Integrated Blockchain-Cloud Architecture for Healthcare

Subjects: Health Care Sciences & Services

Contributor: Leila Ismail, Robertas Damaševičius

Blockchain is a disruptive technology for shaping the next era of a healthcare system striving for efficient and effective patient care. This is thanks to its peer-to-peer, secure, and transparent characteristics. On the other hand, cloud computing made its way into the healthcare system thanks to its elasticity and cost-efficiency nature. However, cloud-based systems fail to provide a secured and private patient-centric cohesive view to multiple healthcare stakeholders. In this situation, blockchain provides solutions to address security and privacy concerns of the cloud because of its decentralization feature combined with data security and privacy, while cloud provides solutions to the blockchain scalability and efficiency challenges. Therefore a novel paradigm of blockchain-cloud integration (BcC) emerges for the domain of healthcare.

Keywords: blockchain ; cloud computing ; electronic health records ; health data analytics ; healthcare system ; security ; privacy ; ehealth ; public health ; patient-centric

1. Introduction

The healthcare domain has been revolutionized over the last century by technological advancement [1]. This revolution aims to improve the diagnosis of diseases and their causes, quality of medical supplies, medical treatment, and to establish prevention plans on a global scale. The traditional client/server-based healthcare systems [2][3][4][5][6] suffer from security and privacy issues and lead to scattered patient's medical history delaying patient treatment [7][8]. Moreover, a patient needs to repeat medical tests when moving to another hospital. This increases the cost and time to the patient, and affects the patient's health due to repeated exposure to tests, such as X-rays and MRIs, that may develop side effects [9]. In addition, healthcare organizations are required to install and maintain infrastructure with up-to-date functionalities while complying with healthcare standards and regulations for the management of Electronic Health Records (EHRs). This leads to a high total cost of ownership. To address, these limitations of the client-server-based approach, the on-premise database migrated to cloud where the health records are maintained by a cloud service provider.

Cloud computing [10] allows convenient and on-demand network access to a shared pool of configurable computing resources. Motivated by the pay-as-use cloud model, medical organizations use cloud computing to manage electronic health records (EHRs), reducing the cost of ownership. The five-year cost of $11 million for an on-premise healthcare system can be reduced to $3.2 million using cloud. This also reduces the infrastructure set-up time from 16-week to 1-week (Healthcare system cost reduction using cloud-based approach: https://ehrintelligence.com/news/how-cloud-ehr-reduces-operating-costs-increases-computing-power, accessed on 27 May 2021). In addition, cloud provides efficient health records' access to multiple healthcare providers from a shared storage improving patient care. The number of health records is increasing at a rapid pace with the introduction of smart healthcare and IoT with biosensors for personalized patient-centric healthcare. The scalability and elasticity features of cloud computing aid in health records management, which requires powerful computing and large storage, for near real-time patient care. However, a cloud-based system suffers from the issues of security and privacy. Security issue refers to data integrity where the health records are under a constant threat of being modified. Privacy refers to the problem of unobservability, also known as data leakage, in which the patients' health records are being used without any track [11].

Currently, machine learning in cloud computing plays a pivotal role in disease diagnosis, but predominantly among the people living in remote areas where medical facilities are scarce. Diagnosis systems based on machine learning act as secondary readers and assist radiologists in the proper diagnosis of diseases, whereas cloud-based systems can support telehealth services and remote diagnostics [12].

Recent years have witnessed the Blockchain revolution paving the way towards its adoption by many application in the health domain, such as health records management [13][14][15][16][17], medical supply chain management [18][19], and

medical insurance claims [20][21]. The characteristics of blockchain make it a great potential for providing a patient-centric healthcare system, involving health stakeholders such as the patients, health professionals, insurance providers, pharmaceutical firms, and health governmental authorities.

From the technical aspect, blockchain is a peer-to-peer distributed system, which enables users to maintain a ledger of transactions that is replicated over multiple user servers [22]. The architecture allows all the network participants, i.e., health stakeholders, to verify and process health data transactions without the need for a trusted third party. In addition, the data stored in the blockchain is immutable, i.e., once the data is stored it cannot be modified or deleted, leading to enhanced security. This immutability enables audit trail, bringing in accountability, adding trust to the system, and alleviating privacy concerns [23][24]. These distinctive features of blockchain have triggered its wide adoption for health records management to address security and privacy issues, while providing access to patient's health history to multiple stakeholders for patient-centric health services. However, blockchain poses scalability issues as the network grows [25] and consequently more hardware and human resources have to be provisioned for the operation and maintenance of the blockchain platform, thus increasing the health organization's on-site cost. Moreover, blockchain suffers from the issues of high energy consumption (Bitcoin mining consumes more electricity a year than Ireland: https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes-electricity-ireland, accessed on 27 May 2021 and Bitcoin energy consumption index: https://digiconomist.net/bitcoin-energy-consumption, accessed on 27 May 2021) adding to blockchain operational cost.

2. Background and Motivation

2.1. Background

2.1.1. Cloud Computing

Cloud computing technology offers a shared pool of configurable hardware resources and software services over the Internet [10]. These resources can be speedily allocated and released without the system administrator's intervention. Cloud computing is mainly characterized by on-demand service, rapid elasticity, pay-per-use model, and multi-tenancy. Figure 1 shows the general overview of the cloud system architecture. The architecture consists of (1) cloud consumers that are individual users (patients and allied healthcare professionals) and/or organizations (hospitals) that uses the cloud services, (2) cloud broker that enables the communication between the cloud consumers and the cloud, and (3) cloud entity that makes the cloud services available to the consumers. The cloud consists of three layers: (1) physical resource layer, (2) resource abstraction and control layer, and (3) service layer. The physical layer consists of the hardware resources for processing, storage, and networking, and the facility resources for cooling, ventilation, power, and supply. The resource abstraction and control layer consists of the system components that enable access to the physical resources through a software abstraction. Abstraction components include virtual computing and virtual storage elements. This layer is also responsible for the efficient allocation and usage monitoring of the physical resources. The service layer consists of the interfaces required to access the cloud services. These services by the cloud are classified into Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS makes software available remotely to multi-tenant users as a web-based service, google mail for example. PaaS provides the environment and tools required to develop web-based applications, Amazon Web Services for example (Amazon Web Services (AWS) - Cloud computing services: https://aws.amazon.com/, accessed on 27 May 2021). IaaS offers virtualized hardware hosted in cloud data centers to the end-users for operations. The hardware involves storage, computing servers, and network components. NTT communications (NTT communications: https://www.ntt.com/en/index.html, accessed on 27 May 2021) is an example of IaaS.

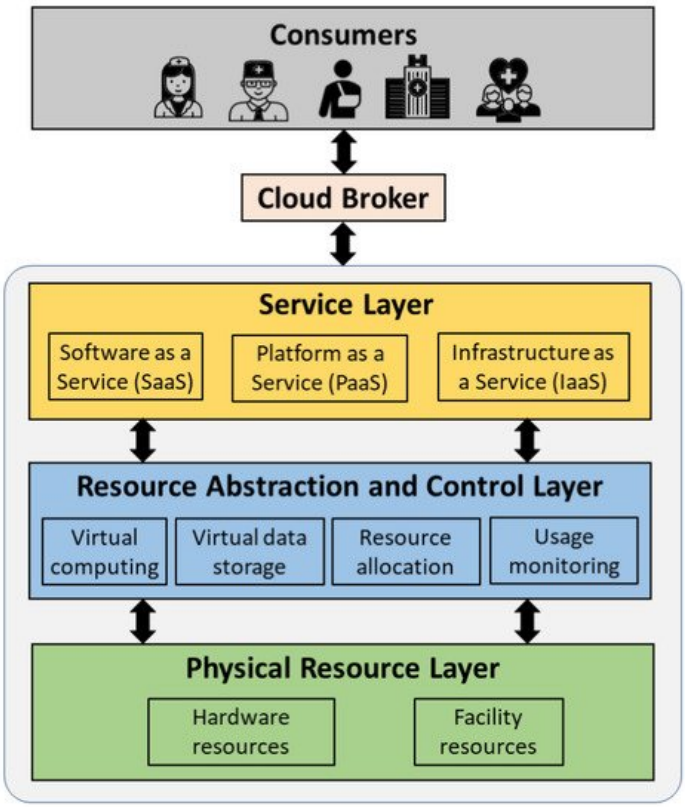

Figure 1. Overview of a cloud system architecture.

The cloud network can be divided into three main categories:

- *Public cloud:* Allows public access to systems and services without any restrictions and is less secure.
- *Private cloud:* Allows members of the organization that manages the cloud to access the systems and services and is more secure than a public cloud. A private cloud when shared among multiple organizations is known as a community cloud.
- *Hybrid cloud:* Combination of a public and private cloud that enables greater flexibility. The critical and confidential activities can be managed using the private cloud while the general activities can be managed using the public cloud.

With the emergence of cloud computing, the healthcare system migrated from client/ server-based to cloud-based. Cloud solves the issues of fragmented health records and the high total cost of ownership existing in the client/server-based healthcare system. This is thanks to the on-demand access, replication, and pay-as-use characteristics of the cloud. A cloud-based healthcare system is implemented using a private cloud to allow only authorized data access based on access control rights. Several cloud-based healthcare systems are proposed in the literature where a patient/allied health professional can obtain a cohesive view of the patient's medical history stored in third-party cloud storage [26][27][28]. Although, cloud-based approach improves system scalability and reduces the total cost of ownership, the health records managed by the cloud service provider are under constant security and privacy threats [29][30]. The patients' records can be easily tampered with or can be accessed without his/her knowledge [11]. Consequently, a more robust healthcare management system is required to address the shortcomings of the cloud-based approach.

2.1.2. Blockchain

Blockchain is a peer-to-peer distributed system that maintains a synchronized ledger of transactions that is replicated over network participants. It was introduced for the exchange of e-currency in a network without the intervention of a third-party [31]. Since then, blockchain has spread in several application domains such as healthcare, education, industry and marketplace, digital media, government, and entertainment. Blockchain has the following properties:

- *Decentralization:* Blockchain eliminates the intervention of a third-party entity for the processing of transactions and maintaining the ledger data. The transactions are validated and executed by the agreement of the majority of the participants that maintain the network.
- *Immutability:* The blockchain is a continuous chain of blocks where a block is connected to its preceding block by including the hash of the latter while hashing the former. A block is composed of a block header consisting of metadata

and a block body consisting of valid transactions [22]. If a malicious entity attempts to tamper with the data of a block in past, the hash of the block will change leading to a different hash value than the one used to calculate the hash of the succeeding block. Consequently, the malicious entity needs to re-hash all the subsequent blocks in the chain up till the last block. This re-hashing is compute-intensive especially when there are several replicated copies of the ledger in the network. Thus, any data modification attempt is discouraged leading to immutability.

- *Transparency:* Each operation performed in the network to access the data stored in the ledger is considered as a transaction in the blockchain. Each node in the network that holds the copy of the ledger can track any unauthorized or malicious data access, making the blockchain secure and transparent.

- *Traceability:* The replicated ledger in the blockchain enables efficient tracing of any transaction by the nodes maintaining the ledger. This discourages any malevolent activity, making the network more secure, efficient, and transparent.

- *Consensus:* Each transaction in the blockchain is verified and processed by the agreement of most of the participants holding the ledger copy. This enables transactions between participants who do not know and trust each other.

Figure 2 shows how a transaction is processed in the blockchain network. To initiate a new transaction, the transaction data is hashed by the transaction initiator, such as allied health professionals and patients. The digital signature of the transaction is generated by encrypting the hashed data. The encryption is performed using the private key of the transaction initiator. The transaction data and the corresponding digital signature are broadcasted to the network for processing. Each validating node in the network validates the transaction when received. This is by ensuring the authenticity of the transaction initiator and the integrity of the transaction data. The authenticity is verified if the digital signature is successfully decrypted using the transaction initiator's public key. The integrity is verified if the hashed data obtained from the decryption operation matches the hash of the transaction data. The transaction, if valid, is broadcasted in the network to include it in the block. A miner (node that generates a block) creates a block of the received valid transactions after verifying each transaction for its validity. The selection of a miner that generates a block and the procedure of verifying and appending the generated block to the chain depends on the consensus protocol used by the blockchain network. The consensus protocols in blockchain are classified into compute-intensive-based, capability-based and voting-based [22]. The selected miner generates the hash of the block, also known as the digital signature, and broadcasts the block in the network. The block's hash is generated by first hashing the block header and then hashing the obtained hashed value. The version in the block header represents the version of the protocol used and the timestamp represents the block generation time. The Merkle root is a single hash value obtained from iterative pair-wise hashing of the transactions in the block data. Each validating node will update their ledger copy by adding the block if valid [22].

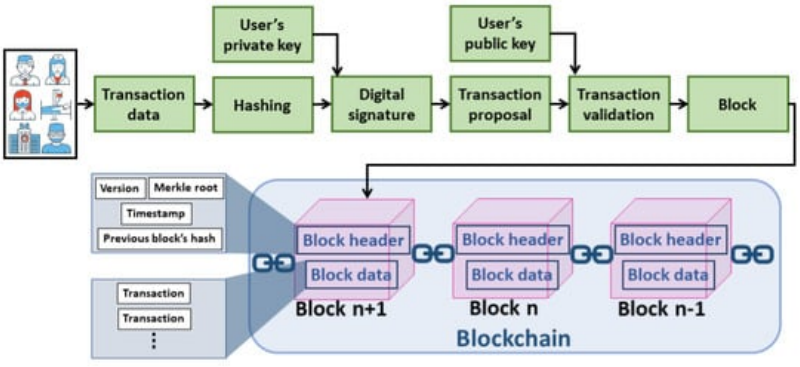

Figure 2. Processing of a transaction in blockchain.

The blockchain network can be a public, private, consortium, or hybrid. The public network is the one where any entity can join the network with no prior permission and view the transaction data. On the other hand, a private network, organized by a single organization, is the one where the participation is subjected to prior permission and the data can be accessed based on access control rights. A private blockchain is suitable for healthcare as only authorized members can join the network and the ledger is updated/queried using access control rights. A consortium blockchain is the one where a group of predetermined organizations governs the network. A hybrid blockchain lies between the public and the private ones where the ledger can be viewed by any network participant, but the modifications to the ledger are subject to access control. The distinctive features of the blockchain described above promise a great potential of the technology in the healthcare domain. A blockchain-based healthcare system has the following benefits:

- *Provenance:* The immutable blockchain ledger enables audit trail increasing the trust in the network. Any fraud in the network along with its source can be easily traced. This discourages malicious activities.

- *Protection against natural disasters:* In case of a natural disaster such as forest fires, hurricanes, and floods, a database and its regional replicas might be unavailable. In such a scenario, the globally replicated blockchain ledger can aid in fault tolerance.

- *Real-time data access:* Patient's health records can be accessed in real-time from the local or the nearest copy of the ledger to avoid life-threatening situations.

- *Accurate patient care:* The cohesive view of a patient's health records provided by the blockchain enables allied health professionals in better prognosis/diagnosis.

Several blockchain-based healthcare data management systems have been proposed in the literature [13][14][15][16][17]. However, with the increasing amount of health records, the scalability [25][32] and energy consumption (Bitcoin mining consumes more electricity a year than Ireland: https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes-electricity-ireland, accessed on 27 May 2021 and Bitcoin energy consumption index: https://digiconomist.net/bitcoin-energy-consumption, accessed on 27 May 2021) of blockchain is an issue. In addition, the on-premise blockchain deployment increases the total cost of ownership for healthcare organizations.

2.2. Motivation of Integrated BcC for Healthcare

Security and privacy are the main requirements for an effective, trustworthy, patient-centric, and accurate healthcare system. The cloud-based system provides scalability and cost-effectiveness for managing ever-growing health records. However, security and privacy threats become a critical issue due to the involvement of a third-party service provider. Consequently, the healthcare domain seeks a more robust solution for the management of health records. Blockchain, a peer-to-peer network allows transactions between multiple network participants eliminating the need for a third party. Every event in the network is recorded on an immutable ledger, which is replicated over multiple network nodes. Blockchain enables transparent auditing, authorized data access, and immutability, thus providing secure and private management of health records. However, the scalability and the total cost of ownership question the implementation of blockchain in the healthcare domain where the number of health records is continuously increasing. The integrated BcC healthcare system enhances the scalability and reduces the cost while maintaining the security and privacy of the health records.

Recently, there has been growing interest in AI-based healthcare where the health records are analyzed using AI and machine learning algorithms to support allied health professionals with better prognosis and diagnosis of diseases. The accuracy of the AI and machine learning can be improved resulting in a more accurate diagnosis and prognosis of a disease when more instances of data are used for training the models. In this context, an integrated BcC healthcare system would certainly revolutionize the way health professionals provide patient care. The blockchain will facilitate private and secure integration of data from multiple hospitals leading to a rich, secure and accurate database for the AI models and the cloud will enhance the scalability of the system. The incorporation of AI within an integrated BcC healthcare system could lead towards a better patient-centric, secure and private healthcare where the high availability of data from multiple sources, thanks to blockchain, can aid in better diagnosis and prognosis of disease using the AI and machine learning techniques in a scalable cloud environment.

3. Taxonomy and Strength/Weaknesses of Integrated BcC Healthcare System Architectures

The individual benefits of cloud and blockchain technologies have led to the emergence of integrated BcC architectures where the limitations of the stand-alone approaches are addressed. In this section, we present an analysis and classification of those architectures. We compare the BcC development platforms and services.

3.1. Encapsulated Architecture

In this architecture, the blockchain platform and its underlying implementation are encapsulated within a cloud environment as shown in Figure 3. We formulate the encapsulated architecture as stated in Equation (1). This architecture has been proposed by several works in the literature [33][34][35][36][37][38][39]. The network participants (users) are the different health stakeholders such as allied health professionals, patients, health insurance companies, pharmaceutical firms, and the health governmental authorities. The allied health professionals include doctors, nurses, dietitians, medical technologists, therapists, and pathologists. The users can connect to the platform via Remote Procedure Call (RPC), Representational state transfer (REST) Application Programming Interface (API), web API, or Simple Object Access Protocol (SOAP). The health records can be generated by the allied health professional upon patient's visit or by the patient using sensors. A gateway device is used to process the sensor data. The cloud platform consists of a certificate

authority, security management module, and operation management module, in addition to the blockchain as a service. The security management module involves identity and access management, cloud firewall, and web application firewall, and the operation management module includes bill management, data replication and recovery, resource monitoring (CPU, memory, and storage usage) and logs service. The blockchain encapsulated within the cloud consists of an application layer, distributed computing layer, and storage layer. The blockchain ledger in the cloud database is stored using the InterPlanetary File System (IPFS) [40] or storj (Decentralized cloud storage—Storj: https://storj.io/, accessed on 27 May 2021). The health transaction execution flow in this architecture is as follows:

(1)

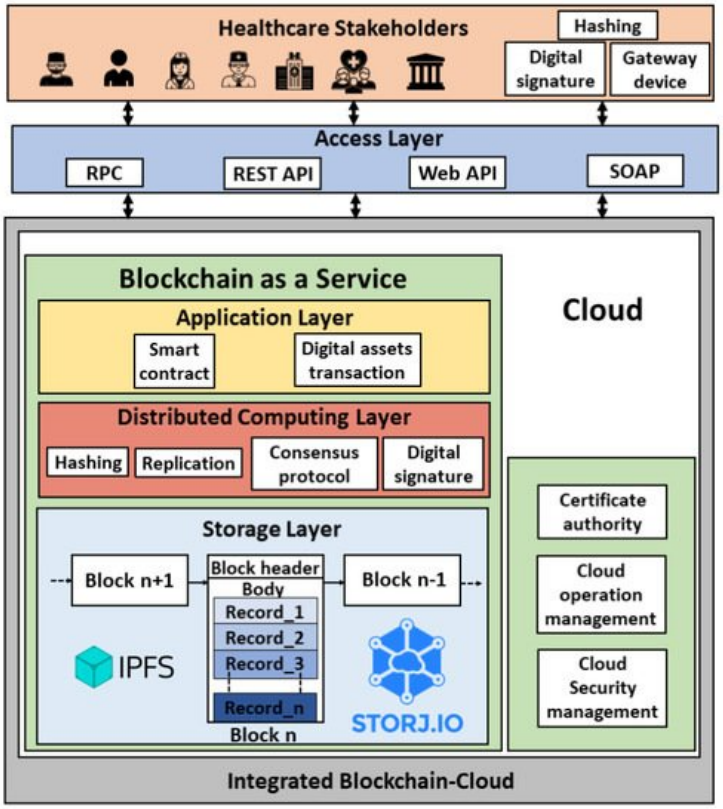

Figure 3. Encapsulated BcC architecture for healthcare.

Step 1:A transaction initiator (network participant) hashes the health record (transaction payload).

Step 2: The digital signature of the payload is generated by encrypting the hashed transaction.

Step 3: The transaction payload along with the digital signature is broadcasted to the blockchain nodes running in the cloud instances.

Step 4: The transaction is validated, and the block is generated based on the consensus mechanism.

Step 5: The block is updated to the ledger.

Several cloud service providers such as Microsoft Azure (Azure blockchain service: https://docs.microsoft.com/en-us/azure/blockchain/service/overview, accessed on 27 May 2021), Amazon (AWS Blockchain: https://aws.amazon.com/blockchain/, accessed on 27 May 2021), and Oracle (Oracle blockchain platform: https://www.oracle.com/ae/blockchain/, accessed on 27 May 2021) offer cloud-based solutions to help organizations adopt blockchain with ease. In 2015, Microsoft introduced Ethereum Blockchain as a Service (EBaaS) on its cloud platform Azure (Azure's Ethereum BaaS: https://azure.microsoft.com/en-us/blog/ethereum-blockchain-as-a-service-now-on-azure/, accessed on 27 May 2021). With BaaS, the compute and storage-intensive blockchain runs in the cloud and is managed by the cloud service provider. Blockchain is offered as a service, like any other cloud service, to the consumers (healthcare organizations) to develop and host their blockchain solutions, functions, and smart contracts. The organizations are only charged based on what they use, thanks to the pay-as-use cloud model. For instance, BaaS offered by Amazon Web Services charges $0.067/h for a medium instance peer node, $0.10/GB-month for node storage and data written to the network, and $0.05/GB for more than 150 TB/month data transfer (Amazon managed blockchain

pricing: https://aws.amazon.com/managed-blockchain/pricing/, accessed on 27 May 2021). Table 1 shows the encapsulated architecture-based cloud platforms that offer BaaS. It shows the blockchain development platforms supported by these cloud platforms, the type of blockchain network, the consensus mechanism used. In addition, it states whether or not the platform supports the channel. A channel is a private sub-network of communication between specific network participants to perform private and confidential transactions (Channels—Hyperledger Fabric: https://hyperledger-fabric.readthedocs.io/en/release-2.2/channels.html, accessed on 27 May 2021). The channel has its ledger which can only be accessed by the channel members. This is in addition to the main blockchain ledger. The concept of channel is important for healthcare applications in situations such as confidential patient treatment, biomedical research, and formulation of government policies and prevention plans.

Table 1. Encapsulated architecture-based development platforms.

Encapsulated BcC Platforms		Blockchain Network	Consensus	Description	Channel Support
Cloud	Blockchain				
Microsoft Azure	Ethereum, Hyperledger Fabric, Corda, Chain, and Quorum	Consortium	Istanbul byzantine fault tolerance	Azure Blockchain Service is a BaaS with built-in consortium management that enables quick network deployment and operations with smart contract capabilities. It can be deployed using Azure portal/CLI or through Microsoft Visual Studio Code using the Azure blockchain extension. The services are offered in two tiers: (1) basic, for development and testing, and (2) standard, for deployment.	Yes (Hyperledger Fabric)
Amazon	Hyperledger Fabric	Consortium	-	Amazon Managed Blockchain enables easy creation of blockchain networks. The platform uses a voting API, that allows network participants to vote for adding/removing members.	Yes
Oracle	Hyperledger Fabric	Hybrid	Raft	Oracle Blockchain Platform enables blockchain configuration, development and execution of smart contracts, and monitoring through a web console. External applications update/query via client SDKs or REST API calls.	Yes
IBM	Hyperledger Fabric	Private, public and hybrid	Pluggable consensus	IBM Blockchain Platform allows to develop, test and deploy blockchain applications with smart contract capabilities using Visual Studio code extension. The platform supports multiple languages for the development of smart contracts.	Yes
Google	Ethereum	Hybrid	Configurable consensus	Google blockchain enables deployment of blockchain applications with easy API integration. It allows the use of a traditional SQL database for blockchain data update/query.	No
SAP	Multichain, Hyperledger Fabric and Quorum	-	-	SAP Cloud Platform Blockchain Service enables development and deployment of blockchain applications from scratch, allows to link external blockchain nodes to the cloud or to connect an external blockchain to SAP's powerful memory data platform, HANA.	Yes (Hyperledger Fabric)
Hewlett-Packard (HP)	Ethereum	-	-	HPE Mission Critical Blockchain enables fault tolerant and highly scalable blockchain applications development with smart contract integration.	No
Alibaba	Hyperledger Fabric, Ant and Quorum	Consortium	-	Alibaba Cloud BaaS is developed on top of Alibaba cloud container service for Kubernetes clusters enabling quick development and deployment of blockchain solutions. Alibaba Cloud BaaS API allows users to manage the blockchain objects and cloud resources.	Yes (Hyperledger Fabric)

Encapsulated BcC Platforms		Blockchain Network	Consensus	Description	Channel Support
Cloud	**Blockchain**				
Huawei	**Hyperledger Fabric**	**Consortium**	**Solo, fast byzantine fault tolerance, and Kafka**	**Huawei Blockchain Service based on Huawei containers enables easy creation, deployment, and management of blockchain solutions.**	**Yes (Hyperledger Fabric)**
Baidu	**Permissioned Ethereum, Hyperledger Fabric, and Baidu XuperChain**	**-**	**Pluggable consensus**	**Baidu BaaS enables easy development and deployment of blockchain applications with multichain and smart contracts features.**	**Yes**

[1] Azure blockchain services https://docs.microsoft.com/en-us/azure/blockchain/service/overview, accessed on 27 May 2021; [2] AWS Blockchain https://aws.amazon.com/blockchain/, accessed on 27 May 2021; [3] Oracle blockchain platform https://www.oracle.com/ae/blockchain/, accessed on 27 May 2021; [4] IBM blockchain https://www.ibm.com/ae-en/blockchain, accessed on 27 May 2021; [5] Google cloud BaaS https://cloud.google.com/blog/products/data-analytics/building-hybrid-blockchain-cloud-applications-with-ethereum-andgoogle-cloud, accessed on 27 May 2021; [6] SAP blockchain applications and services https://www.sap.com/mena/products/intelligenttechnologies/blockchain.html, accessed on 27 May 2021; [7] HP blockchain solutions https://www.hpe.com/us/en/solutions/blockchain.html, accessed on 27 May 2021; [8] Alibaba cloud blockchain https://www.alibabacloud.com/products/baas, accessed on 27 May 2021; [9] Huawei blockchain service https://www.huaweicloud.com/intl/en-us/product/bcs.html, accessed on 27 May 2021; [10] Baidu blockchain service https://github.com/xuperchain/xuperchain, accessed on 27 May 2021.

In summary, encapsulated BcC healthcare system architecture incorporates blockchain technology and its functionalities within the cloud platform. The healthcare stakeholders have to trust the cloud service provider as the underlying blockchain is implemented and managed by the latter. Consequently, security and privacy issues are not completely addressed by the encapsulated BcC architecture. In this architecture, the system is upgraded by the cloud service provider.

3.2. Non-Encapsulated Architecture

To address the issues of security and privacy existing in encapsulated BcC architecture, non-encapsulated BcC architecture has been proposed in the literature [41][42][43][44][45][46][47][48][49][50][51][52][53][54][55][56][57][58][59][60][61][62][63][64] where the cloud and the blockchain technologies are integrated without encapsulating one into another as shown in Figure 4. We formulate the non-encapsulated architecture as stated in Equation (2). Compared to an encapsulated architecture where the blockchain ledger consisting of health records is managed by the cloud service provider, in non-encapsulated architecture, the health records are managed in the cloud database while the associated meta-data, such as health record's hash, record update, and query events, and access control policy, is recorded in the blockchain. The medical records in the cloud database are stored using IPFS or storj. The blockchain ledger is replicated across multiple healthcare organizations' databases. This architecture consists of an additional integrator component compared to the encapsulated one. The integrator enables communication between the cloud and the blockchain platforms. The health transaction execution flow in this architecture is executed as follows:

(2)

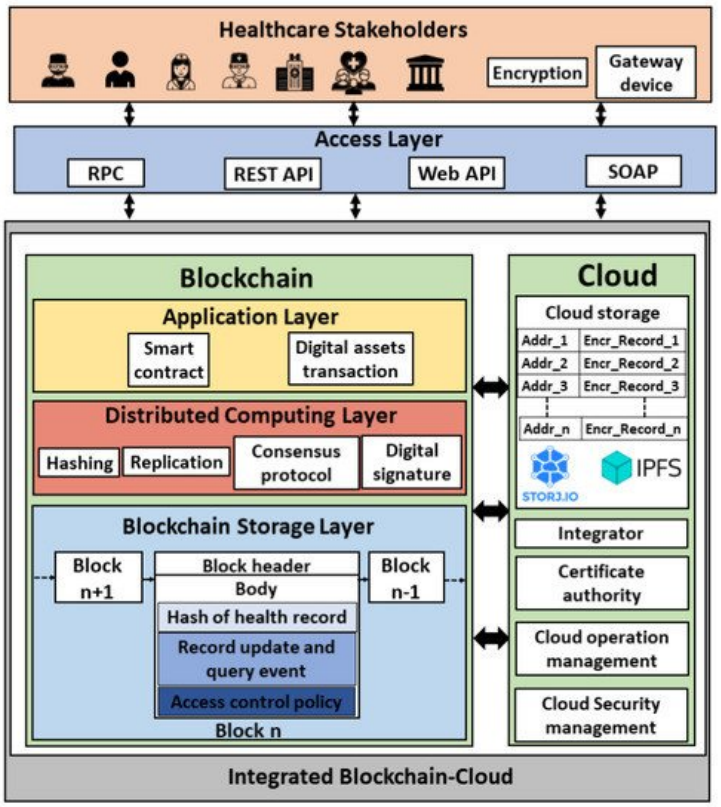

Figure 4. Non-encapsulated BcC architecture for healthcare.

Step 1: The health records data is encrypted by the transaction initiator (network participant) and broadcasted to the third-party cloud database.

Step 2: The data is stored in the cloud database.

Step 3: The meta-data of the health record such as the hash of the data, the address in the cloud where the data is stored, and the access control list containing the IDs of the authorized participants is sent to the blockchain by the integrator.

Step 4: The meta-data is recorded in the blockchain as a transaction and the ledge is updated upon consensus.

The off-chain storage for health records in the cloud database enhances the scalability of the system, whereas the meta-data of the transactions in the blockchain ledger aids in security and privacy. The inclusion of the health record's hash in the blockchain transaction ensures the integrity of the record and the inclusion of record update/query events discourages unobserved access enhancing the system privacy. Table 2 shows the contents of the off-chain storage and the blockchain transactions for the non-encapsulated architecture proposed in the literature. It shows that [41][42][43][44][45][46][47][48][49][50][51][52] store the encrypted health records data in the cloud database, whereas [53] stores the extraction signature along with the encrypted health records data, and [54][55][56][57][58][59][60][61][62][63][64][65] store the clear health records data in the cloud. Extraction signature is the one generated for the health records data after removing the sensitive information from the originally signed data [64]. Regarding the blockchain transaction, some works include the hash of the health records that are stored in the cloud database as transaction payload. This ensures security in terms of data integrity because any modification to the record will result in a new hash value that will be different from the one stored in the blockchain. Other works record either data update and/or query events to the cloud database as transactions in the blockchain. It is crucial to record the cloud data update and query events as blockchain transactions to ensure the privacy of health records because any malicious access to the database will be logged and audit-trailed. Consequently, this discourages malevolent activities. However, very few works [42][51][59][61] consider security and privacy in their non-encapsulated BcC architecture (Table 2). In addition, [45][47][49][53][54][55][56][59][61] include the access control policy in the blockchain transactions for authorized cloud data access.

Table 2. Contents of off-chain cloud storage and blockchain transaction in non-encapsulated BcC architectures proposed in the literature.

Work	Cloud Database	Blockchain Transaction		Inclusion of Health Record's Hash	Access Control Policy
		Transaction Types			
		Record Update Event	Record Query Event		
[41]	Encrypted health record	✓	✓	✗	✗
[42]		✓	✓	✓	✗
[43]		✓	✓	✗	✗
[44]		✓	✗	✓	✓
[45]		✓	✗	✗	✗
[46]		✗	✗	✗	✗
[47]		✓	✗	✓	✓
[48]		✓	✗	✓	✗
[49]		✓	✗	✗	✗
[50]		✓	✗	✓	✓
[51]		✓	✓	✓	✗
[52]		✓	✓	✗	✗
[53]	Encrypted health record and the extraction signature	✓	✓	✗	✓
[54]	Health record	✓	✓	✗	✓
[55]		✓	✗	✓	✗
[56]		✗	✓	✗	✓
[57]		✓	✗	✗	✗
[58]		✓	✗	✓	✗
[59]		✓	✓	✓	✓
[60]		✓	✓	✗	✗
[61]		✓	✓	✓	✓
[62]		✓	✓	✗	✗
[63]		✗	✓	✗	✗
[64]		✓	✓	✗	✗

In summary, non-encapsulated BcC architecture is suitable for healthcare applications as it is more secure and private compared to the encapsulated architecture. The patients' medical records are stored in the cloud, but the blockchain is implemented outside the cloud and each healthcare stakeholder owns a copy of the ledger that consists of the medical metadata leading to a secure and private healthcare system. In this architecture, the system is upgraded by the cloud service provider hosting the health records. However, in both encapsulated and non-encapsulated architectures, the patients' medical records are stored in the third-party cloud database which might delay the patient treatment as the data is not locally available to the allied health professionals.

Table 3 shows the strengths and weaknesses of cloud-based, blockchain-based, and integrated BcC healthcare systems. It shows whether or not these systems satisfy the security, privacy, scalability, and real-time data access requirements. The elastic and dynamic characteristics of a cloud-based system offer scalability, but the system suffers from the issues of security, privacy, and real-time data access. A blockchain-based system ensures security, privacy, and real-time data access (from the local copy of the ledger), but is not scalable. The encapsulated BcC system offers scalability as the blockchain is implemented within the cloud. However, cloud storage suffers from security, privacy, and real-time data access issues. The non-encapsulated BcC system is secure, private, and scalable. However, as the health records are stored in the cloud, real-time data access is an issue.

Table 3. Strengths and weaknesses of cloud-based, blockchain-based and integrated BcC healthcare systems.

Healthcare System		Security	Privacy	Scalability	Real-Time Data Access	Remarks
Cloud-based		✗	✗	✓	✗	The system scales but suffers from security and privacy issues. The health records can not be accessed in real-time as they are stored in the cloud.
Blockchain-based		✓	✓	✗	✓	The system ensures security and privacy, and enables real-time of the health records from the local copy of the ledger. However, it does not scale.
Integrated BcC	Encapsulated	✗	✗	✓	✗	The system scales but suffers from security and privacy issues. The health records can not be accessed in real-time as they are stored in the cloud.
	Non-encapsulated	✓	✓	✓	✗	The system scales and ensures security and privacy. The health records can not be accessed in real-time as they are stored in the cloud.

Security: ✓ → the system ensures data integrity and ✗ → the system does not ensure data integrity. Privacy: ✓ → the system ensures data privacy and ✗ → the system does not ensure data privacy. Scalability: ✓ → the system scales when the number of nodes increases and ✗ → the system does not scale. Real-time data access: ✓ → the system allows real-time access of health records and ✗ → the system does not allow real-time access of health records.

References

1. Ismail, L.; Materwala, H.; Karduck, A.P.; Adem, A. Requirements of Health Data Management Systems for Biomedical Care and Research: Scoping Review. J. Med. Internet Res. 2020, 22, e17508.
2. Rind, D.M.; Kohane, I.S.; Szolovits, P.; Safran, C.; Chueh, H.C.; Barnett, G.O. Maintaining the confidentiality of medical records shared over the Internet and the World Wide Web. Ann. Intern. Med. 1997, 127, 138–141.
3. Schoenberg, R.; Safran, C. Internet based repository of medical records that retains patient confidentiality. BMJ 2000, 3 21, 1199–1203.
4. Uckert, F.; Görz, M.; Ataian, M.; Prokosch, H.U. Akteonline-an electronic healthcare record as a medium for information and communication. Stud. Health Technol. Inform. 2002, 90, 293–297.
5. Grant, R.W.; Wald, J.S.; Poon, E.G.; Schnipper, J.L.; Gandhi, T.K.; Volk, L.A.; Middleton, B. Design and implementation of a web-based patient portal linked to an ambulatory care electronic health record: Patient gateway for diabetes collab orative care. Diabetes Technol. Ther. 2006, 8, 576–586.
6. Gritzalis, D.; Lambrinoudakis, C. A security architecture for interconnecting health information systems. Int. J. Med. Info rm. 2004, 73, 305–309.
7. Ismail, L.; Materwala, H. BlockHR: A Blockchain-based Framework for Health Records Management. In Proceedings of the 12th International Conference on Computer Modeling and Simulation, Brisbane, Australia, 23–25 June 2020; pp. 16 4–168.
8. Ismail, L.; Materwala, H.; Khan, M.A. Performance Evaluation of a Patient-Centric Blockchain-based Healthcare Recor ds Management Framework. In Proceedings of the 2020 2nd International Electronics Communication Conference, Sin gapore, 8–10 July 2020; pp. 39–50.
9. Chang, P.; Bjornstad, K.; Rosen, C.; McNamara, M.; Mancini, R.; Goldstein, L.; Chylack, L.; Blakely, E. Effects of iron io ns, protons and X rays on human lens cell differentiation. Radiat. Res. 2005, 164, 531–539.
10. Mell, P.; Grance, T. The NIST Definition of Cloud Computing. 2011. Available online: (accessed on 27 May 2021).
11. Pfitzmann, A.; Köhntopp, M. Anonymity, unobservability, and pseudonymity—A proposal for terminology. In Designing P rivacy Enhancing Technologies; Springer: Berlin/Heidelberg, Germany, 2001; pp. 1–9.
12. Vivek Lahoura; Harpreet Singh; Ashutosh Aggarwal; Bhisham Sharma; Mazin Mohammed; Robertas Damaševičius; Se ifedine Kadry; Korhan Cengiz; Cloud Computing-Based Framework for Breast Cancer Diagnosis Using Extreme Learni ng Machine. *Diagnostics* **2021**, *11*, 241, 10.3390/diagnostics11020241.

13. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
14. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. 2018, 39, 283–297.
15. Li, H.; Zhu, L.; Shen, M.; Gao, F.; Tao, X.; Liu, S. Blockchain-based data preservation system for medical data. J. Med. Syst. 2018, 42, 141.
16. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. J. Med. Syst. 2018, 42, 136.
17. Dey, T.; Jaiswal, S.; Sunderkrishnan, S.; Katre, N. HealthSense: A medical use case of Internet of Things and blockchain. In Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 7–8 December 2017; pp. 486–491.
18. Jamil, F.; Hang, L.; Kim, K.; Kim, D. A novel medical blockchain model for drug supply chain integrity management in a smart hospital. Electronics 2019, 8, 505.
19. Jayaraman, R.; Salah, K.; King, N. Improving Opportunities in healthcare supply chain processes via the Internet of Things and Blockchain Technology. Int. J. Healthc. Inf. Syst. Inform. (IJHISI) 2019, 14, 49–65.
20. He, X.; Alqahtani, S.; Gamble, R. Toward privacy-assured health insurance claims. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1634–1641.
21. Ismail, L.; Zeadally, S. Healthcare Insurance Frauds: Taxonomy and Blockchain-based Detection Framework (Block-HI). IEEE IT Prof. 2020.
22. Ismail, L.; Materwala, H. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. Symmetry 2019, 11, 1198.
23. Bordel, B.; Alcarria, R.; Martin, D.; Sanchez-Picot, A. Trust provision in the internet of things using transversal blockchain networks. Intell. Autom. Soft Comput. 2019, 25, 155–170.
24. Le Nguyen, B.; Lydia, E.L.; Elhoseny, M.; Pustokhina, I.; Pustokhin, D.A.; Selim, M.M.; Nguyen, G.N.; Shankar, K. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. Comput. Mater. Contin. 2020, 65, 87–107.
25. Ismail, L.; Materwala, H. Blockchain Paradigm for Healthcare: Performance Evaluation. Symmetry 2020, 12, 1200.
26. Bahga, A.; Madisetti, V.K. A cloud-based approach for interoperable electronic health records (EHRs). IEEE J. Biomed. Health Inform. 2013, 17, 894–906.
27. Fernández-Cardeñosa, G.; de la Torre-Díez, I.; López-Coronado, M.; Rodrigues, J.J. Analysis of cloud-based solutions on EHRs systems in different scenarios. J. Med. Syst. 2012, 36, 3777–3782.
28. Zangara, G.; Corso, P.P.; Cangemi, F.; Millonzi, F.; Collova, F.; Scarlatella, A. A Cloud Based Architecture to Support Electronic Health Record; IOS Press: Amsterdam, The Netherlands, 2014; Volume 207, pp. 380–389.
29. Patil, H.K.; Seshadri, R. Big data security and privacy issues in healthcare. In Proceedings of the 2014 IEEE International Congress on Big Data, Anchorage, AK, USA, 27 June–2 July 2014; pp. 762–765.
30. Abbas, A.; Khan, S.U. e-Health cloud: Privacy concerns and mitigation strategies. In Medical Data Privacy Handbook; Springer: Basel, Switzerland, 2015; pp. 389–421.
31. Nakamoto, S. Bitcoin: A Peer-To-Peer Electronic Cash System. 2008. Available online: (accessed on 27 May 2021).
32. Ismail, L.; Materwala, H.; Zeadally, S. Lightweight blockchain for healthcare. IEEE Access 2019, 7, 149935–149951.
33. Cao, S.; Zhang, G.; Liu, P.; Zhang, X.; Neri, F. Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Inf. Sci. 2019, 485, 427–440.
34. Al Omar, 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.
35. Kurdi, H.; Alsalamah, S.; Alatawi, A.; Alfaraj, S.; Altoaimy, L.; Ahmed, S.H. Healthybroker: A trustworthy blockchain-based multi-cloud broker for patient-centered ehealth services. Electronics 2019, 8, 602.
36. Kubendiran, M.; Singh, S.; Sangaiah, A.K. Enhanced Security Framework for E-Health Systems using Blockchain. J. Inf. Process. Syst. 2019, 15.

37. Nagasubramanian, G.; Sakthivel, R.K.; Patan, R.; Gandomi, A.H.; Sankayya, M.; Balusamy, B. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. Appl. 2020, 32, 639–647.
38. Kaur, H.; Alam, M.A.; Jameel, R.; Mourya, A.K.; Chang, V. A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. J. Med. Syst. 2018, 42, 156.
39. Park, J.; Park, S.; Kim, K.; Lee, D. CORUS: Blockchain-based trustworthy evaluation system for efficacy of healthcare remedies. In Proceedings of the 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Nicosia, Cyprus, 10–13 December 2018; pp. 181–184.
40. Benet, J. Ipfs-content addressed, versioned, p2p file system. arXiv 2014, arXiv:1407.3561.
41. Du, Y.; Liu, J.; Guan, Z.; Feng, H. A medical information service platform based on distributed cloud and blockchain. In Proceedings of the 2018 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, USA, 21–23 September 2018; pp. 34–39.
42. Thwin, T.T.; Vasupongayya, S. Blockchain based secret-data sharing model for personal health record system. In Proceedings of the 2018 5th International Conference on Advanced Informatics: Concept Theory and Applications (ICAICTA), Krabi, Thailand, 14–17 August 2018; pp. 196–201.
43. Zheng, X.; Mukkamala, R.R.; Vatrapu, 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.
44. Rouhani, S.; Butterworth, L.; Simmons, A.D.; Humphery, D.G.; Deters, R. MediChain TM: A secure decentralized medical data asset management system. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1533–1538.
45. Wang, H.; Song, Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. J. Med. Syst. 2018, 42, 152.
46. Christo, M.S.; Sarathy, P.; Priyanka, C. An Efficient Data Security in Medical Report using Block Chain Technology. In Proceedings of the 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 4–6 April 2019; pp. 606–610.
47. Feng, T.; Jiao, Y.; Fang, J. Secure Sharing Model Based on Block Chain in Medical Cloud (Short Paper). In International Conference on Collaborative Computing: Networking, Applications and Worksharing; Springer: Cham, Switzerland, 2019; pp. 429–438.
48. Xu, J.; Xue, K.; Li, S.; Tian, H.; Hong, J.; Hong, P.; Yu, N. Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet Things J. 2019, 6, 8770–8781.
49. Chen, L.; Lee, W.K.; Chang, C.C.; Choo, K.K.R.; Zhang, N. Blockchain based searchable encryption for electronic health record sharing. Future Gener. Comput. Syst. 2019, 95, 420–429.
50. Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. Blockchain-based medical records secure storage and medical service framework. J. Med. Syst. 2019, 43, 5.
51. Wang, S.; Zhang, D.; Zhang, Y. Blockchain-based personal health records sharing scheme with data integrity verifiable. IEEE Access 2019, 7, 102887–102901.
52. Wang, Y.; Zhang, A.; Zhang, P.; Wang, H. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. IEEE Access 2019, 7, 136704–136719.
53. Liu, J.; Li, X.; Ye, L.; Zhang, H.; Du, X.; Guizani, M. BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
54. Theodouli, A.; Arakliotis, S.; Moschou, K.; Votis, K.; Tzovaras, D. On the design of a Blockchain-based system to facilitate Healthcare Data Sharing. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy in Computing and Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1374–1379.
55. Badr, S.; Gomaa, I.; Abd-Elrahman, E. Multi-tier blockchain framework for IoT-EHRs systems. Procedia Comput. Sci. 2018, 141, 159–166.
56. Nguyen, D.C.; Nguyen, K.D.; Pathirana, P.N. A mobile cloud based iomt framework for automated health assessment and management. In Proceedings of the 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Berlin, Germany, 23–27 July 2019; pp. 6517–6520.

57. Guo, R.; Shi, H.; Zheng, D.; Jing, C.; Zhuang, C.; Wang, Z. Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system. IEEE Access 2019, 7, 88012–88025.
58. 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.
59. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In Proceedings of the 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.
60. Iqbal, J.; Umar, A.I.; Amin, N.; Waheed, A. Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain. Int. J. Distrib. Sens. Netw. 2019, 15, 1550147719875654.
61. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. Sensors 2019, 19, 326.
62. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Continuous patient monitoring with a patient centric agent: A block architecture. IEEE Access 2018, 6, 32700–32726.
63. 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.
64. Steinfeld, R.; Bull, L.; Zheng, Y. Content extraction signatures. In International Conference on Information Security and Cryptology; Springer: Berlin/Heidelberg, Germany, 2001; pp. 285–304.
65. Xia, Q.; Sifah, E.B.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information 2017, 8, 44.
