IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 16, 2021, accepted November 5, 2021, date of publication November 18, 2021,
date of current version December 6, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3129284

Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR

RAHUL GANPATRAO SONKAMBLE[1,2], SHRADDHA P. PHANSALKAR[1], VIDYASAGAR M. POTDAR[3], AND ANUPKUMAR M. BONGALE[2], (Senior Member, IEEE)

[1]Computer Engineering, MIT ADT University, Pune 412201, India
[2]Department of Computer Science and Information Technology, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Lavale, Pune, Maharashtra 412115, India
[3]Blockchain Research and Development Laboratory, Curtin University, Bentley, WA 6102, Australia

Corresponding author: Anupkumar M. Bongale (ambongale@gmail.com)

This work was supported by Research Support Fund of Symbiosis International (Deemed University).

ABSTRACT Interoperability in Electronic Health Records (EHR) is significant for the seamless sharing of information amongst different healthcare stakeholders. Interoperability in EHR aims to devise agreements in its interpretation, access, and storage with security, privacy, and trust. A study and survey of the state-of-the-art literature, prototypes, and projects in standardization of the EHR structure, privacy-preservation, and EHR sharing are very essential. The presented work conducts a systematic literature review to address four research questions. 1) What are the different standards for common interpretation, representation, and modeling of EHR to achieve semantic interoperability? 2) What are the different privacy-preservation techniques and security standards for EHR data storage? 3) How mature is blockchain technology for building interoperable, privacy-preserving solutions for EHR storage and sharing? 4) What is the state-of-the-art for cross-chain interoperability for EHR sharing? An exhaustive study of these questions establishes the potential of a blockchain-based EHR management framework in privacy preservation, access control and efficient storage. The study also unveils challenges in the adoption of blockchain in EHR management with the state-of-the-art maturity of cross-chain interoperable solutions for sharing EHR amongst stakeholders on different blockchain platforms. The research gaps culminate in proposing a blockchain-based EHR framework called as MyBlockEHR with privacy preservation and access control design. The proposed framework employs partitioning of EHR to on-chain and off-chain storages for performance guarantees with the retrieval of valid off-chain data. The framework is deployed on the Ethereum test network with Solidity smart contracts. It is observed that different test cases on the partitioning of the EHR data, yielded better read-write throughput and effective gas price than fully on-chain storage.

INDEX TERMS Blockchain, cross-chain, EHR, interoperability, partitioning.

I. INTRODUCTION

Interoperability in the healthcare sector is the ability of the healthcare systems to share, interpret and use Electronic Health Record (EHR) coherently [1]. Interoperable solutions to EHR management are critical for seamless transfers of patient data and treatment details for improving the effectiveness of healthcare services with reduced cost and time. EHR refers to patient data that is recorded, processed, and analyzed at various healthcare organizations [2]. As this data originates from different organizations, it follows local standards and healthcare terminologies. The EHR standards of different healthcare organizations are not uniform, causing a low level of interoperability in healthcare information systems among the organizations [3], [4]. Hence interoperable EHR solutions aim for standardization of EHR structure. EHR sharing and interoperability amongst the different healthcare organizations is a critical area of research [5].

Patient-controlled interoperable solutions imply that the patient owns their EHR and they permit or deny access to

The associate editor coordinating the review of this manuscript and approving it for publication was Mingjun Dai.

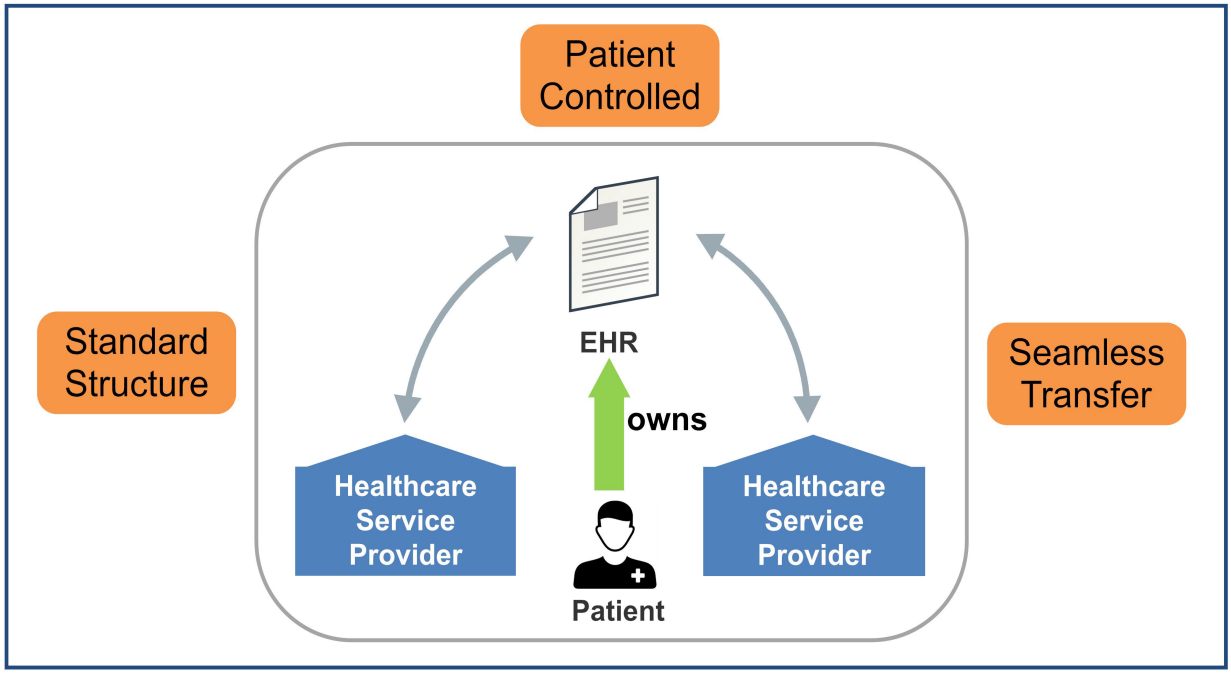

FIGURE 1. EHR interoperability goals.

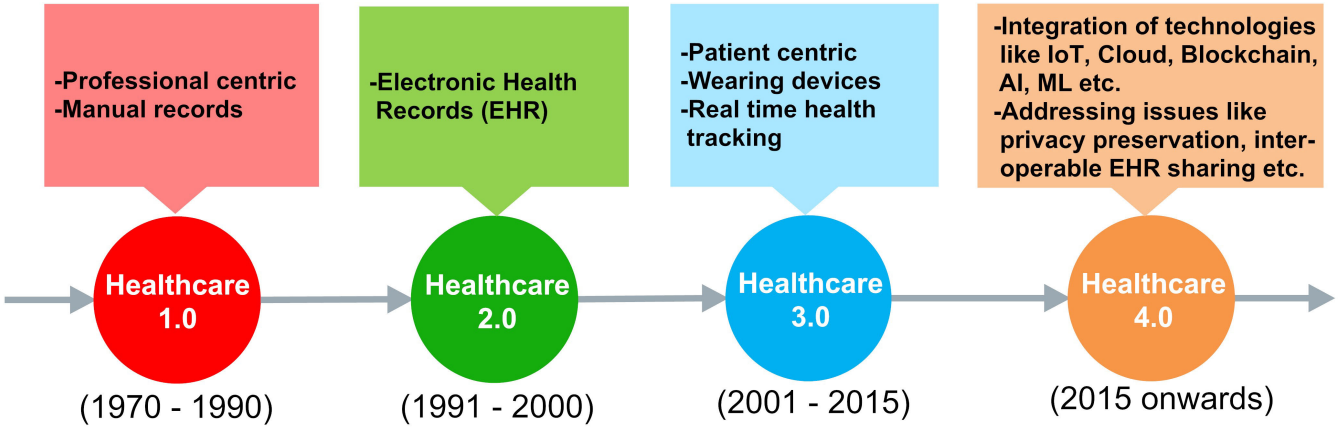

FIGURE 2. Evolution of challenges in data sharing in the healthcare sector across the different eras.

their records to other stakeholders [6]. Seamless EHR sharing amongst different healthcare stakeholders (like Hospital A to Hospital B or Hospital to Insurance) is essential for a better healthcare. Delivery Seamless transfers of EHR lead to time and cost-effective interoperable solutions [1].

Standardization of EHR structure, patient-controlled data access, and seamless transfers of EHR across the different healthcare service providers are the goals of EHR interoperability in modern healthcare systems [1]. This is depicted in Fig. 1. EHR representation and its sharing in the healthcare sector have evolved through different eras, as shown in Fig. 2. It is pretty significant and exciting to study how the challenges in EHR sharing evolved across the eras in healthcare.

Healthcare 1.0 [7] marked the creation of manual records for the ease of use of the service providers. Healthcare 2.0 era was the digitization of health records with electronic health records [7]. With healthcare 3.0 [7], remote and real-time capturing of health data was possible by integrating wearable Internet of Thing (IoT) devices with the information system. This era also marks emphasis on the privacy consideration to EHR. Healthcare 4.0 [7] emerges with the need for integration of different healthcare information systems for seamless transfers of EHR. Besides, these information systems should guarantee privacy preservation and patient-controlled access to EHR to build interoperable EHR sharing.

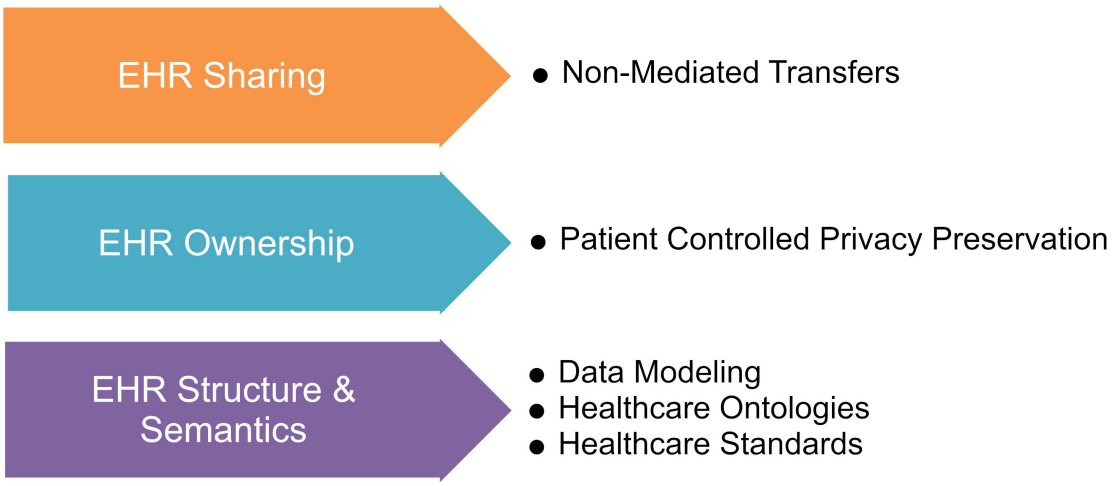

FIGURE 3. EHR management challenges in interoperable solutions.

A. SIGNIFICANCE & RATIONALE

In the healthcare sector, interoperable data integration faces challenges with data semantics, data ownership, and data sharing with constraints of data privacy, security, time and cost-effectiveness [5], [8]. With diversities in the structure and semantics of EHR, there arise problems while exchanging data with other healthcare organizations or external entities. According to [5], 70% of physicians are reportedly affected by incompatible data generated by different healthcare organizations. Thus, data needs to have common representation and interpretation to be semantically interoperable. Thus, heterogeneous EHR structure poses to be a challenge to EHR interoperability [9].

Privacy of healthcare data is a significant concern [5]. Healthcare data is very personal, sensitive, and vulnerable to attacks. Privacy threats and lack of trust challenges healthcare data sharing. As per the Deloitte Health Consumer Survey, only 46% of healthcare consumers are willing to share their data in the initial phase of treatment [10]. Here the ownership of EHR is a significant concern. This issue can be handled by privacy preservation techniques and patient-controlled access in EHR interoperability solutions [7]. EHR sharing across multiple stakeholders is another critical management issue. The EHR must be shared seamlessly, but it should also be free from intermediaries to build trust in the EHR management [11].

Literature shows that interoperable solutions in EHR management should address these challenges for effective patient-care, as shown in Fig. 3. EHR structure and semantic interoperability deal with EHR representation using healthcare standards, ontologies, and data modeling [9], [12]. EHR ownership is realized with a patient-controlled privacy-preserving mechanism. It implies that the EHR is owned and the access is controlled by the patient to audit sharing of their personal data [13]. EHR sharing in interoperable solutions aims to facilitate sharing of EHR across different healthcare systems. EHR sharing should be non-mediated [14] i.e., without any intermediaries. It is an important aspect for privacy preservation [11].

Thus, it is essential to study these challenges to EHR interoperability with a systematic literature review to analyze the maturity of the current solutions. The study also aims to evaluate blockchain technology to realize of interoperable solutions in EHR management [15], [16].

B. MOTIVATION

EHR management challenges fall in the three major areas of concern as described in Fig. 3 [9], [11]–[13]. Blockchain technology offers a promising solution to the data ownership, sharing, and an audited trail of healthcare records [7]. The stakeholders share EHR on a decentralized ledger in a transparent manner. The immutability of the records, provenance tracking, and the access controls with smart contracts make this a better technology to manage the EHR systems [6], [13], [14], [17]–[19].

However, EHR management on the blockchain system is challenged with few performance issues as described in [6], [13], [14], [17]–[24]. Few models and frameworks tried to address performance issues [17], privacy, and security [6].

1) EHR transactions are high in volume and need to be stored on the distributed storage on the blockchain.
2) EHR transactions are personal medical records, and their privacy is endangered with distributed storage.
3) EHR transactions are higher in volume and incur heavy on-chain computations.
4) EHR exchanges on cross-chain systems imply the need for sharing over heterogeneous platforms, which is a significant challenge.

The motivation of this work is two-fold. We aim to outline and evaluate the different standards and techniques to achieve interoperability in EHR structure, storage and

sharing. The existing literature shows the increase in the adoption of blockchain technology for the implementation of trusted, transparent EHR management systems with challenges [6], [13], [14], [17]–[21], [23]. Hence evaluation of blockchain-based EHR management systems is essential.

However, these decentralized EHR management systems lack scalability and offer lesser privacy to sensitive health data [25]. This work proposes a framework that offers better privacy, scalability, and cost over existing blockchain-based EHR management solutions with standardization of EHR structure and semi-centralized storage. The prototype is implemented and evaluated with experimental validations on a blockchain framework with smart contracts.

C. OBJECTIVES

1) The first objective of the work is to evaluate the state-of-the-art works in the following areas of interoperability in EHR management:
   a. Semantic interoperability: This study focuses on standards in EHR structure [9], [26], [27]–[31], representation [9], [32]–[39], and data modeling techniques [12], [40]–[47] that can be suitable for EHR.
   b. Privacy-preserving EHR storage: This study evaluates significant privacy preservation techniques [11], [17], [20]–[22], [48]–[59] to protect sensitive patient data from unauthorized users. A study of data security standards for EHR data is also carried out.
2) The second objective of the work is to investigate blockchain-based solutions to address the issues in first objective with the study of the literary works on adopting blockchain in EHR management [6] [13] [14], [17]–[23]. The study was further carried out to investigate the research gaps in EHR deployment on the blockchain.
3) The third objective is to address gaps in EHR management over blockchain with the proposed framework MyBlockEHR:
   a. Performance: Partitioning EHR data to on-chain and off-chain storage for better performance and throughput [6].
   b. Privacy: The data partitioning strategy in data storage should preserve the sensitive patient data from unauthorized access [6].
   c. Trusted data storage: The off-chain data storage needs to be trustworthy, tamper-proof, and available to the blockchain-based EHR management systems with smart contract oracles that validate data from off-chain storage with on-chain hash [6].
   d. Access control: Patient-centric access control implies that patients will be owners of the data, and access to EHR will be granted to other stakeholders with patient permission [6] [13] [60].

   The prototype is to be experimentally verified with smart contracts deployed on the network and evaluated for scalability and cost for different test cases.
4) The fourth objective of the study is to analyze the cross-chain interoperability issues in sharing EHR amongst different stakeholders over different blockchain platforms. With the study, we uncover the maturity of existing solutions like [15], 16], 61]–[94] and put forth the need for modeling a trust-based, non-intermediated solution for EHR exchange over cross-chain platforms [15], [16], [61]–[65].

D. RESEARCH GOALS

This research aims to analyze the existing studies, standards, tools, and techniques in realizing interoperable EHR management in the three areas of focus, i.e. semantic interoperability, privacy-preserving techniques for EHR storage, and non-mediated EHR sharing. The research questions are listed in Table 1 to carry out the study of EHR management and application of blockchain technology of the same. The scope of our work is described with a structure diagram, as shown in Fig. 4.

II. RESEARCH METHOD

The literature review is carried out with guidelines for Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow diagram stated in [95]. We have adapted the PRISMA flow diagram as shown in Fig. 5.

Seventy-eight research papers and articles from 2007-2021 were reviewed in our work. Blockchain is a recent technology. That's why there are undergoing industry-based products and projects. Hence, we have also referred to 80 web sources for our review. This topic's relevance led to finding web sources in healthcare ontologies, EHR standards, cross-chain solutions and blockchain platforms. We included research works, proof-of-concepts, prototypes in the focus areas of interoperability. Since the application of blockchain in the healthcare sector has been recent, prominent blockchain-based solutions to the healthcare sector have been referred since 2016. The white papers, official websites, and web blogs have been referred for blockchain engines.

A. ELIGIBILITY CRITERIA AND INFORMATION SOURCES

As our focus was addressing interoperability in EHR with blockchain, projects on blockchain applications for EHR management and privacy preservation techniques were surveyed. For cross-chain projects in blockchain, the official websites and white papers were referred.

1) INCLUSION & EXCLUSION CRITERIA

We have listed inclusion and exclusion criteria for different categories of searches in Table 2. We applied Google search engine for all searches, and they were conducted from January 2020 to August 2021.

B. KEYWORD SEARCH

The work focuses on three aspects of interoperability i.e., semantic interoperability, patient-centric privacy-preserving techniques, and cross-chain interoperability. Hence, related

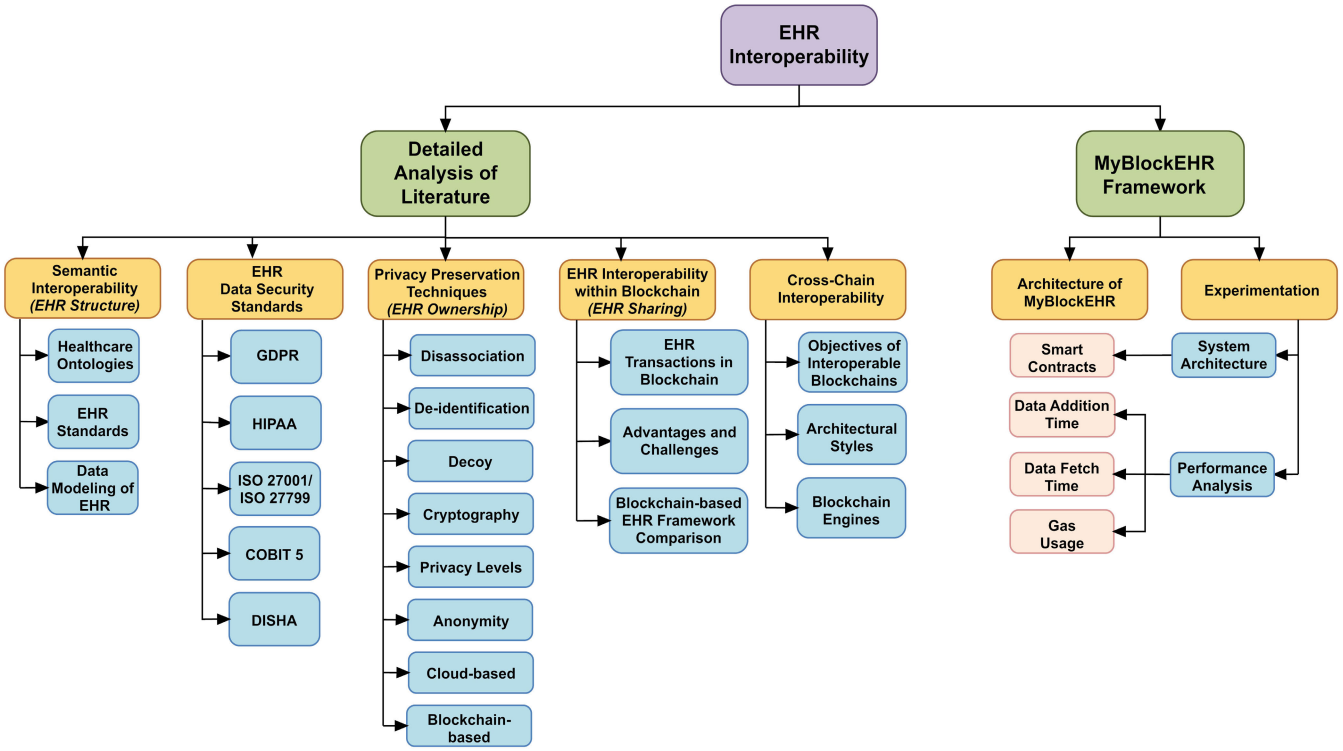

FIGURE 4. Structure of the presented research paper.

TABLE 1. Research questions for the literature review.

Research Questions (RQ)	Justification
RQ.1 What are the different standards for common interpretation, representation, and modeling of EHR to achieve semantic interoperability?	The study of standards in EHR representations, ontologies and big data models for EHR is carried out to address the issues in semantic interoperability of EHR.
RQ.2 What are the different privacy-preserving techniques and security standards for EHR data storage?	As EHR is sensitive data, its privacy is utmost important. Hence, critique on the privacy-preserving techniques [11] [17] [20-22] [48-59] for EHR is done with respect to performance metrics like retrieval time, access cost, and storage cost. We have also discussed security standards in section III.
RQ.3 How mature is blockchain technology for building interoperable, privacy-preserving solutions for EHR storage and sharing?	The study of blockchain architecture is carried out to evaluate its application in EHR storage and exchange. The study of challenges [6] [13] [14] [17-24] in implementing EHR management on the blockchain is carried out to realize the prototype MyBlockEHR for efficient EHR management.
RQ.4 What is the state-of-the-art for cross-chain interoperability for EHR sharing?	As EHR is shared across healthcare stakeholders, it should be interoperable. In that regards, evaluation of the maturity of the existing interoperability solutions [15] [16] [61-94] with architectural styles and blockchain engines to achieve cross-chain EHR sharing is carried out.

phrases were used as search terms in the Google search engine. Table 3 shows the related phrases used for interoperability concepts.

We have applied snow-balling techniques to retrieve top-ranked web pages, white papers, and research papers.

III. DETAILED ANALYSIS OF LITERATURE

The need for interoperability in healthcare systems was focused on in many research works. We surveyed on research works in prominent areas, namely a) Semantic Interoperability, b) EHR data security standards, c) Privacy Preservation Techniques d) EHR interoperability within the blockchain, and e) Cross-chain interoperability.

A. SEMANTIC INTEROPERABILITY

Structural interoperability defines syntax, format, and organization of data for standard representation [1]. Semantic interoperability implies that the sender machine and

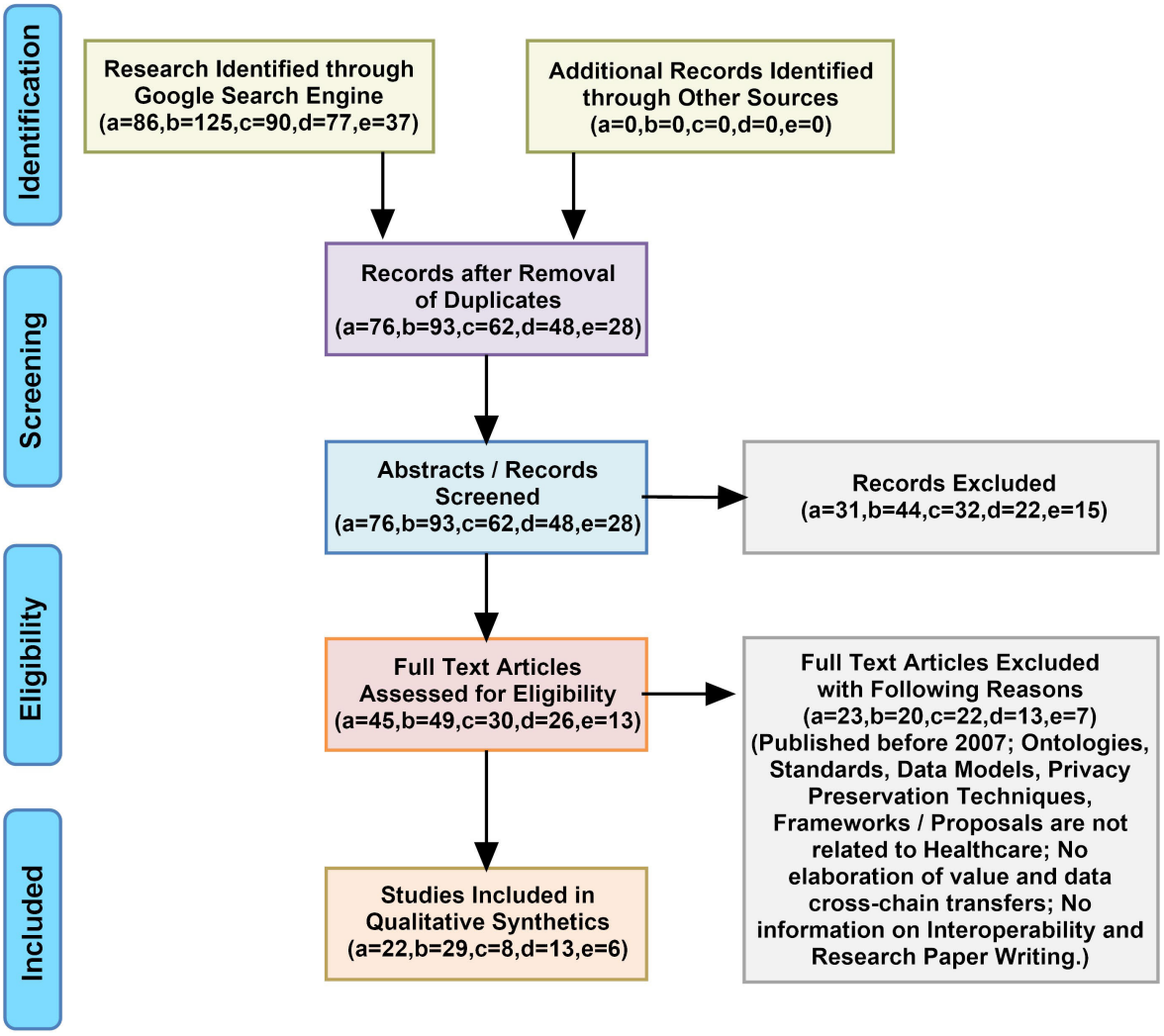

FIGURE 5. The adapted PRISMA flow diagram for systematic review detailing searches, number of abstracts/records screened and full-text articles retrieved where a = Semantic Interoperability, b = Privacy Preservation Techniques, c = EHR Interoperability within Blockchain, d = Cross-chain Interoperability, e = General Information on Interoperability and on writing review paper.

receiver system agree on the common understanding of the data [8]. After sharing data, the meaning of data had to be preserved and unaltered [26]. Both the structural and semantic interoperable systems should interpret data based on a common understanding of vocabulary and standard definitions.

Semantic interoperability in healthcare data is classified at two levels in [96], i.e. partial and full semantic interoperability. Partial semantic interoperability means that the health records are translated in an intermediate standard, acceptable to the sender and receiver systems. Full semantic interoperability means that the first health records are collected in the sender's standards, translated into intermediate standards, and then reproduced in the local standards of the receiver.

In this work, we review semantic interoperability of EHR with the study of popular healthcare ontologies, EHR standards, and EHR data models as shown in Fig 6.

1) HEALTHCARE ONTOLOGIES

Semantic interoperability in EHR requires working with semantic patterns and ontologies frameworks for heterogeneous healthcare data [97]. Such heterogeneous data forms heterogeneous EHR models.

Healthcare ontology is a model which represents the set of concepts within healthcare domains. An ontology represents the different domain terms in terms of labeled graphs and relationships between them. To show the relationships between such terms rich set of constructs are required. So, the ontological framework gives interoperable meaning to heterogeneous EHR models in labeled graphs, relationship diagrams and constructs. Ontologies are the best tools for data modeling of healthcare terms and act as bridges between heterogeneous EHR models. Semantic patterns are data representations of repetitive objects, terms, and terminologies in ontology libraries.

TABLE 2. Inclusion and exclusion criteria for review.

Topics of study	Inclusion Criteria	Exclusion Criteria
Semantic interoperability in EHR	The work must refer to EHR data standards or healthcare ontologies, or big data models popularly employed for EHR management.	Papers presenting ontologies and standards other than health records, big data models for non-medical applications.
Privacy preservation techniques in EHR	The work must refer to different privacy-preserving techniques for EHR data storage. Works on blockchain and smart contract based EHR privacy techniques were also included.	Privacy Preservation techniques applied to non-medical use cases.
Cross-chain interoperability	White papers or official websites, or web blogs describing exchange mechanisms across different platforms of blockchain are considered. The projects where these standards are employed for healthcare use cases are included.	-

TABLE 3. Keyword search used.

Interoperability concepts	Keywords
Semantic interoperability	• Semantic interoperability in EHR • EHR standards • Ontology in healthcare • EHR data model in EHR
Privacy preservation techniques	• Patient-centric privacy preservation
Blockchain in the healthcare sector	• Blockchain in EHR
Interoperable projects for cross-chain platforms with architectural strategies and blockchain engines	• Blockchain interoperability solutions
Information for specific cross-chain solution / project	• Name of the cross-chain project along with keyword "Blockchain"

In this work, we study the features of significant ontologies employed for healthcare data interpretation as described in Table 4.

2) EHR STANDARDS

Semantics act as dictionaries with medical terminologies, whereas standards in semantic interoperability refer to representations for transmitting data between two different systems. They are the most essential building blocks in interoperable EHR sharing. Standards may be among three types i.e., messaging, terminology and document. Messaging standards focus on structure, content and other data requirements to enable effective EHR sharing. Terminology standards deal with disease and medication specific codes. With the help of document standards, type and location of information can be identified. Significant healthcare standards are described in Table 5.

EHR standards are being adopted across the globe. As per news article [98], the USA is collaboratively developing EHR standards with HL7, National Council for Prescription Drug Programs (NCPDP), X12, and other Health Standards Collaborative (HSC) members. As per the declaration provided by Ubitech company [99], Europe is developing an EHR interoperability framework by using standards such as OpenEHR, DICOM, ICD-10, Diagnostic and Statistical Manual of Mental Disorders (DSM) [100], and Medical Dictionary for Regulatory Activities (MEDRA) [101]. Indian ministry has suggested the healthcare organizations to use EHR standards such as SNOMED-CT, ICD-11, LOINC, DICOM, HL7, etc. [102]. As per [103], healthcare systems in the US and Canada support the HL7 standard.

France approved the use of Hprim Santé and PN13 standards, which are adopted from HL7 [104]. As per an article on healthcare interoperability worldwide standards, Germany has adopted eXtensible Data Types (xDT) [104], [105]. As per [106], China has adopted HL7-based EHR standards since 2013. Standards like HL7, SNOMED-CT, CDA, and ICD are popularly employed by Australia, Denmark, England, Netherlands and Ireland [27].

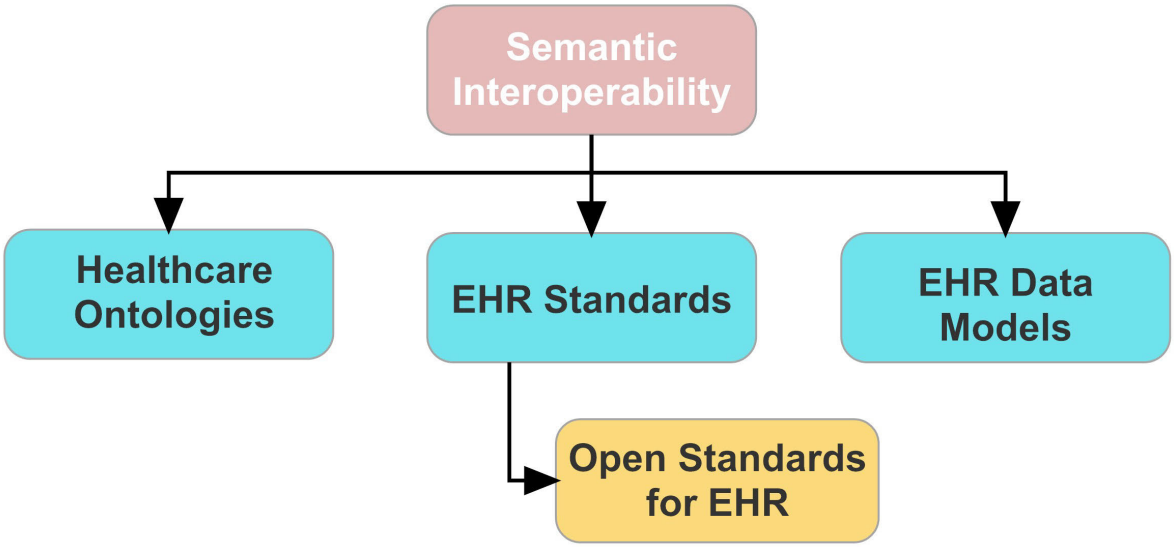

FIGURE 6. Focus areas in semantic interoperability.

TABLE 4. Significant ontologies in healthcare data.

Works	Name	Features	Developed / Maintained by
[32]	Ontology Web Language (OWL)	• It facilitates ontology representation as semantic web standards. • It represents rich and complex level knowledge about things or group of things and relations among them. • It is built upon Resource Description Framework (RDF). • SPARQL Protocol and RDF Query Language (SPARQL) is used for querying.	World Wide Web Consortium (W3C)
[33]	Gene Ontology (GO)	• It reveals genetic information of species ranging from the molecular level to organism level. • It is the foundation for computational analysis, molecular biology and medical experiments. • It is built upon RDF. • It uses OWL for knowledge representation. • SPARQL is used for querying.	Go Consortium
[34] [35]	General Architecture for Languages, Encyclopedias and Nomenclatures in Medicine (GALEN)	• It represents clinical terminologies written in GALEN Representation And Integration Language (GRAIL). • Uses modifiers to describe categories of objects (organic, inorganic, biological, non-biological). • It uses aspects and modalities to describe the modifiers.	OpenGALEN
[36]	Common Anatomy Reference Ontology (CARO)	• It facilitates interoperability between existing anatomy ontologies for different species. • It is represented in OWL formats.	Individual-Private
[37]	Systematized Nomenclature of Medicine (SNOMED*)	• It builds ontology based on general medical science and prevents redundancies and inconsistencies among large terminologies. • It is represented in OWL format.	SNOMED International
[9] [38] [39]	International Classification of Diseases (ICD-10*)	• It used to classify diagnosis codes. • SPARQL is used for querying.	National Centre for Health Statistics

OpenEHR [107] and (Fast Healthcare Interoperability Resources) FHIR [108] are popular open standards adopted by many research works. OpenEHR is used to create EHR standards, archetypes and to build information in the health-care sector. OpenEHR is the most popular standard for EHR persistence with over 300 archetypes specified in its reference model.

FHIR is the HL7 standard mainly designed for EHR interoperability. HL7 FHIR is a lightweight standard used for EHR sharing using RESTful Application Programming

TABLE 5. Significant standards in healthcare data sharing.

Works	Name	Type	Application Use case	Developed / Maintained by
[9]	HL7 (Health Level 7)V2.x	Messaging	• It facilitates clinical and administrative data sharing amongst different stakeholders in a hospital.	HL7
[27]	Digital Imaging and Communications in Medicine (DICOM)	Messaging	• It is a standard for biomedical image storage, interpretation and transmission.	DICOM Standards Committee
[28]	International Classification of Primary Care (ICPC-2)	Terminology	• It provides specific codes for clinical terms in clinical decision support system for primary care operations. • This standard is divided into seven components dealing with symptoms, diagnostic, treatment, tests, and administrative referrals.	Family Medicine Research Centre (FMRC)
[9]	The International Statistical Classification of Diseases and Related Health Problems, Tenth Revision, Australian Modification (ICD-10-AM)	Terminology	• It provides specific codes for clinical terms in clinical decision support system in disease vocabulary.	National Centre for Health Statistics
[27]	SNOMED Clinical Terms (CT)	Terminology	• It provides specific codes for clinical terms in primary healthcare.	OpenEHR
[27]	Logical Observation Identifiers Names and Codes (LOINC)	Terminology	• It provides standard for identification of clinical information in e-Laboratory results. • It facilitates sharing & grouping of test results for clinical research.	OpenEHR
[9]	Clinical Document Architecture (CDA)	Document	• E-sharing of EHR in terms of a document. • The document contains information in the form of text, image, sound, and other multimedia forms.	HL7
[27] [29]	Continuity of Care Document (CCD)	Document	• It maintains only critical information of patient for continuity of care. • It facilitates sharing of content of patient being transferred from one care setting to another.	HL7
[27] [30]	HL7 Discharge Summary (DS)	Document	• It maintains discharge summary. • It contains information as an image, free text or coded data. • It is compliant to CDA and HL7.	HL7
[27] [31]	Reference Information Model (RIM)	Conceptual	• A static model of health information flow and context in HL7 standards development group. • It uses Unified Service Action Model (USAM).	HL7
[27]	Healthcare Information Systems Architecture (HISA)	Architecture	• Provides open architecture that is independent of the application and technical specifications. • It is used to integrate healthcare data from heterogeneous platforms.	European Committee for Standardization (CEN)

Interface (API). The comparative analysis between these two standards from perspectives of structure, complexity, and interoperability is presented in Table 6.

3) DATA MODELING OF EHR

EHR consists of personal details of the patient, their treatment, clinical trials, and follow-ups. EHR thus is a collection of heterogeneous data representations (text, images, documents, video, etc.) With digitization in the healthcare sector, a massive volume of EHR is generated. The data structure used for storing EHR and related operations are called as the data model. Thus, big data models are the best candidates for the representation of EHR [41].

We studied the projects and research works proposing and implementing the data management systems for EHR using different data models, with the diversities from the traditional relational database management systems to Not only SQL (No-SQL) big data models. We analyzed different models employed for EHR in terms of object complexity and performance metrics like retrieval time, scalability, isolation, and consistency. The works are evaluated, and findings are outlined in Table 7 below.

TABLE 6. Comparative analysis between OpenEHR and FHIR as EHR standards.

Features	OpenEHR	FHIR
Main Purpose	Complex Data modeling.	Interoperable EHR sharing.
Focus	It has a strong focus on data persistence, with APIs and EHR sharing as a secondary focus.	Integrating different discrete elements of the EHR ecosystem such that coherent information of healthcare for data sharing.
Building Blocks	It uses over 300 complex archetypes.	Have around 100 resources.
Complexity of Data	It defines EHR with greater detail in terms of structure and complex features.	It uses simple lightweight and ubiquitous data representation which is easier for data aggregation.
Data Modeling	It uses two-level modeling, i.e., ontology and archetypes.	It uses query constructs and data modeling.
Data Volume	It takes the whole volume of existing data.	It works on the 80:20 principles i.e., at least 80% of the system can implement this standard.

B. EHR DATA SECURITY STANDARDS

1) GDPR

The General Data Protection Regulation (GDPR) [109] is a regulation on data protection and privacy in the European Union (EU) & European Economic Area (EEA). This regulation addresses the transfer of personal data outside the EU and EEA. GDPR binds any healthcare organization or individual collecting and processing data. Consent, purpose, data minimization, transparency, accuracy, privacy-by-design or privacy-by-default, data subject rights, retention period, accountability, security protections, and data breach protection are the general principles that safeguard data with the new GDPR [109]. Healthcare organizations are expected to follow these GDPR principles. As per the vision of the 21st century [109], privacy to EHR is one of the six quality performances of the healthcare sector along with safety, effectiveness, timeliness, efficiency, and equity.

2) HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

HIPAA [48] is important rule defined by US regulations that safeguard the individual's right to the ownership and sharing of health data. HIPAA standard applies to healthcare stakeholders (healthcare providers, health plans, and healthcare clearinghouses) [110] who carry out EHR exchanges. Privacy rule protects health information identities created or received by the above-mentioned healthcare stakeholders. Identities maintained by other healthcare stakeholders are not protected under HIPAA [110]. According to HIPAA, healthcare stakeholders may use or disclose identity without an individual's consent for treatment, payment, and medical operations. For other purposes, an individual's consent is mandatory. Individuals should be informed of the usage or disclosure of their identities [110].

3) INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) 27001/ISO 27799

ISO 27001 and ISO 27799 are the international standards that can be used in combination to protect sensitive healthcare data [111]. ISO 27001 adopts the Plan-Do-Check-Act cycle for information security worldwide in government and commercial organizations [112]. ISO 27002 implemented ISO 27001, providing the security controls guidance [112] and is already being used in the healthcare sector for worldwide security management such as Australia, Canada, France, South Africa, United Kingdom, and many more [113]. ISO 27799 implements the standard ISO 27002, providing guidance on best practices to protect confidentiality, integrity, and availability of personal health data [112]. Healthcare organizations certified with ISO 27001 are expected to improve health data security in conformance with ISO 27799 [113].

4) CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT 5)

COBIT 5 framework helps to govern and manage enterprise Information Technology (IT) in healthcare [14], [114]. COBIT 5 framework consists of 5 principles, process domains, IT-related guidelines, and ISO/IEC 15504 based process capability model [115]. Principles of COBIT 5 can be applied to the healthcare sector [115]. IT goals of COBIT 5 can be mapped with e-healthcare governance [115]. COBIT 5 frameworks can be used for healthcare with seven categories [114] as follows:

a. Principles, policies, and processes can be translated into practical guidance of daily management activities in healthcare
b. Processes can be aligned with practices and activities at healthcare, which achieves objectives to produce outputs mapped IT goals.

TABLE 7. Evaluation of performance of data models in EHR management.

Works	Data Model	Document Types	Data Store Examples	Retrieval Performance	Object Complexity	Features	Consistency	Isolation	Scalability
[12] [40]	Relational Database Management System (RDBMS)	Relations / Tables	MySQL	• Depends on complexity of the query, the structure and size of the database size.	L	• Tabular structure. • Indexed.	H	H	L
[41]	Object Relational Database (ORM)	XML	EXISTDB	• Can be improved via multi-indexing techniques and query styles.	M	• Object oriented programming structures with relational databases.	H [1]	H	L
[42 - 45]	Graph-based	Nodes and edges BLOBS	Neo4J, Infinite Graph, InfoGrid	• Low latency for clinical queries. • Not suitable for complex queries.	H	• Network of related objects is created. • Ideal for mapping relations in social networks.	M	H	H
[42] [44]	Document oriented	Document-based JSON	Mongo dB CouchDB, RavenDB.	• Performance improves with dynamic indexing.	M	• Store data as a document in key-value structure. • Nested sub-documents.	H	H	M
[42] [44] [46]	Column family	Column, super-column, column family	HBASE Cassandra	• Good for aggregated queries.	L	• Related features are stored in a single column family.	H [2]	L	H
[42] [44]	Key-value based	Key-value	DynamoDB, Azure Table Storage, Riak, Redis	• Good for fetching bulk records.	L	• Unique key. • The Entire object is stored as a value.	H [2]	L	H
[47]	Blockchain databases	Files	Distributed Ledger Technology (DLT)	• Transaction based. Poor retrieval time. Low throughput.	Tx	• Every writes and read operation is saved as an immutable transaction. • For write operation, gas cost is required.	H	H	L

L= Low, M= Medium, H= High, 1= High as compared to RDBMS and low as compared to NoSQL, 2=High for Reading queries, Tx=Transaction based

c. Organizational structures can be mapped as decision making entities in healthcare
d. Culture, ethics, and behavior of healthcare stakeholders is a success factor in governance and management activities.
e. As information is pervasive, it is very often the essential product at the operational level in healthcare
f. Infrastructure, technology, and application facilitate IT processing and services in healthcare.
g. Skilled personnel are required for carrying out precise decisions and taking corrective actions in healthcare.

5) DIGITAL INFORMATION SECURITY IN HEALTHCARE ACT (DISHA)

Ministry of Health & Family Welfare (MoHFW), Government of India, have issued DISHA [14] draft for healthcare security in November 2017 [116], [117]. If sensitive health data gets compromised it may lead to harm, violence, discrimination in society, and embarrassments to individuals. DISHA will give complete control of health data to the patient [116], [117]. A patient will decide to whom their data should be accessible. They should know to whom data will be transmitted. In case of emergency, their data will be shared with their family members. If any person commits the serious breach to the patient's data without any consent, then person shall be punished with imprisonment for 3 years to 5 years or charged with fine minimum of ₹5,00,000 ($6725.40). As per security compliance, this fine will be compensated to the concerned patient [116]. DISHA will be regulated by National Electronic Health Authority (NeHA), and various State Electronic Health Authorities (SeHA) [116], [118].

C. PRIVACY PRESERVATION TECHNIQUES

Patient-centric healthcare services demand integration amongst different healthcare information systems [7]. As the data is shared amongst different stakeholders, the privacy of EHR can be compromised [13]. Healthcare 4.0 is expected to implement patient-centric privacy preservation techniques [7].

Patient-controlled privacy preservation implies that the EHR is owned by the patient and can confer as well as

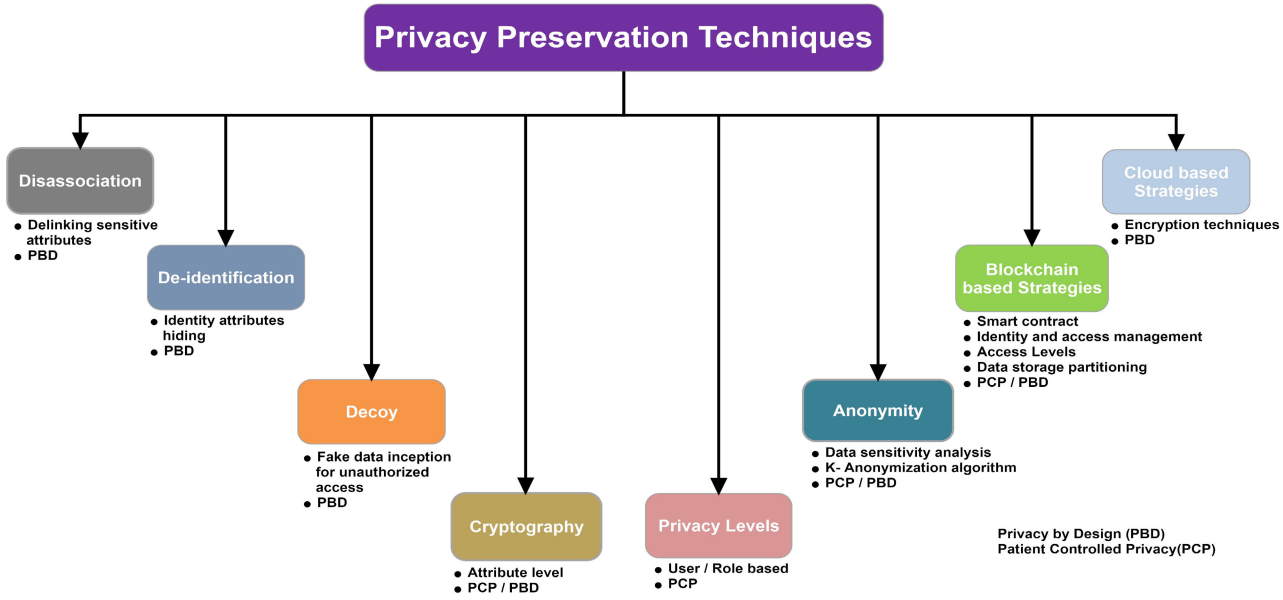

FIGURE 7. Privacy preservation techniques.

revoke the rights to access the same with other stakeholders. With patient-centric interoperability, there is sharing of EHR data amongst different healthcare information systems, which may lead to breaching patient privacy [13], even if the information sharing is limited to authorized healthcare actors. Often patients or data custodians are unaware that their information is disclosed. The threats to the privacy of healthcare data include tampering, loss, and unauthorized disclosure of data [119].

Effective Identity and Access Management (IAM) system [48] offer better privacy and access control solutions to data sharing problems. Data anonymization offers privacy to identity attributes [57], [58] of the patient data like name, address, and personal details. The use of patient-centric access control can help the patient to confer and revoke the rights to access their data. Role-based access levels with different levels of access granularities can be used as access management policy.

Fig. 7 shows popular privacy preservation techniques employed for EHRs [11], [17], [20]–[22], [49]–[59]. Privacy preservation techniques for EHR offer data security but cost additional storage and loss of performance. The overheads with encryption time, retrieval time, and compliance checks during EHR access hamper the throughput. In this section, we outline different privacy preservation techniques of EHR and evaluate their performance.

Additionally, approaches for privacy preservation in blockchain-based ecosystems are also outlined below in Table 8. These solutions leverage the blockchain trust guarantees with additional privacy preservation policies for EHR data. They are further evaluated for performance metrics to get a broader view, as described in Table 8. Research study on privacy preservation techniques on EHR helps in classifying the techniques as following types:

1) **Disassociation:** The process of delinking highly sensitive attributes from identity attributes is disassociation. This helps in hiding the identity of the patients with rare medical conditions from adversaries.
2) **De-identification:** The removal of personal data from the health records for privacy preservation is de-identification. Encoding, hashing, generalization of specific data are some of the strategies to de-identify the personal data in EHR.
3) **Decoy:** It is a strategy for creating deception of the EHR dataset for protecting from the adversary. This aims to increase the probability of false-positive and make it challenging to retrieve actual data.
4) **Encryption/Cryptography:** It aims to apply encryption techniques on the sensitive data in EHR. A symmetric key, asymmetric key encryption techniques are employed with a digital signature to verify the authenticity and authority of the data.
5) **Privacy Levels:** Every healthcare service provider has predefined access privileges which define what can be accessed, how it can be accessed, and when it can be accessed.
6) **Anonymity:** Sensitive data or identity data in the EHR is suppressed by replacing it with wild characters, or generalized with general values to avoid specifics.
7) **Blockchain-based privacy preservation techniques:** Blockchain supports pseudo-anonymity of the patients in EHR. Smart contracts deployed on the blockchain can help exercise the access rights of the user. Partitioning the EHR attributes to on-chain distributed ledgers

and off-chain databases are also applied in some of the works [6], [17], [22].

8) **Cloud-based privacy preservation techniques:** As cloud providers offer services for the users, they often deploy encryption techniques [48] in the cloud to secure data.

We have made the following observations on performance evaluation on privacy preservation techniques for EHR data from Table 8.

1) ACCESS COST

a. On-premise approach: Access cost is higher when EHR management frameworks leverage security standards [49], [50]. Privacy preservation techniques implemented in [52]–[54] show higher access costs in computation with encryption and decryption overheads.
b. Cloud-based approach: As cloud-based data storage is remotely accessed. Hence, access cost is higher. The data is accessed through third-party intervention. Hence, security standards for data is established. Techniques like attribute-based encryption [52], [53], anonymity, and cryptography [48] are popularly employed on cloud-based data storage for privacy preservation. Hence, this results in additional access costs as discussed in [52], [53].
c. Blockchain-based approach: Blockchain-based solutions need user authentications and validation of the data through consensus before sharing with healthcare stakeholders [13]. Hence, access cost is much higher in comparison to on-premise as well as a cloud-based approach [17], [21], [22].

2) STORAGE COST

a. On-premise approach: Storage cost is affected by on-premise centralized storage.
b. Cloud-based approach: Cloud service providers offer pay per use model. Hence, in this approach, storage cost will be recurring as per the accounting model of cloud service providers.
c. Blockchain-based approach: As distributed replicated ledger is used in blockchain, storage cost will be higher [17], [21], [22] in comparison to the above two approaches.

3) RETRIEVAL TIME

a. On-premise approach: Retrieval time will be significantly less for on-premise centralized storage.
b. Cloud-based approach: As data is remote in location, retrieval time will be higher than the on-premise approach.
c. Blockchain-based approach: In this approach, health data validation and user authentication are carried through smart contracts. Because of these factors, retrieval time is highest than on-premise as well as a cloud-based approach [17], [21], [22].

4) SECURITY VULNERABILITY

a. On-premise approach: Often, centralized approaches are vulnerable to security attack [6] like performance bottleneck, denial of service attacks, tampering of the data, single point of failure, and many more.
b. Cloud-based approach: In this approach, the cloud service provider acts as a third-party. We need to trust these third parties for the security of health data. Often there is a lack of trust in this approach. Client data can be compromised through different computing layers [120]. Work in [121] puts forth the need for basic security requirements like data privacy, data confidentiality, and data integrity for sensitive data to be preserved.
c. Blockchain-based approach: In this approach, health data becomes immutable because of transparency, consensus algorithms, and hashing techniques. Privacy is preserved with encryption techniques. Hence the basic security requirements i.e. data privacy, confidentiality, and integrity can be preserved [14].

The section D shows how blockchain architecture is conducive for the privacy preservation of EHR data.

D. EHR INTEROPERABILITY WITHIN BLOCKCHAIN

Before the rise of Healthcare 3.0, EHR management systems preserved patient records in central storage. Although central storage offered better isolation, they were vulnerable to various types of attacks on privacy, security, and reliability, such as malware and brute force attacks.

The central authorities own traditional databases. Blockchain is an encrypted distributed ledger and a global database [20]. It uses a distributed system where the updated data is validated, distributed, and stored on every node in the network with immutability guarantees. Nodes in the network will observe any modification in data. So, it is challenging to mutate the system by fake documents, transactions, and information without consensus. Blockchain, as a decentralized ledger overcomes the problem of a single point of failure.

Blockchain systems offer immutability to the EHR storage. The decentralized ledger offers better accessibility of the records to the distributed healthcare stakeholders [14]. It offers a platform for the trust-based sharing of health transactions, which the regulators can approve and validate to offer provenance of records.

Fig. 8 shows the architecture of the blockchain that stores EHR transactions. EHR transaction is a collection of personal details of patient, clinical trials, diagnostic reports, and treatment data. Blockchain-based EHR solutions offer advantages but pose practical problems in their implementations, as shown in Fig. 9.

1) CHALLENGES OF EHR MANAGEMENT WITH BLOCKCHAIN

a: SCALABILITY

Every health transaction on the EHR blockchain is validated, mined, and then added to the block on the blockchain [122]. With the increasing velocity of these transactions, the time for validation is very high. The system is non-scalable.

TABLE 8. Privacy preservation techniques.

Works	EHR Privacy Technique Used	Approach	PBD / PCP	Access Cost	Storage Cost	Retrieval Time
[49]	Disassociation	• Prevention of data linkage using dis-association of patient disease data. • Features de-identification.	PBD	H	Increases with increase in diagnosis codes.	H
[50]	Deid software	• The modified version of open source "deid" program is used for de-identification.	PBD	H	Increases with increase in the number of EHR.	H
[51]	Decoy Technique	• Because of the decoy technique, the unauthorized users will get access to only fake data.	PBD	H	Increase with the increase in decoy data	H
[52]	Cryptography	• Multi-authority attribute-based encryption for multiple EHR ownership.	PCP	Proportional to the number of attributes	L	Proportional to the number of attributes
[53]	Cryptography	• Privacy is preserved using attribute-based signcrytion and access control.	PCP	Proportional to the number of attributes	L	Proportional to the number of attributes
[54]	Cryptography	• Attribute-based encryption for cloud-based storage with selectively authorized users' mechanism.	PCP	H	H as cloud storage is involved	H
[55]	Privacy Levels	• Group privacy policies.	PCP	NE	NE	NE
[48]	Cloud-based	• Inbuilt Amazon Web Services (AWS) encryption features are used to achieve privacy.	PBD	NE	NE	NE
[56]	Anonymity	• Irrespective of the sensitivity of data, privacy-preserving approach, K^m-anonymity is proposed.	PCP	Increases with the database size and the value of K	Increases with the database size and the value of K	Increases with the database size and the value of K
[57]	Anonymity	• K-Anonymization-based global optimal de-identification algorithm is proposed.	PCP	L	NE	L
[58]	Anonymity	• K-anonymization & clustering-based anonymity scheme in Wireless Sensor Network (WSN) is presented.	PBD	L	H as Metadata is on all WSN nodes	L
[59]	Blockchain	• In the proposed model, privacy is preserved using attribute-based signcrytion and access control.	PCP	NE	NE	NE
[11]	Blockchain	• In the proposed model, purpose-centric access model is presented with Healthcare Data Gateway (HDG) application.	PCP	NE	NE	NE
[20]	Blockchain	• In the proposed model, access control challenges to sensitive data are addressed. • Invited users will have access to EHR.	PCP	NE	NE	NE
[17]	Blockchain	• A blockchain-based model is proposed which monitors malicious access to healthcare data. • Off-chain storage is recommended.	PBD	Increases with the database size	Off-chain storage cost increases as the size of the record increases	H as the database is retrieved from the existing off-chain database
[21]	Blockchain	• Privacy is guaranteed with the combination of access control protocol and encryption.	PCP	Access cost increases with an increase in the number of EHR users	H	H
[22]	Blockchain	• Multiple healthcare data ownership using multi-authority attribute-based encryption is addressed. • Partitioning techniques in blockchain (on-chain and off-chain).	PCP	Access cost increases with the increase in the number of EHR users & attributes	H	H

L= Low, M= Medium, H= High, PCP= Patient Controlled Privacy, PBD= Privacy by Design, NE= Not Evaluated

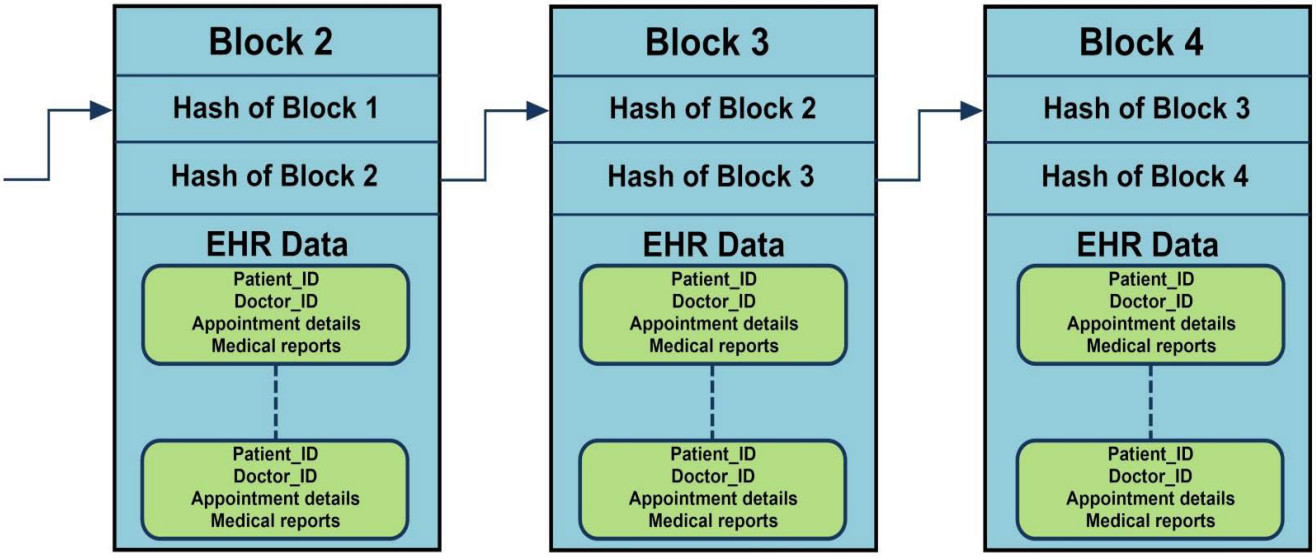

FIGURE 8. Sample of EHR transactions in blockchain.

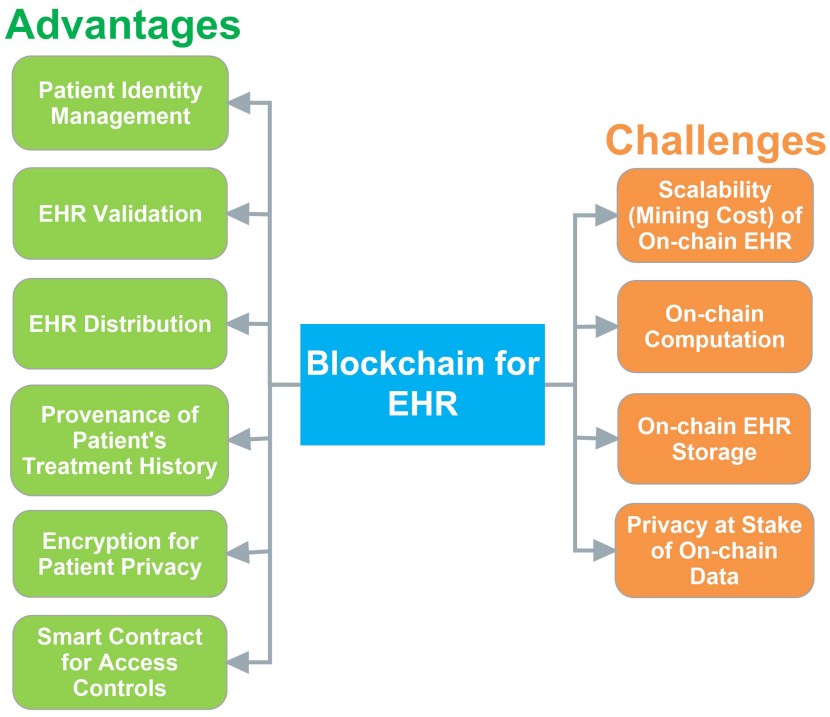

FIGURE 9. Advantages and challenges of EHR management on blockchain.

b: ON-CHAIN COMPUTATION

The EHR transactions are logged on the distributed ledger and verified with on-chain smart contracts. This is costly as the compute required for consensus is large [123].

c: ON-CHAIN EHR STORAGE

The on-chain transactions are recorded on the distributed ledger and replicated for accessibility. This requires substantial on-chain data storage [123].

d: PRIVACY AT STAKE FOR ON-CHAIN DATA

As the EHRs are stored on the blockchain, they are available to all the validators and DLT nodes. Thus, the privacy of the sensitive on-chain data is at stake [25].

It is thus evident that blockchain-based EHR management needs leveraged techniques for better trust and performance. Various EHR frameworks have been proposed or implemented on blockchain platforms. A comparison of such frameworks is shown in Table 9. We also present

TABLE 9. Comparison of blockchain-based EHR frameworks.

Works	EHR Standards	Blockchain Platform	Access Control	Consensus	Smart Contracts	Performance
[14]	No standardization in EHR structure	Hyperledger Fabric, Hyperledger Composer, Docker OS	Cryptographic keys, Patients can read / write / grant / revoke access.	Byzantine Fault Tolerance (BFT)	Chain codes: Membership, Read / Write Access to EHR To Valid Roles.	Changing network parameters, Block sizes, Round trip time, Read latency, and Cost
[18]	No standardization in EHR structure	Ethereum	Cryptographic keys.	Not stated	For sending the authenticated blocks to authorized users with hash verification.	Transaction cost
[20]	No standardization in EHR structure	No experimental setup	Membership verification Keys.	Notary Based	Nil	Throughput and Number of users
[17]	No standardization in EHR structure	Cloud-based Setup	Cryptography keys sensitivity analysis of data.	Consensus nodes act as orderers to confirm the order of transactions in the blocks.	Triggers as oracle smart Contracts of report actions to databases based on the sensitivity.	Number of users and Latency
[21]	No standardization in EHR structure	No experimental setup	Digital signature and hashing of data.	hybrid Practical BFT	Not built.	Security and Efficiency
[23]	No standardization in EHR structure	Ethereum, Dogecoin, Bitcoin and Analytical hierarchy processing	Digital signature and hashing of data.	Not considered, Default consensus protocols	Not built.	Proportion of Sent transactions, Received transactions, Failed transactions, nodes, and cost.
[6]	Customized data model conforming to FHIR	Hyperledger Fabric on-chain and off-chain storage	HIPAA compliant AWS cloud storage, Hybrid cryptosystem and Encryption of off-chain data on cloud.	Practical BFT	Chain codes to define role-based access control.	No performance metrics detailed.
[13]	EHR in JSON format	Simulation of the blockchain environment	Blockchain adapter: decryption keys and hashes, Data segmentation.	Not described	Smart contract to list "allowed list" of authorized stakeholders.	Access time to receive permissions and access data
[19]	No standardization in EHR structure	Hyperledger Fabric	Patient-centric access control policy defined for an emergency with certificate authority.	Practical BFT	Smart contracts to check to add patient data, health records, and if authorized users are granted access.	Transaction response time and Memory storage

a blockchain-based framework for privacy-preserving and patient-controlled trustworthy EHR management system named MyBlockEHR, detailed in section V.

E. CROSS-CHAIN INTEROPERABILITY

Cross-chain interoperability should be visualized as a mechanism by which one blockchain can communicate with another blockchain with the same or different platforms [61], [62]. In most literary works on EHR, all the actors are assumed on a single blockchain system. EHR can be shared across health organizations, which have built systems on different blockchain platforms in the real world. Hence inter-organizational interoperability of EHR demands that cross-chain interoperability should be investigated for data sharing [24].

In this section, we investigate cross-chain interoperability in two ways.

a) Study of architectural styles of crypto-based cross-chain interoperability for EHR sharing.
b) Analyzing the existing blockchain interoperability engines for EHR sharing.

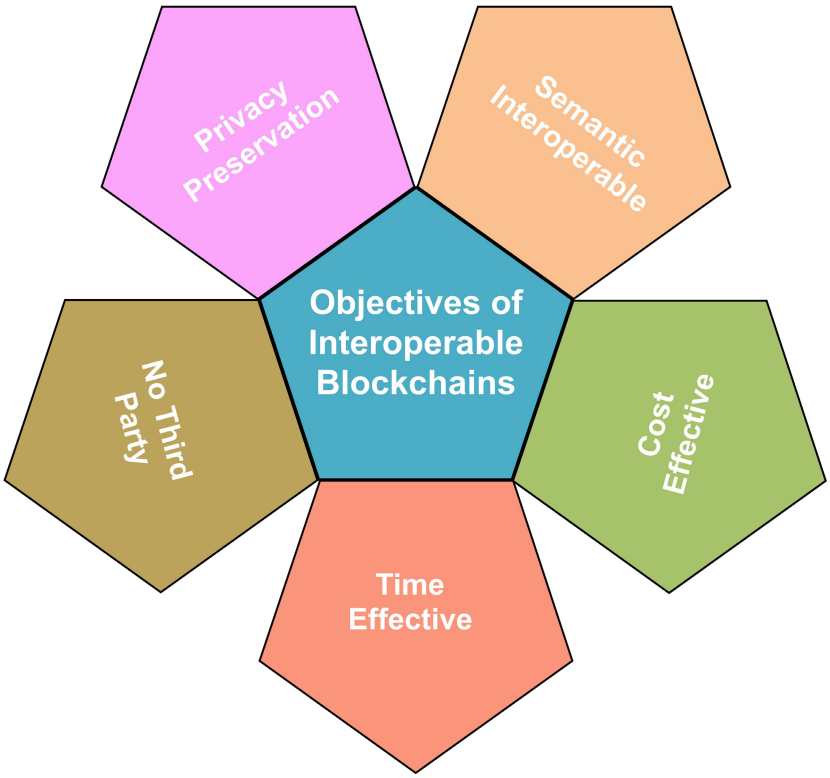

FIGURE 10. Objectives of interoperable blockchains for EHR.

We carried out studies to evaluate the following objectives of EHR sharing, as shown in Fig. 10.

a) Privacy preservation of the EHR during sharing: The privacy of the EHR must be safeguarded while sharing.
b) No third party involved in sharing: Trusted sharing with no intermediaries should be realized.
c) Semantically Interoperable: The data must be commonly interpreted between two exchanging parties. The message standards should be uniform or standardized.
d) Cost-effective: The sharing should not incur additional cost.
e) Seamless (time effective): The data sharing should not incur latencies in transmissions.

1) STUDY OF ARCHITECTURAL STYLES OF CRYPTO-BASED CROSS-CHAIN INTEROPERABILITY FOR EHR SHARING

Vitalik Buterin, the inventor of Ethereum, described three architectural styles for cross-chain interoperability as shown in Fig. 11 [61], [62]:

1) **Notaries:** Two or more blockchains are connected through a single third party or group of parties. There are two strategies of notaries depending on a number of third parties, i.e. Single Notary & Multi-signature Notary [61]. Notary acts as validators of the transactions with check-lists like digital signature verification and integrity checks.

   a. Single Notary: It connects two or more blockchains using one trusted third party [61] [62]. Cryptocurrency exchanges are typical examples of single notaries.

   b. Multi-signature Notary: It relies on multiple third parties. Multiple third parties should sign transactions before broadcasting to another blockchain. Therefore, it is more secure than a single notary strategy. BitGo was the first multi-signature wallet launched in 2013 [61].

2) **Sidechains / Relays:** There is no need for a third party as notaries for communication between blockchains. Blockchains will directly communicate with each other through a piece of automated code called a smart contract. A smart contract of blockchain A will be able to read, validate and act upon events from blockchain B. Partial copy of a ledger of one blockchain must be stored on the ledger of another blockchain. There are two types of relays: One-way and Two-way relays [62] depending on the communication direction:

   a. One-way relay: A smart contract of blockchain A will be able to read from blockchain B, but a smart contract of blockchain B will not be able to read from blockchain A.

   b. Two-way relay: A smart contract of blockchain A will be able to read from blockchain B, and a smart

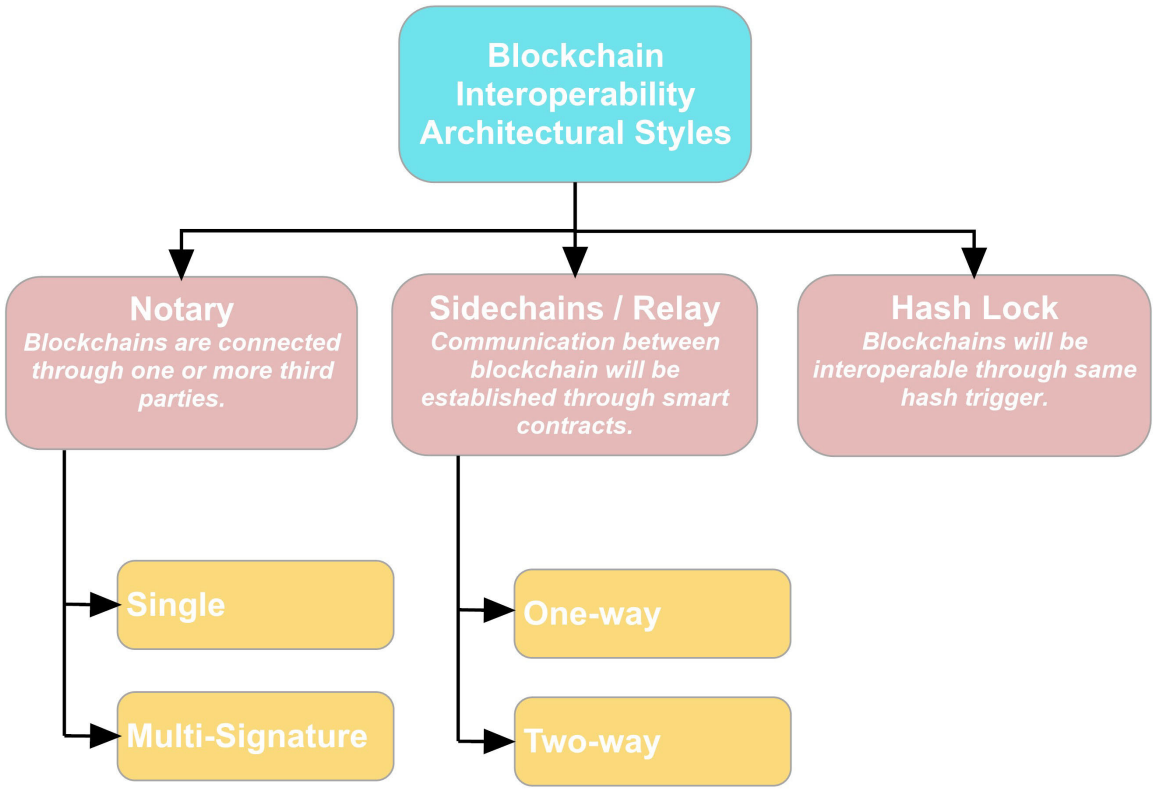

FIGURE 11. Blockchain interoperability architectural styles.

contract of blockchain B will be able to read from blockchain A.

3) **Hash Locking** [61], [62]**:** There will neither be a third-party entity as notaries nor partial storage of another ledger as in relay. In a hash locking interoperable solution, two or more blockchain platforms will be interoperable through the same hash trigger. Operations on blockchain A and blockchain B will have the same trigger hash for a specific time duration. Within that time duration, the receiver on either of the blockchains should access the value else, it will go back to the sender after the time is out.

The limitation and advantages of the above architectural styles are shown in Table 10.

2) BLOCKCHAIN ENGINES

In this section, we analyze the popular projects in blockchain interoperability. We have reviewed some projects in Table 11, achieving blockchain interoperability with different platforms. Most of these approaches are implemented on cryptocurrency transactions. Data interoperability is constrained to issues like structure, semantics, privacy, and ownership. With EHR, sharing additionally need to be privacy-preserving. In this Table 11, we analyzed the existing interoperable solutions for their suitability to EHR sharing either with some prototypes or with the architectural feasibility study.

IV. DISCUSSION

The objective of this section is to summarize the observations made in the previous section to address our research questions. It aims to discuss the need, goals, and challenges in the implementation of the interoperable solutions in the health record management and propose an interoperable framework for efficient, trust-based EHR sharing with blockchain.

The work also discusses how cross-chain interoperability works with architectural solutions and blockchain engines to evaluate their adoption in privacy-preserving EHR sharing amongst similar and heterogeneous blockchain systems.

A. RQ.1 WHAT ARE THE DIFFERENT STANDARDS FOR COMMON INTERPRETATION, REPRESENTATION, AND MODELING OF EHR TO ACHIEVE SEMANTIC INTEROPERABILITY?

We first looked at the importance of semantic interoperability in healthcare data. A literature study shows that the reviewed works [8], [24], [124]–[126] focus on the use of ontologies for knowledge representation of EHR. Ontologies offer clear organization of knowledge, systematic retrieval of information, and the ability to represent multi-dimensional healthcare data. They are thereby applied for semantic data representation for common interpretations of EHR.

OpenEHR is one of the most popular interoperable standards for EHR representation. The reference model of OpenEHR represents the structure of EHR data, clinical

TABLE 10. Study of cross-chain architectural styles for EHR management.

Style	Features	Limitations	Advantages
Notary	• Trusted Third party. • Multiple third parties can improve authenticity.	• Cannot build a non-mediated solution for EHR transfers. • Privacy of EHR will be compromised.	-
Sidechains / Relay	• A partial copy of the ledger is replicated.	• Privacy of EHR will have to be enforced across both parties.	• Non-mediated.
Hash Locking	• Hash Trigger. • The same trigger operation will cause operations across both the parties.	• Synchronous changes will be carried out.	• Non-mediated. • Data Privacy is guaranteed.

trials, and patient records in the standard format. This representation can be uniformly modeled to handle the issue of semantic interoperability very effectively. The attribute level description, the archetype of the EHR with the distribution of EHR at two levels, i.e. personal data and clinical trial, can be effectively modeled for complex solutions in decision support systems with OpenEHR standard.

FHIR on the contrary offers lightweight EHR modeling by working on the resources commonly agreed upon by most healthcare organizations. The data elements that are specific to a particular use case are created as FHIR extensions. FHIR resources are easily modelled by XML and JSON constructs and thus are more portable.

Many big data stores offer flexible data models to represent heterogeneous EHR with text, image, voice, and video data. Table 7 discusses the comparative analysis of the different big data stores and evaluates their architectural styles for modeling EHR with performance metrics like retrieval time and consistency semantics. Mongo DB offers document-oriented and semi-structured architecture to model EHR documents and the EHR attributes as nested sub-documents and is most popular in the studied works. The (Creation, Retrieval, Update and Delete) CRUD guarantees of Mongo DB offer sufficiently strong consistency guarantees with better performance. Its dynamic indexing feature results in better retrieval speeds as per the studied projects.

B. RQ.2 WHAT ARE THE DIFFERENT PRIVACY-PRESERVING TECHNIQUES AND SECURITY STANDARDS FOR EHR DATA STORAGE?

Healthcare data is susceptible and personal to a patient. Hence literature [48], [109] states that EHR data privacy should be an indispensable feature of interoperable EHR solutions. Literature discusses several different strategies employed in EHR management, like de-identification [50], [57], [127], disassociation [49], encryption techniques [52]–[54], [60] and tunable access-control levels, role-based and attribute level accesses for privacy preservation [22], [55], [59], [128] of EHR. The application of data partitioning, delinking, and perturbations offers privacy-preserving solutions to data storage and blockchain-based EHR management solutions [6], [17], [22].

The privacy preservation techniques, when implemented as PBD [109], lead to overhead on performance in terms of storage and access time. Hence to build a robust and efficient EHR management system, evaluation and choice of privacy preservation techniques for EHR are essential.

With patient-centric privacy preservation, patients own the data and should be able to confer access to the other stakeholders at their discretion. Patients should be able to track the provenance of their records to realize more trustworthy health data exchanges.

IAM solutions, data anonymization, role-based access control, patient-centric access-controls for EHR are some of the objectives of EHR privacy preservation system. Blockchain-based EHR management solutions offer pseudo-anonymity, encryption, the provenance of records, immutability, and trust-based EHR sharing with its design. These decentralized solutions offer patient-centric privacy preservation with data partitioning of EHR and leveraged access-controls [6], [17], [22].

Section B in ''Detailed Analysis of Literature'' also discusses the standard security frameworks [14], [48], [109]–[118] that are used to evaluate the healthcare data systems.

C. RQ.3 HOW MATURE IS BLOCKCHAIN TECHNOLOGY FOR BUILDING INTEROPERABLE, PRIVACY-PRESERVING SOLUTIONS FOR EHR STORAGE AND SHARING?

Literature [11], [17], [20]–[22], [59] shows that the application of blockchain-based solutions offers promising solutions to address the objectives like robust interfacing, non-tampered data storage, and integrated solutions with stakeholders. Blockchain-based solutions are decentralized and promise immutability to EHR. The adoption of blockchain in healthcare applications provides potent features like integrity, traceability, and confidentiality of data and results in decentralized and trustworthy storage and exchanges of health records. Privacy in the blockchain is challenged because of the decentralized ledger where every ledger node holds the data. On-chain data storage and computations are costly for big data applications like EHR management. Privacy preservation of sensitive data on the blockchain can

TABLE 11. Blockchain cross-chain interoperable solutions.

Works	Interoperability Solutions	Consensus Algorithm	Interoperability Strategy	Validators	Tokens	Research Works / Projects in Healthcare Sector
[61] [62] [64] [66] [67]	Cosmos	Tendermint BFT	Notary	Required	Yes (Atom)	• EHR management with blockchain networks employs Cosmos. • Sharing across the chain is supposed to be carried out through third-party hubs. • Data sharing is possible with smart contracts. • Privacy preservation guarantees are trivial.
[61] [62] [65][68-70]	Polkadot	Nominated Proof of Stake (PoS)	Notary	Required	Yes (DOT)	• Pulse project is built using Polkadot for EHR accessibility. • It uses AI and blockchain for security. • It has ability to run multiple parallel chains for transaction processing to improve scalability. • Privacy preservation guarantees are not investigated.
[72-74]	ICON	Loop Fault Tolerance	Notary	Required	Yes (ICX)	• Project ICONLOOP is based on ICON. • Suitable in healthcare for identity authentication, digital certification, and visitor check-in / check-out details. • Privacy preservation guarantees are trivial.
[15] [75 - 77]	AION	BFT and Proof of Intelligence	Notary	Required	Yes (AION)	• AION Transwarp Conduit (TWC) is explored for message transfers between two blockchains using a signatory-based approach. • EHR sharing using AION TWC is being explored.
[15] [16] [78 – 81]	Blocknet	PoS	Notary	Required	Yes (Block)	• Using XBridge and XRouter of Blocknet applications can share EHR. • Mediated solutions. • Privacy is preserved with EHR sharing using the NoID protocol.
[15] [63] [82] [83]	Metronome	Some concepts from both PoS and Proof of Work (PoW)	Notary	Required	Yes (MET)	• Metronome is going to build application where patient can monitor, control access and monetize data under proposal. • Metronome-based EHR sharing project needs to be further researched with the aspects of privacy preservation.
[62] [84]	BTCRelay	PoW	Relay (One Way)	Not Required	No	• Employed for value exchanges. • The architecture was found less suitable for EHR sharing.
[62] [69] [85]	DogEthereum	PoW	Relay (Two Way)	Required	No	• Employed for value exchanges. • The architecture was found less suitable for EHR sharing.
[15] [86] [87]	Wanchain	PoS	Notary	Required	Yes (Wancoin)	• Employed for value exchanges. • The architecture was found less suitable for EHR sharing.
[88] [89]	Block Collider	Proof of Distance (PoD)	Relay (Two way)	Not Required	Yes (Emblem)	• Employed for value exchanges. • The architecture was found less suitable for EHR sharing.
[15] [90] [91]	Ark	Delegated PoS	Notary	Required	Yes (Ark)	• Employed for value exchanges. • The architecture was found less suitable for EHR sharing.
[92 - 94]	Lamden	Delegated PoS and BFT	Hash Locking	Not Required	Yes (Tau)	• Employed for value exchanges. • Architecture found less suitable for EHR sharing.

be enforced with strategies like encryption, signcryption, and off-chain data storage.

Identity management can be implemented with a blockchain design that guarantees pseudo-anonymity [56]–[58]. Identity management for the user access control can be enforced with smart contracts.

Offloading EHR data to off-chain storage can optimize the requirement of computation on the blockchain. However, the off-chain stores may not guarantee immutability and tamper-proof EHR. [6] handles this with cloud-based storage of hash for tracing the tamper of data.

D. RQ.4. WHAT IS THE STATE-OF-THE-ART FOR CROSS-CHAIN INTEROPERABILITY FOR EHR SHARING?

Blockchain solutions should provide a distributed framework for interconnected healthcare organizations. However, cross-platform (cross-chain) data exchanges are significant for the exchange of values across two blockchains. Our study helps us to outline the goals of EHR interoperability in cross-chain exchanges. The existing blockchain platforms [129]–[135] are critically analyzed for their application to healthcare data exchanges concerning these goals.

Existing cross-chain architectures [70], [85], [88], [136]–[144] have been successfully applied to cryptocurrency exchanges. We analyzed Notary, Sidechains, and Hash locks for their suitability in EHR exchanges.

Studies of few interoperable projects like Cosmos [64], PULSE [65], [71] show that they can be employed for data transfers across two chains. However, they need to be evaluated for data privacy guarantees and non-intermediated solutions.

The literature study shows that the framework for privacy preservation [70], [137]–[141] in cross-chain data exchanges is, however in the modeling phase, and there is a need to develop more matured prototypes.

The discussions on the research questions in the areas of interoperability under this study help us discover the research gaps in the existing solutions of the EHR management framework.

a. The EHR management frameworks are less sensitized towards adopting of open EHR standards, which can lead to better semantic interoperability with common representation and interpretation.
b. The EHR frameworks using decentralized blockchain ledger are less explored towards a hybrid architecture of on-chain and off-chain data segmentation, which can be used for better privacy and throughput guarantees.
c. The EHR framework should always guarantee retrieval of valid data both on-chain as well as off-chain
d. The framework should yield better performance concerning both compute time and cost, which are enormous with blockchain-based solutions [123].

In the next section, we present a prototype of MyBlockEHR to meet privacy, integrity, and performance requirements in implementing EHR frameworks on a blockchain platform. The experimentation section validates the proposed framework. Its implementation with on-chain and off-chain data storage and smart contracts demonstrates trust-based EHR storage. The off-chain storage is verified for data retrieval. We evaluate the test prototype of our implementation with the evaluation of its responsiveness and cost.

V. MYBLOCKEHR FRAMEWORK

A. MYBLOCKEHR ARCHITECTURE

The artifacts of the proposed MyBlockEHR architecture, as shown in Fig. 12, aim to address the challenges of deploying EHR management with blockchain and leverage its advantages. The EHR structure can be built using standards like OpenEHR [107] or FHIR [108]. Section ''EHR standards'' in ''Semantic interoperability'' discusses the features of each of these interoperable standards in Table 5.

1) MEMBERSHIP AND CA AUTHORITY

The framework uses a role-based system like the work in [6] that attributes different roles to the actors. For presented use cases of the system, we outline three significant roles as follows.

- Membership Certification Authority: Every member is conferred with a symmetric key pair. Public key implements the unique identity of every member of the system. This stands for the authentication of the member. The private key is used to authorize the owner of the record and implement a digital signature. This is like enterprise application platforms [14], 21].
- Patients: The patients are the owners of their EHR, like proposed in [6], [13]. They grant access to the other users.
- Doctors: They get lease rights of the EHR. Rights can be conferred with event-based or time-based scenarios. The rights can be revoked by the authority or by the patients.

2) INFORMATION & ACCESS MANAGEMENT

a: ACCESS- CONTROL POLICY

The patient controls the access to their EHR data [6], [13]. Blockchain system guarantees public key and private keys for digital identity and pseudo-anonymity [56]–[58]. Patients define access policy for all the users (clinicians, doctors, etc.) of EHR. These can be defined as access privileges like Read and Download with access control policies. Smart contracts can be used to enforce the consent of the patients for updates [6], [13], [14], [18], [19].

b: ON-CHAIN DATA STORAGE

Most of the EHR frameworks [14], [22], [23] add the patient records on the on-chain database, which are stored on decentralized ledgers of blockchain nodes. However, there is a limitation to on-chain data storage, and the system cannot scale with data explosion [23]. The decentralized storage is replicated and copied on multiple ledgers and endangers the

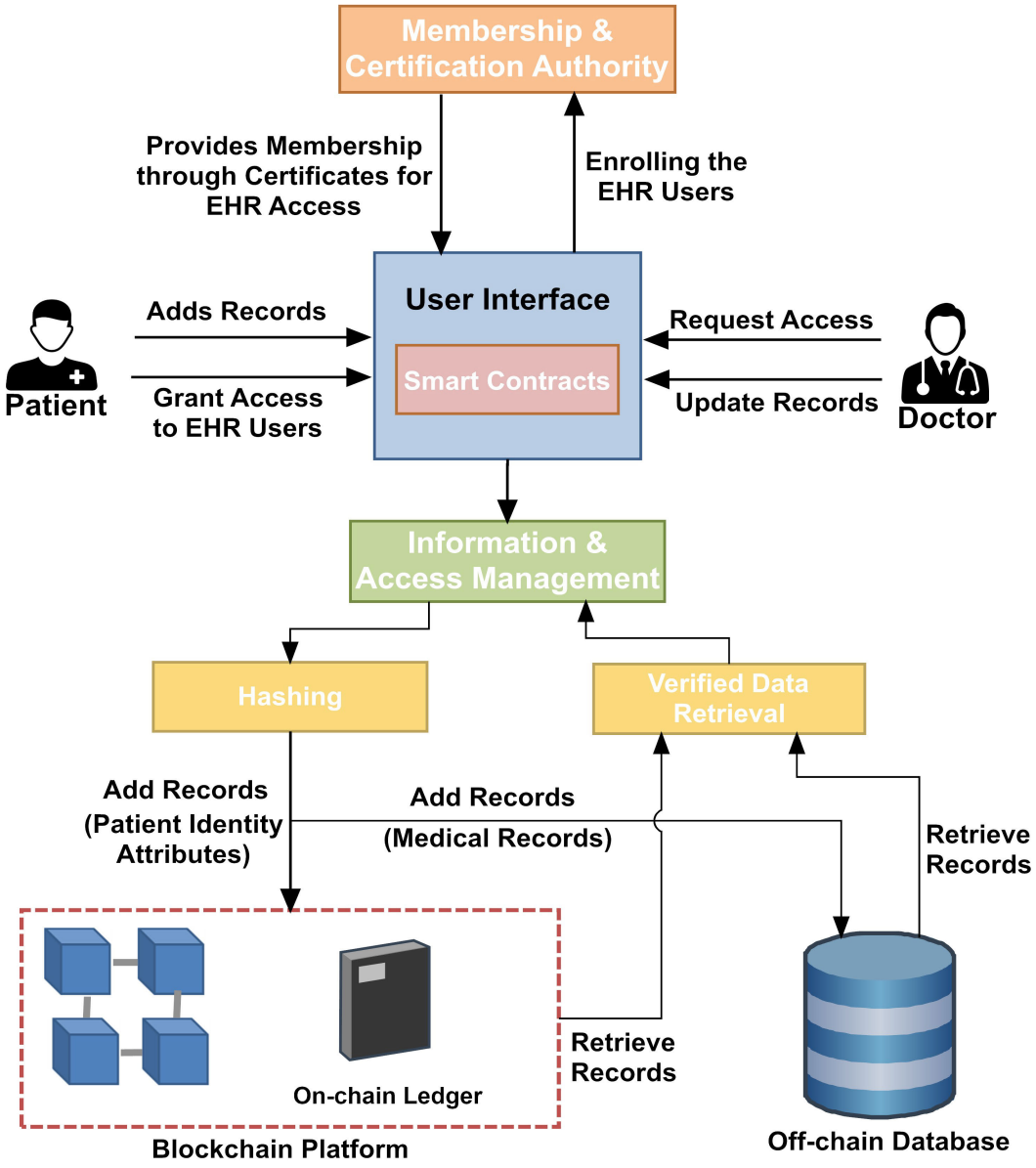

FIGURE 12. MyBlockEHR architecture.

privacy of sensitive records [25]. This can be compensated by augmenting off-chain data storage with on-chain data storage. EHR data is thereby partitioned. We put the light-weight EHR attributes, and the transaction details on the blockchain ledgers for the persistence of the records, and these transaction details are always tamper-resistant.

c: OFF-CHAIN DATA STORAGE

MyBlockEHR conceptualizes EHR storage on on-chain as well as off-chain data storage. Off-chain data storage will store the bulkier medical records like scan images, medical reports with patient identity attributes [6]. There will also be a referential key to associate with the on-chain treatment details for retrieval.

We propose a document-oriented No-SQL data store, Mongo dB, for off-chain data storage for its advantages as discussed in section III in "Data modeling of EHR" of semantic interoperability. The off-chain storage will have large, heterogeneous data records like medical reports, prescriptions, and scanned images. The document-oriented approach uses document-subdocuments to model heterogeneous records in EHR [12]. Mongo dB is suitable for CRUD operations and offers better concurrency guarantees [12], as discussed in Table 7. On-cloud deployment of the data model can also be considered for better throughput and performance. Mongo dB offers better indexing techniques for efficient query retrievals [40]. The retrieval speed can be further improved with proper key indices.

3) SMART CONTRACTS

Off-chain data storages are vulnerable to attacks and tampers as access to data cannot be audited [6], [17]. Hence a data validation scheme that can leverage the immutability of on-chain records is desirable. Our architecture proposes a validation scheme that will ensure that the data on the off-chain data stores is free from an accidental tamper. This can be assured with a smart contract that performs the hash verification of the data fetched from off-chain storage with the on-chain hash value of the counter-part record. This will ensure that data is verified every time data is fetched from off-chain storage.

The proposed EHR partitioning system aims to achieve tamper-proof storage of the EHR on off-chain big data stores of MongoDB. Its encrypted hash signature is stored on on-chain data storage. This preserves the privacy of the patient data by putting its encrypted signature on the blockchain against the entire record. Also, lesser the storage of the on-chain, better the scalability of the system with lesser mining time and storage cost. This is further experimented and discussed in the results section.

The proposed architecture uses an encryptor module, which can affect computation time for verified access. Additionally, inserting the data into on-chain and off-chain data stores will also affect the performance. We evaluate the following scheme on a test network for response time and throughput of the transaction in the experimentation section below.

B. EXPERIMENTATION

1) PRELIMINARIES

a: ETHEREUM

Ethereum is prominently used to write simple, smart contracts and develop Decentralized Applications (DApps) [145]. The main idea behind Ethereum is to provide the capability of the execution of logic through smart contracts. Smart contracts can be written in Solidity or Vyper language. Ethereum also provides cryptocurrency as Ether and Ethereum accounts can be managed by different Ethereum wallets. Currently, there are 31 Ethereum wallets [146], i.e. MetaMask, MyCrypto, Trust, TokenPocket, to name a few. Smart contract deployments on the Ethereum main network require cost, which is measured in terms of gas. Generally, gas is represented in Wei. For demonstration purposes, tests on the deployment of such smart contracts can be very costly. So, wallets like MetaMask provides test Ethereum networks, i.e. Rinkeby [147], Ropsten [148], Kovan [149], and Goerli [150], for test deployment of research projects. We thereby, deployed our prototype for MyBlockEHR on the Rinkeby test network.

b: INFORMATION TRANSACTION

When information is stored or retrieved from Ethereum, it is stored in terms of the transaction. The general Ethereum transaction format is as follows [151]:

- Transaction Hash: It is a transaction hash of 66 characters generated after transaction execution.
- Status: It indicates the status of transaction, i.e. success or failure.
- Block: It is the number of block in which this transaction was recorded.
- Timestamp: It gives information about the date and time of mining of transaction.
- From: This is the address of the party who is initiating this transaction.
- To: This is the address of the party who is receiving this transaction.
- Value: The amount of Ethers transferred during this transaction is indicated by this field.
- Transaction Fee: This is the fee that is given to the miner for processing this transaction.
- Gas Price: This field indicates the cost per gas unit in terms of Ethers or Gwei for processing the transaction.
- Gas Limit: This is the specified higher limit of gas that is provided for the transaction.
- Gas Used by a Transaction: It gives the exact quantity of gas used for the transaction execution.
- Nonce: It is a sequential running number for an address starting with 0 for the first transaction. It will be incremented by one with the following transactions.
- Input Data: It gives additional information about the transaction.

c: SMART CONTRACT

Smart contract is a piece of code that can automatically execute with set certain business rules, terms or conditions [152]. Solidity [153] is a popular language to write the smart contract in Ethereum.

There are web-based and desktop-based Integrated Development Environments (IDE) to write the smart contracts [154]. Programming languages like Javascript or Python can encapsulate calls to Solidity smart contracts. Web3.js [155] is an Ethereum JavaScript API which provides a collection of libraries to interact with local or remote Ethereum nodes.

d: Mongo dB

Mongo dB [156] is the document-oriented NoSQL database. Heterogeneous documents having different formats and values can be stored in Mongo dB. It is much faster than traditional relational database management systems for retrieval time. JSON documents are created in Mongo dB. It also supports deep query ability. Indexing technique is an important factor for the faster execution of queries. Mongo dB allows single-field indexing, compound indexing, multikey indexing, geospatial indexing, text indexing, and hash indexing.

2) SYSTEM ARCHITECTURE

Fig. 13 indicates system architecture. Smart contracts, i.e. Register_Patient, Add_Medical_Record, and Fetch_Record are written in Solidity language. These smart contracts are deployed on the Ethereum blockchain. Patient's identity attributes and base64 encoded string of medical record

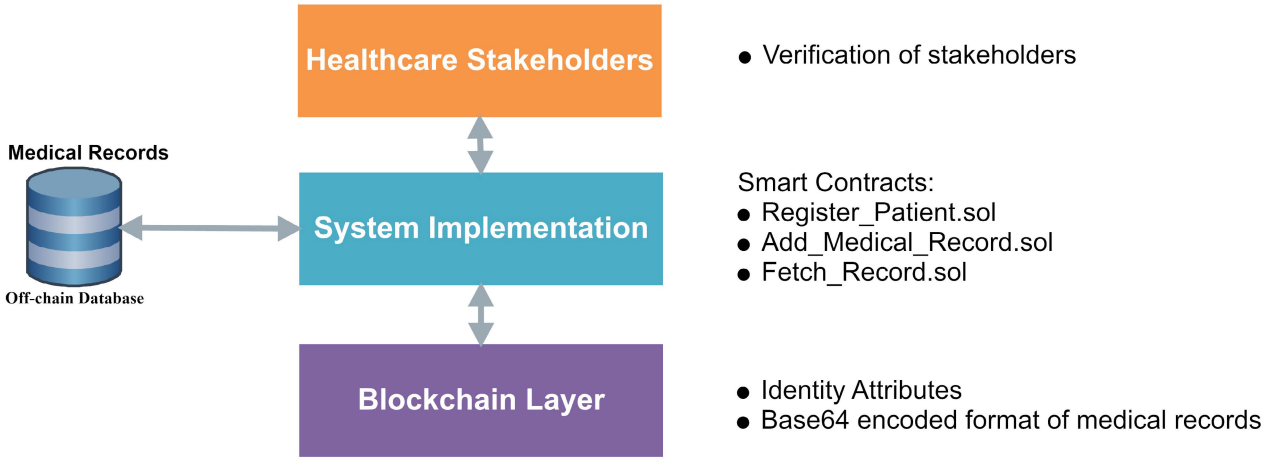

FIGURE 13. System architecture.

images are stored on-chain. Medical records are saved on off-chain storage. Off-chain data is accessible to oracle smart contracts.

a: TRANSACTION

The system includes smart contracts transactions as follows:

- Register_Patient: Using this smart contract, basic information of the patient, i.e. Patient ID, patient name, and referred doctor name, is stored on-chain.
- Add_Medical_Record: The patient's identity attributes are saved on-chain. The base64 encoding and hash of these records will also be stored on-chain. Entire medical records are stored off-chain.
- Fetch_Record: In this smart contract, we are trying to fetch patient's records with the help of Patient ID. At the same time, patient's off-chain medical records are also fetched after validating. Validation is done by verifying recalculated hash value with the on-chain stored hash value.

Apart from these smart contracts, there are two essential functions as follows:

- Base64 encoding [157]: As an image, document-based medical records cannot be saved on-chain, we have encoded medical images in base64 encoded format and saved on-chain. An example of working base64 encoding is as shown in Fig 14.
- Hash function: We have applied hash function on patient information as well as on his medical record. We have used keccak256 [158] hashing function. This function returns 256 bits unique hash value of data. We verify the data by fetching its hash value from on-chain records.

Following is an example of keccak256 hash for a sample medical record with the following structure:

Patient ID + Patient name + Referred doctor name + base64 of medical record1+ base64 of medical record2+ base64 of medical record3+ base64 of medical record4.

0x4.918d39f5bf28adda7788eec4ec0c8adaf2d3a7f95
ea8e3e69cbdad22db9a86

3) SYSTEM IMPLEMENTATION

The system was implemented with Ethereum smart contracts deployed on Rinkeby test net blockchain using Metamask.

Following smart contracts are included in our framework:

- Register_Patient.sol
- Add_Medical_Record.sol
- Fetch_Record.sol

User interaction with the system

User interaction with the system is shown in Fig. 15. Stepwise workflow is shown below.

Workflow:

A Addition of patient's identity attributes:

A1. Patient's identity attributes are passed to smart contract from the user interface.

A2. The hash value of identity attributes is calculated with the keccak256 hashing algorithm.

A3. Above calculated hash is also passed to the smart contract.

A4. Patient's identity attributes along with hash are saved on the Ethereum test network.

B Addition of medical records:

B1. As medical records cannot be saved on-chain, they are encoded in base64 format. For Case 2, Case 3, Case 4, and Case 5, medical records are encoded into base64. For case 6, medical records are saved off-chain on localhost Mongo dB server.

B2. The hash value of medical records is calculated with the keccak256 hashing algorithm.

B3. Above calculated hash and base64 encoded images are also passed to their respective smart contracts.

B4. Encoded medical records along with hash are saved on the Ethereum test network.

```

xE7s8uHoBzc0f8VxFLqu47puGMXN2Gm6fhx401VnrBruPTZ2bKxy8OCR4eFjU+XK9GS1XGlU681GI3Zc3/M8P46DwCsWsz09ha5SZsGCWblcMGtm95w5/
TMHuvtzXq5Rz/tu4Lq+23Dj0HU8J/adOBM7XkQNHPO3qanrRG6rchz2+Jn/
6QxTuUdvYJD2cSqppJJKKqmkkoqqaTy9IsrdsWX2HXafIWvvhs3w9DzfceD1Dih71QiZ+vu6vb9hzds2bll98FNO/
dVqvVKpdJoNGBD5jw+jJjzKSiKmuaQ77gZlzJcD7YWF4q52XNnLVmyaGjmwLUXnLdwVs+sPifvBAG3jxuO4VExhCqypXgR/w/
FtSJDpxz71Y0dX6TQ9X50u1IrViqppJJKKqmkkoqqaTy9AjcI7K2oDbFiq1Vi/
9cw2vEs6Jm5HoN1xuZig6PVjbvOvTQpl2PbNgxfHxislyfmqrkcznf9QoFjFSlUiHX013sKuWLhWwu68VxGEZRI2zyOTVdHhkbGx+frtRq9UY4XcbQFWWz
mepi6cJGZflTi9OlFCuVVFJJJZVUUkkllVRSeYYpliOKFVqLkRwHvRCq5QU4BFabsedhyXLufGjfd+5+cNP2vXuGR0MnW67gCNjs6yrN7O+9aOUZi4cWLF
Yatm7bs2Llzz4HhkaA0gOmrlA/6u3NXXHbOq1/6woXzu2d1O3HY7PKdDFyqjuWKGpnSmvVqkOWY/
ASD2FrKPDelWKmkkkoqqaSSSiqppJLKs4BihcYYhJEIk1UoSuI4/nQtrER+Jodjn3NksvntOx7+/g8e3DM8NjZVPTIygQlp7syZyxYtuPjclecsG5o/
uzTYW+jrdQp+yywGp/FbxrHI8B/Pw4MwjJwwNHQL/
latO+Nj4ZHjY9u3796x78it962thlGj3qhUJuYM9i2cP7jq4pWvfOnlSwdzMKva1OTMrh5KI7rLiRuZbGCJIXcJUoqVSiqppJJKKqmkkkoqqTzbKFbTs/
zKZpFwG02n1nTjbJbwqf3HKhu2H/rK91c/
smHL+GSFOKp8Pr94aP75y89Yde4ZKxcO9pcKhUyUz0e+Z2xWJilGFOM06HvkolBWChvbZf7nGRrkmu8kzIjFvVynXIuOTzd2jJRXr92+Zt2mHTv3T5fr1e
hI6EbkGtiKnK2HIi/+PVv33zbPdOxO3J8ZMGcwUvPX3npRedefelZQ4NBt4v/
ngmEwnEvcurWCOYah0JFUbUCqRTk5cVNY3RSZBdELMiYwKlao04ajEw2G7nBKMkCXfd4OV798K5v3XrX/
avXxp7faJBjw73gwvNfeOVlr7hmxYxukzwwbjRKGS/
jWYObKd83eQYfk2KlGQVTSSWVVFJJJZVUUkkllladRIpuXL7bZLlxPLoNrN4x85pu33fXAumNjZTfrLls0/8YXXnHj85+3eH6xN+PkYidn8/6Z8C0TJBVEV
OZLrju3L+tEXgZOGNjk7U+wfU+VFSt+tAOuzcJhMy+6T6wA98TX2DlxkXv6TdxTb+ymgzWVVFJJJZVUUkkllVSeaTmdXbgdv1m3PcuS7HeIwvBI9Y77t33
DUnQ9sufWe1Y9s3ZELMnPywfXPv+wVN155/tIBXAMheB4Z3WNrOYPrUbL7Ixv/
lFAsigg7dOeKLbYplkkOEj9G3ninRcREqiLPxr61KZbMfiZ5R+yeQrFie1nU2qUsCkign47oVFJJJZVUUkkllVRSeUb5VWjgfIdByVqT2FsqjmJP2/
WSfyJwIDZVx9k23PzcV+66595Nh48erddHr776/
F9626suWTKYdY27XdY6AkKY2typxQQiyjcswEu2K446jDJ8y8QnG2B+BO2L2zk3+ILrYS1yjhx3PvelL3/i898ad2YUu/Mrzpj9q7/4+lXLB3Llej/
+gpzrG+LDfsfFYt9J5cVtjkJ7/+RP/uSp4KlxfApDbWWRT27oPXYhbvv62G3xq6TA9j/
3dCIsZ8u49dVLKVYqqaSSSiqppJJKKqk8sxKdcEdrUSzlUvfk2uY6jUbdCfwj1XD/lHfXgxtvue2h7XsOk5biBVde+JLrLj5/6eyBTCZjt/
j1WhzAMrMO7zVXXMNaW7yTWIM53cRLmZ+ihI6YpBfuSdSiVdWTGUbOcbrz2M0y/
QMzN+wena6HlVplfHxs2eKhhXNKUeiaEDLivOpT+UIpVshVfMJ1z9Eeyu5TE4uFKcyPpLFYSTtkYkqIkjnjcVz5bM0SY5/
Xrq0ft7oEc1zc4UZ4WlleOppTSSWVVFJJJZVUUknlGRfPOWEGsbjdGmNimyTCM9C+7vtTNWfngbEPffxra9bvGC83+/
pLL7/+qre88vIls4slro+sL5v7oziD5UzWZVAkzmsfbfMEqEm9xaksQYnbBp32pseeby7nD2plSFoUu77lcRiqnnfhsuUrlw0uXPLpL31r05bt905NNSYr
uupLN7VipZJKKqmkkkoqSSyjMoFrqLGrShPT6Cxo8vNvwKE5br1n1v4/6J93/k83feuymMc4uXzH/zz9z4ttdcvrg/
```


FIGURE 14. Base64 encoding of an image-based medical prescription.

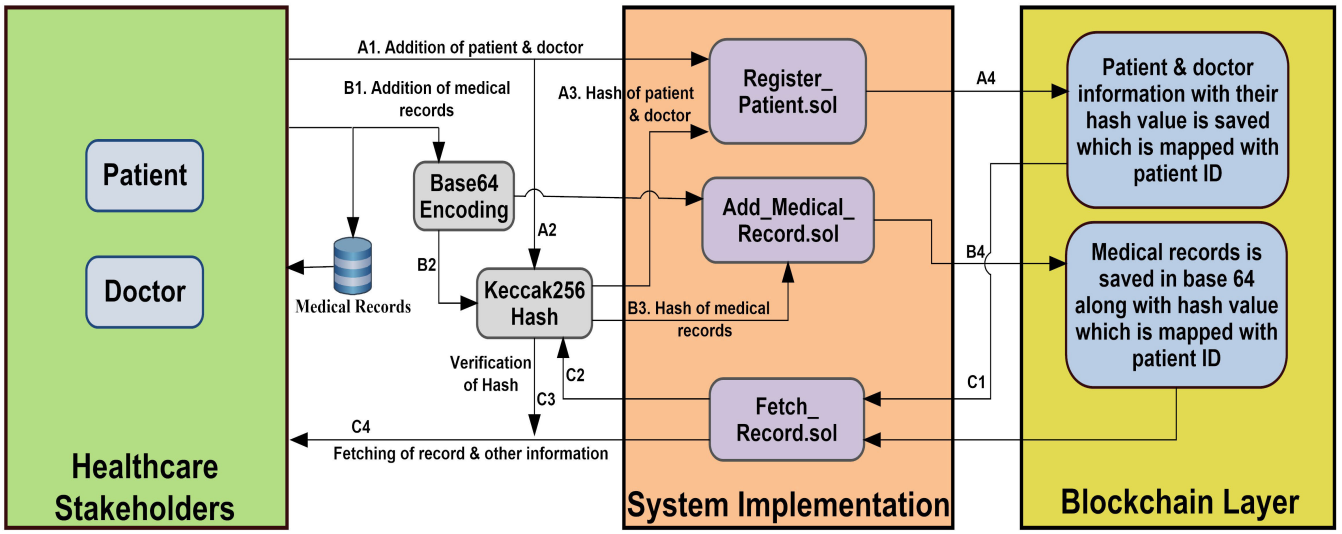

FIGURE 15. User interaction in the system.

C Fetching of medical records and patient's information:

C1. Healthcare stakeholders can access patient's information and medical records from the user interface. This data can be accessed by invoking a smart contract responsible for fetching from the Ethereum test network.

C2. Keccak256 hash will be recalculated.

C3. The recalculated hash will be validated by comparing with the on-chain hash for verification.

C4. If hash values are same, then data will be retrieved on the user interface

4) IMPLEMENTATION

a: SYSTEM CONFIGURATION

We have deployed smart contracts to observe their performance for different sizes of EHR. We have deployed smart contracts on the Rinkby test network of MetaMask 9.2.0. The user interface has been written in HyperText Markup

Pseudocode of the Smart Contracts for Patient Records

Structure of patient's identity attributes and medical records
Define structure of the patient as per requirement.
If "patient's identity attributes"
then structure patient {patient_id, patient_name, referred_doctor_name}
else if "patient records are also needing to be stored"
then structure patient {patient_id, patient_name, referred_doctor_name, record1, record2. . . }
Register_Patient.sol
function addpatient (variables of Patient Identity attributes)
add new data of the patient and associated doctor
add the hash value of the patient record
end function
Add_Medical_Record.sol
if "case 1" then
calculate hash of Patient Identity attributes
function addrecord (variables of Patient Identity attributes)
add data of the patient and associated doctor
end function
if "case 2" then
calculate base64 encoding value of the medical record
calculate hash of Patient Identity attributes and base64
function addrecord (variables of Patient Identity attributes, base64 of the medical record)
add data of patient, associated doctor, and base64 of medical record
end function
if "case 3" then
calculate base64 encoding value of each of two medical records
calculate hash of Patient Identity attributes and base64 values
function addrecord(variables of Patient Identity attributes, base64 of each of two medical records)
add data of the patient, associated doctor, and base64 of each of two medical records
end function
if "case 4" then
calculate base64 encoding value of each of three medical records
calculate hash of Patient Identity attributes and base64 values
function addrecord(variables of Patient Identity attributes, base64 of each of three medical records)
add data of patient, associated doctor and base64 of each of three medical records
end function
if "case 5" then
calculate base64 encoding value of each of four medical records
calculate hash of Patient Identity attributes and base64 values
function addrecord(variables of Patient Identity attributes, base64 of each of four medica records)
add data of the patient, associated doctor, and base64of each of four medical records
end function
if "case 6" then
calculate hash of Patient Identity attributes and Medical records
function (Patient Identity attributes)
Patient Identity attributes will be saved on-chain
end function
Original medical records will be saved off-chain on the local host Mongo dB database.

(Continued.) Pseudocode of the Smart Contracts for Patient Records

Fetch_Record.sol
function fetchdata(Patient ID)
if "Patient ID = true"
then recalculate the hash of stored data on-chain and off-chain
validation of records is done by comparing hash with the stored hash value
if (both hash values are the same)
then fetch data
else
throw error indicating data has been compromised
else
throw error indicating patient record is not available
end function

Language (HTML) and collaborated with node JavaScript & web3 Java Script. Node version was V14.16.0. User interface was provided through Firefox 86.0 browser. We have used visual studio 1.54.2 as an editor for HTML and JavaScript.

We have written smart contracts in Solidity language on Remix IDE. This deployment was done on Ubuntu (18.04.5 LTS) 64-bit operating system, 7.6 GB RAM, Intel processor (i5-8500 CPU @ 3.00GHz × 6). We have used the localhost Mongo dB server.

We uploaded data on the Ethereum test network for the following test cases as described in Table 12. Test case 1 implies that patient identity attributes, i.e. Patient ID, Patient Name, and Referred doctor, are recorded on-chain. Case 2,3,4,5 increase the EHR size and heterogeneity with an increase in the number of medical images (1 to 4). The record size and type are not varied in the presented experimentation. This implies that the tests cases have increasing size and heterogeneity of the data. Test case 6 shows the proposed partitioning of EHR with patient's identity attributes stored on-chain and four medical records and their base64 values stored off-chain.

b: EVALUATION METRICS

As part of the medical record, we selected a blood report image. Same image has been used for all cases. We have used the following terms for evaluation of experimentation:

Data addition time (T_a): Data addition time is the time required to:

- calculate keccak256 hash of identity attributes and medical records (T_{hash})
- encode medical report in base64 format (T_{encode})
- add identity attributes on-chain ($T_{add\_identity}$)
- add base64 encoded medical records on-chain ($T_{add\_records}$)
- add original medical records on localhost Mongo dB server ($T_{add\_off-chain}$).

$$T_a = T_{hash} + T_{encode} + T_{add\_identity} + T_{add\_records} + T_{add\_off-chain} \quad (1)$$

As we have used localhost Mongo dB server, the time required to add records i.e $T_{add\_off-chain}$ was minimal. Hence, we also write (1) as:

$$T_a = T_{hash} + T_{encode} + T_{add\_identity} + T_{add\_records} \quad (2)$$

Data fetch time (T_f): Data fetch time is the time required to:

- Recalculate keccak256 hash of identity attributes and medical records for verification (T_{rehash})
- Fetch identity attributes from the blockchain ($T_{fetch\_identity}$)

TABLE 12. Cases used in experimentation.

Case No.	Cases	On-chain and off-chain data		Total on-chain Response Time (ms)	Required gas (Wei)
		On-chain	Off-chain		
1	Patient ID, Patient Name, Referred Doctor	uint, string, string	-	38780.7	0.0002
2	Patient ID, Patient Name, Referred Doctor, Medical record image1	uint, string, string, base64	-	39205.2	0.0002032
3	Patient ID, Patient Name, Referred Doctor, Medical record image1, Medical record image2	uint, string, string, base64, base64	-	40448.5	0.0002362
4	Patient ID, Patient Name, Referred Doctor, Medical record image1, Medical record image2, Medical record image3	uint, string, string, base64, base64, base64	-	40655.6	0.0002692
5	Patient ID, Patient Name, Referred Doctor, Medical record image1, Medical record image2, Medical record image3,Medical record image4	uint, string, string, base64, base64, base64, base64	-	44154.3	0.000358
6	Identity attributes on on-chain and actual medical records off-chain	uint, string, string	base 64, base 64, base 64, base 64, Medical Record 1 Medical Record 2, Medical Record 3, Medical Record 4	38780.7	0.0002

- Fetch base64 encoded medical records from the blockchain (T_{fetch_base64})
- Fetch original medical records from localhost Mongo dB server ($T_{fetch\_off\_chain}$).

Data fetch time (T_f) can be represented as:

$$T_f = T_{rehash} + T_{fetch\_identity} + T_{fetch\_base64} + T_{fetch\_off\_chain} \quad (3)$$

As we have used localhost Mongo dB server, the time required to fetch records i.e $T_{fetch\_off-chain}$ was minimal. We also write (3) as:

$$T_f = T_{rehash} + T_{fetch\_identity} + T_{fetch\_base64} \quad (4)$$

Total response time (T_r): Total response time is the addition of data addition time (T_a) and data fetch time (T_f).

$$\sum T_r = \sum T_a + \sum T_f \quad (5)$$

Gas: The fee is required for every transaction to execute related operations on the Ethereum blockchain. This fee is called as gas.

c: PERFORMANCE ANALYSIS

We can observe that from Fig. 16 that as on-chain record size increases (Case 1 to Case 5), total response time increases. This implies that as the EHR size and complexity increase, on-chain total response time also increases. In Case 6, we have applied the proposed EHR partitioning to on-chain and off-chain. Case 6 in Fig. 16 indicates total response time, which is majorly for on-chain storage. Fig. 17 indicates off-chain response time of Table 13 and shows the off-chain response time with a rise in the number of medical record images stored on premise Mongo dB server. It is evident from Fig. 16 & Fig. 17 that the total response times of the same number of (4) medical records for on-chain and off-chain are 44154.3ms and 48.9ms, respectively. This shows that the proposed partitioning scheme for EHR works better than the on-chain EHR storage for response time.

TABLE 13. Off-chain response time.

No. of Medical Records	Total off-chain Response Time (ms)
1	17.3
2	26.8
3	39.4
4	48.9

We have observed that gas required for on-chain storage in Fig. 18. As shown in Fig. 18, as on-chain record size increases, gas required also increases. This shows that the proposed partitioning scheme for EHR works better than the on-chain EHR storage for transaction cost.

VI. LIMITATIONS OF THE WORK

Our review is limited by the weaknesses of the selected literature. As blockchain technology is emerging, its application in the healthcare sector is also under experimentation. Hence many of the selected works were limited to prototype-based validations.

The documentation was limited to 78 works (including white papers) from 2007 to 2021 and 80 web sources. This causes a risk of bias in the overall work. We used popularity ranking and manual screening for the resources on healthcare

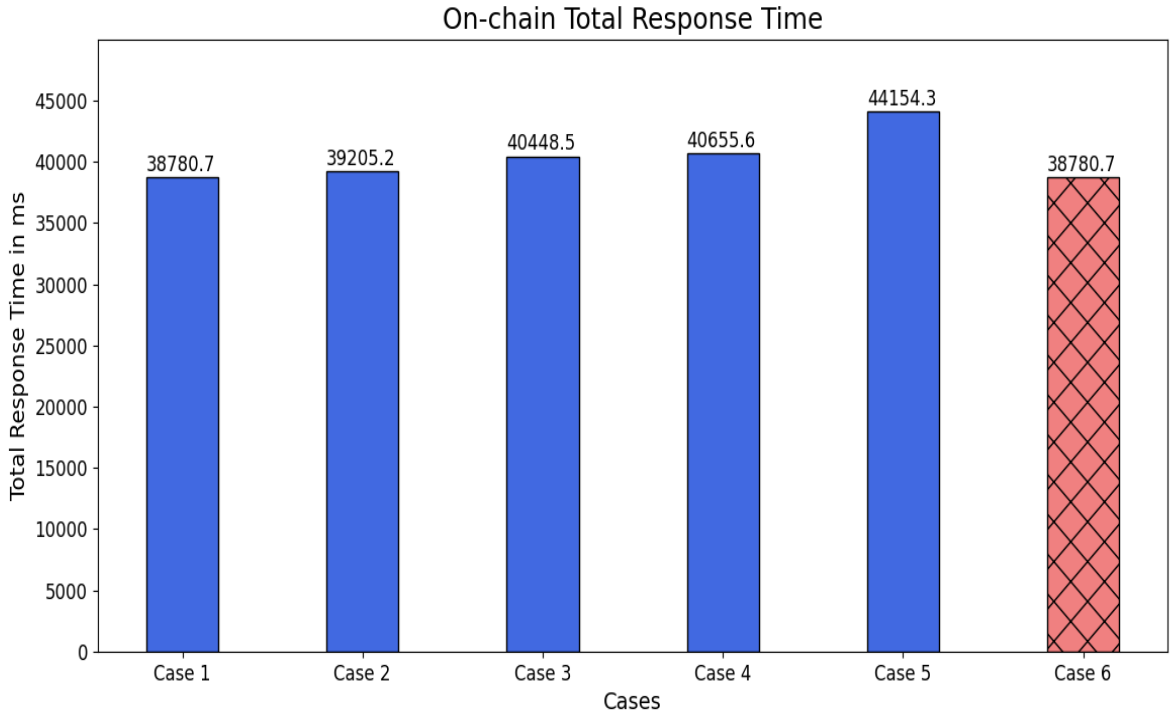

FIGURE 16. On-chain total response time for EHR for all mentioned cases.

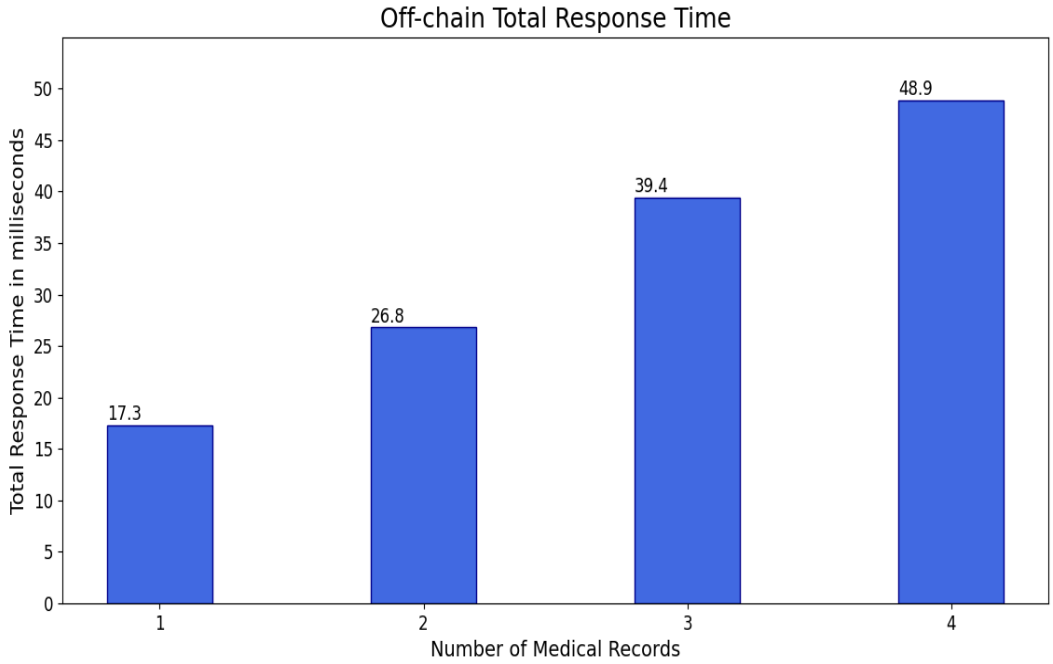

FIGURE 17. Off-chain total response time for incremental medical records.

sector evolution, blockchain evolution, blockchain concepts, and state of the art literary works done in healthcare data interoperability.

Review on interoperability in EHR has been limited to the stated three areas, i.e. structure and semantic interoperability, patient-centric privacy preservation, cross-chain interoperability.

The works on semantic interoperability focus on the popular ontologies, standards, and data stores. The most common open standards for EHR are evaluated for interoperability.

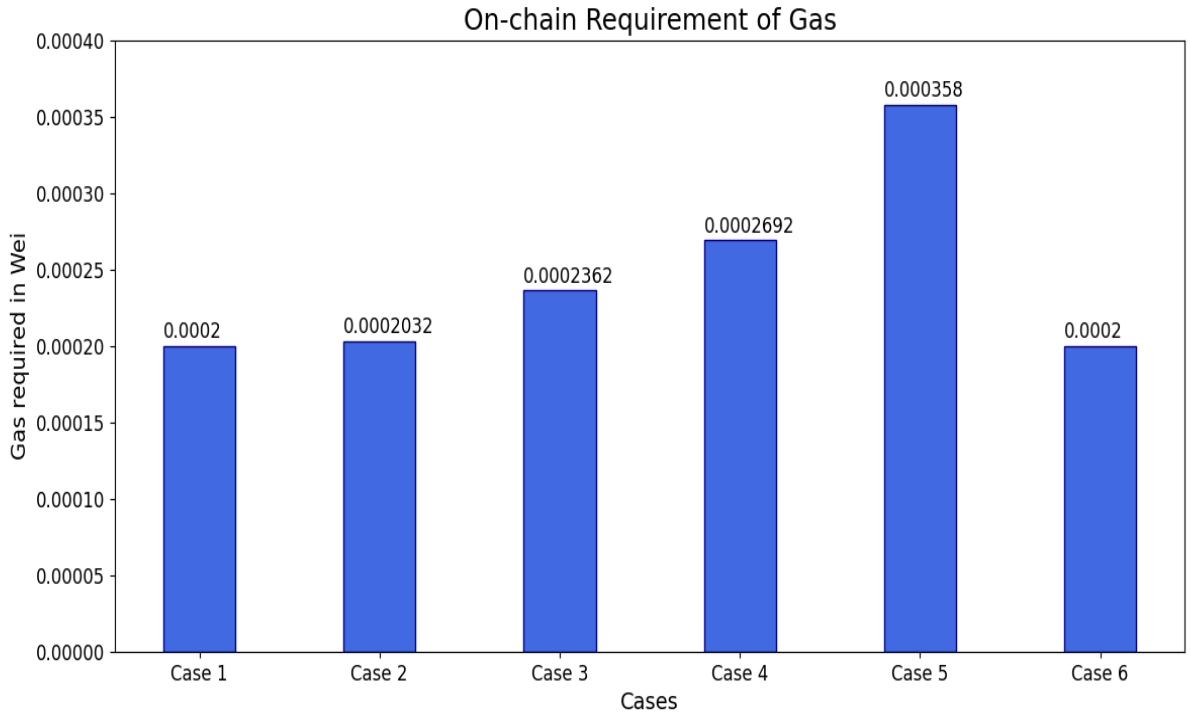

FIGURE 18. Gas usage for all mentioned cases.

The works on privacy-preserving techniques is limited to the works in healthcare data privacy, and the evaluation is done based on limited performance and consistency metrics.

The reviews on the cross-chain interoperability platforms are limited by the availability of technical white papers. These works were analyzed for the underlying goals of secure and seamless data transfer, while other performance features like scalability, responsiveness, storage, and cost are not evaluated. The choice of blockchain engines for the study was also done on the popularity ranking and may have introduced bias.

This work also presents an architecture of MyBlockEHR: framework of blockchain-based tamper-proof EHR storage with off-chain storage augmentation. The experimentation is based on the proof-of-concept implementation on the test network and lacks the evaluation in performance by choice of the hashing function, partitioning strategy, and No-SQL data store. The work on the article is limited to demonstrate smart contract implementation for verifiable off-chain data retrieval with different EHR sizes. The test cases are limited to two scenarios that are complete on-chain EHR versus on-chain and off-chain storage. We observe the two scenarios for different EHR sizes regarding the number of medical images as test cases. The experiments are also limited with the uniformity of the medical record images (size and type). The performance is limited with two significant performance metrics, i.e. total response time and gas price.

VII. CONCLUSION & FUTURE WORK

A. CONCLUSION

This work, presents the importance of EHR interoperability in terms of EHR structure, EHR ownership, and EHR sharing for seamless healthcare services. This review presents an exhaustive survey of healthcare ontologies for EHR knowledge representation, open standards for EHR interpretation, and big data stores for EHR modeling. This helps researchers to analyze how literature works have addressed the challenges of non-uniform semantics and the heterogeneous structure of EHR for semantic interoperability.

The two prominent open standards for EHR are evaluated for interoperability guarantees. A comparative analysis of data stores to represent the heterogeneous EHR structure is carried out using the performance metrics and consistency semantics. It is conclusively found that document-based data stores can model the EHR structure very effectively with respect to storage, search, and retrieval efficiency.

This review prioritizes privacy preservation of the patient data as an indispensable feature of an interoperable solutions. The review presents extensive research on literary works on privacy preservation for EHR by classifying them into prominent techniques. The blockchain-based privacy preservation techniques were also studied to consider their adoption in the proposed framework for realizing patient-centric EHR ownership.

The work presents the significance of the adopting blockchain to EHR as it offers a promising solution by design

towards immutable EHR storage, EHR traceability, and IAM with pseudo-anonymity. However, with the study of challenges in adopting blockchain to EHR management, our study reiterates the findings that it is vulnerable to privacy attacks with decentralized ledgers and is computationally intensive with on-chain data.

The survey evaluates the potential in adopting blockchain for interoperable, privacy-preserving, trusted solutions to data exchanges across different healthcare sector stakeholders for patient-centric services. The significant contribution of our work is a framework of prototype MyBlockEHR for trust-based, privacy-preserving EHR management. Its implementation with on-chain/off-chain data partitioning and smart contract demonstrates that it shows better performance, access control, and verifiability over the centralized EHR systems and non-partitioned blockchain-based EHR management framework.

The work highlights how interoperability across blockchain platforms is another research challenge for inter-organization exchange of health reports with interoperability goals in healthcare data. The data interoperability solutions across different blockchain engines are reviewed for the realization of the objectives of EHR exchange. Our study finds the need for good research work on cross-chain data exchanges in healthcare data. Thus, our study of healthcare data interoperability encourages more prototype testing and integration strategies for trust-based healthcare services.

B. FUTURE WORK

The findings of the exhaustive survey and the proposed framework with experimental findings highlight the need for future work in the following areas:

Semantic interoperability in EHR:

- A Study of ontologies discovers that they are incredibly narrow in terms of use cases and applications. Hence are limited in scope. Also, they are guided by OWL and RDF structures which focus on the representations. They can be leveraged with the application of Natural language processing and deep learning methods for better interpretation with more accuracy.
- Integration of blockchain-based decentralized systems with ontologies and EHR standards for semantic interoperability will guarantee trust-based and tamper-proof data exchanges with the common understanding of the health record. The current implementations of Ontologies are centralized in the architecture and face scaling issues. Also, these implementations are focused only on query optimizations and lack privacy issues which can be the area of research in future work.

Privacy preservation techniques

- Privacy preservation techniques with blockchain encourage more research for data partitioning techniques on on-chain and off-chain storage.
- Patient-centric privacy preservation is the forthcoming research area for EHR management on the blockchain. This will encourage more works on patient-controlled access control, data flow monitoring, and tracking provenance of data.
- Incentivization techniques for data sharing can be built with blockchain integrated platforms to encourage patients to share more data for research in a trusted manner in the future.

Blockchain frameworks for EHR interoperability

- Existing blockchain frameworks work on customized semantics and EHR structures. Adoption of open standards will improve the semantic interoperability of the EHR framework.
- Blockchain platforms are challenged by a lack of scalability and excessive power consumption issues. EHR management faces big data problems like velocity and volume of data. The Study of solutions to reduce the on-chain storage and on-chain computations of EHR needs further research.
- Distributed ledger in blockchain distributed the data in distributed system, and the privacy of patient data is threatened. Building blockchain-based solutions with leveraged privacy preservation techniques is the future research area.
- The development of smart–contracts, access control techniques for patient-controlled audits is of utmost importance in Healthcare 4.0.
- Building of verifiable, tamper-resistant off-chain storage will be the concern of future research.

Cross-chain interoperability

- Cross-chain interoperability for healthcare data should be seamless exchange across the different systems. Seamless transfer of data across different blockchain-based systems is the area of work.
- Healthcare data exchanges need to be privacy-preserving and should desire non-intermediated solutions. Building a data-sharing framework between two blockchain-based healthcare ecosystems to preserve the patient-privacy is the most critical research challenge put forth by the work.

ACKNOWLEDGMENT

The authors would like to thank Symbiosis International (Deemed University), Curtin University, and MIT ADT University for continuous support and guidance to carry out research to accomplish the objectives. They are also thankful to the anonymous reviewers for revising the manuscript to the best version.

APPENDIX

ABBREVATIONS

AI	Artificial Intelligence.
API	Application Programming Interface.
AWS	Amazon Web Services.
BFT	Byzantine Fault Tolerance.
CARO	Common Anatomy Reference Ontology.

CCD	Continuity of Care Document.
CDA	Clinical Document Architecture.
CEN	European Committee for Standardization.
COBIT	Control Objectives for Information and related Technology.
CRUD	Creation, Retrieval, Update and Delete.
CT	Clinical Terms.
DApp	Decentralized Application.
DICOM	Digital Imaging and Communications in Medicine.
DISHA	Digital Information Security in Healthcare Act.
DLT	Distributed Ledger Technology.
DS	Discharge Summary.
EEA	European Economic Area.
EHR	Electronic Health Record.
EU	European Union.
FHIR	Fast Healthcare Interoperability Resources.
FMRC	Family Medicine Research Centre.
GALEN	General Architecture for Languages, Encyclopedias and Nomenclatures in Medicine.
GDPR	General Data Protection Regulation.
GO	Gene Ontology.
GRAIL	GALEN Representation And Integration Language.
HDG	Healthcare Data Gateway.
HIPAA	Health Insurance Portability and Accountability Act.
HISA	Healthcare Information Systems Architecture.
HL7	Health Level 7.
HTML	HyperText Markup Language.
IAM	Identity and Access Management.
ICD-10*	International Classification of Diseases.
ICD-10-AM	The International Statistical Classification of Diseases and Related Health Problems, Tenth Revision, Australian Modification.
ICPC-2	International Classification of Primary Care.
IDE	Integrated Development Environment.
IoT	Internet of Things.
ISO	International Organization for Standardization.
IT	Information Technology.
LOINC	Logical Observation Identifiers Names and Codes.
ML	Machine Learning.
MoHFW	Ministry of Health & Family Welfare.
NE	Not Evaluated.
NeHA	National Electronic Health Authority.
No-SQL	Not only SQL.
ORM	Object Relational Database.
OWL	Ontology Web Language.
PBD	Privacy by Design.
PCP	Patient Controlled Privacy.
PoD	Proof of Distance.
PoS	Proof of Stake.
PoW	Proof of Work.
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses.
RDBMS	Relational Database Management System.
RDF	Resource Description Framework.
RIM	Reference Informa tion Model.
RQ	Research Questions.
SeHA	State Electronic Health Authorities.
SNOMED*	Systematized Nomenclature of Medicine.
SPARQL	SPARQL Protocol and RDF Query Language.
TWC	Transwarp Conduit.
USAM	Unified Service Action Model.
W3C	World Wide Web Consortium.
WSN	Wireless Sensor Network.

REFERENCES

[1] *Interoperability in Healthcare, HIMSS*. Accessed: Jun. 8, 2020. [Online]. Available: https://www.himss.org/resources/interoperability-healthcare

[2] K. Adane, D. Muluye, and M. Abebe, "Processing medical data: A systematic review," *Arch. Public Health*, vol. 71, no. 1, pp. 1–6, Dec. 2013.

[3] J. Sorace, H.-H. Wong, T. DeLeire, D. Xu, S. Handler, B. Garcia, and T. MaCurdy, "Quantifying the competitiveness of the electronic health record market and its implications for interoperability," *Int. J. Med. Informat.*, vol. 136, Apr. 2020, Art. no. 104037.

[4] S. Watford, S. Edwards, M. Angrish, R. S. Judson, and K. Paul Friedman, "Progress in data interoperability to support computational toxicology and chemical safety evaluation," *Toxicol. Appl. Pharmacol.*, vol. 380, Oct. 2019, Art. no. 114707.

[5] M. Azarm-Daigle, C. Kuziemsky, and L. Peyton, "A review of cross organizational healthcare data sharing," *Proc. Comput. Sci.*, vol. 63, pp. 425–432, Jan. 2015.

[6] A. Dubovitskaya, F. Baig, Z. Xu, R. Shukla, P. S. Zambani, A. Swaminathan, M. M. Jahangir, K. Chowdhry, R. Lachhani, N. Idnani, M. Schumacher, K. Aberer, S. D. Stoller, S. Ryu, and F. Wang, "ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care," *J. Med. Internet Res.*, vol. 22, no. 8, Aug. 2020, Art. no. e13598.

[7] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," *Comput. Commun.*, vol. 153, pp. 311–335, Mar. 2020.

[8] H. Figge, "Interoperability: Sharing and interpreting data with health information technology," *USPharm*, vol. 39, no. 11, pp. 50–52, 2014. Accessed: Jun. 8, 2020. [Online]. Available: https://www.uspharmacist.com/article/interoperability-sharing-and-interpreting-data-with-health-information-technology

[9] S. D. Cannoy and L. Iyer, "Semantic web standards and ontologies in the medical sciences and healthcare," in *Semantic Web Technologies and e-Business: Toward the Integrated Virtual Organization and Business Process Automation*. Hershey, PA, USA: IGI Global, 2007, pp. 405–420.

[10] *Six Assumptions for Measuring Health Disruption*, Deloitte, London, U.K., Apr. 2020.

[11] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, 2016.

[12] S. M. Freire, D. Teodoro, F. Wei-Kleiner, E. Sundvall, D. Karlsson, and P. Lambrix, "Comparing the performance of NoSQL approaches for managing archetype-based electronic health record data," *PLoS ONE*, vol. 11, no. 3, Mar. 2016, Art. no. e0150069.

[13] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. P. Tsai, and C.-R. Shyu, "A patient-centric health information exchange framework using blockchain technology," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 8, pp. 2169–2176, Aug. 2020.
[14] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102407.
[15] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," 2020, *arXiv:2005.14282*.
[16] BLOCKNET, Jessica Galang. (Apr. 10, 2018). *Healthcare and the Blocknet: The Challenge of Interoperability*. Accessed: Apr. 6, 2021. [Online]. Available: https://theblocknetchannel.medium.com/healthcare-and-the-blocknet-the-challenge-of-interoperability-5c61dcb738e1
[17] Q. I. 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, pp. 14757–14767, 2017, doi: 10.1109/ACCESS.2017.2730843.
[18] A. A. Alomar, M. Z. A. Bhuiyan, and A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Gener. Comput. Syst.*, vol. 95, pp. 511–521, Jun. 2019.
[19] A. R. Rajput, Q. Li, and M. T. Ahvanooey, "A blockchain-based secret-data sharing framework for personal health records in emergency condition," *Healthcare*, vol. 9, no. 2, p. 206, Feb. 2021.
[20] 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*, vol. 8, no. 2, p. 44, 2017.
[21] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and secure medical data sharing via blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 136, Aug. 2018.
[22] 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.
[23] A. Garrido, L. J. Ramírez López, and N. B. Álvarez, "A simulation-based AHP approach to analyze the scalability of EHR systems using blockchain technology in healthcare institutions," *Informat. Med. Unlocked*, vol. 24, Jan. 2021, Art. no. 100576.
[24] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, "A blockchain-based approach to health information exchange networks," in *Proc. NIST Workshop Blockchain Healthcare*, vol. 1, 2016, pp. 1–10.
[25] M. Uddin, M. S. Memon, I. Memon, I. Ali, J. Memon, M. Abdelhaq, and R. Alsaqour, "Hyperledger fabric blockchain: Secure and efficient solution for electronic health records," *Comput., Mater. Continua*, vol. 68, no. 2, pp. 2377–2397, 2021.
[26] *Understand the Three Levels of Interoperability*, Health, Wolters Kluwer, Alphen aan den Rijn, The Netherlands, 2014. Accessed: Jun. 8, 2020. [Online]. Available: https://www.wolterskluwer.com/en/expertinsights/understand-the-three-levels-of-interoperability
[27] (2013). *Overview of Healthcare Interoperability Standards*. Health Information and Quality Authority. Accessed: Nov. 12, 2020. [Online]. Available: https://www.hiqa.ie/sites/default/files/2017-01/Healthcare-Interoperability-Standards.pdf
[28] *ICPC 2 PLUS*. Wikipedia. Accessed: Nov. 12, 2020. [Online]. Available: https://en.wikipedia.org/wiki/ICPC_2_PLUS#:~:text=ICPC%20is%20being%20developed%20by,in%201998%20as%20ICPC%2D2
[29] M. Michelle. (2012). *5 Things to Know About CCD*. HealthcareITNews. Accessed: Nov. 21, 2020. [Online]. Available: https://www.healthcareitnews.com/news/5thingsknowaboutccd#:~:text=What%20exactly%20is%20a%20CCD,v3%20standards%2C%22%20Brull%20said
[30] *HL7 International*. Accessed: May 2, 2021. [Online]. Available: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=233
[31] Lyniate. *Rim Reference Information Model*. Accessed: Nov. 21, 2020. [Online]. Available: https://www.lyniate.com/knowledge-hub/rim-reference-information-model/
[32] *OWL*. Accessed: Apr. 2, 2021. [Online]. Available: https://www.w3.org/OWL/
[33] *GO*. Accessed: Apr. 2, 2021. [Online]. Available: http://geneontology.org/
[34] *GO*. Accessed: Apr. 2, 2021. [Online]. Available: https://bioportal.bioontology.org/ontologies/GALEN
[35] A. L. Rector, J. E. Rogers, and P. Pole, "The GALEN high level ontology," Medical Inform. Group, Dept. Comput. Sci., Univ. Manchester, Manchester, U.K., Tech. Rep. M13 9PL, 1996, Accessed: May 2, 2021. [Online]. Available: https://www.opengalen.org/download/mie-96.pdf
[36] *Biomedical Ontologies and Controlled Vocabularies*. Univ. Michigan Library, Ann Arbor, MI, USA. Accessed: Nov. 12, 2020. [Online]. Available: https://guides.lib.umich.edu/ontology/ontologies
[37] (2017). *SNOMED CT Standard Ontology Based on the Ontology for General Medical Science, BioPortal*. Accessed: Nov. 20, 2020. [Online]. Available: https://bioportal.bioontology.org/ontologies/SCTO
[38] *ICD*. Accessed: Apr. 2, 2021. [Online]. Available: https://bioportal.bioontology.org/ontologies/ICD10
[39] G. Jiang, H. R. Solbrig, and C. G. Chute, "Using semantic web technology to support ICD-11 textual definitions authoring," in *Proc. 4th Int. Workshop Semantic Web Appl. Tools Life Sci. (SWAT4LS)*, 2012, pp. 38–44.
[40] N. Gupta and R. Agrawal, *NoSQL Security, Advances in Computers*, vol. 109. Amsterdam, The Netherlands: Elsevier, 2018, pp. 101–132, doi: 10.1016/bs.adcom.2018.01.003.
[41] R. Sánchez-de-Madariaga, A. Muñoz, R. Lozano-Rubí, P. Serrano-Balazote, A. L. Castro, O. Moreno, and M. Pascual, "Examining database persistence of ISO/EN 13606 standardized electronic health record extracts: Relational vs. NoSQL approaches," *BMC Med. Informat. Decis. Making*, vol. 17, no. 1, pp. 1–14, Dec. 2017.
[42] V. Abramova and J. Bernardino, "NoSQL databases: MongoDB vs Cassandra," in *Proc. Int. C* Conf. Comput. Sci. Softw. Eng.*, 2013, pp. 14–22.
[43] A. Gamal, S. Barakat, and A. Rezk, "Standardized electronic health record data modeling and persistence: A comparative review," *J. Biomed. Informat.*, vol. 114, Feb. 2021, Art. no. 103670.
[44] Y. Y. Hong, A. T. Nur, A. K. Haris, and K. D. Sarinder, "Electronic health record integration," in *Encyclopedia of Bioinformatics and Computational Biology*. New York, NY, USA: Academic, 2019, pp. 1063–1076, doi: 10.1016/B978-0-12-809633-8.20306-3.
[45] *neo4j*. Accessed: Apr. 3, 2021. [Online]. Available: https://neo4j.com/developer/graph-database/
[46] K. K. Lee, W. C. Tang, and K. S. Choi, "Alternatives to relational database: Comparison of NoSQL and XML approaches for clinical data storage," *Comput. Methods Programs Biomed.*, vol. 110, no. 1, pp. 99–109, 2013.
[47] S. Tai, J. Eberhardt, and M. Klems, "Not acid, not base, but salt," in *Proc. 7th Int. Conf. Cloud Comput. Services Sci.*, 2017, pp. 755–764.
[48] Aws. (2020). *Architecting for HIPAA Security and Compliance on Amazon Web Services*. Whitepaper. Accessed: Nov. 9, 2020. [Online]. Available: https://d0.awsstatic.com/whitepapers/compliance/AWS_HIPAA_Compliance_Whitepaper.pdf
[49] G. Loukides, J. Liagouris, A. Gkoulalas-Divanis, and M. Terrovitis, "Disassociation for electronic health record privacy," *J. Biomed. Informat.*, vol. 50, pp. 46–61, Aug. 2014.
[50] K. Tu, J. Klein-Geltink, T. F. Mitiku, C. Mihai, and J. Martin, "De-identification of primary care electronic medical records free-text data in Ontario, Canada," *BMC Med. Informat. Decis. Making*, vol. 10, no. 1, p. 35, Dec. 2010.
[51] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography," *IEEE Access*, vol. 5, pp. 22313–22328, 2017, doi: 10.1109/ACCESS.2017.2757844.
[52] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013, doi: 10.1109/TPDS.2012.97.
[53] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption," *Future Generat. Comput. Syst.*, vol. 52, pp. 67–76, Nov. 2015.
[54] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Inf. Syst.*, vol. 48, pp. 132–150, Mar. 2015.
[55] S. Sadki and H. E. Bakkali, "PPAMH: A novel privacy-preserving approach for mobile healthcare," in *Proc. 9th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2014, pp. 209–214.
[56] M. Terrovitis, N. Mamoulis, and P. Kalnis, "Privacy-preserving anonymization of set-valued data," *Proc. Very Large Data Bases Endowment*, vol. 1, no. 1, pp. 115–125, 2008.
[57] K. El Emam, F. K. Dankar, R. Issa, E. Jonker, D. Amyot, E. Cogo, J. P. Corriveau, M. Walker, S. Chowdhury, R. Vaillancourt, and T. Roffey, "A globally optimal k-anonymity method for the de-identification of health data," *J. Amer. Med. Inf. Assoc.*, vol. 16, no. 5, pp. 670–682, 2009.
[58] P. Belsis and G. Pantziou, "A k-anonymity privacy-preserving approach in wireless medical monitoring environments," *Pers. Ubiquitous Comput.*, vol. 18, no. 1, pp. 61–74, 2014.

[59] H. Yang and B. Yang, "A blockchain-based approach to the secure sharing of healthcare data," *Nisk J.*, pp. 100–111, Nov. 2017.
[60] M. Barua, X. Liang, R. Lu, and X. Shen, "ESPAC: Enabling security and patient-centric access control for ehealth in cloud computing," *Int. J. Secur. Netw.*, vol. 6, nos. 2–3, pp. 67–76, 2011.
[61] M. Lacity, Z. Steelman, and P. Cronan, "Towards blockchain 3.0 interoperability: Business and technical considerations," *BC CoE*, vol. 1, 2019. [Online]. Available: https://cpb-us-e1.wpmucdn.com/wordpressua.uark.edu/dist/5/444/files/2019/05/BCCoEWhitePaper012019Open.pdf
[62] T. Koens and E. Poll, "Assessing interoperability solutions for distributed ledgers," *Pervas. Mobile Comput.*, vol. 59, Oct. 2019, Art. no. 101079.
[63] D. Shifrin. (May 1, 2017). *Entrepreneurship Health Tech*. Metronome: Tech, Alignment and Trust in Healthcare. Accessed: Apr. 6, 2021. [Online]. Available: https://www.healthfurther.com/the-future-of-health/2017/05/01/metronome-tech-alignment-and-trust-in-healthcare/
[64] J. L. B. Cisneros, F. M. Aarestrup, and O. Lund, "Public health surveillance using decentralized technologies," *Blockchain Healthcare Today*, vol. 1, pp. 1–14, Mar. 2018.
[65] Plato. (Mar. 9, 2021). *The Pulse Network: An Ultimate Medical Solution on Polkadot*. Coinpedia. Accessed: Apr. 5, 2021. [online] Available: https://zephyrnet.com/the-pulse-network-an-ultimate-medical-solution-on-polkadot/
[66] *Cosmos FAQ*. COSMOS. Accessed: Aug. 5, 2020. [Online]. Available: https://cosmos.network/resources/faq
[67] J. Kwon and E. Buchman, "A network of distributed ledgers," COSMOS, White Paper, Jul. 2018, pp. 1–41. [Online]. Available: https://v1.cosmos.network/resources/whitepaper
[68] Polkadot. (2020). *W3F Initiates Launch: Polkadot is Live*. Polkadot Launch. Accessed: Aug. 5, 2020. [Online]. Available: https://polkadot.network/web3foundationinitiateslaunchpolkadotislive/#:~:text=Launch%20builds%20on%20the%20success,together%2C%20seamlessly%20and%20at%20scale
[69] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," White Paper, 2016. [Online]. Available: https://polkadot.network/PolkaDotPaper.pdf
[70] *Polkadot*. Accessed: Aug. 5, 2020. [Online]. Available: https://polkadot.network/
[71] *Pulse*. Accessed: Apr. 6, 2021. [Online]. Available: https://www.pulsemed.network/
[72] J. Martin. (May 29, 2020). *South Korea's ICON Releases Blockchain Interoperability Protocol*. Cointelegraph. Accessed: Oct. 3, 2020. [Online]. Available: https://cointelegraph.com/news/south-koreas-icon-releases-blockchain-interoperability-protocol
[73] (2018). *ICON Hyperconnect the World*. Whitepaper, ICON Foundation. Accessed: Oct. 3, 2020. [Online]. Available: https://icon.foundation/resources/whitepaper/ICON_Whitepaper_EN.pdf
[74] Cryptopedia, Min Kim. (Mar. 16, 2021). *ICON (ICX): Revolutionizing the Blockchain Landscape in Korea and Beyond*. Accessed: Apr. 6, 2021. [Online]. Available: https://www.gemini.com/cryptopedia/icon-network-enterprise-blockchain
[75] M. Spoke, "Aion: Enabling the decentralized internet," AION, London, U.K., White Paper, 2017. Accessed: Oct. 3, 2020. [Online]. Available: https://whitepaper.io/document/31/aion-whitepaper
[76] J. G. Betakit. (Aug. 30, 2017). *Nuco Launches Aion Framework to Tackle Blockchain's Interoperability Problem*. Accessed: Apr. 6, 2021. [Online]. Available: https://betakit.com/nuco-launches-aion-framework-to-tackle-blockchains-interoperability-problem/
[77] Aion. *[ARCHIVE] Blockchain Interoperability—The Aion Transwarp Conduit (TWC)*. Accessed: May 7, 2021. [Online]. Available: https://aion.theoan.com/blog/blockchain-interoperability-the-aion-transwarp-conduit-twc/
[78] *Development Roadmap*. Blocknet. Accessed: Oct. 3, 2020. [Online]. Available: https://blocknet.co/roadmap
[79] A. Culwick and D. Metcalf, "The blocknet design specifications," Blocknet, Indianapolis, IN, USA, White Paper, Mar. 2018. Accessed: Oct. 3, 2020. [Online]. Available: https://docs.blocknet.co/project/blocknet-whitepaper.pdf
[80] *Overview*. Blocknet Documentation. Accessed: Oct. 3, 2020. [Online]. Available: https://docs.blocknet.co/#technical-overview
[81] Blocknet Documentation. *XRouter*. Accessed: Apr. 6, 2021. [Online]. Available: https://docs.blocknet.co/protocol/xrouter/introduction/
[82] Metronome. *Messari*. Accessed: Oct. 3, 2020. [Online]. Available: https://messari.io/asset/metronome/profile
[83] (Aug. 15, 2019). *Metronome*. Github. Accessed: Oct. 3, 2020. [Online]. Available: https://github.com/autonomoussoftware/documentation/blob/master/owners_manual/owners_manual.md
[84] *BTC Relay*. BitcoinWiki. Accessed: Oct. 2, 2020. [Online]. Available: https://en.bitcoinwiki.org/wiki/BTC_Relay
[85] *DogEthereum Token*. CoinLore. Accessed: Aug. 29, 2020. [Online]. Available: https://www.coinlore.com/coin/dogEthereum-token
[86] *Wanchain Foundation Limited*, Profile Report, Singapore CrossAngle Pte. Ltd. Accessed: Oct. 2, 2020. [Online]. Available: https://xangle.io/project/report/WAN/en
[87] Wanchain. *Building Super Financial Markets for the New Digital Economy*. Whitepaper. Accessed: Oct. 2, 2020. [Online]. Available: https://www.wanchain.org/files/Wanchain_White_Paper_EN.pdf
[88] *Block Collider*. Accessed: Oct. 2, 2020. [Online]. Available: https://www.blockcollider.org/
[89] Block Collider Team. (2018). *Block Collider*. Whitepaper. Accessed: Oct. 2, 2020. [Online]. Available: https://s3.amazonaws.com/blockcollider/blockcollider_wp.pdf
[90] (Sep. 27, 2019). *ARK Ecosystem*. Whitepaper, Version 2.1.0, ARK.io. Accessed: Oct. 3, 2020. [Online]. Available: https://ark.io/Whitepaper.pdf
[91] *Block Collider SpecR Handbook*. Speculative Rationality. Accessed: Oct. 3, 2020. [Online]. Available: https://spec rationality.com/block-collider/
[92] (Sep. 16, 2020). *Lamden Mainnet Launches With Supercharged Performance & Python Ease*. Press Release, Cointelegraph. Accessed: Oct. 3, 2020. [Online]. Available: https://cointelegraph.com/press-releases/lamden-mainnet-launches-with-supercharged-performance-python-ease
[93] *Lamden (Blockchain Service)*. Icodrops. Accessed: Oct. 3, 2020. [Online]. Available: https://icodrops.com/wpcontent/uploads/2018/01/Lamden-Competitors.jpg
[94] S. Farmer. (Apr. 21, 2018). *A Complete Overview of the Lamden Suite*. The Official Blog of the Lamden Blockchain Project. Accessed: Oct. 3, 2020. [Online]. Available: https://blog.lamden.io/a-complete-overview-of-the-lamden-suite-2eb43c730b40
[95] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Keele Univ., Durham Univ., Tech. Rep., 2007. [Online]. Available: https://userpages.uni-koblenz.de/~laemmel/esecourse/slides/slr.pdf
[96] V. Stroetman, D. Kalra, P. Lewalle, A. Rector, J. Rodrigues, K. Stroetman, G. Surjan, B. Ustun, M. Virtanen, and P. Zanstra, "Semantic interoperability for better health and safer healthcare," in *Research and Deployment Roadmap for Europe, SemanticHEALTH Report*. European Commission, 2009, p. 34. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/9bb4f083-ac9d-47f8-ab4a-76a1f095ef15
[97] C. Martínez-Costa, R. Cornet, D. Karlsson, S. Schulz, and D. Kalra, "Semantic enrichment of clinical models towards semantic interoperability. The heart failure summary use case," *J. Amer. Med. Inform. Assoc.*, vol. 22, no. 3, pp. 565–576, May 2015.
[98] H. Nelson. (2021). *Feds Release Patient Matching Specification Draft for Public Comment*. Accessed: Aug. 19, 2021. [Online]. Available: https://ehrintelligence.com/news/feds-releases-patient-matching-specification-draft-for-public-comment
[99] UBITECH. *EHR Interoperability*. Accessed: Aug. 20, 2021. [Online]. Available: https://ubitech.eu/technology/ehr-interoperability/
[100] C. Kendra. (2021). *Diagnostic and Statistical Manual (DSM) Overview*. Accessed: Aug. 20, 2021. [Online]. Available: https://www.verywellmind.com/thediagnosticandstatistical-manual-dsm-2795758
[101] MedDRA. (2021). *SNOMED CT MedDRA Mappings are Now Available*. Accessed: Aug. 20, 2021. [Online]. Available: https://www.meddra.org/news-and-events/news/snomed-ct-meddra-mappings-are-now-available
[102] M. M. Pai, R. Ganiga, R. M. Pai, and R. K. Sinha, "Standard electronic health record (EHR) framework for Indian healthcare system," *Health Services Outcomes Res. Methodol.*, vol. 21, no. 3, pp. 1–24, Jan. 2021.
[103] P. Muñoz, J. Trigo, I. Martínez, A. Muñoz, J. Escayola, and J. García, "The ISO/EN 13606 standard for the interoperable exchange of electronic health records," *J. Healthcare Eng.*, vol. 2, no. 1, pp. 1–24, Mar. 2011.
[104] F. Oemig and R. Snelick, *Healthcare Interoperability Standards Compliance Handbook*. Cham, Switzerland: Springer, 2016.
[105] *European Commission*. Accessed: Aug. 19, 2021. [Online]. Available: https://ec.europa.eu/eip/ageing/standards/ict-and-communication/other-ict/xdt_en.html
[106] H. Meng, H. Mao, C. Chi, and D. Zhao, "Analysis of HL7 EHRS functional model and suggested applications in China," in *Proc. MEDINFO Precision Healthcare Through Inform. 16th World Congr. Med. Health Inform.*, vol. 245, 2018, p. 174.

[107] *openEHR*. Accessed: May 2, 2021. [Online]. Available: https://www.openehr.org/
[108] *HL7FHIR*. Accessed: May 2, 2021. [Online]. Available: https://www.hl7.org/fhir/
[109] U. Mustafa, E. Pflugel, and N. Philip, "A novel privacy framework for secure M-health applications: The case of the GDPR," in *Proc. IEEE 12th Int. Conf. Global Secur., Saf. Sustainability (ICGS3)*, Jan. 2019, pp. 1–9, doi: 10.1109/ICGS3.2019.8688019.
[110] S. J. Nass, L. A. Levit, and L. O. Gostin, Eds., *The HIPAA Privacy Rule: Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, vol. 4. Washington, DC, USA: Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information, 2009. Accessed: Sep. 23, 2021. [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK9573/
[111] Lexigram. *Security Standards in Healthcare*. Accessed: Sep. 23, 2021. [Online]. Available: https://www.lexigram.io/lexipedia/security-standards-in-medicine/
[112] S. Tyali and D. Pottas, "Information security management systems in the healthcare context," in *Proc. South African Inf. Secur. Multi-Conf.*, Port Elizabeth, South Africa, May 2010, p. 17.
[113] ISO. *Health Informatics—Information Security Management in Health Using ISO/IEC 27002*. Accessed: Sep. 23, 2021. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:27799:ed-2:v1:en
[114] H. Nugroho, "Proposed IT governance at hospital based on COBIT 5 framework," *IJAIT Int. J. Appl. Inf. Technol.*, vol. 1, no. 2, pp. 52–58, Aug. 2017.
[115] M. Kozina and I. Sekovanic, "Using the cobit 5 for E-health governance," in *Proc. Central Eur. Conf. Inf. Intell. Syst., Fac. Org. Inform. Varazdin*, 2015, p. 203.
[116] *Digital Information Security in Healthcare, Act Draft*. Accessed: Oct. 10, 2021. [Online]. Available: https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf
[117] V. Soni. (2019). *What is Digital Information Security in Healthcare Act (DISHA) in India*. Tech Zone. Accessed: Oct. 10, 2021. [Online]. Available: https://www.znetlive.com/blog/digital-information-security-healthcare-act-disha/
[118] V. Luniya. (2021). *India: DISHA India's Probable Response to the Law on Protection of Digital Health Data*. Classic Law and Associates. Accessed: Oct. 10, 2021. [Online]. Available: https://www.mondaq.com/india/healthcare/1059266/disha-india39s-probable-response-to-the-law-on-protection-of-digital-health-data
[119] HIPAA Journal. *HIPAA Compliance Checklist*. Accessed: Sep. 29, 2021. [Online]. Available: https://www.hipaajournal.com/hipaa-compliance-checklist/
[120] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Comput. Sci. Rev.*, vol. 33, pp. 1–48, Aug. 2019.
[121] CSA. (2017). *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. Accessed: Sep. 29, 2021. [Online]. Available: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/
[122] L. Ismail and H. Materwala, "Blockchain paradigm for healthcare: Performance evaluation," *Symmetry*, vol. 12, no. 8, p. 1200, Jul. 2020.
[123] A. H. Mayer, C. A. da Costa, and R. D. R. Righi, "Electronic health records in a blockchain: A systematic review," *Health Informat. J.*, vol. 26, no. 2, pp. 1273–1288, Jun. 2020.
[124] M. W. L. Moreira, J. J. P. C. Rodrigues, A. K. Sangaiah, J. Al-Muhtadi, and V. Korotaev, "Semantic interoperability and pattern classification for a service-oriented architecture in pregnancy care," *Future Gener. Comput. Syst.*, vol. 89, pp. 137–147, Dec. 2018.
[125] A. Wulff, B. Haarbrandt, E. Tute, M. Marschollek, P. Beerbaum, and T. Jack, "An interoperable clinical decision-support system for early detection of SIRS in pediatric intensive care using openEHR," *Artif. Intell. Med.*, vol. 89, pp. 10–23, Jul. 2018.
[126] J. Mcmurray, L. Zhu, I. McKillop, and H. Chen, "Ontological modeling of electronic health information exchange," *J. Biomed. Informat.*, vol. 56, pp. 169–178, Aug. 2015.
[127] J. Gardner and L. Xiong, "HIDE: An integrated system for health information DE-identification," in *Proc. 21st IEEE Int. Symp. Comput.-Based Med. Syst.*, Jyvaskyla, Finland, 2008, pp. 254–259, doi: 10.1109/CBMS.2008.129.
[128] L. Chen and D. B. Hoang, "Novel data protection model in healthcare cloud," in *Proc. IEEE Int. Conf. High Perform. Comput. Commun.*, Sep. 2011, pp. 550–555, doi: 10.1109/HPCC.2011.148.
[129] *Ethereum*. Accessed: Jun. 24, 2020. [Online]. Available: https://Ethereum.org/en/
[130] *Hyperledger Fabric*. Accessed: Jun. 24, 2020. [Online]. Available: https://www.hyperledger.org/use/fabric
[131] *IBM Blockchain*. Accessed: Oct. 28, 2020. [Online]. Available: https://www.ibm.com/in-en/blockchain
[132] *MultiChain*. Accessed: Jun. 24, 2020. [Online]. Available: https://www.multichain.com/
[133] *Ripple*. Accessed: Jun. 24, 2020. [Online]. Available: https://ripple.com/?c1=GAW_SE_NW&source=INTL_BRND&cr2=search__-__intl__-__brandcrypto____exm&kw=ripple_cryptocurrency_exm&cr5=468798687342&cr7=c&utm_source=GAW_SE_NW_INTL_BRND&utm_medium=cpc&utm_campaign=search____intl____brandcrypto____exm&gclid=CjwKCAjw_Y_8BRBiEiwA5MCBJrYIurz1bJ9uDGL7X2Bt2WG4yYhsH72qdofwAe7TAGqmEX8gM8G69BoCBjgQAvD_BwE
[134] *R3*. Accessed: Jun. 24, 2020. [Online]. Available: https://www.r3.com/corda-platform/
[135] *Openchain*. Accessed: Jun. 24, 2020. [Online]. Available: https://blockchain.oodles.io/openchain-blockchain-solutions/
[136] *BTC Relay*. Accessed: Aug. 29, 2020. [Online]. Available: http://btcrelay.org/
[137] *Cosmos*. Accessed: May 7, 2021. [Online]. Available: https://cosmos.network/
[138] *Icon*. Accessed: May 7, 2021. [Online]. Available: https://iconrepublic.org/
[139] *Aion*. Accessed: May 7, 2021. [Online]. Available: https://mainnet.theoan.com/#/dashboard
[140] *Blocknet*. Accessed: May 7, 2021. [Online]. Available: https://blocknet.co/
[141] *Metronome*. Accessed: May 7, 2021. [Online]. Available: https://metronome.io/
[142] *Wanchain*. Accessed: May 7, 2021. [Online]. Available: https://www.wanchain.org/
[143] *Ark*. Accessed: May 7, 2021. [Online]. Available: https://ark.io/
[144] *Lamden*. Accessed: May 7, 2021. [Online]. Available: https://lamden.io/en/
[145] *Ethereum Whitepaper*. Accessed: Mar. 19, 2021. [Online]. Available: https://Ethereum.org/en/whitepaper/
[146] *Find a Wallet*. Accessed: Mar. 19, 2021. [Online]. Available: https://Ethereum.org/en/wallets/find-wallet/
[147] *Rinkeby Test Network*. Accessed: Mar. 19, 2021. [Online]. Available: https://rinkeby.etherscan.io/
[148] *Ropsten Test Network*. Accessed: Mar. 19, 2021. [Online]. Available: https://ropsten.etherscan.io/
[149] *Koven Test Network*. Accessed: Mar. 19, 2021. [Online]. Available: https://kovan.etherscan.io/
[150] *Goerli Test Network*. Accessed: Mar. 19, 2021. [Online]. Available: https://goerli.etherscan.io/
[151] *Etherscan*. Accessed: Mar. 19, 2021. [Online]. Available: https://etherscan.io/
[152] *What are Smart Contracts on Blockchain*. Accessed: Aug. 17, 2021. [Online]. Available: https://www.ibm.com/in-en/topics/smart-contracts
[153] *SOLIDITY*. Accessed: Aug. 17, 2021. [Online]. Available: https://soliditylang.org/
[154] *Integrated Development Environments (IDES)*. Accessed: Mar. 19, 2021. [Online]. Available: https://Ethereum.org/en/developers/docs/ides/#:~:text=Remix%20%2D%20Web%2Dbased%20IDE%20with,a%20test%20blockchain%20virtual%20machine.&text=EthFiddle%20%2D%20Web%2Dbased%20IDE%20that,and%20debug%20your%20smart%20contract
[155] *Web3.Js*. Accessed: Mar. 19, 2021. [Online]. Available: https://web3js.readthedocs.io/en/v1.3.4/
[156] *Mongo DB*. Accessed: Aug. 17, 2021. [Online]. Available: https://www.mongodb.com/
[157] *BASE64*. Accessed: Aug. 17, 2021. [Online]. Available: https://www.base64encode.org/
[158] *Keccak*. Accessed: Mar. 26, 2021. [Online]. Available: https://keccak.team/keccak.html

RAHUL GANPATRAO SONKAMBLE is currently pursuing the Ph.D. degree with the Department of Computer Science and Information Technology, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Lavale, Pune, Maharashtra, India. He is also an Assistant Professor in computer science and engineering with MIT ADT University, Pune. He is author of three books. He has published eight research papers and presented seven research papers in international journals and conferences, respectively. His research interest includes blockchain interoperability.

SHRADDHA P. PHANSALKAR received the Ph.D. degree from the Department of Computer Science and Information Technology, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Lavale, Pune, Maharashtra, India. She is currently a Professor with MIT ADT, Pune. She specializes in the area of distributed systems, cloud computing and blockchain, and DLT. She has published two book chapters, several research journal papers and presented few research papers in international conferences respectively. Her research interests include the area of blockchain in finance and healthcare, decentralization of machine learning, and federated machine learning in healthcare.

VIDYASAGAR M. POTDAR received the Ph.D. degree from Curtin University, Australia. He is currently the Director of the Blockchain Research and Development Laboratory, Curtin University. His articles have 3734 citations, with an H-index of 33 and an i10-index of 77. He has secured over $2 million dollars from industry and government for blockchain research. His research interests include blockchain and distributed ledgers, energy management & informatics, the Internet of Things, big data analytics and cybersecurity. He is a winner of eight research and commercialization awards. He is also the Guest Editor of the top journals like IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS (IF 7.377). He has received many research awards.

ANUPKUMAR M. BONGALE (Senior Member, IEEE) received the Ph.D. degree from Visvesvaraya Technological University (VTU), Belgaum, Karnataka, India. He is currently working as an Associate Professor with the Department of Computer Science and Information Technology, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Lavale, Pune, Maharashtra, India. He has filed a patent and has published book chapters. He also published several research articles in reputed international journals and conferences. His research interests include wireless sensor networks, machine learning, optimization techniques, and swarm intelligence.