Healthcare Security based on Blockchain

Taghreed Almalki †, Shahad Alzahrani ††, and Wajdi Alhakami †††
s44180660@students.tu.edu.sa s44180412@students.tu.edu.sa whakami@tu.edu.sa
College of Computers and Information Technology Taif University, Taif, Saudi Arabia

Summary
One of the most important inventions and developments in the digital world today is the healthcare system based on blockchain technology. Healthcare is an important field that requires the application of security mechanisms due to the sensitivity of patient data. The association of blockchain with healthcare contributed to achieving better security mechanisms than the traditional approach. The new approach operates in a decentralized system, which in turn, improves security in the healthcare environment. Consequently, blockchain technology has emerged as one of the most crucial solutions to security violations and challenges in the healthcare industry. This paper provides a comprehensive review of several experts' recent protection and detection approaches in this domain. It is also imperative to note that the paper focuses only on the recent techniques that have been published during 2017-2020. The sophisticated procedures have been investigated and discussed in terms of similarities and differences to highlight the significance of the protection needed to secure the healthcare environment.

Key words:
Healthcare, Blockchain

1. Introduction

Healthcare is an important field from the social perspective, as it can handle a range of vital issues that are directly related to the enhancement of our lives. The quality of our lives can be fulfilled by fixing real health issues [1, 2]. Healthcare advocates and e-health partitions provide pervasive access to medical data and support various applications such as mobile telemedicine, patient observation, and emergency procedures [3, 4]. Information about patient history is stored in healthcare systems on special servers to provide necessary patient data. The patient's information can generally be used to monitor any chances for epidemics and analyze healthcare services in both urban and rural areas [5]. This information is also valuable to researchers in different fields to help understand various phenomena and master specific challenges [5].
Data security is considered a vital component, especially in the healthcare system, to protect important data or secure sensitive data. Healthcare data, in general, include all the details of patients, such as their medical history and personal information. This information should not be disclosed to any untrusted third party to prevent security problem and the improper use of information [6]. Moreover, the integrity of all patient data must be maintained to ensure that the data have not been altered or disclosed during transmission [7]. The unauthorized disclosure of patient's personal information can causes a negatige and dangerous effect and tarnish the reputation of healthcare institutions [2]. Additionally, the deployment of new technologies in healthcare applications, such as wireless medical sensor network (WMSN), MobiCare [8], and UbiMon (Ubiquitous monitoring environment for wearable and implantable sensors) [9] without considering security, that increases the vulnerability of patient privacy. Therefore, it is critical to secure the physiological information of a patient, thereby making security a requirement of healthcare utilities [10]. Table 1 illustrates the description of security requirements in the healthcare environment.

Table 1: Description the security requirements in healthcare

Criteria	Discerption
Confidentiality	Keeps the patient's health information not accessible by unauthorized parties. IoT consists of many applications and devices connected to prevent wrong diagnostics [11] [12].
Privacy	Privacy indicates that information and health data are valid to authorized users only. Patient data should not be given to any third party without their permission. It is also responsible for ensuring that the data is securely stored and transmitted [12].
Authentication	Ensures that anyone dealing with health data is authenticated or a legitimate party with permission to add, edit, or delete data. Data authentication is achieved by using signatures and checking encryptions to establish a secure communication channel [13].
Integrity	The integrity of all patient data must be maintained to ensure that the data received have not been altered during transmission [7].

Medical establishments save medical records in various formats that aren't compatible with other nations and labs within the same institution. Healthcare facilities require a system for managing and saving medical records. It is necessary to keep these records secure rather than saving them only. Consequently, many proposals have been presented to use blockchain for securing medical records and sensitive data [14]. Since its introduction in bitcoin by Satoshi Nakamoto in 2008 and implementation in 2009, the use of blockchain technology has witnessed significant growth [15, 16]. Fig. 1 shows that the blockchain market has been rapidly growing since 2016. The market revenue is expected to increase from $5000 in 2016 to $20,000 in 2025 [17].

Manuscript received August 5, 2021
Manuscript revised August 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.8.20

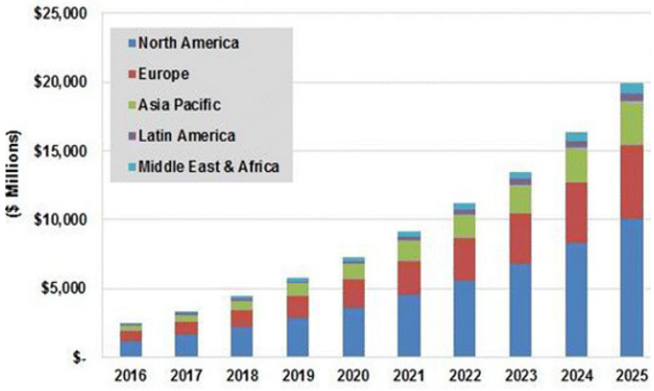

Fig. 1. Blockchain Revenue by Region, World Market 2016-2025 [28]

Bitcoin was initially introduced with blockchain technology to avoid double-spending. Today, blockchain technology is increasingly used in different financial services such as digital modules, coins and paper money allowance, and online payment [18, 19]. Moreover, it could be applied to many areas such as smart contracts [20], public services [21], healthcare [22], transportation [23]; Internet of Things (IoT) [24], reputation systems [25] and security services [26]. These fields use blockchain in various methods.

Blockchain can be known as the trust protocol, which is a concept of security measure that used to decentralize. It contains a function that used to make a global index for all transactions that happen to particular network and keep them immutable. [27, 28]. Additionally, we can't delete the information without completely changing the contents of the blockchain. Moreover, blockchain considered a list of ordered blocks, where each block contains transactions [15]. The blockchain block is connected to the previous block and contains a hash from the previous block. [29, 30]. It generates trust and agreement directly in communication between two parties, without any third party [15, 30]. Consequently, blockchain is considered to be secure from hackers [29]. Fig. 2 shows the structure of blockchain [31].

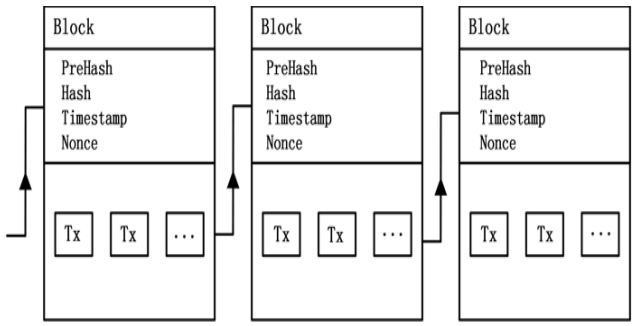

Fig. 2.The Structure of Blockchain.[31]

Blockchain technology can be used in various applications. In addition, blockchain technology is not equal to Bitcoin, as Bitcoin is one of the most popular blockchain technologies [32, 33]. However, experts believe that blockchain can be used to discover solutions in a variety of fields, including voting, identity management, governance, supply chain, and energy resources. Blockchain technique is expected to take advantage of the existing IT facilities in the coming years across many domains. For example, enhancements in new technological aspects are allowing for significant progress in the healthcare division. Therefore, it is important to consider patients' health data security and accessibility for communication and integration in Electronic Healthcare Record (EHR) systems while sharing patients' private medical information. [34]. Thus, we can explain the use of blockchain in sharing patient's information with the following steps:

(i) Healthcare institutions gather data from patients using medical sensors and devices.

(ii) An event is created and sent to a blockchain service. The blockchain service then adds a new event to the new block with other events received.

(iii) The service then replies to the provider with the hash of the block and the event's hash.

(iv) The providers of healthcare add new entries to medical stock to explain the data. If the inventory doesn't exist, a new inventory will be created. The patient can access their inventory by decrypting it.

Fig. 3 displays the process of sharing patient's medical information using blockchain technology [35].

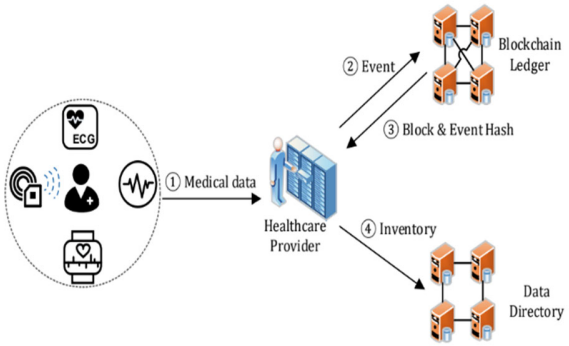

Fig. 3. The Process of Sharing Patient's Medical Information [35]

This paper proposes a comprehensive survey of the recent protection and detection strategy conducted by multiple experts in this domain. Consequently, it focuses only on the recent techniques that have been published during 2017-2020. Nevertheless, sophisticated measures have been investigated and discussed to highlight the significance of the protection needed to secure the healthcare environment.

The paper is divided into four main sections. Section 2 presents several familiar applications of blockchain technology to provide essential security objectives to protect systems against potential attacks. Section 3 presents recently published work by different researchers. Several published works on the association of healthcare with blockchain are carefully selected for this section. Section 4 discusses the similarities and differences of several mechanisms and

security requirements introduced in the literature review in section 3. Finally, the paper is concluded in section 5.

1.1 The Application of Blockchain

This section introduces some common applications of blockchain technology, such as smart contracts, cloud computing, smart home, education, and healthcare to provide remarkable security objectives required to protect systems against potential threats and attacks.

i. Smart Contract

Smart-contract considered a type of digital contract that takes control over users' assets in a digital environment. It also puts the form of rights and obligations for each user and executes them programmatically. A smart contract is a computer procedure and a contract for each user to respond to messages received, store the data, or send messages. It is the same as a case where a trustworthy person can temporarily hold the assets, and it will follow the order already considered programmed [20, 36].

ii. Cloud Computing

Cloud computing has been widely used to deliver many services via the Internet, including data storage and software. Blockchain technology is considered an ideal choice to make existing computing systems strong and consistent. Therefore, merging blockchain methodologies with cloud computing systems gives potential functionality, better security, and improved privacy [37].

iii. Smart Home

Every smart home have a local private blockchain that keeps track of transactions and also has a policy starter to enable the user from the transaction that is incoming and outgoing. Starting with the genesis transaction, the transactions of every device are linked together as an unchangeable register in the blockchain. It has decentralization characteristics, as it helps provide information and store data. These characteristics make it impossible to amend or change any record attached to the blockchain. There are two headers in every local block in the blockchain – policy header and block header. The policy header can authorize devices and put the control policy for each user into action. On the other hand, the block header contains a hash for the previous block to make the blockchain immutable[38].

iv. Education

Certifications considered significant in education and companies, as personal education records became fundamental for professional jobs. Therefore should be store these records in the long-term ledgers available that cannot tamper with most of the certification authorities, educational organizations, or training facilities issue paper, not digital certificates. Blockchain technology is set to support the shift from paper to digital certificates, which can further help establish a learning history. The Blockchain Education Platform is a practical solution for issuing, monitoring, validating, and sharing certificates. It is based on the Ethereum blockchain and uses smart contracts to support the certification process [39].

v. Healthcare

Nowadays, one of the most important study topics is health. [40] Healthcare is one of the biggest sectors that contain high percentage risks, garners attention from different technological organizations, and requires security methodologies. Given the sensitivity of patient health information, patient privacy seems to be a challenge in the sector. As patient information is usually stored in the cloud, it is hard for users to control their data. However, with the General Data Protection Regulation (GDPR) development, patients have the right to know the location of their data and its accessibility. To that end, blockchain has solved these issues and provides an effective mechanism for controlling access to maintain privacy [40]. We also take advantage of blockchain, which is decentralized in nature that may offer a unique solution for healthcare [41], provide patients' data, and protect their privacy. It makes patients the decision-maker in choosing who has the right to access their private information [40]. Blockchain is used to provide security techniques for highly sensitive data, access data from any location, and share the data securely and confidentially [42]. Moreover, blockchain technology has provided an efficient and secure infrastructure and enabled integration with private health records [43, 44]. It can also be used to present secure communication among basic stakeholders and deliver efficient reports for clinics [44, 45].

2. Related work

The application of security in healthcare is crucial to secure patient data and protect it from potential threats [46]. Therefore, numerous studies have been conducted by several researchers to address the security mechanisms using various approaches detailed below:

Jennath et al. [47] proposed a solution based on blockchain for solving security and privacy issues of healthcare records. It is designed so that only the patient has the right to decide who can have access to their data from the healthcare providers. Furthermore, all transactions on patient data can be recorded in an auditable record for future reference. This record is a tamper-proof digital ledger. Managing digital identity for the suggested framework will result in a unique identity for patients to keep track of all medical history and enable data management. The suggested solution is built on blockchain and can handle issues regarding healthcare, such as securing health data and installing blockchain software across various hospital networks. Moreover, the updated structure can handle critical data security and deployment challenges to give the healthcare community a method to relate diverse and heterogeneous providers. At the same time, it can help secure sensitive healthcare information [48].

You et al. [49] introduced a feature-based decentralized signature scheme for healthcare blockchain. It provides effective verification that preserves the privacy and integrity

of EHR data and the site's identity. They also described a comprehensive on-chain and off-chain collaborative storage system to store and verify EHR data efficiently. Analyses and tests have shown that their design is successful and publishable.

Xia et al. [50] suggested a framework based on blockchain with data sharing. The proposed framework is sufficient to handle access control issues related to sensitive information in the cloud by using immutability and embedded autonomy features in the blockchain. They utilized the methods for secure cryptography to provide sufficient access control to vital data shared using blockchain. These methods also offered permissions to build a scheme that allows data owners and users to access medical files electronically from a shared repository after verifying their IDs and cryptographic keys. All requests are then given onward servicing and put into a closed blockchain architecture with a set of permissions.

Koosha et al. [40] observed a design using blockchain-for electronic health applications that provide an effective access control technique to maintain privacy. Using one of the most important advantages of blockchain proprietary features – maintaining users' persistence and anonymity while editing classic blockchain architecture to defeat its challenges in IoT applications – Instead of the fundamental and original data, they saved the hash of patient medical data. Users can store access control methodologies over their information in blockchain to settle the accessibility and limitations. They also provided a security analysis of their proposed infrastructure.

Xia et al. [51] proposed MeDShare, a system that deals with the issue of medical data sharing among the dishonest environment of big medical data custodians. It is completely built on blockchain technology that provides auditing, data provenance, and management of shared medical data in cloud depository in giant data entities. Moreover, MeDShare also keeps track of entities that gain access to data for the mischievous utilization of the custodian system. Therefore, by executing on MeDShare, cloud service providers can achieve data provenance and auditing while sharing medical data with entities at the minimum possible risk to data privacy.

Jinglin et al. [52] examined the likelihood of trying blockchain technology to keep the confidentiality of the health care data safe and sound within the cloud containing private and delicate information. The privacy and honour of the data in the healthcare cloud should be kept safe at any cost from the attackers and from the attempts that are not authorized in the ecosystem or network. This is why the researchers use blockchain technology as they attach the data to the chain with the consent of the stakeholders within the blockchain on the algorithm named 'proof of stake.' However, when we consider the ERM blockchain, we find that the biggest stake is situated in the healthcare centre. Also, all the stakeholders and physicians have their own accumulative ownership. The blockchain networks welcome the arrival of insurance companies to verify the claims files by the patient.

Uddin et al. [53] proposed a tier-based End-to-End framework for continuous patient monitoring with a patient central agent (PCA) as its focal point. When data streaming from body area sensors needs to be stored securely, the PCA manages a blockchain component to preserve privacy. In order to enforce the security of data through various parts of a continuous, real-time patient monitoring architecture, PCA-based architecture has a lightweight communication protocol. The architecture controls the insertion of data into a personal blockchain to benifits data sharing among integration and healthcare professionals to electronic health records while making sure privacy. The results of the simulations showed that the PCA-based End-to-End architecture can improve security and privacy in RM.

In their studies, Kenichi et al. [54] focused on the salient functions of blockchain and how it maintains the privacy of personal health data (PHD) and improves individual healthcare expertise, clearing that blockchain can change existing data utilization. For example, it may be collected, owned, managed, shared and sold. However, with blockchain technology in healthcare, no third party can control and misuse the data, as it keeps the information confidential. Moreover, they proposed i-Blockchain, an individual-focused framework for using PHD, presented with infrastructure, protocols, and application scenarios.

Chen et al. [55] proposed a blockchain-based scheme that is searchable encrypted for electronic health records. The EHR index is built using complex logical expressions and stored in the blockchain. The data owners have full control over who can see their EHRs data because only the index is migrated to the blockchain to facilitate propagation. Furthermore, the usage of blockchain technology protects the anti-tampering, index integrity, and traceability of EHR's index. The performance of the suggested scheme is evaluated by taking into account two aspects: the overhead of transactions on smart contract in Ethereum and the overhead of extracting document IDs from EHRs. The blockchain can thus facilitate access to EHRs stored on the blockchain with a higher level of confidence and sharing of such data.

Jamal et al. [56] proposed a blockchain-based arcitacture, called DSS-RE, that is accessible, scalable access, and supports decentralized. It also improves health data exchange, data security, data access control, and data privacy. It will bring together the interests of healthcare professionals and patients in the pursuit of better patient health outcomes and cost savings for all healthcare stakeholders. This framework updates without affecting the integrity, confidentiality of patient data, and security and will greatly facilitate real-time access. It will also allow users to examine their medical records regardless of their history, which is a challenging task to accomplish with today's fragmented systems.

Griggs et al. [57] proposed the use of blockchain-based smart contracts to facilitate secure analysis and management of medical sensors. Using a private blockchain based on the Ethereum protocol, they created a system where the sensors

communicate with a smart device that calls smart contracts and writes records of all events on the blockchain. This smart contract system would support real-time patient monitoring and medical interventions, while maintaining a secure record of the individuals who have initiated these activities. This would resolve many security vulnerabilities associated with remote patient monitoring and automate the delivery of notifications to all parties involved in a HIPAA compliant manner. Data on the blockchain only contains information about transactions but not sensitive health data. As the patients are anonymized by their account addresses, the data is not easily linked to a specific person, thus making it permissible under HIPAA. Fig.4 shows their system.

Tang et al. [58] utilized the emerging blockchain technology to EHRs; blockchain-based EHRs. They made a state-of-the-art EHR paradigm that can help in handling centralized cloud issues. The first step is to formally discover the system structure of blockchain-based EHRs in the consortium blockchain setting. Additionally, the problem of authentication is vital for EHRs. Therefore, they also suggested an authentication scheme for blockchain-based EHRs. The scheme is identity-based, with many authorities fighting against collusion attacks out of N from N–1 authority. Furthermore, the scheme is proved to be secured to be used in a model like the random oracle model. It is also proved to have more effective verification and signing algorithms than the current authentication schemes of blockchain-based EHRs.

Tomasz et al. [59] suggested a safety model using blockchain technology for electronic health. to confirm data integrity in e-health systems that use authorized blockchain with off-chain information storing. Unlike the current solutions, their model allowed for removing information, which is a legal requirement in many e-health systems in several countries. Moreover, their suggestion can be easily integrated using service-oriented architecture, reducing costs and system deployment efforts. Their paper also discussed several blockchain-related security issues that must be considered while developing blockchain in e-health systems. Fig.5 explains the proposed system.

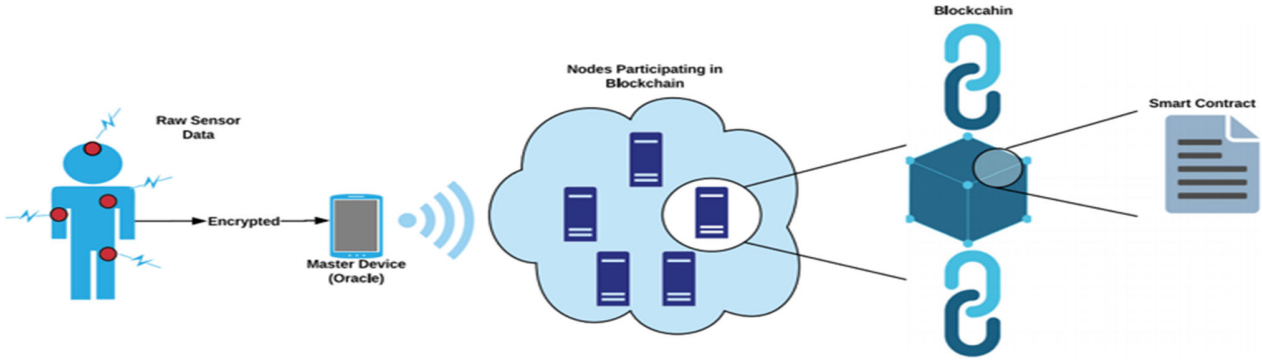

Fig.4. Raw sensor data is aggregated by the master device and then sent to nodes in the blockchain for processing by the smart contract [57]

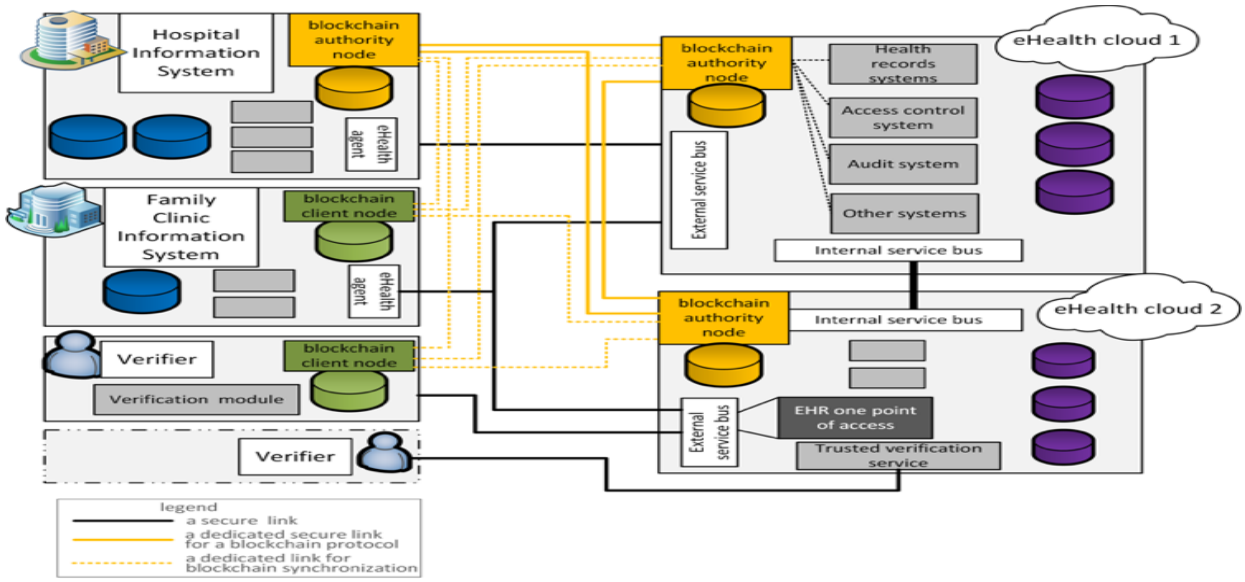

Fig.5. Integration of the blockchain-based eHealth integrity model (BEIM) [59]

Cresitello-Dittmar [60] proposed a blockchain application in the authentication and validation of identity. The basic idea was to allow a third party service to verify identities from blockchain IDs, known as addresses. When an address is added to the blockchain, an identification issuing service would bind a public key by default and transfer the ownership of the corresponding private key to the entity. This way, an entity can sign a message which can be verified with a public key stored in the blockchain. Hence, it would serve as a single sign-on portal where the application would need to request a digital signature and the ID from an entity requesting access to a certain service. The proposed system is inspired by an idea proposed by Cresitello-Dittmar for storing certain ID information of an entity on the blockchain. It is a good idea to store non-sensitive information on the blockchain. However, it is important to understand that data stored must be limited in size, as it is replicated in each network node. This will consequently affect the overall performance of blockchain authentication and authorization protocol.

Rateb et al. [61] proposed BiiMED: a Blockchain framework for Enhancing Data Interoperability and Integrity in EHR Sharing. Suggested solutions include an Access Management System that allows the sharing of electronic health records between various medical service providers and a trusted, decentralized external auditor to ensure data integrity. The purpose of this study was to establish a foundation for further research aimed at developing a decentralized EHR management system for ensuring confidentiality, authentication, and encryption, and data sharing between healthcare facilities using blockchain technology. According to the test results, BiiMED can significantly enhance the integrity and interoperability of the data. Fig 6. displays the proposed solution for the health information system and BiiMED.

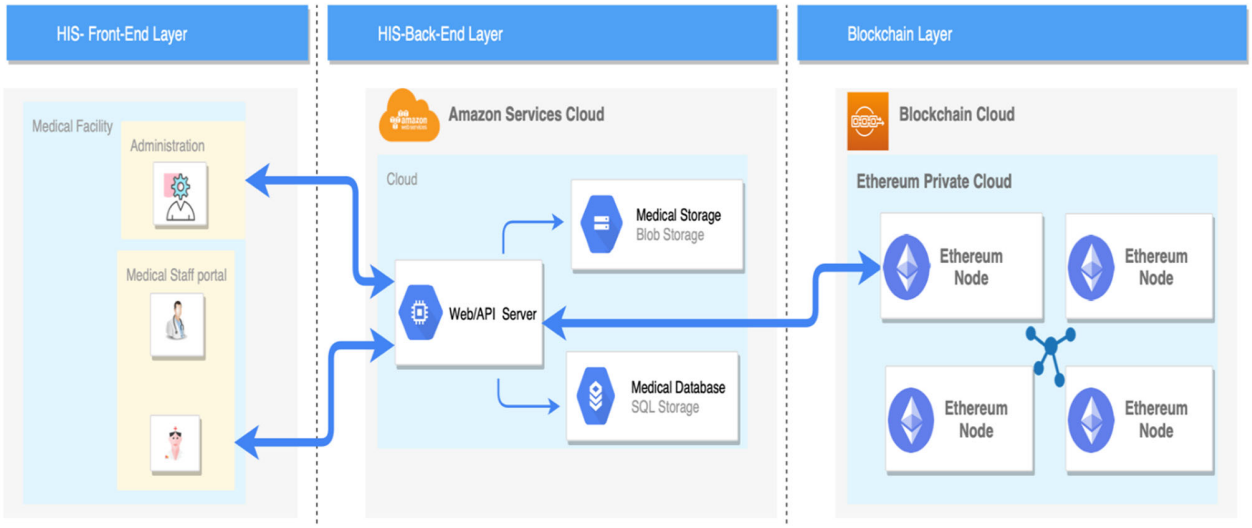

Fig.6. the architecture of the proposed solution (HIS and BiiMED) [61]

BL et al. [62] proposed a system that connects healthcare providers associated with storing and sharing electronic health records using blockchain, as they relied on multi-level authentication to protect electronic health records from counterattacks such as phishing, dictionary, cold wallets, and hot wallet attacks. However, the method suggested by blockchain needs tremendous storage to hold the data, which remains a difficult task.

Nagasubramanian et al. [63] realized the need to design a system using cloud that helps ensure authentication and maintain the integrity of health records. The keyless signature infrastructure used in the Suggested system for ensuring the confidentiality of digital signatures also ensures the aspects of authentication. The proposed blockchain technology also manages data integrity. The performance of the proposed framework is evaluated by comparing factors such as average time, size, and the cost of data storage and retrieval of the blockchain technology with conventional data storage techniques. The results showed that the response time of the proposed system is about 50% shorter than the conventional techniques. The researchers also expressed that the cost of storage of the system with blockchain is about 20% lesser as compared to the existing techniques.

Abbas et al. [64] presented a modern decentralized authentication model in a distributed hospital network through using blockchain. The blockchain-based method is prepared to allow the storing of information in secure manner in a geographically various hospital network. The results of deep simulations clarify the potential utility of the proposed architecture. Fig 7 presents the workflow of the suggested architecture.

XINYIN et al. [65] clarified the structure of a blockchain-based identity management and user

authentication (PBBIMUA) scheme for an e-health environment. Their blueprint met overall security requirements for medical data. The security and estimation analysis also showed that the performance, in terms of lightweight construction, low network latency, and high-security standards, is more enhanced than known methodologies. Moreover, the experimental results showed that the system has good efficiency. The results of the accurate security analysis also confirmed that their proposal is safe and can avoid potential attacks such as replays, the man in the middle (MITM) and impersonation attacks.

The on-demand digital healthcare ecosystem has been on the horizon to enhance preventive and precision medical situation at patient level. It also enhances the effectiveness and quality while reducing the cost of healthcare delivered by professionals. Brogan et al. [66] showed how distributed ledger technologies could play a key role in advancing electronic health by ensuring authenticity and integrity of data generated by wearable and embedded devices. They demonstrated the use of Masked Authenticated Messaging extension module of the IOTA protocol to securely share, store, and retrieve encrypted method data. The following points would demonstrate that it was possible to:

(i) Use a distributed ledger to broadcast and receive authenticated, encrypted activity data from a wearable device. The main usage and integrity of the data were authenticated through the MAM structure. The data was then structured using FHIR and coded with LOINC.

(ii) Enable structural and semantic interoperability across a diverse digital healthcare ecosystem.

(iii) Change authentication keys during a broadcast stream to demonstrate how patients could revoke access to their future data.

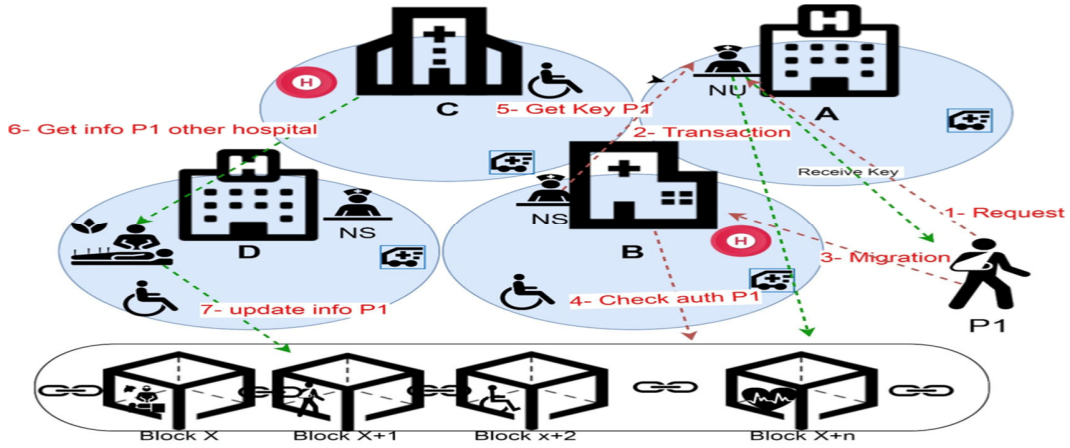

Fig.7. the architecture of the proposed method.[64]

CHUN et al. [67] created a data collection scheme based on the blockchain method for medical settings to secure patient privacy and provide more personalized healthcare services. They built a group authentication method for different authorized users (e.g. patients, physicians, family, and friends) to access a patient's health records when needed. Certified group members agree on a group session key and use it to protect sensitive patient information. In an event where a new member joins or an old member leaves the medical group, the group session key must be updated. The electronic medical system will be safer, more reliant, and useful through the proposed scheme.

Xiang et al. [68] found that finding the validation of medical data for different users while providing security assurances for e-health systems is an exciting challenge. They introduced an approved blockchain-based identity management system and user authentication (PBBIMUA) environmental health scheme. Their program meets the comprehensive safety requirements of medical information. Security analysis and testing showed that the performance is more improved than the current methods, with a lightweight design, low latency network, and high levels of security. The results also showed that the system works well.

Mohsin et al. [69] aimed at building a working verification framework for patients between the access point and node database. Two categories are used for this purpose. They initially proposed a new hybrid biometric pattern model based on the integration algorithm to combine radio frequency identification and fingerprint vein (FV) biometric features to increase random levels and the safety of pattern structure. They then developed a mix of steganography, blockchain, and encryption techniques to make a pattern for the hybrid model. When sending a pattern from a registration device (access point) to the node database, the process ensures that the FV biometric authentication system remains secure by meeting the overall requirements for confidential information security, integrity, and accessibility. Blockchain is used to amend the available and integrated data integrated.

Particle swarm optimization steganography and general encryption techniques are also secretly utilized in the transmission channel. The suggested framework was tested against 106 samples chosen from the database with 6000 samples of FV images. The results showed that (1) a high resistance framework is protected from spoofing and brute-force attacks; notably, most biometric authentication systems are at the risk of such methods and (2) the suggested framework was more profitable than the benchmark with 55.56% protection in biometric templates.

Reliable, convenient exchange of information on individual health is a matter of concern for the inter-personal and cross health industries. Thus, Liang et al. [70] proposed an innovative user-centric health data sharing solution by utilizing a decentralized and permissioned blockchain. It is aimed at protecting privacy using channel formation scheme and enhancing identity management using a membership service supported by the blockchain. A mobile application is deployed to collect health data from personal wearable devices, manual input, and medical devices. The application also makes the data synchronize on the cloud to share it with health insurance institutions and healthcare providers. To maintain the integration of health data within all records, a proof of integrity and validation is permanently retrieved from cloud database and settled to the blockchain network. Therefore, the health data of every patient delivers intense and increased value of healthcare, benefiting both healthcare providers and medical researchers.

Rupa et al. [71] designed the Ethereum platform within the blockchain and developed a model with improved technical features to reduce frauds in medical organizations. In this methodology, a regulatory body will let the healthcare centres (hospitals) face medical certificates for people required in a decentralized manner. Here, the smart contract system structure helps in validating the certificate from any authorized person around the world. The strong point of the research presents the blockchain-based model as a solution to the proof of medical evidence certification. For each accredited health centre, one individual block must be allocated to store the patient's health evidence as a transfer. It cannot be changed, tracked, or deleted. Any authorized person can check that evidence at any time and from anywhere, as it is centralized.

Madani et al. [72] suggested smart contracts based on Ethereum blockchain to give patients control over their data in a decentralized, immutable, transparent, traceable, reliable, and secure way. The proposed system uses the decentralized storage of Interplanetary File Systems (IPFS) and Oracle reputation-based re-encryption to fetch securely, store, and share patient medical data. They have also made the smart contract source code publicly available on Github.

Patrick et al. [73] showed a main case of using blockchain in public healthcare in South Africa. They described the potential use of blockchain in enhancing data health and integrity in patient-centered healthcare. It can also be used to help address issues related to accountability, unauthorized update of prescriptions, corruption in the supply chain, and financing of the healthcare system. Additionally, automated processes within the blockchain can reduce the workload associated with various validations across the entire healthcare chain and within the clinical test research. We compared the previous researches more clearly and succinctly in Table 2.

Table 2: related work summary

Author	***Year***	***Contribution***	***Security factors***
Jennath et al. [47]	2020	Designed a transparent platform for consent-based data sharing	Privacy
You et al. [49]	2018	Decentralized signature scheme	Privacy, Integrity, and Authentication
Xia et al. [50]	2017	To ensure control over access to sensitive, confidential data shared and transmitted using blockchain technology, encryption techniques that are considered secure are used.	Privacy and Authentication
Koosha et al. [40]	2019	Blockchain architecture for e-health	Confidential Integrity and Availability
Uddin et al. [53]	2018	Presented a tier-based End-to-End design for continued patient monitoring with a patient-centric agent (PCA)	Privacy
Jinglin et al. [52]	2019	Used an IoT module to intercept and fetch data generated by a patient's wearable device through blockchain storage technology	Confidentiality
Chen et al. [55]	2019	A blockchain-based searchable encryption scheme for EHRs	Privacy
Kenichi et al. [54]	2018	Used i-blockchain, an individual-centric framework for using personal health data	Confidentiality
Xia et al. [51]	2017	MeDShare	Privacy and Integrity
Jamal et al. [56]	2019	Blockchain framework called DASS-CARE	Privacy, Confidentiality, and Integrity
Rateb et al. [61]	2020	BiiMED: A Blockchain Framework	Authentication, Integrity, and privacy
Griggs et al. [57]	2018	Used a private blockchain based on Ethereum protocol	Privacy
BL et al. [62]	2019	A system that connects healthcare providers associated with storing and sharing electronic health records	Authentication
Tang et al. [58]	2019	Used an identity-based signature scheme	Authentication
Abbas et al. [64]	2020	A comparative analysis of the proposed blockchain	Authentication

Author	*Year*	*Contribution*	*Security factors*
		model with a network model without the blockchain	
XINYIN et al. [65]	2020	Used blockchain-based identity management and user authentication (PBBIMUA) scheme	Authentication
Brogan et al. [66]	2018	Used the IOTA protocol masked authenticated message extension module.	Authentication, Integrity
Chun et al. [67]	2020	Used a data collection scheme based on blockchain for medical settings	Authentication
Tomasz et al. [59]	2019	Blockchain e-health safety model	Authentication, Integrity, and Confidentiality
Cresitello-Dittmar [60]	2016	Enabled a third-party service to check IDs known as addresses for blockchain IDs.	Authentication
Nagasubramanian et al. [63]	2020	Evaluated the performance of the proposed framework in blockchain technology in terms of comparing parameters such as average time, volume, and the cost of storing and retrieving data with traditional data storage techniques	Authentication and Integrity
Xiang et al. [68]	2020	Used permission blockchain-based on identity management and user authentication (PBBIMUA) structure	Authentication
Madani et al. [72]	2020	Smart contracts based on the Ethereum blockchain	Integrity
Mohsin et al. [69]	2019	- a novel hybrid biometric system that relies on a merge algorithm combining the biometric characteristics of radio-frequency Identification with an FV. - Developed a mix of encryption, blockchain and hybrid pattern steganography algorithms.	Authentication, Confidentiality, Integrity, and Availability
Liang et al [70]	2017	It used channel form design and enhanced identity management with blockchain-powered membership service.	Integrity
Rupa et al. [71]	2020	Blockchain with Ethereum platform	Integrity
Patrick et al. [73]	2019	Use Case for applied blockchain for people healthcare in South Africa	Integrity

From many researchers' viewpoints, blockchain is confirmed to have an abnormal potential in the healthcare aspect. All efforts are needed to be directed towards EHR management that could connect to incongruent systems to promote EHR security. Blockchain technology can also be used to support access control, medicine prescription, disease data management, clinical trials, and anti-counterfeiting medicine, and observe an audit trial for health activities. However, the researches showed that blockchain is still incomplete and immature for application in healthcare, especially in the areas of health insurance. Research on blockchain and its usage in healthcare data management is increasing simultaneously. Moreover, efficient methods to develop this startup technology for application in the health and life insurance sectors require further research and innovation [74].

3. Discussion

In this section, we discuss how to secure a healthcare environment with the characteristics of blockchain technology. As we have seen in many recently published studies, the confidentiality of patient data is one of the essential components of the healthcare system. Several papers investigated the confidentiality of patient information through various approaches using blockchain technology. Examples include the IoT model for fetching patient information using wearable devices, blockchain architecture for e-health, and smart contracts based on the Ethereum blockchain. However, these technologies fulfil various safety factors of the healthcare system and are not just limited to the confidentiality of patient data. Some of the technologies mentioned in the papers that caught our attention were concerned with preserving patient data integrity. It is a key feature of blockchain technology, which relies mainly on the idea of a hash function that detects any change or modification to patient information. However, the real problem with blockchain technology is that healthcare providers can access patient data protected against any unauthorized access from inside or outside of the healthcare system. Therefore, we recommend the following:

If the data requires high speed without the concern for confidentiality or in some special case where the concern for data integrity is more than confidentiality, it is preferred to use the hash function only. But if the data need to be confidential and private and the time factor does not have a significant impact, it is preferable to encrypt the data to the hash value. This will affect the speed of obtaining information, but the patient will be guaranteed confidentiality and safe information against any modification.

Authentication is another important security requirement. However, we noticed a relatively small number of studies that discussed this factor compared to privacy and data integrity. Studies focused on this aspect stated that the identity of all members of the healthcare system must be authenticated to access health records faster through a session key for the group authorized to access patient data, such as doctors, patients, and family, provided that the key is updated and changed as soon as any new member joins or leaves the group. It is also important to verify their collective identity and authorization to access the information. Another important feature of blockchain technology in the healthcare environment is applying technologies that enabled the patient to control their data and determine accessibility.

Some healthcare blockchain models are secure against different attacks. For example, a model gathers patient health data through patients-worn devices and stores it in a blockchain. It provides privacy and integrity of the patient data in the healthcare system. It is protected against the appending attack, as the properties of the blockchain do not allow the creation of fake blocks, and miners in clusters verify any new patient information. The model is also protected from modification attacks, as the blockchain features reveal any modifications to hash and patient data policies. Those dealing with the blockchain within hospitals and health centres are unlikely to create a harmful block on purpose. Finally, this model manages the availability of patient data because of the verified blockchain's distributed properties, where information is kept instead of a central server in all mining nodes, thereby protecting it against both normal and distributed denial of service attacks. Other examples include the blockchain-based identity management model and the User Authentication System (PBBIMUA). This model protects against many attacks, such as return attacks, as the proposed model can analyze the timestamp of messages and discover sent back messages. The model also protects against a MITM attack, owing to an advantage of the blockchain in detecting modifications or changes to the data through the hash function. Therefore, even if the attacker intercepts the patient data during transmission, he will not change it. Lastly, in a stolen smart card attack, even if the attacker intercepted the smart card information and obtained information, the hash function, which is considered one-way, makes it impossible for the attacker to guess the data. Moreover, if the data encrypted, it will be more difficult for the attacker to obtain any information. This model provided many security features such as non-repudiation and anonymity of patients using a public key for each patient as their identifier rather than the true identity. Another approach provided an authentication security factor where the blockchain-based healthcare app will provide an additional security measure – a one-time password – to eliminate the attack on users' wallets. Furthermore, the blockchain architecture technique for e-health focused on providing authentication and integrity through biometric devices. The e-health system is thus protected against impersonation attacks to gain access to confidential and sensitive information. The blockchain is characterized by preserving the integrity of its data from any content. Consequently, the node will detect any spoofing using the ledger, as the attacker prevents data from outside the chain. As breaking this sequence is not possible, this technology is highly resistant to spoofing attacks.

4. Conclusion

The world today is paying more attention to secure healthcare for protecting its elements, including patient data. One of the security features that has been recently adopted is the integration of blockchain technology. Moreover, many recent works available in the literature are leading security frameworks designed for incorporating the security factor within the healthcare environment. This paper introduced a comprehensive survey that details the most recent approaches to integrate blockchain technology to ensure the security requirements and aspects in the healthcare industry. Most of the presented and selected work have been published between 2017 and 2020. This paper aims to demonstrate only recent approaches and techniques for investigating security in healthcare. On the other hand, more investigations are kept for future work and ongoing for newly published work involving security in healthcare.

Acknowledgment

References

[1] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani. 2018. Applications of blockchains in the Internet of Things: A comprehensive survey. IEEE Communications Surveys Tutorials 21 (2018), 1–1.

[2] De Aguiar, E. J., Faiçal, B. S., Krishnamachari, B., & Ueyama, J. (2020). A Survey of Blockchain-Based Strategies for Healthcare. ACM Computing Surveys (CSUR), 53(2), 1-27.

[3] C. Doukas, T. Pliakas, and I. Maglogiannis, "Mobile health- care information management utilizing cloud computing and android os," in 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology, pp. 1037–1040, 2010.

[4] Ni, W., Huang, X., Zhang, J., & Yu, R. HealChain: A Decentralized Data Management System for Mobile Healthcare Using Consortium Blockchain. In 2019 Chinese Control Conference (CCC) (pp. 6333-6338). IEEE. 27-30 July 2019

[5] De Aguiar, E. J., Faiçal, B. S., Krishnamachari, B., & Ueyama, J. (2020). A Survey of Blockchain-Based Strategies for Healthcare. ACM Computing Surveys (CSUR), 53(2), 1-27.

[6] Hussien, H. M., Yasin, S. M., Udzir, S. N. I., Zaidan, A. A., & Zaidan, B. B. (2019). A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. Journal of medical systems, 43(10), 320.

[7] Aghili, S. F., Mala, H., Shojafar, M., & Peris-Lopez, P. (2019). LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. Future Generation Computer Systems, 96, 410-424.

[8] Chakravorty, R. A Programmable Service Architecture for Mobile Medical Care. In Proceedings of 4th Annual IEEE International Conference on Pervasive Computing and Communication Workshop (PERSOMW'06), Pisa, Italy, 13–17 March 2006.

[9] Ng, J.W.P.; Lo, B.P.L.; Wells, O.; Sloman, M.; Peters, N.; Darzi, A.; Toumazou, C.; Yang, G.-Z. Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon). In Proceedings of 6th International Conference on Ubiquitous Computing (UbiComp'04), Nottingham, UK, 7–14 September 2004.

[10] Kumar, P., & Lee, H. J. (2012). Security issues in healthcare applications using wireless medical sensor networks: A survey sensors, 12(1), 55-91.

[11] N. Abbas, M. Asim, N. Tariq, T. Baker, S. Abbas, A Mechanism for Securing IoT- enabled Applications at the Fog Layer, Journal of Sensor and Actuator Networks 8 (1) (2019).

[12] Tariq, N., Qamar, A., Asim, M., & Khan, F. A. (2020). Blockchain and Smart Healthcare Security: A Survey. Procedia Computer Science, 175, 615-620.

[13] Al-Zubaidie, M., Zhang, Z., & Zhang, J. (2019). Ramhu: A new robust lightweight scheme for mutual users authentication in healthcare applications. Security and Communication Networks, , vol. 2019, Article ID 3263902, 26 pages, 2019.

[14] Maesa, D. D. F., & Mori, P. (2020). Blockchain 3.0 applications survey. Journal of Parallel and Distributed Computing, 138, 99-114

[15] Fakhri, D., & Mutijarsa, K. Secure IoT communication using blockchain technology. In 2018 International Symposium on Electronics and Smart Devices (ISESD) (pp. 1-6). IEEE. 23-24 Oct. 2018

[16] Berentsen, A. (2019). Aleksander Berentsen Recommends "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto. In *21st Century Economics* (pp. 7-8). Springer, Cham.

[17] Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of Blockchain technology: pros, cons and SWOT. Cluster Computing, 22(6), 14743-14757.

[18] Peters, G., Panayi, E., & Chapelle, A. (2015). Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective. *Journal of Financial Perspectives*, *3*(3).

[19] Foroglou, G., & Tsilidou, A. L. (2015, May). Further applications of the blockchain. In *12th student conference on managerial science and technology* (pp. 1-8).

[20] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858. 22-26 May 2016

[21] Akins, B. W., Chapman, J. L., & Gordon, J. M. (2014). A whole new world: Income tax considerations of the Bitcoin economy. *Pitt. Tax Rev.*, *12*, 25.

[22] Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017, September). Towards using blockchain technology for IoT data access protection. In *2017 IEEE 17th international conference on ubiquitous wireless broadband (ICUWB)* (pp. 1-5).

[23] Yuan, Y., & Wang, F. Y. Towards blockchain-based intelligent transportation systems. In *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)* (pp. 2663-2668).

[24] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 2016, pp. 1-3. 14-16 Sept. 2016

[25] M.SharplesandJ.Domingue,"The blockchain and kudos: A distributed system for educational record, reputation and reward," in Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 2015, pp. 490–496.

[26] C.Noyes,"Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning," arXiv preprint arXiv:1601.01405, 2016.

[27] Singh, M., Singh, A., & Kim, S. Blockchain: A game changer for securing IoT data. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)* (pp. 51-55). IEEE. 5-8 Feb. 2018

[28] M. Pilkington, Blockchain technology: principles and applications. research handbook on digital transformations, F. X. Olleros and M. Zhegu, Eds., 2016.

[29] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., ... & Rimba, P. A taxonomy of blockchain-based systems for architecture design. In *2017 IEEE international conference on software architecture (ICSA)* (pp. 243-252). IEEE. 3-7 April 2017

[30] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). IEEE. 25-30 June 2017

[31] C. Li, X. Chen, Y. Chen, Y. Hou and J. Li, "A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network," in IEEE Access, vol. 7, pp. 2026-2033, 2019.

[32] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, ''Blockchain technology: Beyond bitcoin,'' Appl. Innov., vol. 2, nos. 6–10, p. 71, 2016.

[33] A. A. Monrat, O. Schelén and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," in *IEEE Access*, vol. 7, pp. 117134-117151.

[34] M. Zarour *et al*., "Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records," in *IEEE Access*, vol. 8, pp. 157959-157973.

[35] Shen, B., Guo, J., & Yang, Y. (2019). MedChain: efficient healthcare data sharing via blockchain. Applied sciences, 9(6), 1207.

[36] Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. IJ Network Security, 19(5), 653-659.

[37] K. Gai, J. Guo, L. Zhu and S. Yu, "Blockchain Meets Cloud Computing: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2009-2030.

[38] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 618-623). IEEE. 13-17 March 2017.

[39] Kolvenbach, S., Ruland, R., Gräther, W., & Prinz, W. (2018). Blockchain 4 education. In Proceedings of 16th European Conference on Computer-Supported Cooperative Work-Panels, Posters and Demos. European Society for Socially Embedded Technologies (EUSSET).

[40] Hossein, K. M., Esmaeili, M. E., & Dargahi, T. Blockchain-Based Privacy-Preserving Healthcare Architecture. In 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE) (pp. 1-4). IEEE. 5-8 May 2019

[41] Prokofieva, M., & Miah, S. J. (2019). Blockchain in healthcare. Australasian Journal of Information Systems, 23.

[42] Pardakhe, N. V., & Deshmukh, V. M. Machine Learning and Blockchain Techniques Used in Healthcare System. In 2019 IEEE Pune Section International Conference (PuneCon) (pp. 1-5). IEEE. 18-20 Dec. 2019

[43] J. Zhang, N. Xue and X. Huang, "A Secure System For Pervasive Social Network-Based Healthcare," in *IEEE Access*, vol. 4, pp. 9239-9250.

[44] Zubaydi, H. D., Chong, Y. W., Ko, K., Hanshi, S. M., & Karuppayah, S. (2019). A review on the role of blockchain technology in the healthcare domain. Electronics, 8(6), 679.

[45] Rabah, K. Challenges & opportunities for blockchain powered healthcare systems: A review. Mara Res. J. Med. Health 2017, 1, 45–52.

[46] T. Mcghin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," Journal of Network and Computer Applications, vol. 135, pp. 62–75, 2019.

[47] Jennath, H. S., Anoop, V. S., & Asharaf, S. (2020). Blockchain for Healthcare: Securing Patient Data and Enabling Trusted Artificial Intelligence. INTERNATIONAL JOURNAL OF INTERACTIVE MULTIMEDIA AND ARTIFICIAL INTELLIGENCE, 6(3), 15-23

[48] Cyran, M. A. (2018). Blockchain as a foundation for sharing healthcare data. *Blockchain in Healthcare Today*, *1*, 1-6.

[49] Sun, Y., Zhang, R., Wang, X., Gao, K., & Liu, L. A., decentralizing attribute-based signature for healthcare blockchain. In 2018 27th International conference on computer communication and networks (ICCCN) (pp. 1-9). IEEE. 30 July-2 Aug. 2018

[50] Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information, 8(2), 44.

[51] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," in *IEEE Access*, vol. 5, pp. 14757-14767.

[52] C. Esposito, A. De Santis, G. Tortora, H. Chang and K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," in *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31-37

[53] M. A. Uddin, A. Stranieri, I. Gondal and V. Balasubramanian, "Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture," in *IEEE Access*, vol. 6, pp. 32700-32726.

[54] Ito, K., Tago, K., & Jin, Q. i-Blockchain: A blockchain-empowered individual-centric framework for privacy-preserved use of personal health data. In 2018 9th International Conference on Information Technology in Medicine and Education (ITME) (pp. 829-833). IEEE. 19-21 Oct. 2018.

[55] Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. Future Generation Computer Systems, 95, 420-429.

[56] Al-Karaki, J. N., Gawanmeh, A., Ayache, M., & Mashaleh, A. DASS-CARE: a decentralized, accessible, scalable, and secure healthcare framework using blockchain. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 330-335). IEEE. 24-28 June 2019

[57] Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, *42*(7), 1-7.

[58] F. Tang, S. Ma, Y. Xiang and C. Lin, "An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records," in *IEEE Access*, vol. 7, pp. 41678-41689.

[59] Hyla, T., & Pejaś, J. (2019). eHealth integrity model based on permissioned blockchain. *Future Internet*, *11*(3), 76.

[60] Cresitello-Dittmar, B. (2016). Application of the blockchain for authentication and verification of identity. Independent Paper.

[61] Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) (pp. 310-317). IEEE. 2-5 Feb. 2020

[62] Radhakrishnan, B. L., Joseph, A. S., & Sudhakar, S. Securing Blockchain based Electronic Health Record using Multilevel Authentication. In 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS) (pp. 699-703). IEEE. 15-16 March 2019

[63] Nagasubramanian, G., Sakthivel, R. K., Patan, R., Gandomi, A. H., Sankayya, M., & Balusamy, B. (2020). Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Computing and Applications, 32(3), 639-647.

[64] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K. -K. R. Choo and M. Aledhari, "Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain," in *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 8, pp. 2146-2156

[65] X. Xiang, M. Wang and W. Fan, "A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems," in *IEEE Access*, vol. 8, pp. 171771-171783.

[66] Brogan, J., Baskaran, I., & Ramachandran, N. (2018). Authenticating health activity data using distributed ledger technologies. *Computational and structural biotechnology journal*, *16*, 257-266.

[67] C. -T. Li, D. -H. Shih, C. -C. Wang, C. -L. Chen and C. -C. Lee, "A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System," in *IEEE Access*, vol. 8, pp. 173904-173917.

[68] X. Xiang, M. Wang and W. Fan, "A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems," in *IEEE Access*, vol. 8, pp. 171771-171783

[69] Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Albahri, A. S., Alsalem, M. A., & Mohammed, K. I. (2019). Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication. Computer Standards & Interfaces, 66, 103343

[70] Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC) (pp. 1-5). IEEE. 8-13 Oct. 2017

[71] Rupa, C., & Midhunchakkaravarthy, D. Preserve Security to Medical Evidences using Blockchain Technology. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 438-443). IEEE. 13-15 May 2020

[72] M. M. Madine *et al*., "Blockchain for Giving Patients Control Over Their Medical Records," in *IEEE Access*, vol. 8, pp. 193102-193115, 2020.

[73] Ndayizigamiye, P., & Dube, S. Potential Adoption of Blockchain Technology To Enhance Transparency and Accountability in the Public Healthcare System in South Africa. In 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC) (pp. 1-5). IEEE. 21-22 Nov. 2019

[74] Pandey, P., & Litoriya, R. (2020). Implementing healthcare services on a large scale: challenges and remedies based on blockchain technology. Health Policy and Technology, 9(1), 69-78.