#)]
40. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. An Efficient Selective Miner Consensus Protocol in Blockchain Oriented IoT Smart Monitoring. In Proceedings of the 2019 IEEE International Conference on Industrial Technology (ICIT), Melbourne, VIC, Australia, 13–15 February 2019; pp. 1135–1142.

41. Sharma, P.K.; Kumar, N.; Park, J.H. Blockchain Technology Toward Green IoT: Opportunities and Challenges. *IEEE Netw.* **2020**, *34*, 263–269. [[CrossRef](#)]
42. Zhou, Q.; Huang, H.; Zheng, Z.; Bian, J. Solutions to Scalability of Blockchain: A Survey. *IEEE Access* **2020**, *8*, 16440–16455. [[CrossRef](#)]
43. Dwivedi, A.D.; Malina, L.; Dzurenda, P.; Srivastava, G. Optimized Blockchain Model for Internet of Things Based Healthcare Applications. In Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1–3 July 2019; pp. 135–139.
44. Marjani, M.; Nasaruddin, F.; Gani, A.; Karim, A.; Hashem, I.A.T.; Siddiqua, A.; Yaqoob, I. Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges. *IEEE Access* **2017**, *5*, 5247–5261. [[CrossRef](#)]
45. Ermakova, T.; Ere, K.; Huenges, J.; Zarnekow, R. Cloud Computing in Healthcare—A Literature Review on Current State of Research. In Proceedings of the Americas Conference on Information Systems, Chicago, IL, USA, 15–17 August 2013.
46. Shailaja, K.; Seetharamulu, B.; Jabbar, M.A. Machine Learning in Healthcare: A Review. In Proceedings of the 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 29–31 March 2018; pp. 910–914.
47. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT Integration: A Systematic Survey. *Sensors* **2018**, *18*, 2575. [[CrossRef](#)] [[PubMed](#)]
48. Faust, O.; Hagiwara, Y.; Hong, T.J.; Lih, O.S.; Acharya, U.R. Deep Learning for Healthcare Applications Based on Physiological Signals: A Review. *Comput. Methods Programs Biomed.* **2018**, *161*, 1–13. [[CrossRef](#)] [[PubMed](#)]
49. Kuo, T.-T.; Zavaleta Rojas, H.; Ohno-Machado, L. Comparison of Blockchain Platforms: A Systematic Review and Healthcare Examples. *J. Am. Med. Inform. Assoc.* **2019**, *26*, 462–478. [[CrossRef](#)]
50. 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. *Univers. Access Inf. Soc.* **2019**, *18*, 837–869. [[CrossRef](#)]
51. Aggarwal, S.; Chaudhary, R.; Aujla, G.S.; Kumar, N.; Choo, K.-K.R.; Zomaya, A.Y. Blockchain for Smart Communities: Applications, Challenges and Opportunities. *J. Netw. Comput. Appl.* **2019**, *144*, 13–48. [[CrossRef](#)]
52. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [[CrossRef](#)]
53. AbuNaser, M.; Alkhatib, A.A.A. Advanced Survey of Blockchain for the Internet of Things Smart Home. In Proceedings of the 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 9–11 April 2019; pp. 58–62.
54. Wang, Y.; Cang, S.; Yu, H. A Survey on Wearable Sensor Modality Centred Human Activity Recognition in Health Care. *Expert Syst. Appl.* **2019**, *137*, 167–190. [[CrossRef](#)]
55. Qadri, Y.A.; Nauman, A.; Zikria, Y.B.; Vasilakos, A.V.; Kim, S.W. The Future of Healthcare Internet of Things: A Survey of Emerging Technologies. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1121–1167. [[CrossRef](#)]
56. Qayyum, A.; Qadir, J.; Bilal, M.; Al-Fuqaha, A. Secure and Robust Machine Learning for Healthcare: A Survey. *IEEE Rev. Biomed. Eng.* **2021**, *14*, 156–180. [[CrossRef](#)]
57. Karthick, G.S.; Pankajavalli, P.B. A Review on Human Healthcare Internet of Things: A Technical Perspective. *SN Comput. Sci.* **2020**, *1*, 198. [[CrossRef](#)]
58. Sworna, N.S.; Islam, A.K.M.M.; Shatabda, S.; Islam, S. Towards Development of IoT-ML Driven Healthcare Systems: A Survey. *J. Netw. Comput. Appl.* **2021**, *196*, 103244. [[CrossRef](#)]
59. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for Healthcare Data Management: Opportunities, Challenges, and Future Recommendations. *Neural Comput. Appl.* **2021**. [[CrossRef](#)]
60. Haghi Kashani, M.; Madanipour, M.; Nikravan, M.; Asghari, P.; Mahdipour, E. A Systematic Review of IoT in Healthcare: Applications, Techniques, and Trends. *J. Netw. Comput. Appl.* **2021**, *192*, 103164. [[CrossRef](#)]
61. Imran; Ahmad, S.; Kim, D.H. A Task Orchestration Approach for Efficient Mountain Fire Detection Based on Microservice and Predictive Analysis in IoT Environment. *J. Intell. Fuzzy Syst.* **2021**, *40*, 5681–5696. [[CrossRef](#)]
62. Varshney, T.; Sharma, N.; Kaushik, I.; Bhushan, B. Architectural Model of Security Threats and Their Countermeasures in IoT. In Proceedings of the 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 18–19 October 2019; pp. 424–429.
63. Kumar, S.A.; Vealey, T.; Srivastava, H. Security in Internet of Things: Challenges, Solutions and Future Directions. In Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; pp. 5772–5781.
64. Khari, M.; Kumar, M.; Vij, S.; Pandey, P.; Vaishali. Internet of Things: Proposed Security Aspects for Digitizing the World. In Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 16–18 March 2016; pp. 2165–2170.
65. Qiu, T.; Chen, N.; Li, K.; Atiquzzaman, M.; Zhao, W. How Can Heterogeneous Internet of Things Build Our Future: A Survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2011–2027. Available online: <https://ieeexplore.ieee.org/abstract/document/8286847> (accessed on 21 August 2021). [[CrossRef](#)]
66. Imran; Kim, D.H. Artificial Intelligence-Based Modeling Mechanisms for Material Analysis and Discovery. *J. Intell. Pervasive Soft Comput.* **2022**, *1*. Available online: <https://scirep.institute/journals/index.php/jipsc/article/view/2> (accessed on 24 April 2022).

67. Iqbal, N.; Khan, A.N.; Khan, M.A.; Rizwan, A.; Kim, D.-H. Semantic Situation Reporting Mechanism Based on 4W/H Ontology Modeling in Battlefield. *J. Intell. Pervasive Soft Comput.* **2022**, *1*. Available online: <https://scirep.institute/journals/index.php/jipsc/article/view/3> (accessed on 24 April 2022).
68. SAM: The Ultimate Internet Connected Electronics Kit. Available online: <https://www.kickstarter.com/projects/1842650056/sam-the-ultimate-internet-connected-electronics-ki> (accessed on 24 April 2022).
69. Miladinovic, I.; Schefer-Wenzl, S. A Highly Scalable Iot Architecture through Network Function Virtualization. *Open J. Internet Things OJIOT* **2017**, *3*, 127–135.
70. Sobin, C. A Survey on Architecture, Protocols and Challenges in IoT. *Wirel. Pers. Commun.* **2020**, *112*, 1383–1429. [[CrossRef](#)]
71. ICore. Available online: <http://icore-online.org/> (accessed on 24 April 2022).
72. Taylor, M. Why Elastic Scalability Matters in Network Functions Virtualization. *Metaswitch*, 24 February 2015.
73. Mahapatra, T. Composing High-Level Stream Processing Pipelines. *J. Big Data* **2020**, *7*, 1–28. [[CrossRef](#)]
74. Home—FIWARE. Available online: <https://www.fiware.org/> (accessed on 24 April 2022).
75. Heath, N. How IBM’s Node-RED Is Hacking Together the Internet of Things. *TechRepublic*, 13 March 2014.
76. dweet.io. Share Your Thing—Like It Ain’t No Thang. Available online: <https://dweet.io/> (accessed on 24 April 2022).
77. Particle. Connect Your Internet of Things (IoT) Devices. Available online: <https://www.particle.io/> (accessed on 24 April 2022).
78. Ahmad, M.; Alowibdi, J.S.; Ilyas, M.U. VIoT: A First Step towards a Shared, Multi-Tenant IoT Infrastructure Architecture. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–23 May 2017; pp. 308–313.
79. Sandor, H.; Genge, B.; Sebestyen-Pal, G. Resilience in the Internet of Things: The Software Defined Networking Approach. In Proceedings of the 2015 IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, 3–5 September 2015; pp. 545–552.
80. Moon, J.-H.; Shine, Y.-T. A Study of Distributed SDN Controller Based on Apache Kafka. In Proceedings of the 2020 IEEE International Conference on Big Data and Smart Computing (BigComp), Daegu, Korea, 19–22 February 2020; pp. 44–47.
81. Dwivedi, Y.K.; Janssen, M.; Slade, E.L.; Rana, N.P.; Weerakkody, V.; Millard, J.; Hidders, J.; Sniijders, D. Driving Innovation through Big Open Linked Data (BOLD): Exploring Antecedents Using Interpretive Structural Modelling. *Inf. Syst. Front.* **2017**, *19*, 197–212. [[CrossRef](#)]
82. Kwon, D.; Hodkiewicz, M.R.; Fan, J.; Shibutani, T.; Pecht, M.G. IoT-Based Prognostics and Systems Health Management for Industrial Applications. *IEEE Access* **2016**, *4*, 3659–3670. [[CrossRef](#)]
83. Iqbal, N.; Imran, Ahmad, S.; Ahmad, R.; Kim, D.-H. A Scheduling Mechanism Based on Optimization Using IoT-Tasks Orchestration for Efficient Patient Health Monitoring. *Sensors* **2021**, *21*, 5430. [[CrossRef](#)]
84. Wahyudi, A.; Pekkola, S.; Janssen, M. Representational Quality Challenges of Big Data: Insights from Comparative Case Studies. In *Proceedings of the Challenges and Opportunities in the Digital Era*; Al-Sharhan, S.A., Simintiras, A.C., Dwivedi, Y.K., Janssen, M., Mäntymäki, M., Tahat, L., Moughrabi, I., Ali, T.M., Rana, N.P., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 520–538.
85. Amanullah, M.A.; Habeeb, R.A.A.; Nasaruddin, F.H.; Gani, A.; Ahmed, E.; Nainar, A.S.M.; Akim, N.M.; Imran, M. Deep Learning and Big Data Technologies for IoT Security. *Comput. Commun.* **2020**, *151*, 495–517. [[CrossRef](#)]
86. Brous, P.; Janssen, M.; Schraven, D.; Spiegelner, J.; Can Duzgun, B. Factors Influencing Adoption of IoT for Data-Driven Decision Making in Asset Management Organizations. In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, Porto, Portugal, 24–26 April 2017; SCITEPRESS—Science and Technology Publications: Porto, Portugal, 2017; pp. 70–79.
87. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet Things J.* **2019**, *6*, 8182–8201. [[CrossRef](#)]
88. Calvillo-Arbizu, J.; Román-Martínez, I.; Reina-Tosina, J. Internet of Things in Health: Requirements, Issues, and Gaps. *Comput. Methods Programs Biomed.* **2021**, *208*, 106231. [[CrossRef](#)]
89. Sinha, P.; Rai, A.K.; Bhushan, B. Information Security Threats and Attacks with Conceivable Counteraction. In Proceedings of the 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 5–6 July 2019; Volume 1, pp. 1208–1213.
90. Bhushan, B.; Sahoo, G.; Rai, A.K. Man-in-the-Middle Attack in Wireless and Computer Networking—A Review. In Proceedings of the 2017 3rd International Conference on Advances in Computing, Communication Automation (ICACCA) (Fall), Dehradun, India, 15–16 September 2017; pp. 1–6.
91. Gope, P.; Sikdar, B. Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices. *IEEE Internet Things J.* **2019**, *6*, 580–589. [[CrossRef](#)]
92. Xiong, J.; Ren, J.; Chen, L.; Yao, Z.; Lin, M.; Wu, D.; Niu, B. Enhancing Privacy and Availability for Data Clustering in Intelligent Electrical Service of IoT. *IEEE Internet Things J.* **2019**, *6*, 1530–1540. [[CrossRef](#)]
93. Amini, M.R.; Baidas, M.W. Availability-Reliability-Stability Trade-Offs in Ultra-Reliable Energy-Harvesting Cognitive Radio IoT Networks. *IEEE Access* **2020**, *8*, 82890–82916. [[CrossRef](#)]
94. Gazis, V. A Survey of Standards for Machine-to-Machine and the Internet of Things. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 482–511. [[CrossRef](#)]

95. Sinche, S.; Raposo, D.; Armando, N.; Rodrigues, A.; Boavida, F.; Pereira, V.; Silva, J.S. A Survey of IoT Management Protocols and Frameworks. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1168–1190. [[CrossRef](#)]
96. Benkhelifa, E.; Welsh, T.; Hamouda, W. A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3496–3509. [[CrossRef](#)]
97. Ngu, A.H.; Gutierrez, M.; Metsis, V.; Nepal, S.; Sheng, Q.Z. IoT Middleware: A Survey on Issues and Enabling Technologies. *IEEE Internet Things J.* **2017**, *4*, 1–20. [[CrossRef](#)]
98. Hamad, S.A.; Sheng, Q.Z.; Zhang, W.E.; Nepal, S. Realizing an Internet of Secure Things: A Survey on Issues and Enabling Technologies. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1372–1391. [[CrossRef](#)]
99. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of Things Security: A Top-down Survey. *Comput. Netw.* **2018**, *141*, 199–221. [[CrossRef](#)]
100. Imran, Jamil, F.; Kim, D. An Ensemble of Prediction and Learning Mechanism for Improving Accuracy of Anomaly Detection in Network Intrusion Environments. *Sustainability* **2021**, *13*, 10057. [[CrossRef](#)]
101. Bhushan, B.; Sahoo, G. Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks. *Wirel. Pers. Commun.* **2018**, *98*, 2037–2077. [[CrossRef](#)]
102. Xu, R.; Wang, R.; Guan, Z.; Wu, L.; Wu, J.; Du, X. Achieving Efficient Detection Against False Data Injection Attacks in Smart Grid. *IEEE Access* **2017**, *5*, 13787–13798. [[CrossRef](#)]
103. Khan, M.A.; Salah, K. IoT Security: Review, Blockchain Solutions, and Open Challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [[CrossRef](#)]
104. Zha, X.; Zheng, K.; Zhang, D. Anti-Pollution Source Location Privacy Preserving Scheme in Wireless Sensor Networks. In Proceedings of the 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), London, UK, 27–30 June 2016; pp. 1–8.
105. Sicari, S.; Rizzardi, A.; Miorandi, D.; Coen-Porisini, A. REATO: REActing to Denial of Service Attacks in the Internet of Things. *Comput. Netw.* **2018**, *137*, 37–48. [[CrossRef](#)]
106. Huang, K.; Yang, L.-X.; Yang, X.; Xiang, Y.; Tang, Y.Y. A Low-Cost Distributed Denial-of-Service Attack Architecture. *IEEE Access* **2020**, *8*, 42111–42119. [[CrossRef](#)]
107. Restuccia, F.; D’Oro, S.; Melodia, T. Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking. *IEEE Internet Things J.* **2018**, *5*, 4829–4842. [[CrossRef](#)]
108. El Ioini, N.; Pahl, C. A Review of Distributed Ledger Technologies. In Proceedings of the On the Move to Meaningful Internet Systems. OTM 2018 Conferences, Valletta, Malta, 22–26 October 2018; Panetto, H., Debruyne, C., Proper, H.A., Ardagna, C.A., Roman, D., Meersman, R., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 277–288.
109. A Decentralized Scalable Security Framework for End-to-end Authentication of Future IoT Communication—Sheron—2020—Transactions on Emerging Telecommunications Technologies—Wiley Online Library. Available online: <https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3815> (accessed on 22 August 2021).
110. Bdiwi, R.; de Runz, C.; Faiz, S.; Cherif, A.A. A Blockchain Based Decentralized Platform for Ubiquitous Learning Environment. In Proceedings of the 2018 IEEE 18th International Conference on Advanced Learning Technologies (ICALT), Mumbai, India, 9–13 July 2018; pp. 90–92.
111. Tatschner, S.; Jarisch, F.; Giehl, A.; Plaga, S.; Neue, T. The Stream Exchange Protocol: A Secure and Lightweight Tool for Decentralized Connection Establishment. *Sensors* **2021**, *21*, 4969. [[CrossRef](#)] [[PubMed](#)]
112. Singh, S.K.; Kumar, S. Blockchain Technology: Introduction, Integration and Security Issues with IoT. *arXiv* **2021**, arXiv:2101.10921.
113. Kwon, J.H. Tail Behavior of Bitcoin, the Dollar, Gold and the Stock Market Index—ScienceDirect. *J. Int. Financ. Mark. Inst. Money* **2020**, *67*, 101202. Available online: <https://www.sciencedirect.com/science/article/pii/S104244312030086X> (accessed on 22 August 2021). [[CrossRef](#)]
114. Dasgupta, D.; Shrein, J.M.; Gupta, K.D. A Survey of Blockchain from Security Perspective. *J. Bank. Financ. Technol.* **2019**, *3*, 1–17. [[CrossRef](#)]
115. Soni, S.; Bhushan, B. A Comprehensive Survey on Blockchain: Working, Security Analysis, Privacy Threats and Potential Applications. In Proceedings of the 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICT), Kannur, India, 5–6 July 2019; Volume 1, pp. 922–926.
116. Pilkington, M. Blockchain Technology: Principles and Applications. In *Research Handbook on Digital Transformations*; Edward Elgar Publishing: Cheltenham, UK, 2016.
117. Iqbal, N.; Jamil, F.; Ahmad, S.; Kim, D. Toward Effective Planning and Management Using Predictive Analytics Based on Rental Book Data of Academic Libraries. *IEEE Access* **2020**, *8*, 81978–81996. [[CrossRef](#)]
118. Review of Blockchain Technology: Types of Blockchain and Their Application | Andreev | Intellect. Sist. Proizv. Available online: <http://izdat.istu.ru/index.php/ISM/article/view/4030> (accessed on 22 August 2021).
119. Ismailisufi, A.; Popović, T.; Gligorić, N.; Radonjic, S.; Šandi, S. A Private Blockchain Implementation Using Multichain Open Source Platform. In Proceedings of the 2020 24th International Conference on Information Technology (IT), Zabljak, Montenegro, 18–22 February 2020; Available online: <https://ieeexplore.ieee.org/abstract/document/9070689> (accessed on 22 August 2021).
120. Baliga, A.; Subhod, I.; Kamat, P.; Chatterjee, S. Performance evaluation of the quorum blockchain platform. *arXiv preprint* **2018**, arXiv:1809.03421.

121. She, W.; Gu, Z.-H.; Lyu, X.-K.; Liu, Q.; Tian, Z.; Liu, W. Homomorphic Consortium Blockchain for Smart Home System Sensitive Data Privacy Preserving. *IEEE Access* **2019**, *7*, 62058–62070. [CrossRef]
122. Zhang, X.; Chen, X. Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-Hoc Network. *IEEE Access* **2019**, *7*, 58241–58254. [CrossRef]
123. Karamitsos, I.; Papadaki, M.; Barghuthi, N.B.A. Design of the Blockchain Smart Contract: A Use Case for Real Estate. *J. Inf. Secur.* **2018**, *9*, 177. [CrossRef]
124. Glaser, F. Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain Enabled System and Use Case Analysis. In Proceedings of the 50th Annual Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, 4–7 January 2017.
125. Garewal, K.S. Merkle Trees. In *Practical Blockchains and Cryptocurrencies: Speed up Your Application Development Process and Develop Distributed Applications with Confidence*; Garewal, K.S., Ed.; Apress: Berkeley, CA, USA, 2020; pp. 137–148. ISBN 978-1-4842-5893-4.
126. Mohamed, K.S. Cryptography Concepts: Integrity, Authentication, Availability, Access Control, and Non-Repudiation. In *New Frontiers in Cryptography: Quantum, Blockchain, Lightweight, Chaotic and DNA*; Mohamed, K.S., Ed.; Springer International Publishing: Cham, Switzerland, 2020; pp. 41–63. ISBN 978-3-030-58996-7.
127. Mohanta, B.K.; Panda, S.S.; Jena, D. An Overview of Smart Contract and Use Cases in Blockchain Technology. In Proceedings of the 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 10–12 July 2018; pp. 1–4.
128. Jamil, F.; Iqbal, N.; Imran; Ahmad, S.; Kim, D. Peer-to-Peer Energy Trading Mechanism Based on Blockchain and Machine Learning for Sustainable Electrical Power Supply in Smart Grid. *IEEE Access* **2021**, *9*, 39193–39217. [CrossRef]
129. Hofmann, F.; Wurster, S.; Ron, E.; Böhmecke-Schwafert, M. The Immutability Concept of Blockchains and Benefits of Early Standardization. In Proceedings of the 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), Nanjing, China, 27–29 November 2017; pp. 1–8.
130. Vashi, S.; Ram, J.; Modi, J.; Verma, S.; Prakash, C. Internet of Things (IoT): A Vision, Architectural Elements, and Security Issues. 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. 492–496.
131. Survey on Blockchain for Internet of Things—ScienceDirect. Available online: <https://www.sciencedirect.com/science/article/pii/S0140366418306881> (accessed on 23 August 2021).
132. Wong, Z.S.Y.; Zhou, J.; Zhang, Q. Artificial Intelligence for Infectious Disease Big Data Analytics. *Infect. Dis. Health* **2019**, *24*, 44–48. [CrossRef]
133. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of Blockchains in the Internet of Things: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1676–1717. [CrossRef]
134. Dhanvijay, M.M.; Patil, S.C. Internet of Things: A Survey of Enabling Technologies in Healthcare and Its Applications. *Comput. Netw.* **2019**, *153*, 113–131. [CrossRef]
135. Fuller, T.; Fox, B.; Lake, D.; Crawford, K. Improving Real-Time Vital Signs Documentation. *Nurs. Manag.* **2018**, *49*, 28–33. [CrossRef]
136. Gogate, U.; Bakal, J. Healthcare Monitoring System Based on Wireless Sensor Network for Cardiac Patients. *Biomed. Pharmacol. J.* **2018**, *11*, 1681–1688. [CrossRef]
137. Alam, T. *mHealth Communication Framework Using Blockchain and IoT Technologies*; Social Science Research Network: Rochester, NY, USA, 2020.
138. Aung, M.S.H.; Alquaddoomi, F.; Hsieh, C.-K.; Rabbi, M.; Yang, L.; Pollak, J.P.; Estrin, D.; Choudhury, T. Leveraging Multi-Modal Sensing for Mobile Health: A Case Review in Chronic Pain. *IEEE J. Sel. Top. Signal Process.* **2016**, *10*, 962–974. [CrossRef]
139. Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0. *J. Ind. Inf. Integr.* **2020**, *18*, 100129. [CrossRef]
140. Marques, G.; Saini, J.; Pires, I.M.; Miranda, N.; Pitarma, R. Internet of Things for Enhanced Living Environments, Health and Well-Being: Technologies, Architectures and Systems. In *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*; Singh, P.K., Bhargava, B.K., Paprzycki, M., Kaushal, N.C., Hong, W.-C., Eds.; Advances in Intelligent Systems and Computing; Springer International Publishing: Cham, Switzerland, 2020; pp. 616–631. ISBN 978-3-030-40305-8.
141. Maksimović, M. The Roles of Nanotechnology and Internet of Nano Things in Healthcare Transformation. *Tecnológicas* **2017**, *20*, 139–153. [CrossRef]
142. Usak, M.; Kubiak, M.; Shabbir, M.S.; Viktorovna Dudnik, O.; Jermstittiparsert, K.; Rajabion, L. Health Care Service Delivery Based on the Internet of Things: A Systematic and Comprehensive Study. *Int. J. Commun. Syst.* **2020**, *33*, e4179. Available online: <https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.4179> (accessed on 23 August 2021). [CrossRef]
143. Santos, J.; Rodrigues, J.J.P.C.; Silva, B.M.C.; Casal, J.; Saleem, K.; Denisov, V. An IoT-Based Mobile Gateway for Intelligent Personal Assistants on Mobile Health Environments. *J. Netw. Comput. Appl.* **2016**, *71*, 194–204. [CrossRef]
144. Mehdi, H.; Zarrabi, H.; Zadeh, A.K.; Rahmani, A. Self-Adaptive Sampling Rate to Improve Network Lifetime Using Watchdog Sensor and Context Recognition in Wireless Body Sensor Networks. *Majlesi J. Electr. Eng.* **2020**, *14*, 11–22. [CrossRef]
145. Abu Bakar, N.A.; Wan Ramli, W.M.; Hassan, N.H. The Internet of Things in Healthcare: An Overview, Challenges and Model Plan for Security Risks Management Process. *Indones. J. Electr. Eng. Comput. Sci.* **2019**, *15*, 414. [CrossRef]

146. Anwar, M.; Abdullah, A.H.; Qureshi, K.N.; Majid, A.H. Wireless Body Area Networks for Healthcare Applications: An Overview. *Telkommika Telecommun. Comput. Electron. Control* **2017**, *15*, 1088. [CrossRef]
147. Azeez, N.A.; der Vyver, C.V. Security and Privacy Issues in E-Health Cloud-Based System: A Comprehensive Content Analysis. *Egypt. Inform. J.* **2019**, *20*, 97–108. [CrossRef]
148. Lam, M.C.; Ayob, M.; Lee, J.Y.; Abdullah, N.; Hamzah, F.A.; Zahir, S.S.M. Mobile-Based Hospital Bed Management with Near Field Communication Technology: A Case Study. *Eng. Technol. Appl. Sci. Res.* **2020**, *10*, 5706–5712. [CrossRef]
149. Khanna, A.; Kaur, S. Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. *Wirel. Pers. Commun.* **2020**, *114*, 1687–1762. [CrossRef]
150. Abidi, B.; Jilbab, A.; Mohamed, E.H. Wireless Body Area Networks: A Comprehensive Survey. *J. Med. Eng. Technol.* **2020**, *44*, 97–107. [CrossRef]
151. Ibrahim, M.; Iqbal, M.A.; Aleem, M.; Islam, M.A. SIM-Cumulus: An Academic Cloud for the Provisioning of Network-Simulation-as-a-Service (NSaaS). *IEEE Access* **2018**, *6*, 27313–27323. [CrossRef]
152. Khan, R.A.; Pathan, A.S.K. The State-of-the-Art Wireless Body Area Sensor Networks: A Survey. *Int. Int. Distrib. Sens. Netw.* **2018**, *14*, 1550147718768994. Available online: <https://journals.sagepub.com/doi/full/10.1177/1550147718768994> (accessed on 23 August 2021). [CrossRef]
153. Liu, Y.; Zhang, L.; Yang, Y.; Zhou, L.; Ren, L.; Wang, F.; Liu, R.; Pang, Z.; Deen, M.J. A Novel Cloud-Based Framework for the Elderly Healthcare Services Using Digital Twin. *IEEE Access* **2019**, *7*, 49088–49101. [CrossRef]
154. Boumezbeur, I.; Zarour, K. Privacy Preserving Requirements for Sharing Health Data in Cloud. In Proceedings of the Information Systems and Technologies to Support Learning, Fez, Morocco, 25–27 October 2018; Rocha, Á., Serrhini, M., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 412–423.
155. Darwish, A.; Hassani, A.E.; Elhoseny, M.; Sangaiyah, 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.* **2019**, *10*, 4151–4166. [CrossRef]
156. Navarro-Ortiz, J.; Romero-Diaz, P.; Sendra, S.; Ameigeiras, P.; Ramos-Munoz, J.J.; Lopez-Soler, J.M. A Survey on 5G Usage Scenarios and Traffic Models. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 905–929. [CrossRef]
157. Ibrahim, M.; Nabi, S.; Baz, A.; Alhakami, H.; Raza, M.S.; Hussain, A.; Salah, K.; Djemame, K. An In-Depth Empirical Investigation of State-of-the-Art Scheduling Approaches for Cloud Computing. *IEEE Access* **2020**, *8*, 128282–128294. [CrossRef]
158. Imran, Iqbal, N.; Ahmad, S.; Kim, D.H. Health Monitoring System for Elderly Patients Using Intelligent Task Mapping Mechanism in Closed Loop Healthcare Environment. *Symmetry* **2021**, *13*, 357. [CrossRef]
159. Bansal, M.; Sirpal, V. Fog Computing-Based Internet of Things and Its Applications in Healthcare. *J. Phys. Conf. Ser.* **2021**, *1916*, 012041. [CrossRef]
160. Muñoz, M.O.; Klatzky, R.; Wang, J.; Pillai, P.; Satyanarayanan, M.; Gross, J. Impact of Delayed Response on Wearable Cognitive Assistance. *PLoS ONE* **2021**, *16*, e0248690. [CrossRef]
161. 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]
162. Ibrahim, M.; Imran, M.; Jamil, F.; Lee, Y.-J.; Kim, D.-H. EAMA: Efficient Adaptive Migration Algorithm for Cloud Data Centers (CDCs). *Symmetry* **2021**, *13*, 690. [CrossRef]
163. Harerimana, G.; Jang, B.; Kim, J.W.; Park, H.K. Health Big Data Analytics: A Technology Survey. *IEEE Access* **2018**, *6*, 65661–65678. [CrossRef]
164. Alonso, S.G.; de la Torre Díez, I.; Zapiraín, B.G. Predictive, Personalized, Preventive and Participatory (4P) Medicine Applied to Telemedicine and EHealth in the Literature. *J. Med. Syst.* **2019**, *43*, 140. [CrossRef] [PubMed]
165. Hassan, R.; Qamar, F.; Hasan, M.K.; Aman, A.H.M.; Ahmed, A.S. Internet of Things and Its Applications: A Comprehensive Survey. *Symmetry* **2020**, *12*, 1674. [CrossRef]
166. Nigar, N.; Nazim Uddin, M. An Internet of Things Enabled Intelligent System and Smart Nutrition Card to Enhance Children’s Health Consciousness. In Proceedings of the IEEE International Conference on New Trends in Engineering & Technology (ICNTET) 2018, Chennai, Tamil Nadu, India, 7–8 September 2018.
167. Singh, B.; Bhattacharya, S.; Chowdhary, C.L.; Jat, D.S. A Review on Internet of Things and Its Applications in Healthcare. *J. Chem. Pharm. Sci.* **2017**, *10*, 7.
168. Chelliah, R.; Wei, S.; Daliri, E.B.-M.; Rubab, M.; Elahi, F.; Yeon, S.-J.; Jo, K.H.; Yan, P.; Liu, S.; Oh, D.H. Development of Nanosensors Based Intelligent Packaging Systems: Food Quality and Medicine. *Nanomaterials* **2021**, *11*, 1515. [CrossRef]
169. Thuemmler, C.; Bai, C. *Health 4.0: How Virtualization and Big Data Are Revolutionizing Healthcare*; Springer: Berlin/Heidelberg, Germany, 2017.
170. Khan, S.; Alam, M. Wearable Internet of Things for Personalized Healthcare: Study of Trends and Latent Research. In *Health Informatics: A Computational Perspective in Healthcare*; Patgiri, R., Biswas, A., Roy, P., Eds.; Studies in Computational Intelligence; Springer: Singapore, 2021; pp. 43–60. ISBN 9789811597350.
171. Nice, E.C. Challenges for Omics Technologies in the Implementation of Personalized Medicine. *Expert Rev. Precis. Med. Drug Dev.* **2018**, *3*, 229–231. [CrossRef]
172. Jamil, F.; Qayyum, F.; Alhelaly, S.; Javed, F.; Muthanna, A. Intelligent microservice based on blockchain for healthcare applications. *Comput. Mater. Contin.* **2021**, *69*, 2513–2530. [CrossRef]

173. Moro Visconti, R.; Martiniello, L. Smart Hospitals and Patient-Centered Governance. *Corp. Ownersh. Control.* **2019**, *16*, 14. [[CrossRef](#)]
174. Bohr, A.; Memarzadeh, K. Chapter 1—Current Healthcare, Big Data, and Machine Learning. In *Artificial Intelligence in Healthcare*; Bohr, A., Memarzadeh, K., Eds.; Academic Press: Cambridge, MA, USA, 2020; pp. 1–24. ISBN 978-0-12-818438-7.
175. Wafi, A.; Mirmezami, R. Translational –Omics: Future Potential and Current Challenges in Precision Medicine. *Methods* **2018**, *151*, 3–11. [[CrossRef](#)]
176. Wang, L.; Alexander, C. Chapter 2—Big Data in Personalized Healthcare. In *Big Data in Psychiatry & Neurology*; Moustafa, A.A., Ed.; Academic Press: Cambridge, MA, USA, 2021; pp. 35–49. ISBN 978-0-12-822884-5.
177. Senel, E.; Bas, Y. Evolution of Telepathology: A Comprehensive Analysis of Global Telepathology Literature between 1986 and 2017. *Turk. J. Pathol.* **2020**. [[CrossRef](#)] [[PubMed](#)]
178. Baba, E.; Jilbab, A.; Hammouch, A. A Health Remote Monitoring Application Based on Wireless Body Area Networks. In Proceedings of the 2018 International Conference on Intelligent Systems and Computer Vision (ISCV), Fez, Morocco, 2–4 April 2018; pp. 1–4.
179. Rani, A.A.V.; Baburaj, E. Secure and Intelligent Architecture for Cloud-Based Healthcare Applications in Wireless Body Sensor Networks. *Int. J. Biomed. Eng. Technol.* **2019**, *29*, 186–199. [[CrossRef](#)]
180. Papadopoulou, I.; Koulouglioti, C.; Lazzarino, R.; Ali, S. Enablers and Barriers to the Implementation of Socially Assistive Humanoid Robots in Health and Social Care: A Systematic Review. *BMJ Open* **2020**, *10*, e033096. [[CrossRef](#)] [[PubMed](#)]
181. Rajasekaran, M.P.; Radhakrishnan, S.; Subbaraj, P. Elderly patient monitoring system using a wireless sensor network. *Telemed. e-Health* **2009**, *15*, 73–79. [[CrossRef](#)]
182. Javed, A.R.; Sarwar, M.U.; Beg, M.O.; Asim, M.; Baker, T.; Tawfik, H. A Collaborative Healthcare Framework for Shared Healthcare Plan with Ambient Intelligence. *Hum.-Centric Comput. Inf. Sci.* **2020**, *10*, 40. [[CrossRef](#)]
183. Sahu, M.L.; Atulkar, M.; Ahirwal, M.K.; Ahamad, A. IoT-Enabled Cloud-Based Real-Time Remote ECG Monitoring System. *J. Med. Eng. Technol.* **2021**, *45*, 473–485. [[CrossRef](#)]
184. Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. *Computers* **2020**, *9*, 44. [[CrossRef](#)]
185. Letswamotse, B.B.; Malekian, R.; Chen, C.-Y.; Modiegyinyane, K.M. Software Defined Wireless Sensor Networks (SDWSN): A Review on Efficient Resources, Applications and Technologies. *J. Internet Technol.* **2018**, *19*, 1303–1313.
186. Filippeschi, A.; Schmitz, N.; Miezal, M.; Bleser, G.; Ruffaldi, E.; Stricker, D. Survey of Motion Tracking Methods Based on Inertial Sensors: A Focus on Upper Limb Human Motion. *Sensors* **2017**, *17*, 1257. [[CrossRef](#)]
187. Morishima, S.; Xu, Y.; Urashima, A.; Toriyama, T. Human Body Skin Temperature Prediction Based on Machine Learning. *Artif. Life Robot.* **2021**, *26*, 103–108. [[CrossRef](#)]
188. Wahid, F.; Fayaz, M.; Aljarbouh, A.; Mir, M.; Aamir, M.; Imran. Energy Consumption Optimization and User Comfort Maximization in Smart Buildings Using a Hybrid of the Firefly and Genetic Algorithms. *Energies* **2020**, *13*, 4363. [[CrossRef](#)]
189. Fernández-Caramés, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001. [[CrossRef](#)]
190. Ghaffar, Z.; Alshahrani, A.; Fayaz, M.; Alghamdi, A.M.; Gwak, J. A Topical Review on Machine Learning, Software Defined Networking, Internet of Things Applications: Research Limitations and Challenges. *Electronics* **2021**, *10*, 880. [[CrossRef](#)]
191. Mishra, S.S.; Rasool, A. IoT Health Care Monitoring and Tracking: A Survey. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 1052–1057.
192. Harbi, Y.; Aliouat, Z.; Harous, S.; Bentaleb, A.; Refoufi, A. A Review of Security in Internet of Things. *Wirel. Pers. Commun.* **2019**, *108*, 325–344. [[CrossRef](#)]
193. Panchatcharam, P.; Vivekanandan, S. Internet of Things (IOT) in Healthcare—Smart Health and Surveillance, Architectures, Security Analysis and Data Transfer: A Review. *Int. J. Softw. Innov. IJSI* **2019**, *7*, 21–40. [[CrossRef](#)]
194. Atlam, H.F.; Alenezi, A.; Allassafi, M.O.; Wills, G. Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. *Int. J. Intell. Syst. Appl.* **2018**, *10*, 40–48. [[CrossRef](#)]
195. Dai, H.-N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A Survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [[CrossRef](#)]
196. Wang, Q.; Zhu, X.; Ni, Y.; Gu, L.; Zhu, H. Blockchain for the IoT and Industrial IoT: A Review. *Internet Things* **2020**, *10*, 100081. [[CrossRef](#)]
197. Makhdoom, I.; Abolhasan, M.; Abbas, H.; Ni, W. Blockchain’s Adoption in IoT: The Challenges, and a Way Forward. *J. Netw. Comput. Appl.* **2019**, *125*, 251–279. [[CrossRef](#)]
198. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet Things J.* **2019**, *6*, 2188–2204. [[CrossRef](#)]
199. Imran, M.; Zaman, U.; Imran; Intiaz, J.; Fayaz, M.; Gwak, J. Comprehensive Survey of IoT, Machine Learning, and Blockchain for Health Care Applications: A Topical Assessment for Pandemic Preparedness, Challenges, and Solutions. *Electronics* **2021**, *10*, 2501. [[CrossRef](#)]
200. Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in Internet of Things: Challenges and Solutions. *arXiv* **2016**, arXiv:1608.05187.
201. Zheng, X.; Zhu, Y.; Si, X. A Survey on Challenges and Progresses in Blockchain Technologies: A Performance and Security Perspective. *Appl. Sci.* **2019**, *9*, 4731. [[CrossRef](#)]

202. Casino, F.; Politou, E.; Alepis, E.; Patsakis, C. Immutability and Decentralized Storage: An Analysis of Emerging Threats. *IEEE Access* **2020**, *8*, 4737–4744. [CrossRef]
203. Pan, X.; Pan, X.; Song, M.; Ai, B.; Ming, Y. Blockchain Technology and Enterprise Operational Capabilities: An Empirical Test. *Int. J. Inf. Manag.* **2020**, *52*, 101946. [CrossRef]
204. Buterin: On Settlement Finality—Google Scholar. Available online: https://scholar.google.com/scholar_lookup?title=On%20Settlement%20Finality&publication_year=2016&author=Vitalik%20Buterin (accessed on 21 August 2021).
205. Min, X.; Li, Q.; Liu, L.; Cui, L. A Permissioned Blockchain Framework for Supporting Instant Transaction and Dynamic Block Size. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016; pp. 90–96.
206. Ramachandran, G.S.; Krishnamachari, B. Blockchain for the IoT: Opportunities and Challenges. *arXiv* **2018**, arXiv:180502818.
207. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. *IEEE Access* **2019**, *7*, 66792–66806. [CrossRef]
208. Zhang, A.; Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *J. Med. Syst.* **2018**, *42*, 140. [CrossRef]
209. Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [CrossRef]
210. Gordon, W.J.; Catalini, C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 224–230. [CrossRef]
211. Omar, A.A.; Bhuiyan, M.Z.A.; Basu, A.; Kiyomoto, S.; Rahman, M.S. Privacy-Friendly Platform for Healthcare Data in Cloud Based on Blockchain Environment. *Future Gener. Comput. Syst.* **2019**, *95*, 511–521. [CrossRef]
212. Wang, Z.; Luo, N.; Zhou, P. GuardHealth: Blockchain Empowered Secure Data Management and Graph Convolutional Network Enabled Anomaly Detection in Smart Healthcare. *J. Parallel Distrib. Comput.* **2020**, *142*, 1–12. Available online: <https://www.sciencedirect.com/science/article/pii/S0743731519308470> (accessed on 24 August 2021). [CrossRef]
213. Celesti, A.; Ruggeri, A.; Fazio, M.; Galletta, A.; Villari, M.; Romano, A. Blockchain-Based Healthcare Workflow for Tele-Medical Laboratory in Federated Hospital IoT Clouds. *Sensors* **2020**, *20*, 2590. [CrossRef] [PubMed]
214. Jamil, F.; Kahng, H.K.; Kim, S.; Kim, D.-H. Towards Secure Fitness Framework Based on IoT-Enabled Blockchain Network Integrated with Machine Learning Algorithms. *Sensors* **2021**, *21*, 1640. [CrossRef]
215. 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]
216. Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D.-H. Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals. *Sensors* **2020**, *20*, 2195. [CrossRef]
217. Sukhwani, H.; Wang, N.; Trivedi, K.S.; Rindos, A. Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network). In Proceedings of the 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 1–3 November 2018; pp. 1–8.
218. Aneiros, A.; Hill, J.W.; Hogan, P.R. *Law and the Healthcare Crisis: The Impact of Medical Malpractice and Payment Systems on Physician Compensation and Workload as Antecedents of Physician Shortages—Analysis, Implications, and Reform Solutions*; Social Science Research Network: Rochester, NY, USA, 2021.
219. Pawar, P.; Parolia, N.; Shinde, S.; Edoh, T.O.; Singh, M. EHealthChain—A Blockchain-Based Personal Health Information Management System. *Ann. Telecommun.* **2022**, *77*, 33–45. [CrossRef]
220. Hossein, K.M.; Esmaili, M.E.; Dargahi, T.; Khonsari, A. Blockchain-Based Privacy-Preserving Healthcare Architecture. In Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019; pp. 1–4.
221. Yogeshwar, A.; Kamalakkannan, S. Healthcare Domain in IoT with Blockchain Based Security—A Researcher’s Perspectives. In Proceedings of the 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 6–8 May 2021; pp. 1–9.
222. Tariq, N.; Asim, M.; Al-Obeidat, F.; Zubair Farooqi, M.; Baker, T.; Hammoudeh, M.; Ghafir, I. The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey. *Sensors* **2019**, *19*, 1788. [CrossRef]
223. Myat, S.M.; Soe, T.N. Preserving the Privacy for University Data Using Blockchain and Attribute-Based Encryption. In Proceedings of the 2020 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 27–28 February 2020; pp. 1–5.
224. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things Security: A Survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
225. Imran; Ahmad, S.; Kim, D. Design and Implementation of Thermal Comfort System based on Tasks Allocation Mechanism in Smart Homes. *Sustainability* **2019**, *11*, 5849. [CrossRef]
226. Yang, Y.; Zheng, X.; Tang, C. Lightweight Distributed Secure Data Management System for Health Internet of Things. *J. Netw. Comput. Appl.* **2017**, *89*, 26–37. [CrossRef]
227. Verma, S. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. *Vikalpa* **2019**, *44*, 97–98. [CrossRef]
228. Ahmad, S.; Kim, D.H. Quantum GIS Based Descriptive and Predictive Data Analysis for Effective Planning of Waste Management. *IEEE Access* **2020**, *8*, 46193–46205. [CrossRef]

229. Jirkovský, V.; Obitko, M.; Mařík, V. Understanding Data Heterogeneity in the Context of Cyber-Physical Systems Integration. *IEEE Trans. Ind. Inform.* **2016**, *13*, 660–667. [CrossRef]
230. Palanisamy, V.; Thirunavukarasu, R. Implications of Big Data Analytics in Developing Healthcare Frameworks—A Review. *J. King Saud Univ. Comput. Inf. Sci.* **2019**, *31*, 415–425. [CrossRef]
231. Chang, H.; Choi, M. Big Data and Healthcare: Building an Augmented World. *Healthc. Inform. Res.* **2016**, *22*, 153–155. [CrossRef]
232. Ali, O.; Shrestha, A.; Soar, J.; Wamba, S.F. Cloud Computing-Enabled Healthcare Opportunities, Issues, and Applications: A Systematic Review. *Int. J. Inf. Manag.* **2018**, *43*, 146–158. [CrossRef]
233. Clim, A.; Zota, R.D.; Constantinescu, R. Data Exchanges Based on Blockchain in M-Health Applications. *Procedia Comput. Sci.* **2019**, *160*, 281–288. [CrossRef]
234. Fernández-Caramés, T.M.; Fraga-Lamas, P. Design of a Fog Computing, Blockchain and IoT-Based Continuous Glucose Monitoring System for Crowdsourcing MHealth. *Proceedings* **2018**, *4*, 37. [CrossRef]
235. Weiss, M.; Botha, A.; Herselman, M.; Loots, G. Blockchain as an Enabler for Public MHealth Solutions in South Africa. In Proceedings of the 2017 IST-Africa Week Conference (IST-Africa), Windhoek, Namibia, 31 May–2 June 2017; pp. 1–8.
236. Dias, J.P.; Sereno Ferreira, H.; Martins, Â. A Blockchain-Based Scheme for Access Control in e-Health Scenarios. In Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018), Porto, Portugal, 13–15 December 2018; Madureira, A.M., Abraham, A., Gandhi, N., Silva, C., Antunes, M., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 238–247.
237. Gan, C.; Saini, A.; Zhu, Q.; Xiang, Y.; Zhang, Z. Blockchain-Based Access Control Scheme with Incentive Mechanism for EHealth Systems: Patient as Supervisor. *Multimed. Tools Appl.* **2021**, *80*, 30605–30621. [CrossRef]
238. Sookhak, M.; Jabbarpour, M.R.; Safa, N.S.; Yu, F.R. Blockchain and Smart Contract for Access Control in Healthcare: A Survey, Issues and Challenges, and Open Issues. *J. Netw. Comput. Appl.* **2021**, *178*, 102950. [CrossRef]
239. Kubendiran, M.; Singh, S.; Sangaiah, A.K. Enhanced Security Framework for E-Health Systems Using Blockchain. *J. Inf. Process. Syst.* **2019**, *15*, 239–250. [CrossRef]
240. Franks, P.C. Implications of Blockchain Distributed Ledger Technology for Records Management and Information Governance Programs. *Rec. Manag. J.* **2020**, *30*, 287–299. [CrossRef]
241. Mendu, M.; Krishna, B.; Mohmmad, S.; Sharvani, Y.; Reddy, C.V.K. Secure Deployment of Decentralized Cloud in Blockchain Environment Using Inter-Planetary File System. *IOP Conf. Ser. Mater. Sci. Eng.* **2020**, *981*, 022037. [CrossRef]
242. Kirwan, M.; Mee, B.; Clarke, N.; Tanaka, A.; Manaloto, L.; Halpin, E.; Gibbons, U.; Cullen, A.; McGarrigle, S.; Connolly, E.M.; et al. What GDPR and the Health Research Regulations (HRRs) Mean for Ireland: “Explicit Consent”—A Legal Analysis. *Ir. J. Med. Sci.* **2021**, *190*, 515–521. [CrossRef]
243. Shuaib, M.; Alam, S.; Shabbir Alam, M.; Shahnawaz Nasir, M. Compliance with HIPAA and GDPR in Blockchain-Based Electronic Health Record. *Mater. Today Proc.* **2021**, *158*. [CrossRef]
244. Eberhardt, J.; Tai, S. On or off the Blockchain? Insights on Off-Chaining Computation and Data. In *Proceedings of the Service-Oriented and Cloud Computing*; De Paoli, F., Schulte, S., Broch Johnsen, E., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 3–15.
245. Zheng, X.; Mukkamala, R.R.; Vatrappu, R.; Ordieres-Mere, J. Blockchain-Based Personal Health Data Sharing System Using Cloud Storage. 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. 1–6.
246. Vora, J.; Nayyar, A.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Rodrigues, J.J.P.C. BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
247. Blockchain for Healthcare and Medical Systems: Security & Forensics Book Chapter | IGI Global. Available online: <https://www.igi-global.com/chapter/blockchain-for-healthcare-and-medical-systems/280854> (accessed on 24 August 2021).
248. Ge, C.; Liu, Z.; Fang, L. A Blockchain Based Decentralized Data Security Mechanism for the Internet of Things. *J. Parallel Distrib. Comput.* **2020**, *141*, 1–9. [CrossRef]
249. McKnight, M. IOT, Industry 4.0, Industrial IOT . . . Why Connected Devices Are the Future of Design. *KnE Eng.* **2017**, *2017*, 197–202. [CrossRef]
250. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient Healthcare Data Sharing via Blockchain. *Appl. Sci.* **2019**, *9*, 1207. [CrossRef]
251. Bodkhe, U.; Tanwar, S.; Bhattacharya, P.; Verma, A. Blockchain Adoption for Trusted Medical Records in Healthcare 4.0 Applications: A Survey. In Proceedings of the Second International Conference on Computing, Communications, and Cyber-Security, Delhi, India, 3–4 October 2020; Springer: Singapore, 2021; pp. 759–774.
252. Khatoun, A. A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics* **2020**, *9*, 94. [CrossRef]
253. Hathaliya, J.; Sharma, P.; Tanwar, S.; Gupta, R. Blockchain-Based Remote Patient Monitoring in Healthcare 4.0. In Proceedings of the 2019 IEEE 9th International Conference on Advanced Computing (IACC), Tiruchirappalli, India, 13–14 December 2019; pp. 87–91.
254. Hang, L.; Choi, E.; Kim, D.-H. A Novel EMR Integrity Management Based on a Medical Blockchain Platform in Hospital. *Electronics* **2019**, *8*, 467. [CrossRef]

255. Hossain, M.; Karim, Y.; Hasan, R. FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger. In Proceedings of the 2018 IEEE International Congress on Internet of Things (ICIoT), San Francisco, CA, USA, 2–7 July 2018; pp. 33–40.
256. Thampi, S.M.; Trajkovic, L.; Mitra, S.; Nagabhushan, P.; El-Alfy, E.-S.M.; Bojkovic, Z.; Mishra, D. *Intelligent Systems, Technologies and Applications: Proceedings of Fifth ISTA 2019, India*; Springer Nature: Berlin, Germany, 2020; ISBN 9789811539145.
257. Wang, Z.; Wang, L.; Xiao, F.; Chen, Q.; Lu, L.; Hong, J. A Traditional Chinese Medicine Traceability System Based on Lightweight Blockchain. *J. Med. Internet Res.* **2021**, *23*, e25946. [CrossRef]
258. Almulhim, M.; Islam, N.; Zaman, N. A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications. *Int. J. Comput. Sci. Netw. Secur.* **2019**, *19*, 14.
259. Tahir, M.; Sardaraz, M.; Muhammad, S.; Saud Khan, M. A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics. *Sustainability* **2020**, *12*, 6960. [CrossRef]
260. Khalid, U.; Asim, M.; Baker, T.; Hung, P.C.K.; Tariq, M.A.; Rafferty, L. A Decentralized Lightweight Blockchain-Based Authentication Mechanism for IoT Systems. *Clust. Comput.* **2020**, *23*, 2067–2087. [CrossRef]
261. Gupta, D.S.; Islam, S.H.; Obaidat, M.S.; Karati, A.; Sadoun, B. LAAC: Lightweight Lattice-Based Authentication and Access Control Protocol for E-Health Systems in IoT Environments. *IEEE Syst. J.* **2020**, *15*, 3620–3627. [CrossRef]
262. Ray, P.P.; Dash, D.; Salah, K.; Kumar, N. Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. *IEEE Syst. J.* **2021**, *15*, 85–94. [CrossRef]
263. Lee, C.H.; Yoon, H.-J. Medical Big Data: Promise and Challenges. *Kidney Res. Clin. Pract.* **2017**, *36*, 3–11. [CrossRef]
264. Jagadeeswari, V.; Subramaniaswamy, V.; Logesh, R.; Vijayakumar, V. A Study on Medical Internet of Things and Big Data in Personalized Healthcare System. *Health Inf. Sci. Syst.* **2018**, *6*, 14. [CrossRef]
265. Ahmad, S.; Imran, Iqbal, N.; Jamil, F.; Kim, D. Optimal Policy-Making for Municipal Waste Management Based on Predictive Model Optimization. *IEEE Access* **2020**, *8*, 218458–218469. [CrossRef]
266. Imran, Iqbal, N.; Ahmad, S.; Kim, D.H. Towards Mountain Fire Safety Using Fire Spread Predictive Analytics and Mountain Fire Containment in IoT Environment. *Sustainability* **2021**, *13*, 2461. [CrossRef]
267. Imran, I.; Zaman, U.; Waqar, M.; Zaman, A. Using Machine Learning Algorithms for Housing Price Prediction: The Case of Islamabad Housing Data. *Soft Comput. Mach. Intell.* **2021**, *1*, 11–23.
268. Men, L.; Ilk, N.; Tang, X.; Liu, Y. Multi-Disease Prediction Using LSTM Recurrent Neural Networks. *Expert Syst. Appl.* **2021**, *177*, 114905. Available online: <https://www.sciencedirect.com/science/article/pii/S0957417421003468> (accessed on 24 August 2021). [CrossRef]
269. Che, Z.; Purushotham, S.; Cho, K.; Sontag, D.; Liu, Y. Recurrent Neural Networks for Multivariate Time Series with Missing Values. *Sci. Rep.* **2018**, *8*, 6085. [CrossRef] [PubMed]
270. Johnson, A.E.; Ghassemi, M.M.; Nemati, S.; Niehaus, K.E.; Clifton, D.A.; Clifford, G.D. Machine Learning and Decision Support in Critical Care. *Proc. IEEE* **2016**, *104*, 444–466. [CrossRef]
271. Che, Z.; Liu, Y. Deep Learning Solutions to Computational Phenotyping in Health Care. In Proceedings of the 2017 IEEE International Conference on Data Mining Workshops (ICDMW), New Orleans, LA, USA, 18–21 November 2017; pp. 1100–1109.
272. Hu, Y.; Lee, V.C.S.; Tan, K. An Application of Convolutional Neural Networks for the Early Detection of Late-Onset Neonatal Sepsis. In Proceedings of the 2019 International Joint Conference on Neural Networks (IJCNN), Budapest, Hungary, 14–19 July 2019; pp. 1–8.
273. Jubair, F.; Al-karadsheh, O.; Malamos, D.; Al Mahdi, S.; Saad, Y.; Hassona, Y. A novel lightweight deep convolutional neural network for early detection of oral cancer. *Oral Dis.* **2022**, *28*, 1123–1130. [CrossRef]
274. Shah, S.A.; Ren, A.; Fan, D.; Zhang, Z.; Zhao, N.; Yang, X.; Luo, M.; Wang, W.; Hu, F.; Rehman, M.U.; et al. Internet of Things for Sensing: A Case Study in the Healthcare System. *Appl. Sci.* **2018**, *8*, 508. [CrossRef]
275. Chhetri, S.; Alsadoon, A.; Al-Dala'in, T.; Prasad, P.W.C.; Rashid, T.A.; Maag, A. Deep Learning for Vision-based Fall Detection System: Enhanced Optical Dynamic Flow. *Comput. Intell.* **2021**, *37*, 578–595. Available online: <https://onlinelibrary.wiley.com/doi/epdf/10.1111/coin.12428> (accessed on 23 August 2021). [CrossRef]
276. Li, X.; Pang, T.; Liu, W.; Wang, T. Fall Detection for Elderly Person Care Using Convolutional Neural Networks. In Proceedings of the 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), Shanghai, China, 14–16 October 2017; pp. 1–6.
277. Santos, G.L.; Endo, P.T.; de Monteiro, K.H.C.; da Rocha, E.S.; Silva, I.; Lynn, T. Accelerometer-Based Human Fall Detection Using Convolutional Neural Networks. *Sensors* **2019**, *19*, 1644. [CrossRef]
278. Şengül, G.; Karakaya, M.; Misra, S.; Abayomi-Alli, O.O.; Damaševičius, R. Deep learning based fall detection using smartwatches for healthcare applications. *Biomed. Signal Process. Control* **2022**, *71*, 103242. [CrossRef]
279. Torti, E.; Fontanella, A.; Musci, M.; Blago, N.; Pau, D.; Leporati, F.; Piastra, M. Embedded Real-Time Fall Detection with Deep Learning on Wearable Devices. In Proceedings of the 2018 21st Euromicro Conference on Digital System Design (DSD), Prague, Czech Republic, 29–31 August 2018; pp. 405–412.
280. Mauldin, T.R.; Canby, M.E.; Metsis, V.; Ngu, A.H.H.; Rivera, C.C. SmartFall: A Smartwatch-Based Fall Detection System Using Deep Learning. *Sensors* **2018**, *18*, 3363. [CrossRef] [PubMed]

281. Shi, B.; Grimm, L.J.; Mazurowski, M.A.; Baker, J.A.; Marks, J.R.; King, L.M.; Maley, C.C.; Hwang, E.S.; Lo, J.Y. Prediction of Occult Invasive Disease in Ductal Carcinoma in Situ Using Deep Learning Features. *J. Am. Coll. Radiol.* **2018**, *15*, 527–534. [[CrossRef](#)] [[PubMed](#)]
282. Manzanera, O.M.; Meles, S.K.; Leenders, K.L.; Renken, R.J.; Pagani, M.; Arnaldi, D.; Nobili, F.; Obeso, J.; Oroz, M.R.; Morbelli, S.; et al. Scaled Subprofile Modeling and Convolutional Neural Networks for the Identification of Parkinson's Disease in 3D Nuclear Imaging Data. *Int. J. Neural Syst.* **2019**, *29*, 1950010. [[CrossRef](#)] [[PubMed](#)]
283. Wang, J.; Ding, H.; Bidgoli, F.A.; Zhou, B.; Iribarren, C.; Molloy, S.; Baldi, P. Detecting Cardiovascular Disease from Mammograms With Deep Learning. *IEEE Trans. Med. Imaging* **2017**, *36*, 1172–1181. [[CrossRef](#)] [[PubMed](#)]
284. Liu, C.; Cao, Y.; Luo, Y.; Chen, G.; Vokkarane, V.; Yunsheng, M.; Chen, S.; Hou, P. A New Deep Learning-Based Food Recognition System for Dietary Assessment on An Edge Computing Service Infrastructure. *IEEE Trans. Serv. Comput.* **2018**, *11*, 249–261. [[CrossRef](#)]
285. Lu, Y.; Stathopoulou, T.; Vasiloglou, M.F.; Pinault, L.F.; Kiley, C.; Spanakis, E.K.; Mougiakakou, S. goFOODTM: An Artificial Intelligence System for Dietary Assessment. *Sensors* **2020**, *20*, 4283. [[CrossRef](#)]
286. Liu, C.; Cao, Y.; Luo, Y.; Chen, G.; Vokkarane, V.; Ma, Y. Deepfood: Deep Learning-Based Food Image Recognition for Computer-Aided Dietary Assessment. In Proceedings of the International Conference on Smart Homes and Health Telematics, Wuhan, China, 25–27 May 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 37–48.
287. Lu, N.; Wu, Y.; Feng, L.; Song, J. Deep Learning for Fall Detection: Three-Dimensional CNN Combined with LSTM on Video Kinematic Data. *IEEE J. Biomed. Health Inform.* **2018**, *23*, 314–323. [[CrossRef](#)]
288. Nait Aicha, A.; Englebienne, G.; Van Schooten, K.S.; Pijnappels, M.; Kröse, B. Deep Learning to Predict Falls in Older Adults Based on Daily-Life Trunk Accelerometry. *Sensors* **2018**, *18*, 1654. [[CrossRef](#)]
289. Shojaei-Hashemi, A.; Nasiopoulos, P.; Little, J.J.; Pourazad, M.T. Video-Based Human Fall Detection in Smart Homes Using Deep Learning. In Proceedings of the 2018 IEEE International Symposium on Circuits and Systems (ISCAS), Florence, Italy, 27–30 May 2018; pp. 1–5.
290. Pereira, C.R.; Pereira, D.R.; Papa, J.P.; Rosa, G.H.; Yang, X.-S. Convolutional Neural Networks Applied for Parkinson's Disease Identification. In *Machine Learning for Health Informatics*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 377–390.
291. Latif, S.; Usman, M.; Rana, R.; Qadir, J. Phonocardiographic Sensing Using Deep Learning for Abnormal Heartbeat Detection. *IEEE Sens. J.* **2018**, *18*, 9393–9400. [[CrossRef](#)]
292. Jo, B.W.; Khan, R.M.A.; Lee, Y.-S. Hybrid Blockchain and Internet-of-Things Network for Underground Structure Health Monitoring. *Sensors* **2018**, *18*, 4268. [[CrossRef](#)]
293. Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics* **2022**, *11*, 630. [[CrossRef](#)]
294. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A Decentralized Patient Agent Controlled Blockchain for Remote Patient Monitoring. In Proceedings of the 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 21–23 October 2019; pp. 1–8.
295. Manogaran, G.; Thota, C.; Lopez, D.; Sundarasekar, R. Big Data Security Intelligence for Healthcare Industry 4.0. In *Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing*; Thames, L., Schaefer, D., Eds.; Springer Series in Advanced Manufacturing; Springer International Publishing: Cham, Switzerland, 2017; pp. 103–126. ISBN 978-3-319-50660-9.
296. Rajabion, L.; Shaltoolki, A.A.; Taghikhah, M.; Ghasemi, A.; Badfar, A. Healthcare Big Data Processing Mechanisms: The Role of Cloud Computing. *Int. J. Inf. Manag.* **2019**, *49*, 271–289. [[CrossRef](#)]
297. Pramanik, P.K.D.; Pal, S.; Mukhopadhyay, M. Healthcare big data: A comprehensive overview. *Res. Anthol. Big Data Anal. Archit. Appl.* **2022**, 119–147. [[CrossRef](#)]
298. Persico, V.; Montieri, A.; Pescape, A. On the Network Performance of Amazon S3 Cloud-Storage Service. In Proceedings of the 2016 5th IEEE International Conference on Cloud Networking (Cloudnet), Pisa, Italy, 3–5 October 2016; pp. 113–118.
299. Persico, V.; Botta, A.; Marchetta, P.; Montieri, A.; Pescape, A. On the Performance of the Wide-Area Networks Interconnecting Public-Cloud Datacenters around the Globe. *Comput. Netw.* **2017**, *112*, 67–83. [[CrossRef](#)]
300. Kalyani, Y.; Collier, R. A Systematic Survey on the Role of Cloud, Fog, and Edge Computing Combination in Smart Agriculture. *Sensors* **2021**, *21*, 5922. [[CrossRef](#)]
301. "Fog Computing Challenges: A Systematic Review" by Avirup Dasgupta and Asif Gill. Available online: <https://aisel.aisnet.org/acis2017/79/> (accessed on 24 August 2021).
302. Bhatia, T.; Verma, A.K. Data Security in Mobile Cloud Computing Paradigm: A Survey, Taxonomy and Open Research Issues. *J. Supercomput.* **2017**, *73*, 2558–2631. [[CrossRef](#)]
303. Alharthi, A.; Krotov, V.; Bowman, M. Addressing Barriers to Big Data. *Bus. Horiz.* **2017**, *60*, 285–292. [[CrossRef](#)]
304. Sánchez-Guerrero, R.; Mendoza, F.A.; Diaz-Sanchez, D.; Cabarcos, P.A.; López, A.M. Collaborative Ehealth Meets Security: Privacy-Enhancing Patient Profile Management. *IEEE J. Biomed. Health Inform.* **2017**, *21*, 1741–1749. [[CrossRef](#)]
305. Skourletopoulos, G.; Mavromoustakis, C.X.; Mastorakis, G.; Batalla, J.M.; Dobre, C.; Panagiotakis, S.; Pallis, E. Big Data and Cloud Computing: A Survey of the State-of-the-Art and Research Challenges. In *Advances in Mobile Cloud Computing and Big Data in the 5G Era*; Mavromoustakis, C.X., Mastorakis, G., Dobre, C., Eds.; Studies in Big Data; Springer International Publishing: Cham, Switzerland, 2017; pp. 23–41. ISBN 978-3-319-45145-9.

306. Elbasani, E.; Siriporn, P.; Choi, J.S. A Survey on RFID in Industry 4.0. In *Internet of Things for Industry 4.0: Design, Challenges and Solutions*; Kanagachidambaresan, G.R., Anand, R., Balasubramanian, E., Mahima, V., Eds.; EAI/Springer Innovations in Communication and Computing; Springer International Publishing: Cham, Switzerland, 2020; pp. 1–16. ISBN 978-3-030-32530-5.
307. Li, X.; Li, D.; Wan, J.; Vasilakos, A.V.; Lai, C.-F.; Wang, S. A Review of Industrial Wireless Networks in the Context of Industry 4.0. *Wirel. Netw.* **2017**, *23*, 23–41. [[CrossRef](#)]
308. Mohanty, S.N.; Ramya, K.C.; Rani, S.S.; Gupta, D.; Shankar, K.; Lakshmanaprabu, S.K.; Khanna, A. An Efficient Lightweight Integrated Blockchain (ELIB) Model for IoT Security and Privacy. *Future Gener. Comput. Syst.* **2020**, *102*, 1027–1037. [[CrossRef](#)]
309. Xie, J.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Liu, Y. A Survey on the Scalability of Blockchain Systems. *IEEE Netw.* **2019**, *33*, 166–173. [[CrossRef](#)]
310. Viriyasitavat, W.; Anuphaptrirong, T.; Hoonsopon, D. When Blockchain Meets Internet of Things: Characteristics, Challenges, and Business Opportunities. *J. Ind. Inf. Integr.* **2019**, *15*, 21–28. [[CrossRef](#)]
311. Konstantinidis, I.; Siaminos, G.; Timplalexis, C.; Zervas, P.; Peristeras, V.; Decker, S. Blockchain for Business Applications: A Systematic Literature Review. In *Proceedings of the Business Information Systems*; Abramowicz, W., Paschke, A., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 384–399.