I. J. Computer Network and Information Security, **2023, 6, 103-117**
Published Online on December 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2023.06.09

The Security of Blockchain-based Electronic Health Record: A Systematic Review

C. Eben Exceline
School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India
E-mail: ebencse@gmail.com
ORCID iD: https://orcid.org/0000-0001-9096-058X

Sivakumar Nagarajan*
School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India
E-mail: nsivakumar@vit.ac.in
ORCID iD: https://orcid.org/0000-0002-8945-6412
*Corresponding author

Received: 15 November 2021; Revised: 04 March 2022; Accepted: 29 July 2022; Published: 08 December 2023

Abstract: The healthcare industry makes rampant strides in sharing electronic health records with upgraded efficiency and delivery. Electronic health records comprise personal and sensitive information of patients that are confidential. The current security mechanism in cloud computing to store and share electronic health records results in data breaches. In the recent era, blockchain is introduced in storing and accessing electronic health records. Blockchain is utilized for numerous applications in the healthcare industry, such as remote patient tracking, biomedical research, collaborative decision making and patient-centric data sharing with multiple healthcare providers. In all circumstances, blockchain guarantees immutability, data privacy, data integrity, transparency, interoperability, and user privacy that are strictly required to access electronic health records. This review paper provides a systematic study of the security of blockchain-based electronic health records. Moreover, based on thematic content analysis of various research literature, this paper provides open challenges in the blockchain-based electronic health record.

Index Terms: Electronic Health Record, Blockchain, Cloud Computing, Data Integrity, User Privacy, Data Privacy.

1. Introduction

Cloud computing was used to distribute EHR for several years, with significant advantages such as flexibility and fine-grained access control. Cloud computing also increased the storage and access performance of EHR and was less vulnerable to mistakes. It contributed more to medical malpractice decisions and conflict resolution. Cloud-based EHR did, however, face other security concerns. First of all, the patient and the customer had to trust the third-party cloud service. The attackers could jeopardize the cloud server and change the EHR data. Therefore, in cloud-based EHR systems, it was challenging to preserve data integrity. Secondly, an authorized person could render and deny medical malpractice. So authorization was required for the person entering data in EHR. Thirdly, hospitals retained separate cloud storage such that the health records of the patient had maintained in the hospital database. The patient's health records could be obtained only in a specific hospital. And when a patient went to another hospital, he was to be re-examined for any medical procedure that was compromised in interoperability and resource waste. Cloud computing was based on a group of centralized databases, which might result in massive system failure.

Efforts were made in recent years to implement blockchain in a wide range of applications and multiple contexts. In general, blockchain was deployed to create a fair and open data sharing system in which unauthorized data alteration was auditable and traceable. Blockchain provided high-data security compared to previous technology by using consensus mechanisms and cryptographic primitives. In the fields of insurance and finance, real estate, and government ventures, blockchain was deployed. In the past four years, blockchain was deployed to store and exchange EHR. Blockchain maintained a public distributed ledger on a decentralized peer-to-peer network, which contained a list of data called blocks that were linked to each other using a cryptographic hash [1]. Each block contained a time-stamp and previous block hash, which made data tamper-proof and immutability. Blockchain technology could change the way medical data were processed and recorded, providing medical professionals with secure storage and flexible access to the EHR of patients [2].

In this review, the ability of blockchain-based EHR and its current research state is surveyed through various published articles. Several research articles had demonstrated the potential to use blockchain in order to meet the challenges of EHR sharing and storage. Some of the articles dealt with the creation of the platform for EHR based on the blockchain. A few of the articles applied blockchain to the systems of authentication. Some of the works focused on improving the safety of blockchain-based EHR using cryptographic primitives. Others were associated with the consensus mechanisms. Also, certain articles dealt with cases of application in the healthcare industry, including remote patient monitoring, biomedical research, collaborative decision-making and patient-centered EHR sharing among multiple providers of healthcare. Each literature explained how the proposed blockchain system addressed the security breaches in storing and accessing EHR. All literature claims to be better when compared to other similar approaches. From these published articles this review paper aims to identify which blockchain technology and cryptographic primitive is suitable to securely store and access EHR.

1.1. Motivation

Storing and accessing patient data in a centralized cloud-based EHR can lead to illegal changes and access, as well as denial of service, system failure, and data breaches. The blockchain-based EHR proved to be reliable in terms of data integrity and privacy. There are various types of blockchain and various cryptographic primitives. It is necessary to know which type of blockchain is better suitable for securely accessing EHR and which cryptographic primitive provides better security to EHR for developing a secured EHR system.

1.2. Contribution

The following are the contribution of this survey paper

- Formulated the research questions to narrow the research towards the security of blockchain-based EHR.
- Discussed how various blockchain technology is a step ahead to provide security to EHR.
- Surveyed various literature to identify various cryptographic primitives adopted by blockchain-based EHR and how they improved the security of EHR.
- Identified which blockchain technology and which cryptographic primitive provides better security and effectiveness.
- Surveyed various literature to find research challenges and open questions in applying blockchain for EHR.

2. Method and Study Design

This paper adopted the systematic approach for the literature review as it aims to group and synthesize available scholarly content concerning EHRs and blockchains. Then determine promising research directions. The most critical aspect of a systematic review is the identification of research questions. This review paper addresses how various blockchain technology improved the security of EHR. Therefore, the research questions are formulated in such a way as to identify the technology adopted, the security features that are enhanced and how effective is the technology. The following are the research questions formulated:

Q1: What are all the technologies adopted for storing and accessing EHR?
Q2: How are the various technologies achieve the protection criteria of EHR?
Q3: What are the primitives of the cryptography used in Blockchain-based EHR?
Q4: How do the cryptographic primitives achieve the protection criteria of EHR?
Q5: What is the computational effectiveness of various cryptographic primitives applied to store and access EHR?
Q6: What are all the open challenges in adopting blockchain-based EHR in healthcare?

In this paper, the leading online publications, conferences and white papers from reputable scholarly databases such as PubMed, IEEE, Springer, ACM and ScienceDirect were chosen, covering the field of cloud and blockchain-based EHR. Based on the research questions formulated, this paper selected a total of 59 research articles. Out of them, there are 44 journal articles, 9 conference papers and 6 White papers. In 59 research articles 56 articles, adopted blockchain to secure EHR.

3. Literature Review

In this section articles that are published related to applying blockchain in storing and accessing EHR are discussed. They adopted blockchain-based EHR for various applications. Table 1 shows the intent of several research papers on blockchain implementation in healthcare.

Table 1. The purpose of developing blockchain-based EHR

Purpose	Articles
Data sharing for collaborative decisions and research	[3-18]
Finance in the healthcare industry	[19]
Remote patient monitoring	[20-24]
Access control Mechanisms	[25-29]
Security of EHR	[30-34], [18], [35-38], [26], [39-42], [10], [43-50]

3.1. Cloud Computing

A cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that were dynamically provisioned. They were presented as one or more unified computing resources. It was based on service level agreements established through negotiation between the service providers and consumers [51]. The EHR centered on the cloud was cost-effective and customized, and it needed only the use of the infrastructure and resources. The cloud provided services such as infrastructure, networks, and applications to access and share data between different health experts, research laboratories, and patients. Also, cloud computing supported distributed data networks, parallel processing, and scalable storage. Deploying EHR to cloud-based technologies and platforms, such as applications and websites, was considered. It allowed more accessibility and effective data sharing, which was not possible earlier.

As there were many benefits of the cloud to store EHR, security concerns were dramatically increased compared to conventional client server-based EHR. The cloud server's service level agreement did not guarantee the protection of data. But it aimed to reach the highest possible degree of data privacy. The use of cryptographic primitive items could improve data privacy, data integrity, data authenticity, and user privacy criteria, in cloud-based EHR. However, for the following reasons, data security could not be achieved perfectly. First, the EHR owner did not create the EHR and was built by healthcare service providers. So, it was difficult to maintain the privacy and accuracy of the data. Secondly, to reduce the computing and communication costs, the authenticity of the data was not preserved. Literature [2,3] enhanced the privacy and accuracy of EHR outsourced to the cloud, by authenticating the healthcare provider. Of course, the patient would depend on the healthcare provider.

As the cloud server was a rational entity, a health service provider could compromise with the cloud server resulting in a data integrity breach. Data privacy was achieved in the [52] paper by using a trusted server to maintain the patient's secret keys. While the trusted server might be able to access the patient record, it did not ensure the perfect privacy of data. Data privacy was also achieved in [53], where patients and health service providers authenticate one another by establishing a secure channel through a smartphone. Both articles mentioned above require highly-powered resources that were impractical. The security of the EHR usually relied on data encryption, and access policy enforcement before EHRs outsourced to the cloud [54]. Attribute-based encryption (ABE) was a commonly used encryption technique to secure EHR outsourced to the cloud. This was because it enabled its end-users to have fine-grained access control over EHR.

Table 2. Summary of literature adopted public blockchain for accessing EHR

Scheme	Features	Cryptographic primitive	Advantages	Limitations
[34]	First, to introduce blockchain to secure EHR.	PKI	Data integrity, user privacy.	The patient’s private key can decrypt EHR; EHR is stored publicly.
[18]	Encourages patient to be accountable to their EHR	Biometric Identity-based technique	Data privacy, scalability, and user privacy	-
[6]	Clinical trials	PKI	Data integrity	-
[17]	Support evidence dataversioning	PKI	Data integrity and non-repudiation, avoid notarization problem	-
[47]	Used proof of primitiveness ofdata for verification	Symmetric key encryption and PKI	User privacy	Data is encrypted using the symmetric key, and the symmetric key is encryptedusing PKI
[14]	Lightweight mining algorithm	PKI	Data integrity, Distributed denial of service attack.	Scalability
[4]	DApp with blockchain	PKC with symmetric key cryptography	Data privacy	Traceability
[39]	Password-based key agreement between doctor and patient	Symmetric key encryption/PKE	Resist Password guessing attacks, impersonation attack	Trust cloud
[50]	Construct index for EHRsusing complex logic expressions	Complex query Searchable encryption	Fairness, accuracy, and confidentiality	Scalability

Table 3. Summary of literature adopted private blockchain for accessing EHR

Scheme	Features	Cryptographic primitive	Advantages	Limitations
[55]		PKI	Data integrity, reduced transaction costs	-
[56]	A single view of EHR in the distributed model	PKI	Elasticity, scalability, Interoperability	Duplication, privacy, integrity, and flexibility.
[57]	First Blockchain-based EHR prototype. MedRec	PKI	Data authentication, accountability,and privacy	Obfuscation, Consumes more computational resources,and scalability.
[58]	Proposed healthcare data gateway App	Purpose-centrickeyword search encryption	Data privacy,	Require extensive re-engineering
[32]	Suggested trusted authority for identity verification	Identity-based	At-scale interoperability to share data, patient tracking, identity assurance, and validation	Traceability
[23]	Introduced a fair access control framework to record transactions used to grant, get, delegate, and revoke access	Hierarchical PKI	Data integrity, scalability	High transaction time
[59]	Use keyword search and smart contracts	Symmetric key encryption for public data and PKI for private data.	Privacy, anonymity	-
[35]	Track all events in the database	Muli-authorityAttribute-based signcryption	Data authenticity, data privacy, data integrity, and flexible access control	-
[19]	context-relevant identity management; autonomous transaction validation and processing; prior authorization; and event-driven supply chain management	Identity-basedtechnique	Data privacy, scalability	Availability
[12]	Monitors the node which accesses data for malicious usage from adata custodians system	Identity-based	Data privacy, lightweight, and scalable	Need the assistance of cloud, Key management, recovery of EHR in case of disaster
[45]	Enable access only for the users invited	Identity-based	Data privacy, lightweight, and scalable	
[24]	Mobile health using blockchain	PKI	Data integrity	Denial of service attack
[53]	DApp	PKI	Enhanced diagnosis level	Computational and communication cost is more
[28]	Hides information of signature and encryption to unauthorizedusers	PKI/SKE	Replay attack, binding attacks	Key escrow
[36]	Cross border exchange of EHR	Symmetric key encryption and PKI	_	It does not use open standards andthe risk of not being vendor-neutral.
[60]	Provides read access and writeaccess	Symmetric key encryption and biometric-based	User privacy, interoperability	
[26]	Allows to store keys and small encrypted records directly in blockchain	Blind distributed PRE	Long-standing privacy and security, scalability	The computational cost for registration is high, the possibility for delayed transactions
[49]	Data propagate through the P2P overlay network	PKI	Eclipse attack, Pre-image attack	Scalability, data storage.
[41]	Calculate the significance ofhealth providers	Symmetric key encryption andidentity-based encryption	Data integrity and interoperability	Trust among providers
[25]	Hybrid blockchain edge architecture	Attribute-based	Avoid spoofing attack and fake healthcare provider attack	
[27]	EHR owner can fix valid access period for data	CP-ABE	Fine-grained access control,	Need the assistance of cloud and less data integrity
[5]	Mutual authentication is done using a session key	PRE	A lightweight, improved consensus algorithm,	Collusion attack, key escrow
[11]	Lightweight blockchain	Identity-based	Avoid forking, DoS attack, blocks dropping attack,	Data privacy, fine-grained access control
[43]	_	PRE	Data rekeying, smaller ciphertext	Scalability
[16]	Blockchain with Client hash chain	PKC	Data integrity, scalability, user privacy	_

3.2. Public Blockchain

A public blockchain was a fully open, decentralized, and permission-less information-sharing network. Any user could create a pair of public and private keys and an address that is used to communicate with other peers in the blockchain network. Everyone in the network has the right to read data, build transactions, and add information to the ledger. The first EHR-based blockchain was introduced using public blockchain technology [34]. Public blockchain did not provide perfect data privacy as the data is stored in the public ledger. Any node could enter the network and read EHR without the permission of the patient. Table 2 summarizes the literature that adopted public blockchain and its pros and cons.

3.3. Private Blockchain

A private blockchain contained only the authorized users on a decentralized network, and EHR was maintained by one organization. A private blockchain was suggested to ensure high data integrity and privacy when compared to the public blockchain for storage and accessing EHR [14-16]. If there was a single node to authorize users and validate data on the network, all users must trust a single party. Also, the network was centralized, which was purely against the goal of a decentralized blockchain. In order not to be in control of the single trusted party, super peers in the network were chosen to carry out operations in the EHR that facilitated greater traceability [17-19]. Moreover, in a private blockchain, the transaction records were maintained as public. An adversary could do network analysis and determine the frequency of node visits to a health service provider. It was a data breach. The research was to be pursued about this data breach. Table 3 shows the pros and cons of literature that adopted private blockchain for accessing EHR.

3.4. Consortium Blockchain

A consortium blockchain was a fully open, decentralized network used to share information in a controllable user group. It is also known as a semi-private blockchain connecting users of various clinical organizations. In such a consortium, transactions could only be carried out by peers who were from authorized clinical organizations. The mentioned blockchain addressed technical challenges in the EHR and organizational challenges by developing a structured cross-organization group [15]. Through, a consortium blockchain network linking patients, hospitals, health departments, healthcare communities, insurance companies, and medical researchers as possible. It could be set up to allow EHR to be exchanged, reviewed, and audited [41,42]. The interoperability of the consortium blockchain could help patients establish access control over their EHR outsourced to the cloud between users of different clinical organizations [8] and [7]. Consortium blockchain could be used in cases such as remote patient monitoring, patients related to different health organizations, and inter-organizational biomedical research. It provided high interoperability with data privacy and data integrity. Table 4 describes the literature that adopted consortium blockchain in storing and accessing EHR.

Table 4. Summary of literature adopted consortium blockchain for accessing EHR

Scheme	Features	Cryptographic primitive	Advantages	Limitations
[33]	Combine a fictional record with a valid record	Tokenized identity based	Data privacy, enable real-time claim adjudication	Scalability, Resiliency
[61]	_	Attribute-based	Data privacy, user privacy	User privacy
[44]	Describe collaborative off-chain and on-chain storage system	Attribute-based	Unforgeability, resist collision attack	Signing and verification time is more
[20]	Blockchain applied in WBAN	PKI	High fault tolerance	Delay in block verification, keymanagement
[13]	Parallel healthcare system-based ACP (artificial, computational, and parallel execution)	PKI	Data integrity, interoperability	Key management
[42]	-	Multi-authority identities based	Resist collision attack	-
[7]	-	PKC	Interoperability, integrity	Intruder attack

3.5. Blockchain with Cloud Storage

The EHR was stored in the cloud, and some form of the blockchain was used to support access control. Blockchain only audited an EHR transaction that was processed in the cloud [27,28,50]. The main EHR was kept in the cloud [44,51,53]. Blockchain integration with cloud storage addressed blockchain's scalability issue. But the user must trust the cloud service provider and it might lead to a data privacy breach. Table 5. Summarizes the literature adopted blockchain for accessing EHR stored in the cloud which provides high scalability to the system.

Table 5. Summary of literature adopted blockchain for accessing and cloud for storing EHR

Scheme	Features	Platform	Cryptographic primitive	Advantages	Limitations
[58]	Proposed healthcare data gateway App	Private Blockchain	Purpose-centric keyword searchencryption	Data privacy,	Require extensive re-engineering
[12]	Monitors the node which accesses data for malicioususage from a data custodians system	Private blockchain	Identity-based	Data privacy, lightweight, and scalable	Need the assistance of cloud, Key management, recovery of EHR in case of disaster
[45]	Enable access only for theusers invited	Private blockchain	Identity-based	Data privacy, lightweight, and scalable	
[30]	Designed to provide fine-grained access control in blockchain	Blockchain	Combined attribute and identity-based encryption	Data integrity, data privacy,fine-grained access control	No smart contracts
[46]	Used multiple signatures for better security	Blockchain	Identity-based	Data integrity, interoperability, can handle heterogeneous data	Trust cloud
[21]	Multi-tier blockchainframework	Blockchain	Pseudonym-based encryption with different authorities.	Perfect data privacy.	Computational cost, complex architecture, need lots of resources.
[39]	Password-based key agreement between doctorand patient	Public Ethereum blockchain	Symmetric key encryption/PKE	Resist Password guessing attack, impersonation attack	Trust cloud
[29]	Designed	Private hyperledger fabric blockchain	Attribute-based andPRE	Fine-grained access control, flexibility, and revocability. Secure against collusion attack, replay attack	
[7]	Controllable blockchain-based cloud storage.	Private Blockchain	PKC	Securer against user collision attack.	Single authority to verify all the documents.
[27]	EHR owner can fix valid access period for data	Private Blockchain	CP-ABE	Fine-grained access control,	Need the assistance of cloud and less data integrity
[8]	Cloud assisted blockchain-based EHR	ConsortiumEthereum blockchain	Keyword search encryption and PRE	Data privacy, identity privacy, collusion resistant	Trust on proxy

3.6. *Blockchain with IPFS*

The InterPlanetary File System (IPFS) was a peer-to-peer distributed file storage system that was decentralized. EHR was stored in external storage facilities to solve the problem of scalability in the blockchain. If the data was stored in the cloud, the third-party cloud service provider must be trusted by the consumer. Medical records were encrypted and stored on IPFS. But the generated hash values were stored in the blockchain to provide scalability and data privacy with no trusted authority [26,41,55]. Table 6 describes the literature that adopted blockchain for accessing EHR stored in IPFS. As IPFS is distributed and decentralized, the availability of data is more compared to cloud storage.

Table 6. Summary of literature adopted blockchain for accessing EHR stored in IPFS

Scheme	Features	Platform	Cryptographic primitive	Advantages	Limitations
[19]	context-relevant identity management; autonomous transaction validation and processing; prior authorization; and event-driven supply chain management	Private DLT	Identity-based technique	Data privacy, scalability	Availability
[9]	Enables user and group-based data sharing and containerization	Ethereum blockchain and interplanetary file system	Symmetric key encryption	Semantic interoperability	Maintaining keys
[48]	Combines blockchain, IPFS, and mobilecloud	Ethereum blockchain	IBC	Lightweight, minimal network latency, and dataprivacy	-
[37]	Provides content addressable storage	Ethereum blockchain	Role-based access control	Scalability, information asymmetry	-

3.7. *Multi-tier Framework*

Multi-tier blockchain systems use both public and private blockchains with outsourcing EHR to the cloud were developed by [21]. For patients to collect data from sensors and to build EHR data from scratch, a private blockchain was implemented in the first tier. The second and third-tier used public blockchain involving access to EHR by health professionals or patients and contact between different cloud providers for e-health, respectively. The multi-tier framework was complex, and it was not efficient since the public blockchain did not provide data privacy when it was applied for accessing EHR by health professionals. Magyar also developed a multi-tier framework that adopted both permission and permissionless blockchain. The former was applied to the healthcare providers level and the latter was applied to the situation where there was no open text for a patient available for storing and forwarding level [31]. Zheng et al. categorized the users into public, private, and restricted. The public user could directly decrypt the message from the message. The private user was to know the Merkle hash root to decrypt the message. The restricted users were revoked users and they could be changed when the owner of the message changed the side key. Medicalchain framework adopted two blockchains. One was for accessing the EHR data and the other was for transferring money [60]. All multi-tier blockchain frameworks for accessing and storing EHR provided high computational cost and implementation cost was also high. Table 7 summarizes the literature that adopted a multi-tier blockchain framework for securing EHR.

Table 7. Summary of Multi-tier blockchain frameworks for securing EHR

Scheme	Features	Platform	Cryptographicprimitive	Advantages	Limitations
[60]	Provides read accessand write access	Hybrid hyperledger fabric blockchain and ethereum blockchain	Symmetric keyencryption and biometric-based	User privacy, interoperability	
[21]	Multi-tier blockchainframework	Blockchain with cloudstorage services	Pseudonym basedencryption with different authorities.	Perfect data privacy.	Computational cost, complex architecture, need lots of resources.
[31]	Multi-signature scheme and two-tier blockchain is applied	Permission and permissionless blockchain	PKI	Data integrity, portability,and interoperability	-
[62]	Mask authenticatedmessaging (MAM)protocol is used	Categorize as public modeand private mode, Distributed ledger technology	-	Fees less, granularly-controllable EHR sharing,and highly scalable.	-

4. Study Findings

This section analyzes the study findings according to the research question formulated in this paper to interpret the reviewed articles.

4.1. *Technologies Adopted for Storing and Accessing EHR*

The various technologies adopted to store and access EHR are

- Cloud Computing
- Public blockchain
- Private blockchain
- Consortium blockchain
- Blockchain for accessing and cloud for storing
- Blockchain for accessing and IPFS for storing
- Multi-tier framework.

And some articles combined the technologies and developed a multi-tier framework to provide better security. The articles combined public blockchain and private blockchain and deployed them at various levels in the architecture. Fig. 1. shows the percentage of papers that adopted various types of blockchain to secure EHR from the surveyed articles. Out of 56 articles, 9 papers adopted public blockchain, 25 papers adopted private blockchain, 8 papers adopted consortium blockchain, 10 papers adopted blockchain (includes private, consortium, and public) with cloud, 4 papers adopted blockchain with IPFS, and 4 papers adopted multi-tier framework which applied blockchain in various levels of the architecture.

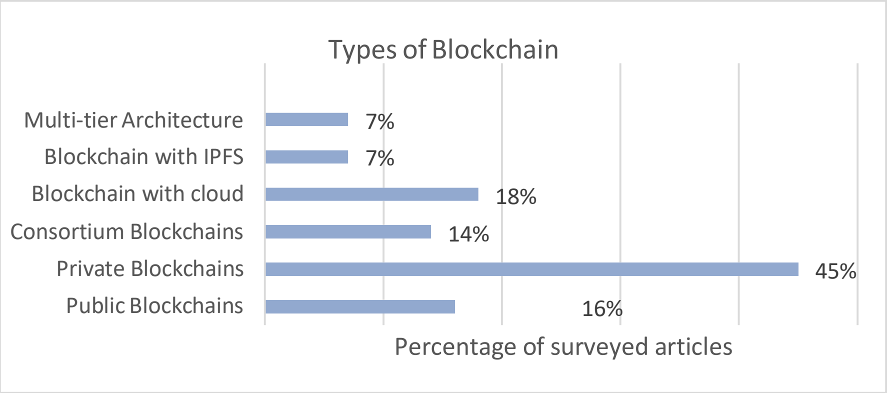

Fig.1. Types of blockchain

4.2. *Security of Technologies Adopted for Storing and Accessing EHR*

This section analyses the research question Q2 how the technologies adopted to store and access EHR satisfy the protection criteria. EHR outsourced to the third party should be tamper-proof, available to the authorized users, and patient-centric to provide data privacy. Access policy should be flexible to access the EHR by the authorized users and it should provide user privacy. Table 8 summarizes the security features of all the technologies used to secure and store EHR. According to the literature discussed, Cloud computing does not provide data integrity because the health provider can collude with the cloud and make a malicious alteration in EHR and there is a possibility of a single point of failure due to a centralized network. Public blockchain did not provide high data privacy because anyone can enter the network and participate in the transactions. Moreover, EHR is stored in the public ledger. But public blockchain provides data integrity, interoperability, and user privacy. Data integrity is achieved in all types ofblockchain because of hashing which connects with all the previous blocks. The interoperability of EHR is achieved because EHR can be easily shared with any of the users in the blockchain. User privacy is also maintained because there is no trusted third party to control the users. Public blockchain also ensures the availability of the EHR becauseeach node in the blockchain has a copy of the EHR. Private blockchain provided high data privacy because the EHR is shared within a limited user group. A single authority will maintain all the identities of the users in the group, which is difficult and may lead to a user privacy breach. Moreover, in private blockchain EHR cannot be shared between various health organizations or professionals resulting in interoperability problems. Consortium blockchain provides fine-grained access control and interoperability because various organizations combine to control the users in the group. Yet it lacked user privacy similar to a private blockchain. The blockchain with cloud storage increased scalability and data privacy because EHR is stored not in the public ledger. But the trust relied on the third-party cloud server. Blockchain with IPFS storage provides high data privacy and high data integrity due to the decentralized storage system and only the hash value of the data is stored in the blockchain. User privacy and interoperability depend on the type of blockchain the system adopts.

Table 8. Summary of the cloud and blockchain-based EHR

Security features	Cloud-based	Public blockchain-based	Private blockchain-based	Consortium blockchain-based	Blockchain with cloud storage	Blockchain with IPFS
Trusting the third party	Y	N	Y	Y	Y	N
Decentralized	N	Y	Y	Y	Y	Y
Distributed	N	N	Y	Y	Y	Y
Identity Management issue	Y	N	Y	Y	Y	N
Tamper proof	N	Y	Y	Y	Y	Y
Traceability	N	Y	Y	Y	Y	Y
Data integrity	N	Y	Y	Y	Y	Y
Data privacy	Y	N	Y	Y	Y	Y
User privacy	N	Y	N	Y	N	Y
Resist Impersonation attack	N	N	Y	Y	Y	Y
Resist spoofing attack	Y	N	Y	Y	Y	Y
Non repudiation	N	Y	Y	Y	Y	Y
Flexibility	Y	N	N	Y	Y	Y
Fine-grained access control	Y	N	Y	Y	Y	N
Scalability	Y	N	N	N	Y	Y
Interoperability	Y	Y	Y	Y	Y	Y
Accountability	N	N	Y	N	N	N
Availability	N	Y	Y	Y	Y	N
Resist Denial of service attack	N	Y	Y	Y	N	N
Resist Collusion attack	Y	Y	Y	Y	Y	Y
Resist Identity guessing attack	N	Y	N	N	N	Y

4.3. *Cryptographic Primitives Adopted in Blockchain-based EHR*

The various cryptographic primitives adopted to secure and access EHR are

- Symmetric key encryption with Public-key cryptography
- Public key cryptography
- Identity-based cryptography
- Attribute-based cryptography
- multi-authority attribute-based cryptography
- PRE

There were also other encryption schemes, which are adapted to provide security according to the requirement of the scheme. They are pseudonym-based encryption, complex query-based searchable encryption, and purpose-centric encryption. Fig. 2. shows the percentage of surveyed articles that adopted various cryptographic primitives to secure EHR. Out of 56 articles 13 articles adopted PKC, 9 articles adopted IBC, 8 articles adopted PRE, 6 articles adopted ABC, 6 articles adopted SKE combined with PKE.

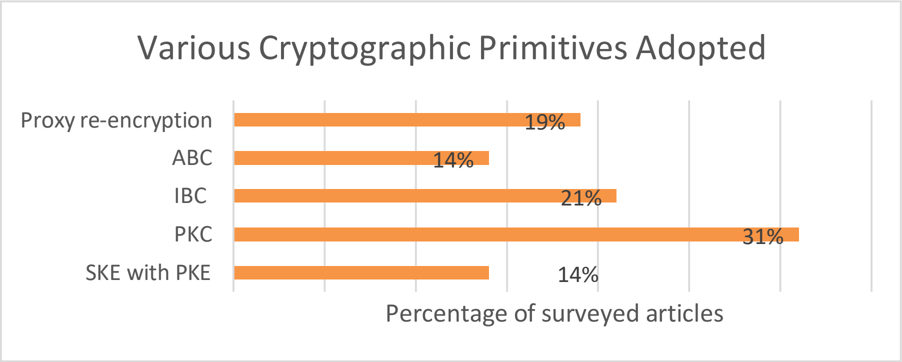

Fig.2. Various cryptographic primitives adopted by blockchain-based EHR

4.4. Security of the Cryptographic Primitives Adopted by Blockchain-based EHR

This subsection analyses the research question Q4 with the literature selected for the review. The security of data in the blockchain depends heavily on cryptography. The so-called cryptographic hashing functions were vital in this context. Hashing was a mechanism by which an algorithm took data input of any size. Then it generates an output containing a constant and fixed-size called hash. The hashes, in blockchain, were used as specific data block identifiers. Each block's hash was created concerning the previous block's hash. These generate a chain of linked blocks. The hash of the block was based on the data stored within that block. It meant that any changes made to the data might entail a change to the hash of the block. This property of hashing maintains the data integrity of EHR. Moreover, asymmetric or public-key cryptography was used to generate public and private key pairs that allowed users to send and receive data securely and to securely store EHR. Private keys were used as digital signatures for transactions, enabling authentication of ownership of the transmitted data.

Table 9 shows the comparison of various cryptographic primitives adopted for the blockchain-based EHR system. The table describes when PKC is adopted data privacy breach occurs. The patients did not know who accessed their EHR. Identity-based and attribute-based cryptography provided data privacy and if a single authority was deployed to manage the identity of the users, there occurs user privacy breaches and it was cumbersome. Pseudonym-based encryption hid the identity of the user from other peers improved user privacy but difficult to achieve data privacy. In PRE, the trust relies on the trusted third-party proxy, which may lead to data privacy breaches and user privacy breaches. In the reviewed articles, mostly the proxy is the cloud server; if the centralized cloud server is compromised, the security of the whole system is reduced. Multi-authority ABC can solve the identity management problem found in single authority schemes, yet there might be a user privacy breach. Speaking about fine-grained access control over EHR ABC schemes are better compared to other cryptographic schemes because access control is embedded within the ciphertext. Because for other cryptographic schemes, separate access control mechanisms have to be developed to access the encrypted EHR.

Table 9. Comparison of cryptographic primitives adopted in blockchain-based EHR

Security	SKE with PKC	PKC	IDC	ABC	M-ABC	PRE	Pseudonym based
Trusting authority	N	N	Y	Y	Y	Y	Y
Data Integrity	Y	Y	Y	Y	Y	Y	Y
Data Privacy	Y	N	Y	Y	N	N	N
User Privacy	Y	Y	N	N	.Y	N	Y
Fine-grained access control	N	N	N	Y	Y	N	Y
Man in the middle attack	N	Y	N	N	N	Y	N
Identity theft	Y	N	Y	Y	Y	Y	N
Revocability	N	N	Y	Y	Y	Y	Y
Impersonation Attack	N	Y	Y	N	N	N	Y
Identity guessing attack	N	N	Y	Y	Y	Y	N

Fig. 3. shows the percentage of surveyed articles that improved various security of EHR. Out of 56 articles, 12 papers improved data integrity beyond applying blockchain, 9 papers improved user privacy, 9 papers improved fine-grained access control, 11 papers improved interoperability, 20 papers improved data privacy, 6 papers improved availability of data, and 11 papers improved scalability.

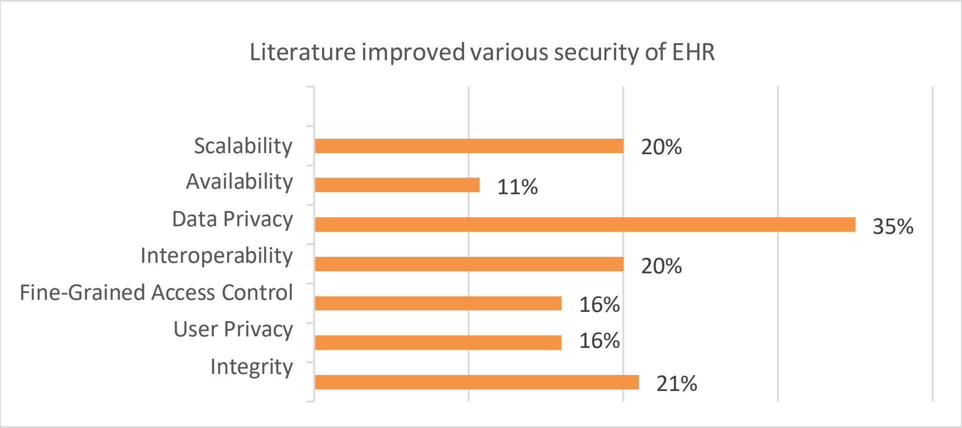

Fig.3. Articles improved various security of blockchain-based EHR

Table 10. Effectiveness of the implemented reviewed articles

Scheme	Cryptographic primitive	Blockchain technology	Observation	Hardware specs	Processing time	Latency	Throughput
(Badr et al., 2018) [21]	Pseudonym based encryption	Multi-tier (Public and Private)	Messages between 6 entities	3 GHz, intel Duocore, 4GB,Ubuntu 12.10	0.075s	N/A	N/A
(Shahnaz etal., 2019) [37]	PKC	BlockchainIPFS	1user	2.5GHz, intel i7 core, 8GB, windows 64 bit.	176s	14 ms	100 users- 250 kb/s
(Roehrs et al., 2019 [38]	PKC	Private Blockchain	100-10000 users	3.3GHz, intel i5, 4 core, 8GB,	N/A	52ms-449ms	5Mb/s-64Mb/s
(Liu et al.,2019) [5]	PRE	Private Blockchain	1 user	2.2GHz, intel i5,8GB,Ubuntu18.04.1	174s	N/A	N/A
(Cao et al.,2019) [39]	SKE/PKI	Public blockchain with cloud storage	15 patients	Intel i5,duo core,8GB, windows 10	N/A	350 ms	N/A
(Shangping Wang et al., 2019) [27]	CP-ABE	Private Blockchain	1 user/20attributes	3GHz, Intel 2 core, 4GB, Ubuntu 16.04	10.1s	N/A	N/A
(Y. Wang et al., 2019) [8]	PRE	Consortium blockchain	Keywords-100	3.2GHz, intel i5, 4GB, windows 10	10.2s	N/A	N/A
(Fan et al., 2018) [28]	SKE/PKI	Private Blockchain	100 users	N/A	N/A	925.2s	N/A
(Xia, Sifah, Asamoah, et al., 2017) [12]	IBC	Private Blockchain	100 users/	N/A	N/A	1286.7s	N/A
(Nguyen etal., 2019) [48]	IBC	Private Blockchainwith IPFS	7user requests	Ubuntu 16.04	725ms	<=30s	8KB-18KB
(Chen et al., 2019) [50]	Searchableencryption	Blockchainwith cloud	1 user/ 100 match documents	Intel i7,4 core,16GB, Ubuntu 16.04	8s-16s	N/A	N/A
(Thwin & Vasupongayya, 2019 [29]	PRE	Private blockchain with cloud	1user,12 MB	2.6 GHz, intel i7, 8 GB,	218ms-3643ms	N/A	N/A
(H. Wang & Song, 2018) [30]	Combined ABEand IBE	Private blockchainwith cloud	1 user, 128MB	2.6 GHz, intel i7, 8 GB,	1402.01ms-4192.9ms	N/A	N/A

4.5. The Computational Effectiveness of Various Cryptographic Primitive Applied to Store and Access EHR

The computational effectiveness of each cryptographic primitive is analysed by the total processing time taken by the system that adopted the cryptographic primitive. Out of 44 journal articles studied in this paper, only 12 articles were implemented and 8-articles calculated the processing time of the algorithms deployed in the system. Moreover, outof the 9 conference papers studied in this paper, only 1 paper is implemented and calculated the processing time. If the number of keywords in the database increases, the searchable encryption execution time increases. Each articleis reviewed according to the cryptographic primitive adopted, type of blockchain adopted, observation points, hardware specifications, processing time of the deployed system, transaction latency, and transaction throughput. Table 10 shows the effectiveness of the implemented articles studied in this paper. In table 10 ‘N/A’ denotes ‘not available’. From table 10, we observed that SKE/PKC adopted articles do not calculate the processing time of the system but the latency, which is high. PKC shows a high computational processing time compared with other cryptographic primitives. IBC shows less processing time and the latency is high compared with other cryptographicprimitives. Adopting CP-ABC shows better effectiveness compared with other cryptographic primitives except for PRE of Thwin et al. Also other cryptographic primitives such as pseudonym-based and searchable encryption show better effectiveness compared with PKC.

4.6. Open Challenges

The following are the open challenges in developing blockchain-based EHR where the researcher can make future developments to improve the security of sharing and storing HER.

- Public blockchain guarantees user privacy, but there is a chance of a 51 percent attack. The miners are attempting to control more than 50 percent of the network's processing power and hash rate, which results in splitting the main blockchain by forking, preventing other miners from processing the block, blocking new transactions, and block verification.
- To correct this shortcoming in the public blockchain, private and permission-based blockchain is adopted to exchange and store EHR. But there will be a breach of user privacy. Moreover, public blockchain does not provide data privacy because EHR is stored in the public ledger.
- In a private blockchain, an open standard is not used, which results in not being vendor-neutral.
- In a private blockchain, data privacy is maintained compared with a public blockchain. However, a trusted node is employed so that the authority can able to trace the user identities, which lacks user privacy.
- An access control policy is stored in smart contracts. It is difficult for a patient to expressively design an access control policy to give selected access to a particular user.
- The increase in the number of participants leads to an increase in the computational resources of the entire blockchain infrastructure. Moreover, blockchain is developed to store only transaction data, but EHR contains images also.
- EHR is a voluminous information system, so the number of transactions in blockchain increases leads to delays in mining blocks in public as well as in private blockchain. Therefore, there is a need for creative mechanisms and algorithms to reduce mining delays.
- Nowadays, blockchain with cloud storage is implemented, which requires less re-engineering. The scalability problem found in blockchain technology is overthrown by adopting cloud storage. Only metadata is stored in the blockchain, although there is necessary to trust the third-party cloud server.
- Consortium blockchain can be deployed to provide interoperability. It is better than private blockchain, but identity management and enforcing access control mechanisms are difficult.
- Research should concentrate on key management and protection. The ability to replace missing or corrupted keys should be easy.
- Apart from these, blockchain technology has specific vulnerabilities that are unique to system architecture and implementation. They are Block withholding attack, double spending attack, block discarding attack, and eclipse attack. Malicious miners post these attacks to receive more incentives [63].

5. Discussions

EHR faced difficulties in adapting to the increasing technological infrastructure that focused on Internet-enabled applications. EHR, as an information system, had unique protection and privacy requirements due to certain legal prerequisites for protecting confidential medical data for patients. When access to health information through smart devices was made more accessible and patients travel to numerous clinical organizations, secure sharing, and access to information were a concern. Particular challenges faced by EHR include authentication, interoperability, secure data sharing, scalability, access to data, data integrity, and user privacy. The blockchain-based EHR literature addressed in this paper had many capabilities and applications that could be implemented in the field of healthcare.Capacity and limitations for applying blockchain to share and access EHR are discussed below.

- The decentralized and distributive nature of the public blockchain guarantees greater transparency compared other blockchain-based techniques.
- The immutability of a blockchain, which comes from linking the hashes of subsequent blocks, brings with it inherent data integrity since blocks cannot be rewritten. The concept is used to protect sensitive medical records created by health practitioners and smart healthcare devices: the immutability of blockchain influences collective medical decisions, financing, and all applications in the healthcare sector.
- All research papers that have been deployed blockchain for sharing and accessing EHR have data integrity. Data security can be improved by storing only the hash value of the contents in the blockchain, thereby preventing spoofing attacks. In contrast to the public blockchain, private and consortium blockchain provides greater transparency. Because a person who changes the record is effectively detectable by having trusted authorities, else blind signature or multiple signature schemes can be adapted to increase the security of the data by checking the identity of the person who accessed the EHR.

- Public blockchain uses PKC to create a key pair and a network address from the user's selected password. There are still no trusted parties to issue keys to users. All transactions are encrypted with the receiver's public key and signed with the sender's private key. It gives exceeding user privacy and non-repudiation.
- For biomedical research use cases, in contrast with other types of blockchain, public blockchain demonstrates greater interoperability. However, the identity of the patients should be shielded from the data requester in order to protect the privacy of the data.
- The disadvantages of the public blockchain include unauthorized network access leading to impersonation attacks. Then open transaction data available to all network users reveal sensitive patient data, slowing network performance and impacting patient care in real-time. Also, the need to pay transaction fees and mining charges limits network usability.
- Data privacy in the public blockchain can be enhanced by storing only the hash value of the modified data in the blockchain. The contents should be stored in secondary storage systems such as cloud or IPFS. The data requester must obtain the patient's permission to access the EHR via blockchain.
- Several research papers have developed many techniques to ensure the protection of data in public blockchain-based EHR, but there is a lack of data privacy. In the public blockchain, data protection is accomplished only when the patient transfers his private key to a trusted person at the time of need. However, it is not applicable at the time of emergency when the patient is not in a state of sharing the private key.
- Greater data privacy can only be achieved through a private blockchain since only authorized users can enter the network. Man in the middle attack is avoided by having trusted authorities, thus ensuring data privacy.
- Private blockchain lacks interoperability; because only restricted users can access data. Moreover, private blockchain uses identity-based or attribute-based cryptography to generate keys. User requests are checked after the identity of the user is confirmed. Though it is a closed environment, users' data are exposed to othersin the network, which lacks user privacy.
- User identity can be hashed, and then cryptographic keys can be created, and the hash value can be used to validate the user and user requests. Otherwise, the user can create a pseudo-identity from which the authority can generate key pairs for the users.
- Scalability was seen as feasible by using blockchain technology to store only the index of records and to have control over EHR outsourced to the cloud or IPFS. This strategy reduces the space complexity associated with the transfer of information. When a blockchain is private, scaling problems are easily solved. Since the participants in the chain can monitor the maximum block size. Furthermore, the private blockchain as a closed network can only contain transactions that are of interest to those users.
- Interoperability, along with data privacy can be achieved by the use of a consortium blockchain that improves connectivity between different clinical organizations. Such blockchain architecture provides the benefit of creating a structured group capable of authorized users, which may enhance security concerns.
- Consortium blockchain can be used in healthcare applications such as remote patient monitoring, patients related to different health organizations, and inter-organizational biomedical research that provides high interoperability with data privacy and data integrity.
- IPFS is a peer-to-peer data storage system, that provides safe data storage since it provides data integrity through a cryptographic identifier that protects data from modification. An effort to modify the data stored on IPFS could only be made by modifying the identifier. All the data files stored on IPFS contain a cryptographically generated hash value. It is unique and is used to identify stored IPFS data files. This secure IPFS protocol storage approach makes it an advantageous alternative for storing EHR. The created cryptographic hash could be stored on the blockchain.
- Storing data in an external storage system brings a denial of service attack either centralized or distributed. If one storage system is crashed, then a lot of information will be lost. So there is a breach in the availability of information, which results in low-quality healthcare delivery.
- Speaking of cryptographic primitives, PRE and ABC show better computational effectiveness when compared to other cryptographic primitives. If PRE is used, the patient must trust the cloud proxy server that re-encrypts the data to the end-users. ABC offers data privacy and fine-grained access control. However, in a decentralized network, selecting trusted individuals to handle attributes is difficult but a consortium blockchain can be adopted with multi-authority.
- Considering real-world scenarios, blockchain-based EHR driven by patients reviewed in this paper is incapable and unsafe for a patient. Since it requires a patient to approve the exchange of a record explicitly. For the situation at the point when a patient is unconscious, a doctor attending to the patient requires the information to play out a medical procedure, and the patient would not have the option to share the EHR. Solutions should be proposed in such a way that the patient can give a trusted person to share and authorize EHR during the time the patient is in an unconscious state.
- Another scenario is, that the key loss which is popular among elderly patients, accessing and authenticating EHR, isan issue in this case. In a real-world implementation, a secondary method of accessing the patient data needs to be discussed.

6. Conclusions

The traditional cloud-based EHR is continuously at security breaches because of the centralized storage system. The decentralization, distribution, and data immutability through encryption and cryptographic primitives of blockchain avoid some security breaches. The introduction of blockchain in healthcare has significant implications for the quality of healthcare delivery, which includes structuring of patients' medical records, clinical trials, remote patient monitoring, medical research and collaborative decisions, finance, biomedical knowledge retrieval, and the healthcare supply chain. Given the research articles reviewed in this paper, blockchain technology has strong potential in addressing various issues related to the secure sharing and storing of EHR. The existing research articles overcame many security breaches in sharing and storing EHR such as data integrity, authentication, interoperability, availability, data privacy, user privacy, authorized accessing, and scalability. According to the study, consortium blockchain with IPFS satisfy more security requirement needed to store and access EHR. Moreover, ABC and PRE show better computational effectiveness compared to other cryptographic primitives. Although PRE shows better effectiveness compared to ABC, in the PRE scheme the users have to trust a third party who is acting as a proxy. Even though blockchain clarified enhancement in the secure sharing and storing of EHR, there are still security challenges, as blockchain has its disadvantages such as mining incentives in the healthcare industry, 51% attack, data privacy in the public blockchain, user privacy and interoperability in a private blockchain and fine-grained access to health records.

References

[1] Sidra Anwar, Sadia Anayat, Sheeza Butt, Saher Butt, Muhammad Saad, "Generation Analysis of Blockchain Technology: Bitcoin and Ethereum", International Journal of Information Engineering and Electronic Business, Vol.12, No.4, pp. 30-39, 2020.

[2] Senny Hapiffah, Ardiles Sinaga, "Analysis of Blokchain Technology Recommendations to be Applied to Medical Record Data Storage Applications in Indonesia", International Journal of Information Engineering and Electronic Business, Vol.12, No.6, pp. 13-27, 2020.

[3] Y. Zhang, C. Xu, H. Li, and X. Liang, “Cryptographic Public Verification of Data Integrity for Cloud Storage Systems,” IEEE Cloud Computing, vol. 3, no. 5, pp. 44–52, 2016, doi: 10.1109/MCC.2016.94.

[4] M. Johnson, M. Jones, M. Shervey, J. T. Dudley, and N. Zimmerman, “Building a Secure Biomedical Data Sharing Decentralized App (DApp): Tutorial,” J Med Internet Res, vol. 21, no. 10, p. e13601, 2019, doi: 10.2196/13601.

[5] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, “A Blockchain-Based Medical Data Sharing and Protection Scheme,” IEEE Access, vol. 7, pp. 118943–118953, 2019, doi: 10.1109/access.2019.2937685.

[6] M. Benchoufi and P. Ravaud, “Blockchain technology for improving clinical research quality,” Trials, vol. 18, no. 1, pp. 1–5, 2017, doi: 10.1186/s13063-017-2035-z.

[7] X. Zhu, J. Shi, and C. Lu, “Cloud health resource sharing based on consensus-oriented blockchain technology: Case study on a breast tumor diagnosis service,” Journal of Medical Internet Research, vol. 21, no. 7, 2019, doi: 10.2196/13767.

[8] Y. Wang, A. Zhang, P. Zhang, and H. Wang, “Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain,” IEEE Access, vol. 7, pp. 136704–136719, 2019, doi: 10.1109/access.2019.2943153.

[9] M. A. Cyran, “Blockchain as a Foundation for Sharing Healthcare Data,” Blockchain in Healthcare Today, 2018, doi: 10.30953/bhty.v1.13.

[10] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, “A Case Study for Blockchain in Healthcare,” Proceedings of IEEE Open & Big Data Conference, vol. 13, p. 13, 2016, [Online]. Available: https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf

[11] L. Ismail, H. Materwala, and S. Zeadally, “Lightweight Blockchain for Healthcare,” IEEE Access, vol. 7, pp. 1–1, 2019, doi: 10.1109/access.2019.2947613.

[12] 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,” IEEE Access, vol. 5, no. July, pp. 14757–14767, 2017, doi: 10.1109/ACCESS.2017.2730843.

[13] S. Wang et al., “Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach,” IEEE Transactions on Computational Social Systems, vol. 5, no. 4, pp. 942–950, 2018, doi: 10.1109/TCSS.2018.2865526.

[14] R. R. Brooks et al., “ Scrybe: A Blockchain Ledger for Clinical Trials ” , [Online]. Available: https://blockchain.ieee.org/images/files/images/clinicaltrialsforum-2018/Clemson_WhitePaper.pdf

[15] J. H. Beinke, C. Fitte, and F. Teuteberg, “Towards a stakeholder-oriented blockchain-based architecture for electronic health records: Design science research study,” Journal of Medical Internet Research, vol. 21, no. 10, 2019, doi: 10.2196/13585.

[16] T. Motohashi, T. Hirano, K. Okumura, M. Kashiyama, D. Ichikawa, and T. Ueno, “Secure and scalable mhealth data management using blockchain combined with client hashchain: System design and validation,” Journal of Medical Internet Research, vol. 21, no. 5, pp. 1–14, 2019, doi: 10.2196/13385.

[17] A. S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P. S. Efraimidis, and E. Kaldoudi, “A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval,” Computational and Structural Biotechnology Journal, vol. 16, pp. 288–297, 2018, doi: 10.1016/j.csbj.2018.08.002.

[18] L. A. Linn and M. B. Koo, “Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research,”

ONC/NIST Use of Blockchain for Healthcare and Research Workshop, pp. 1 – 10, 2016.

[19] W. B. Smith, “Dokchain: Intelligent Automation in Healthcare Transaction Processing,” no. Figure 1, pp. 1 – 15, 2017.

[20] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, “Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring,” Journal of Medical Systems, vol. 42, no. 7, pp. 1 – 7, 2018, doi: 10.1007/s10916-018-0982-x.

[21] S. Badr, I. Gomaa, and E. Abd-Elrahman, “Multi-tier blockchain framework for IoT-EHRs systems,” Procedia Computer Science, vol. 141, pp. 159 – 166, 2018, doi: 10.1016/j.procs.2018.10.162.

[22] X. Zheng, S. Sun, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Meré, “Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies,” Journal of Medical Internet Research, vol. 21, no. 6, 2019, doi: 10.2196/13583.

[23] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, “FairAccess: a new Blockchain-based access control framework for the Internet of Things,” Security and Communication Networks, vol. 9, no. 18, pp. 5943 – 5964, 2016, doi: 10.1002/sec.1748.

[24] D. Ichikawa, M. Kashiyama, and T. Ueno, “Tamper-Resistant Mobile Health Using Blockchain Technology,” JMIR Mhealth Uhealth, vol. 5, no. 7, p. e111, 2017, doi: 10.2196/mhealth.7938.

[25] H. Guo, W. Li, M. Nejad, and C.-C. Shen, “Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture,” 2019, [Online]. Available: http://arxiv.org/abs/1906.01188

[26] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, “Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology,” Sustainable Cities and Society, vol. 39, no. December 2017, pp. 283 – 297, 2018, doi: 10.1016/j.scs.2018.02.014.

[27] S. Wang, X. Wang, and Y. Zhang, “A Secure Cloud Storage Framework With Access Control Based on Blockchain,” IEEE Access, vol. 7, pp. 112713 – 112725, 2019, doi: 10.1109/access.2019.2929205.

[28] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, “SYSTEMS-LEVEL QUALITY IMPROVEMENT MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain,” Journal of Medical Systems, vol. 42, pp. 1 – 11, 2018, doi: 10.1007/s10916-018-0993-7.

[29] T. T. Thwin and S. Vasupongayya, “Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems,” Security and Communication Networks, vol. 2019, 2019, doi: 10.1155/2019/8315614.

[30] H. Wang and Y. Song, “BAB 2 PITA ezahan,” 2018, doi: 10.1007/s10916-018-0994-6.

[31] J. N. Colloquium and B. E. Zrt, “Blockchain : solving the privacy and research availability tradeoff for EHR data,” IEEE 30th Jubilee Neumann Colloquium, pp. 135 – 140, 2017.

[32] Brodersen, C. B. Kalis, C. Leong, E. Mitchell, E. Pupo, and A. Truscott, “Blockchain : Securing a New Health Interoperability Experience,” NIST Workshop on Blockchain & Healthcare, no. August, pp. 1 – 11, 2016, doi: 10.1001/jama.2012.362.4.

[33] K. Culver, “BIR in Billons,” pp. 1 – 10.

[34] D. Ivan, “Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records,” NIST Workshop on Blockchain & Healthcare, no. August, p. 11, 2016, [Online]. Available: https://www.healthit.gov/sites/default/files/9-16-drew_ivan_20160804_blockchain_for_healthcare_final.pdf

[35] H. Yang and B. Yang, “A Blockchain-based Approach to the Secure Sharing of Healthcare Data,” Norwgian Information Security Conference, 2017, [Online]. Available: https://ojs.bibsys.no/index.php/NISK/article/view/462

[36] L. Castaldo and Cinque Vincenzo, Blockchain-Based Logging for the Cross-Border Exchange of eHealth Data in Europe.

[37] A. Shahnaz, U. Qamar, and A. Khalid, “Using Blockchain for Electronic Health Records,” IEEE Access, vol. 7, pp. 147782 – 147795, 2019, doi: 10.1109/access.2019.2946373.

[38] A. Roehrs, C. A. da Costa, R. da Rosa Righi, V. F. da Silva, J. R. Goldim, and D. C. Schmidt, “Analyzing the performance of a blockchain-based personal health record implementation,” Journal of Biomedical Informatics, vol. 92, no. October 2018, p. 103140, 2019, doi: 10.1016/j.jbi.2019.103140.

[39] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, “Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain,” Information Sciences, vol. 485, pp. 427 – 440, 2019, doi: 10.1016/j.ins.2019.02.038.

[40] L. Zhu, Y. Wu, K. Gai, and K. K. R. Choo, “Controllable and trustworthy blockchain-based cloud data management,” Future Generation Computer Systems, vol. 91, pp. 527 – 535, 2019, doi: 10.1016/j.future.2018.09.019.

[41] G. Yang, C. Li, and K. E. Marstein, “A blockchain-based architecture for securing electronic health record systems,” Concurrency Computation , no. July, pp. 1 – 10, 2019, doi: 10.1002/cpe.5479.

[42] F. Tang, S. Ma, Y. Xiang, and C. Lin, “An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records,” IEEE Access, vol. 7, pp. 41678 – 41689, 2019, doi: 10.1109/ACCESS.2019.2904300.

[43] R. H. Hylock and X. Zeng, “A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study,” J Med Internet Res, vol. 21, no. 8, p. e13592, 2019, doi: 10.2196/13592.

[44] Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, “A decentralizing attribute-based signature for healthcare blockchain,” Proceedings - International Conference on Computer Communications and Networks, ICCCN, vol. 2018-July, pp. 1 – 9, 2018, doi: 10.1109/ICCCN.2018.8487349.

[45] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, “BBDS: Blockchain-based data sharing for electronic medical records in cloud environments,” Information (Switzerland), vol. 8, no. 2, 2017, doi: 10.3390/info8020044.

[46] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, “A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment,” Journal of Medical Systems, vol. 42, no. 8, 2018, doi: 10.1007/s10916-018-1007-5.

[47] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, “Blockchain-Based Data Preservation System for Medical Data,” Journal

of Medical Systems, vol. 42, no. 8, pp. 1 – 13, 2018, doi: 10.1007/s10916-018-0997-3.

[48] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems,” IEEE Access, vol. 7, pp. 66792 – 66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[49] S. Rahmadika and K. H. Rhee, “Blockchain technology for providing an architecture model of decentralized personal health information, ” International Journal of Engineering Business Management, vol. 10, pp. 1 – 12, 2018, doi: 10.1177/1847979018790589.

[50] L. Chen, W. K. Lee, C. C. Chang, K. K. R. Choo, and N. Zhang, “Blockchain based searchable encryption for electronic health record sharing,” Future Generation Computer Systems, vol. 95, pp. 420 – 429, 2019, doi: 10.1016/j.future.2019.01.018.

[51] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility,” Future Generation Computer Systems, vol. 25, no. 6, pp. 599 – 616, 2009, doi: 10.1016/j.future.2008.12.001.

[52] V. Casola, A. Castiglione, K. K. R. Choo, and C. Esposito, “Healthcare-Related Data in the Cloud: Challenges and Opportunities,” IEEE Cloud Computing, vol. 3, no. 6, pp. 10 – 14, 2016, doi: 10.1109/MCC.2016.139.

[53] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, and X. Lin, “HealthDep: An Efficient and Secure Deduplication Scheme for Cloud-Assisted eHealth Systems, ” IEEE Transactions on Industrial Informatics, vol. 14, no. 9, pp. 4101 – 4112, 2018, doi: 10.1109/TII.2018.2832251.

[54] Z. Wan, J. Liu, and R. H. Deng, “HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing, ” IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743 – 754, 2012, doi: 10.1109/TIFS.2011.2172209.

[55] C. Mcfarlane, M. Beer, J. Brown, and N. Prendergast, “Patientory : A Healthcare Peer-to-Peer EMR Storage Network,” no. April, pp. 1 – 19, 2017, [Online]. Available: https://patientory.com/patientory_whitepaper.pdf

[56] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, “OmniPHR: A distributed architecture model to integrate personal health records,” Journal of Biomedical Informatics, vol. 71, pp. 70 – 81, 2017, doi: 10.1016/j.jbi.2017.05.012.

[57] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec : Using Blockchain for Medical Data Access and Permission Management,” 2016 2nd International Conference on Open and Big Data (OBD), pp. 25 – 30, 2016, doi: 10.1109/OBD.2016.11.

[58] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control,” Journal of Medical Systems, vol. 40, no. 10, 2016, doi: 10.1007/s10916-016-0574-6.

[59] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, “A Blockchain-Based Approach to Health Information Exchange Networks,” no. 1, pp. 1 – 10.

[60] T. Ammbr, P. Token, S. Has, and B. Cancelled, “Whitepaper 21.” pp. 1 – 42, 2017.

[61] R. Guo, H. Shi, Q. Zhao, and D. Zheng, “Secure Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems,” IEEE Access, vol. 6, pp. 11676 – 11686, 2018, doi: 10.1109/ACCESS.2018.2801266.

[62] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, “Blockchain-based personal health data sharing system using cloud storage,” 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services, Healthcom 2018, 2018, doi: 10.1109/HealthCom.2018.8531125.

[63] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, “Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack,” pp. 458 – 467, 2017, doi: 10.1109/CCGRID.2017.111.

Authors’ Profiles

C. Eben Exceline completed M.Tech in Computer and Information Technology from Manonmaniam Sundaranar University, Tamil Nadu, India. She is currently pursuing Ph.d in Information technology from School of Information Technology and Engineering (SITE), Vellore Institute of Technology, Vellore, Tamil Nadu, India. Her research interests include information security, cloud computing, blockchain technology and their application in electronic health records.

Dr. Sivakumar Nagarajan received his B.E. degree in Computer Science and Engineering from University of Madras and M.Tech from Dr. M.G.R. Educational and Research Institute, Chennai. He received his Ph.D in Computer Science and Engineering from Anna University. He is currently working as an Associate Professor in the School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore, Tamil Nadu, India. His area of interest includes Image Processing, Artificial Intelligence and Machine Learning, and Wireless Sensor Networks.

How to cite this paper: C. Eben Exceline, Sivakumar Nagarajan, "The Security of Blockchain-based Electronic Health Record: A Systematic Review", International Journal of Computer Network and Information Security(IJCNIS), Vol.15, No.6, pp.103-117, 2023. DOI:10.5815/ijcnis.2023.06.09