BlockMed: AI Driven HL7-FHIR Translation with Blockchain-Based Security

Yonis Gulzar[1]*, Faheem Ahmad Reegu[2]*, Abdoh Jabbari[3], Rahul Ganpatrao Sonkamble[4], Mohammad Shuaib Mir[5], Arjumand Bano Soomro[6]

Department of Management Information Systems, College of Business Administration, King Faisal University, Al-Ahsa 31982, Saudi Arabia[1, 5, 6]

Department of Electrical and Electronics Engineering, College of Engineering and Computer Science, Jazan University, Jazan 45142, Saudi Arabia[2, 3]

Pimpri Chinchwad University, Pune, Maharashtra 412106, India[4]

***Abstract*—Blockchain is a peer-to-peer (P2P) network that distributes information and protects data integrity, security, and privacy. Constant simplification is required for information exchange. This comprehensive assessment seamlessly integrates Electronic Health Record (EHRs) with blockchain technology. EHRs are represented with different standards mainly HL7 and FHIR. EHR should be interpreted to both parties after exchange. Such interpretation after exchange may face few interoperable challenges. To overcome EHR interoperability difficulties, 18 blockchain-based alternatives were examined. Despite their promise, these systems have a variety of drawbacks, including reliability, privacy, data integrity, and collaborative sharing. Six phases make up the systematic review: research, investigation, article curation, keyword abstraction, data distillation, and project trajectory monitoring. In total, 18 seminal articles on EHR interoperability and Blockchain integration were identified. Many unique interoperability methods are proposed for Blockchain-integrated EHR systems in these contributions. Several Blockchain applications, standards, and issues associated with EHR interoperability are described and analyzed. Implemented and proposed blockchain-based EHR frameworks are numerous. The security aspects have been covered, but standards compliance and interoperability requirements are lacking. Research in this area is needed. This research study has analyzed the different national and international EHR standards. This paper describes the current state of EHRs, including blockchain-based implementations, along with the interoperability issues between existing blockchain-based EHR frameworks. The research has proposed novel BlockMed framework which is interoperable for the HL7 and FHIR EHR standards. BlockMed framework is evaluated with Data Accuracy, Mapping Quality, Response Time, Latency, Interoperability Coverage, AI Model Efficiency, Consent and Security Management, Cross-Chain Support, Patient and Provider Satisfaction.**

***Keywords*—Blockchain; health care; electronic health records (EHRs); interoperability; and healthcare system**

I. INTRODUCTION

Blockchain technology, characterized by its decentralized nature, fast transaction processing, high security, and privacy features, can significantly shift the traditional healthcare system. Significantly, it becomes a crucial facilitator in upholding the confidentiality and security of patient data. The potential of this technology to significantly transform the transmission and storage of patient's electronic health records is emphasized by its implementation of advanced security measures for the secure transfer of medical data within the healthcare industry, utilizing a robust stochastic. Blockchain technology enhances the level of robustness and security in the field of electronic health records EHRs. The potential impact of this technology on the healthcare industry is a shift towards prioritizing the needs and preferences of patients, as well as enhancing the security, transparency, and compatibility of health data [1]. The potential for a significant shift in health information exchange (HIE) is evident through enhanced efficiency and security in electronic health records EHRs. These repositories contain detailed patient information, including diagnostic and treatment procedures. It is crucial to acknowledge that patient data holds significant value within the healthcare domain, as it serves as essential material for examining healthcare. Electronic health records EHRs serve as stores for highly sensitive medical data, which justifies their classification as repositories for valuable patient insights. The widespread availability of healthcare data plays a crucial role in advancing national healthcare initiatives and improving quality-of-service delivery [2]. The EHR ecosystem is the culmination of a comprehensive and meticulously organized collection of patient health data distributed throughout many healthcare institutions and governmental health authorities [3].

EHRs are digital databases that store a person's whole health history. Medical clinics, institutes, and experts collect and manage this database. Electronic health records and EHRs face many challenges with semantic interpretability. Electronic healthcare systems are prone to cyberattacks, making security a major issue. Cyber-attack victims in healthcare systems make up one-third of all documented cases. Given these conditions, Blockchain technology's ability to establish shared trust and disseminate data could improve collaborative healthcare decisions in telemedicine and precision medicine [4]. As shown by the "Anthem breach attack," which compromised 80 million people's data on February 4, 2015, 88% of attacks target healthcare systems. Rapid growth in electronic health records and EHR databases creates another issue. Patient data, X-ray images, and computed tomography scans comprise the enormous corpus, which demands lots of storage. The average healthcare facility had 665 terabytes of storage in 2015, but by 2020, it had 25,000 petabytes. This storage effort focuses on unstructured medical images. Healthcare systems' variability in database management systems, architectural configurations, and

*Corresponding Author, Email ID: ygulzar@kfu.edu.sa; freegu@jazanu.edu.sa

data infrastructures presents another problem. Thus, inter-provider health data transmission must prioritize data integrity and uniformity [5]. Diversity makes transmitting correct, standardized information difficult and hinders its efficient deployment in relevant circumstances. The study covers the following:

The value of blockchain-based interoperability for EHRs.

Potential snags in integrating blockchain technology into EHRs systems.

The necessity of a blockchain-based system that can communicate with other networks.

Brief overview of the needs, issues, and potential solutions for interoperable EHR.

This article is divided into five sections. Section II reviews the research that specifically relates to blockchain's potential application in healthcare. The systematic review's research methods and procedures are outlined in Section III, and the answers to the review's research questions are presented in Section IV. In Section V of the paper, the findings and implications are provided.

II. Related Work

A. Blockchain

Blockchain, a decentralized system, has revolutionized Internet information sharing. This technology, created for financial applications, eliminates the need for transaction middlemen, including trustworthy third parties in government and business. TTP trustworthiness and authenticity may be damaged by malfunctions or security breaches, threatening the transactional framework. Blockchain is a peer-to-peer database with nodes, contracts, and blocks. In blockchain technology, data is kept in blocks. These blocks store and record numerous data kinds. However, nodes help blockchain network participants communicate and engage. Nodes relay data, transactions, and other information between places. Every node in this framework includes a block of localized data. After a contract is signed, transactions are authenticated [6] [7].

B. Blockchain Technology and Electronic Health Records

Resilience of blockchain-based applications has offered adequate support for the medical sector and medical infrastructure. The literature study presents several tools for interoperability aware EHR maintenance. Because EHRs can communicate, healthcare providers can change patient records using distributed ledger technology. Blockchain-based electronic health records are a cutting-edge method of tracking patients' medical histories and appointments [6].

By handling health insurance claims and refreshing authentications in the payments system, interoperable EHRs streamline the insurance system. Integrating blockchain technology into EHRs would help medical researchers and developers of diagnostic tools and drugs make more accurate statistical estimates from patient data. The significance of Blockchain is demonstrated through analyses of related research, practical examples, and novel approaches to securing data [8].

Removing the middleman from a distributed healthcare system causes a significant disruption in the current healthcare models. Data integrity, security, and privacy can be achieved using blockchain in EHR-based healthcare systems, which are difficult challenges in conventional healthcare systems [9].

Samala et al. explores the integration of blockchain technology in healthcare, focusing on data security, EHR privacy, and patient ownership. The authors argue that traditional EHR systems often lack patient-controlled data access, which blockchain can address by providing decentralized and secure data management. However, the study also notes challenges in scalability and the need for standardized protocols to ensure interoperability across different healthcare systems. A blockchain-based framework utilizing smart contracts to enhance the security and interoperability of EHRs[10]. The framework aims to provide secure data sharing among healthcare providers while maintaining patient privacy. Despite its potential, the study acknowledges challenges related to the integration of existing EHR systems and the computational overhead associated with smart contract execution. De Novi et al. discussed the transformative potential of blockchain technology in healthcare, particularly in enhancing patient identity management and public health data interoperability[11]. The authors highlight the synergy between blockchain, artificial intelligence, and digital twins in creating a more secure and interoperable healthcare ecosystem. However, they also point out the need for regulatory frameworks and the challenges of integrating blockchain with existing healthcare infrastructures[12]. Agbo et al. examines various blockchain-based EHR management systems, evaluating their effectiveness in ensuring data security and interoperability. The study identifies common challenges such as scalability issues, high energy consumption, and the complexity of integrating blockchain with current EHR systems [13]. The authors suggest that future research should focus on developing lightweight blockchain solutions and establishing universal interoperability. Researchers introduced MedBlock, a blockchain-based framework designed to enhance the privacy and interoperability of EHRs. The framework employs a permissioned blockchain and hybrid on-chain/off-chain storage to balance transparency with confidentiality[14]. The study demonstrates MedBlock's ability to achieve high transaction throughput with low latency, though it acknowledges challenges related to cross-blockchain interoperability and the integration with existing EHR systems. Ouaguid et al. analyze various approaches to integrating blockchain into the e-healthcare ecosystem, focusing on data management, security, scalability, and interoperability. The study highlights the advantages of blockchain in providing secure and decentralized data management but also points out limitations such as the incomplete representation of major stakeholders in the blockchain network and the lack of regulatory flexibility to ensure legal interoperability by country. Bathula et al. explores the convergence of blockchain and artificial intelligence in healthcare, addressing challenges in securing EHRs, ensuring data privacy, and facilitating secure data transmission [15]. The study provides a comprehensive analysis of the adoption of these technologies within healthcare, spotlighting their role in fortifying security and transparency. However, it also discusses challenges like data security, privacy, and decentralized computing, forming a robust tripod.

Agbeyangi et al. investigates the implementation of blockchain technology, specifically Hyperledger Fabric, for EHR management at Frere Hospital in South Africa. The study examines the benefits and challenges of integrating blockchain into healthcare information systems, highlighting the role of blockchain in transforming healthcare[16]. The findings underscore the transformative potential of blockchain technology in healthcare settings, fostering trust, security, and efficiency in the management of sensitive patient data. Guo et al. presents hybrid blockchain-edge architecture for managing EHRs with attribute-based cryptographic mechanisms. The architecture introduces a novel attribute-based signature aggregation scheme and multi-authority attribute-based encryption integrated with Paillier homomorphic encryption to protect patients' anonymity and safeguard their EHRs. The study shows that the performance meets real-world scenarios' requirements while safeguarding EHR and is robust against unauthorized retrievals. Building upon these existing studies, the following section details our systematic research approach to analyzing interoperability in blockchain-based EHR systems [17] [18].

III. Research Methodology

The systematic review follows a structured approach consisting of six key stages to ensure a thorough analysis of blockchain interoperability in Electronic Health Records (EHRs). These stages include formulating a query, conducting research, selecting relevant articles, developing a keyword list, extracting data, and mapping. The process was designed to rigorously evaluate existing literature, categorize solutions, and identify challenges in blockchain-based EHR interoperability.

A. Research Question Formulation

The research process began with the formulation of a focused research question aimed at identifying obstacles and solutions for achieving blockchain interoperability in EHR systems. This research question was critical for guiding the literature search and ensuring relevance, as it enabled a targeted approach in understanding the issues associated with blockchain applications in healthcare and evaluating potential solutions. To ensure rigor and relevance, articles were selected based on predefined inclusion and exclusion criteria:

1) Inclusion Criteria

a) Publication date: Only articles published after 2019 were included to reflect the latest advancements in blockchain technology for healthcare.

b) Relevance: Articles specifically addressing blockchain in healthcare with an emphasis on EHR interoperability, security, or data sharing frameworks were prioritized.

c) Language and accessibility: Only English-language articles available through academic databases were considered to maintain consistency and accessibility.

d) Peer-reviewed sources: Preference was given to studies from reputable, peer-reviewed journals and conferences, including IEEE, PubMed, and ScienceDirect, to ensure quality.

2) Exclusion Criteria

a) Lack of focus: Articles that discussed blockchain technology broadly without a focus on healthcare or EHR interoperability were excluded.

b) Inadequate data: Studies with limited sample sizes or weak methodological frameworks were omitted to maintain high research quality.

c) Outdated or duplicate research: Articles presenting redundant information or findings duplicated in more recent studies were excluded to avoid redundancy.

Each selected article was evaluated based on these criteria, allowing for a curated collection of relevant and high-quality studies. The graphical representation of inclusion and exclusion criteria has been presented in Fig. 1.

3) Quality assessment

3) Quality assessment: A systematic quality assessment was performed in the selected articles to ensure reliability. Articles were evaluated based on several metrics:

a) Methodological rigor: Each article's methodology was reviewed for clarity and robustness, with particular attention to research design, data collection methods, and analytical techniques.

b) Data Sources and sample size: Studies that utilized reliable data sources and larger sample sizes were given preference, as these factors increase the generalizability and credibility of findings.

c) Credibility of findings: Each study's conclusions were analyzed for coherence with existing literature and evaluated for clarity, consistency, and validity, ensuring that all sources provided well-substantiated insights.

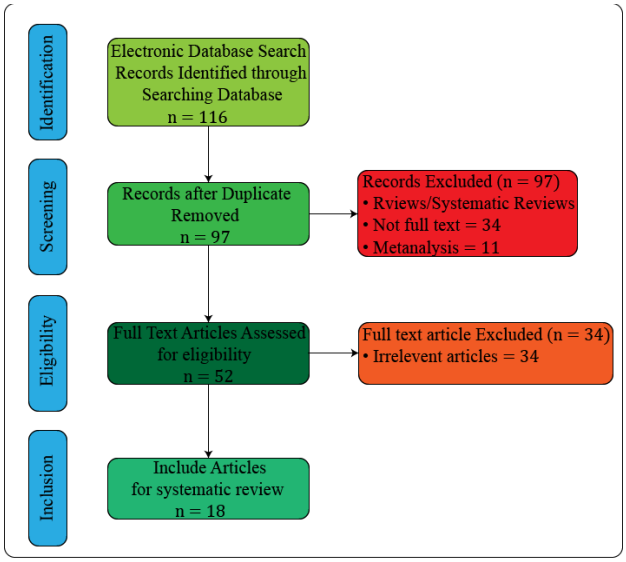

Fig. 1. Flowchart illustrating the criteria used to choose articles for systematic reviews.

4) Data extraction and mapping procedures

4) Data extraction and mapping procedures: Data extraction involved keyword-based searches for terms such as "blockchain," "EHR interoperability," "data privacy," and "healthcare security" across databases like IEEE, PubMed, and ScienceDirect. Using Atlas.ti software, the extracted data was mapped and organized, facilitating the thematic categorization

of research insights. This software-assisted approach streamlined the identification of common challenges, proposed solutions, and emerging trends in blockchain-based EHR interoperability. Atlas.ti further enhanced the efficiency of the data mapping process, allowing for a detailed comparison of various frameworks and solutions.

5) PRISMA flow diagram: To provide transparency in the article selection process, a PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) flow diagram was created. This diagram visualized each stage of the selection process, beginning with the total number of articles identified through database searches and progressing through the screening, inclusion, and exclusion phases. The flow diagram detailed the number of articles removed at each stage, along with reasons for exclusion (e.g., lack of relevance or inadequate data). By mapping the selection process, the PRISMA flow diagram enhanced transparency and ensured a systematic approach in curating the final articles included in the review.

6) Specifications and benchmarks: The review identified specific standards and benchmarks from the literature, highlighting the key interoperability requirements for blockchain-based EHR systems. Table I provides a summary of these benchmarks, including standards such as FHIR for data interchange, HL7 for cross-border data execution, and HIPAA for data privacy and security. These benchmarks were instrumental in categorizing the technical requirements necessary for a robust blockchain-based EHR system.

TABLE I. STANDARDS FOR DATA EXCHANGE

Ref	*Specifications*	*Benchmarks*
[19]	FHIR	Data Interchange
[13]	HL7	Transboundary execution
[20]	HITECH	Metamorphosis
[21]	PHR	Data transmission through APIs
[22]	Open EHRs	Protocol conformity
[23]	DICOM	Safety measures
[24]	SNOMED CT	Harmonious operability
[25]	CEN/ISO EN13606	Confidentiality and safeguarding
	HIPAA	Privacy and data uniformity

Bibliometric analysis was employed to deepen the understanding of blockchain-based EHR interoperability research. By using VOSviewer software, the frequency of author citations, keyword occurrences, and term co-occurrences within the literature was analyzed. The bibliometric analysis also identified collaborative relationships between authors and institutions from different countries, illustrating the global interest in blockchain technology for healthcare interoperability. This systematic methodology provides a solid foundation for evaluating the literature on blockchain-based EHR interoperability. By following a structured approach for article selection, quality assessment, and data mapping, this review ensures that only high-quality, relevant studies inform the analysis. The use of bibliometric analysis and standardized benchmarks further supports a comprehensive understanding of the current challenges and potential solutions in the field.

IV. RESULTS AND DISCUSSION

This section presents the systematic review's results. 116 research articles were pulled for the following search technique from multiple sources. After removing the duplicate records using the first selection procedure, 97 articles were chosen. The removed articles had nothing to do with how EHRs and blockchain's interacted. To streamline the selection process, the chosen articles underwent additional scrutiny. Implementing exclusion criteria resulted in removing 45 articles from the original 97 items. The papers eliminated during screening lacked full text and were therefore ineligible for the meta-analysis. 52 additional publications were checked to see if they qualified for the systematic review. 34 irrelevant items were eliminated from the list of chosen articles throughout the eligibility selection process. To complete the systematic review of Blockchain-based Electronic Health Records 18 publications must meet all the criteria.

These chosen articles are utilized to delineate the requirements and obstacles associated with achieving interoperable EHRs utilizing blockchain technology. The study's inquiries are outlined as follows:

Q1. How can Blockchain-based electronic health records (EHRs) be made interoperable?

Q2. In a Blockchain context, what are the interoperable standards for EHRs look like?

Q3. How does the blockchain-based framework enable EHR exchange between different hospitals using different EHR standards?

A. Q1. How can Blockchain-Based Electronic Health Records (EHRs) be made Interoperable?

The comprehensive literature analysis in this study found three degrees of blockchain-based EHR interoperability criteria. Protocols, standards, and the exchange and management of data across platforms are essential in the technology industry. Patient data privacy and security must be built into the legal and organizational interoperability norms for blockchain-based electronic health records (EHRs). The economic model and partnerships between public and private healthcare organizations are also considered.

The standards specify the variety of protocols for transmitting messages and health data. A solid business plan and knowledge-sharing system are needed to implement the approach at the organizational level. Data standards that ensure data integrity and adaptability are needed to share medical information efficiently. As shown in Table II, interoperability among EHR systems built on blockchain is essential for seamless data exchange. Blockchain-based EHRs offer advantages in filing exact health insurance claims due to their uniform implementation. Data mapping standards must be established and followed to efficiently move data among entities with different ownerships. Federal organizations can more efficiently manipulate health service provider data using logical models and computer language features. Blockchain systems need semantic consistency. Standardized coding procedures improve EHR security. Betek et al. identified blockchain-based EHR needs. These needs included reliable data gathering and

effective EHR-medical researcher information sharing. These requirements are aimed at improving healthcare system administration and reliability. Electronic Health Records (EHRs) compliance with Blockchain technology requires a framework for secure and structured encrypted communication among various systems. Additionally, stakeholders must be able to decrypt these messages. This can be done by setting message standards, values, and technological databases according to norms. Increased collaboration between manufacturers, corporations, researchers, and medical institutions can help meet privacy and security standards. A complete structure of legislation and norms enabling healthcare professionals and patients to communicate data is necessary to protect patient privacy. Blockchain technology secures insurance and incentives for public and private health service organizations, protecting data. To efficiently implement and use EHRs. When systems and organizations share health information, legal frameworks are needed to maintain data integrity. Systems and organizations must build legal frameworks to share information securely.

1) Semantic and technological requirements for blockchain-based EHR interoperability: Interoperable Blockchain-based Electronic Health Record (EHR) systems require specific semantic standards to ensure seamless communication across healthcare networks. Key semantic demands include common practices and methods for data exchange, ensuring data integrity remains unquestionable, and a dictionary of standardized data and communication protocols. Additionally, guidelines for the structured collection and exchange of information are crucial to maintain uniformity across systems. These semantic standards enable various EHR systems to "speak the same language," thus supporting accurate, meaningful data transfer and interpretation [26].

From a technological perspective, interoperable Blockchain-based EHRs must meet specific technical prerequisites to function effectively. These include standards for plug-and-play interoperability of services, permitted types of information and data formats, and data encoding specifications to secure both the production and transmission of data. Furthermore, protocols for safe data transmission are essential to protect sensitive health information during exchanges. Adhering to these technological standards ensures that Blockchain-based EHRs can securely and efficiently exchange data within an interoperable framework [27].

TABLE II. NEED FOR INTEROPERABILITY AMONGST EHR SYSTEMS BUILT ON THE BLOCKCHAIN

Requirements		
Conceptual (syntactic and semantic)	**Technological**	**Organizational and (Legal)**
Agreed vocabulary for messages and clinical documents. Common terminologies and information models for advanced messages	Signal, protocol, and technological plug-and-play compatibility	Fundamentals of doing business collaboration between companies to facilitate the exchange of information
For data accuracy, use standard terms	The seamless exchange of health data is essential for providing adequate healthcare	
To assess the discrepancies, data element mapping to the common terminology	Logical models developed without regard to platform or programming language limitations	Federally mandated program data reporting burden reduced
Integrity of meaning	Coding standard technical concerns need to be resolved	Protecting the confidentiality of medical records
Obtaining a shared dataset Collect the doctors' agreement on the dataset	Strong technical standards for sharing health information throughout institutions	An effective healthcare informatics group capable of handling all tasks Professionals in the healthcare industry coming together to reach an agreement on a particular project
Ability of structured message transmission between two or more systems The capacity to comprehend and use a sent message Creating a well-chosen vocabulary	Define data items, rules, values, and formats Agree on technical data models for database management systems	The collaboration of informaticists, vendors of EHRs, and clinicians in the industry
Information from the exchange Identification of healthcare professionals and patients	Reporting clinical data securely and in a timely manner	Partnerships between public-private entities and government incentives have been adopted more widely
There should be no ambiguity in the data for transmitting systems	Multiple systems exchange data to take action based on what they've learned	ensuring that organizations function under various legal regimes

2) Organizational and legal prerequisites for interoperable blockchain-based EHRs: The successful implementation of interoperable Blockchain-based EHRs also requires certain organizational and legal prerequisites. Collaboration between EHR vendors and healthcare providers is vital, as it enables the development of shared business models that facilitate information exchange. Furthermore, organizations must engage experts who specialize in maintaining the privacy of shared information, as privacy and security are central to handling health data on a Blockchain. Access to data related to insurance and incentive programs is also essential, as it helps create a supportive environment for interoperability while ensuring compliance with relevant policies and regulations. These organizational and legal prerequisites form the foundation for a sustainable and secure interoperable EHR ecosystem [28].

B. Q.2 In a Blockchain Context, What are the Interoperable Standards for EHRs look like?

Table III details the requirements for interoperability between various Blockchain-based EHR applications. The study's authors studied different methods for EHR sharing, security, and interoperability. Several norms are being implemented to make it easier for healthcare providers to employ solutions built on the Blockchain [29][30].

TABLE III. AN EHR INTEROPERABILITY STANDARD BASED ON BLOCKCHAIN TECHNOLOGY

Block-Chain Based Standard Available	Description
FHIR	Data attributes are contained in an HL7-based resource. Adherence to FHIR for Information Exchange standards
HL7	A developing standard based on FHIR. Robust operation on mobile devices.
HITECH	MIPS, HER certification, interoperability, and healthcare system transformation
PHR	HL7 was utilized for tethering and quick data exchange. Interchangeability of PHR and EHIR via APIs.
Open EHR	EHR is developed using open-source components. Clinical deployments that validate EHR standards.
DICOM	Secure transmission of health records and medical images. APIs for integrating various health systems.
SNOMED CT	EHRs' current clinical procedures. Consistency, interoperability, and accuracy.
CEN/ISO EN13606	Semantic guidelines for the exchange of EHR information. Standards of privacy and security for interface access.
HIPAA	Security requirements for patient data privacy. EHR interoperable system with confidence

When thinking about harmonization, it is essential to find the standard that is most compatible with other standards. This is demonstrated by Tables III and IV, further substantiating the superior interoperability qualities of HL7 and FHIR.

TABLE IV. CHARACTERISTICS OF BLOCKCHAIN-DRIVEN EHR STANDARDS

Properties	CEN-13606	CEN	Open-EHRs	HL7	HITECH	DICOM	FHIR
The Better-Workflow	Y	M	Y	Y	Y	M	Y
Reduced-Ambiguity	M	Y	Y	Y	M	Y	Y
Better Quality-of-Care	Y	M	M	Y	Y	Y	Y
In terms of Reliability	M	Y	Y	Y	M	M	Y
The Information-security	M	M	Y	Y	Y	M	Y
Security and the Privacy	M	Y	M	Y	Y	Y	Y

*M-Moderate, Y- Yes

C. Q3. How does the Blockchain-Based Framework Enable EHR Exchange Between Different Hospitals Using Different EHR Standards?

1) Interoperable blockchain-based EHR framework: BCIF-EHR: The BCIF-EHR framework is designed to enable seamless interoperability between healthcare providers, utilizing blockchain technology, HL7 and FHIR standards, and AI-driven data mapping to securely share EHR between hospitals. Below is a breakdown of each component in this framework and how they interact. The block diagram of EHR and standards in presented in Fig. 2.

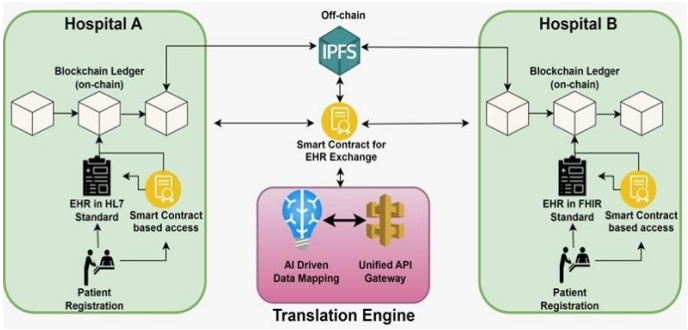

Fig. 2. Blockchain-based interoperable EHR system architecture (BCIF-EHR).

a) Patient registration: When a patient whose EHR system uses the HL7 standard, registers at Hospital A, their information (such as demographics and IDs) is captured in an

HL7 message format. This data flows through the AI-driven data mapping layer in the unified API gateway, which transforms the HL7 message into FHIR resources. This translation ensures that the patient's data can be compatible across different EHR systems.

b) Consent management using blockchain technology: Once the patient agrees to allow other hospitals to access their EHR, the blockchain-based consent management system records this consent immutably. Only authorized entities can access the data, with all data exchanges facilitated securely via HL7 and FHIR protocols.

c) Data exchange request from another hospital: When Hospital B requests access to the patient's medical history from Hospital A (using FHIR-based EHR), the unified API gateway handles the request. The gateway converts the request into an HL7-compliant query, and the AI-driven data mapping layer matches the necessary data fields, ensuring the request aligns with the HL7 structure.

d) Translation engine: The translation engine is an important component who is responsible for providing the interoperability between HL7 and FHIR. Interoperability between these standards will be by AI driven data mapping.

e) Interoperability platform for data processing and storage: After the request, Hospital A's HL7-based EHR sends the relevant data to a interoperability platform. This platform processes the data, ensuring it adheres to both HL7 and FHIR standards, stores it securely, and makes it accessible as FHIR resources.

f) Decentralized IPFS storage: For larger datasets, such as genomic data or medical images, decentralized storage through IPFS (Interplanetary File System) is used. Hospital B can retrieve this data through hash pointers in the FHIR resource, which link to the data stored in IPFS.

g) Data validation and smart contracts for EHR exchange: Before data is transmitted to Hospital B, a data validation process checks compliance with HL7 and FHIR standards. Smart contracts enforce the terms of data exchange, including patient consent, ensuring the conditions are met before the EHR data is shared.

h) Cross-chain support for multi-standard systems: If the patient visits a new healthcare provider that uses blockchain-enabled EHR, cross-chain support enables seamless data transfer across different blockchain networks. This component ensures interoperability across varied healthcare standards.

i) Patient data retrieval and update: When Hospital B receives the patient's data, it can retrieve and integrate it into its FHIR-based EHR system. Any updates made by Hospital B, such as test results, are converted back into HL7 format for Hospital A, ensuring both systems remain synchronized.

j) Secure logging and audit trail: Every transaction and data exchange is securely logged on the blockchain, creating an audit trail that medical professionals can monitor. This ensures data transparency, security, and traceability, reinforcing the trustworthiness of data sharing. Pseudo code of the Algorithm for Patient Registration (HL7 to FHIR) is presented below:

Pseudo code of PatientRegistrationHL7 to FHIR(HL7Message) Algorithm

Input:	***HL7Message***
Output:	***FHIRResource***
Step 1:	HL7Message ← CapturePatientRegistrationDetails()
Step 2:	APIService ← UnifiedAPIGateway(HL7Message)
Step 3:	MappingLayer ← AIDrivenDataMapping(APIService) HL7Segments ← ExtractSegments(HL7Message, ["PID", "OBX", "PV1"])
Step 4:	FHIRMapping ← MapHL7toFHIR(HL7Segments)
Step 5:	FHIRData ← TransformHL7toFHIR(FHIRMapping) FHIRResource ← CreateFHIRResource(FHIRData,
Step 6:	resourceType="Patient") isValid ← ValidateFHIRResource(FHIRResource) If isValid == False then RaiseError("FHIR resource validation failed")
Step 7:	Exit StoreFHIRResource(FHIRResource, InteroperabilityPlatform) ShareFHIRResource(FHIRResource, AuthorizedEntities) Return FHIRResource
	End Algorithm

D. Performance Evaluation Measures

1) Data accuracy and mapping quality: Data accuracy and mapping quality are fundamental for preserving the integrity of health information as it is transferred between healthcare systems, specifically when converting data between HL7 and FHIR standards. High data accuracy ensures that the information remains correct, up-to-date, and relevant, which is essential for providing reliable patient care and enabling informed decisions by healthcare professionals. Mapping quality assesses the effectiveness of data translation between these standards, maintaining platform integrity and reducing errors. The AI-driven data mapping enhances this quality by minimizing inaccuracies and data loss. As illustrated in Fig. 3, the mapping accuracy rate stands at an impressive 99.5%, with only a marginal inaccuracy of 0.2%, reflecting the robustness of data translation across these standards. Furthermore, the data loss rate remains low, averaging around 1.2%, which may be attributed to issues like unsupported fields or technical challenges that occasionally lead to minor data losses. Consistence in data translation is also high, with a consistency rate of 98.9% across multiple translation cycles, underscoring the system's ability to maintain stable data integrity throughout the mapping process.

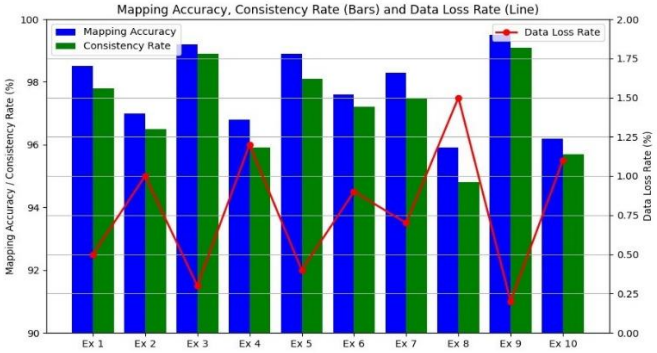

Fig. 3. Comparison of mapping accuracy, consistency rate, and data loss.

2) Response time and latency: Response time, particularly in healthcare environments, is critical for real-time access to

patient data. This measure is evaluated through both average latency and peak load latency, as shown in Fig. 4. Average latency is consistently around 150 milliseconds, which supports the need for rapid data access and retrieval, essential in emergency scenarios where every second counts. Under high transaction loads, the peak load latency reaches about 325 milliseconds, demonstrating the system's ability to perform efficiently even under heavy demand. This stability in latency ensures that the system remains responsive and reliable, which is vital for healthcare professionals who rely on timely data for patient care.

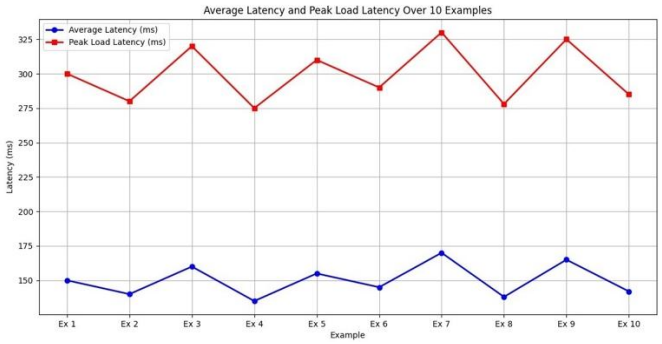

Fig. 4. Average latency and peak load latency across 10 samples.

3) Interoperability coverage: Interoperability coverage, depicted in Fig. 5, assesses the system's ability to handle various HL7 and FHIR standards, such as HL7 v2, v3, and FHIR versions like DSTU2, STU3, and R4. Effective interoperability is essential for consistent communication across diverse healthcare providers and systems, supporting seamless information exchange. The system achieves a high standard compliance rate, with close to 96% of HL7 and FHIR features supported. This high level of compliance ensures that the system adheres to established healthcare data standards, which is critical for effective data interoperability. Additionally, the system maintains a cross-version compatibility rate above 92%, indicating its flexibility to handle both older and newer versions of healthcare standards, a necessary feature for consistent data exchange across different platforms and systems.

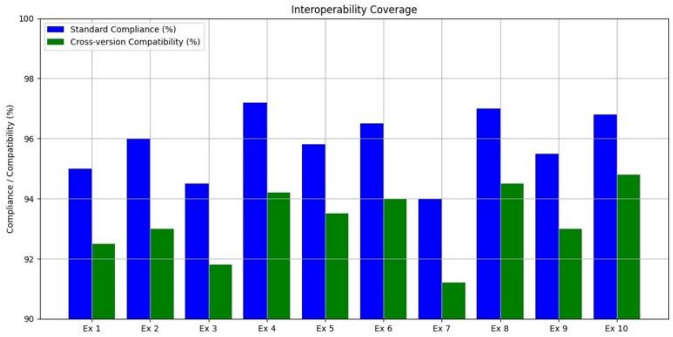

Fig. 5. Interoperabil*ity coverage*.

E. AI Model Efficiency

AI model efficiency plays a crucial role in system performance, affecting mapping speed, training time, and error rates. Fig. 6 provides insights into these metrics, where the AI model's mapping speed ranges from 330 to 370 milliseconds, enabling timely data processing in real-time healthcare environments. Training times for the AI model vary between 24 and 29 seconds, which supports quick model updates and adaptation to evolving data formats. The model error rate is low, around 2%, indicating high accuracy in data mapping with minimal errors. This low error rate is essential for maintaining data integrity across standards, ensuring that the AI-driven mapping layer performs reliably in a healthcare setting.

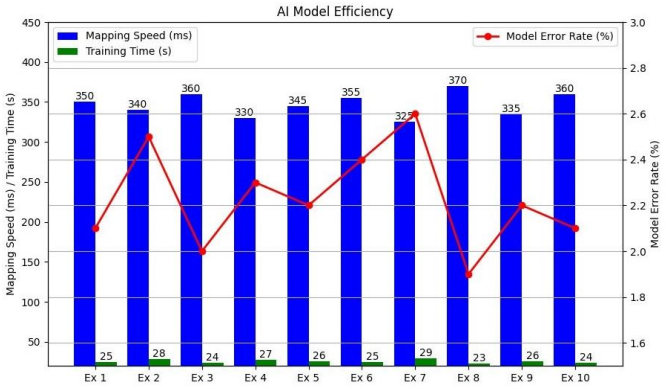

Fig. 6. AI model mapping speed and training time.

F. Consent and Security Management

Consent and security management are essential for safeguarding patient data during exchange.

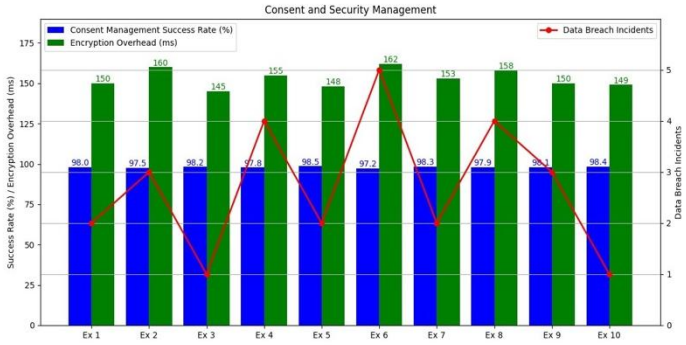

Fig. 7. Consent management success rate and encryption overhead.

Fig. 7 illustrates key metrics related to consent management success rate, encryption overhead, and data breach incidents. Consent management is consistently high, with success rates around 98%, ensuring that patient consent preferences are respected, and only authorized personnel can access sensitive data. Encryption overhead, which varies from 145 to 162 milliseconds, balances data security without causing significant delays, maintaining a secure and efficient data exchange process. The frequency of data breach incidents is minimal, indicating strong access control measures and robust security protocols that protect patient data and support compliance with privacy regulations.

G. Cross-Chain Support Evaluation

Cross-chain support evaluation, depicted in Fig. 8, enables seamless data exchanges across blockchain networks, which is essential for interoperability in multi-network environments.

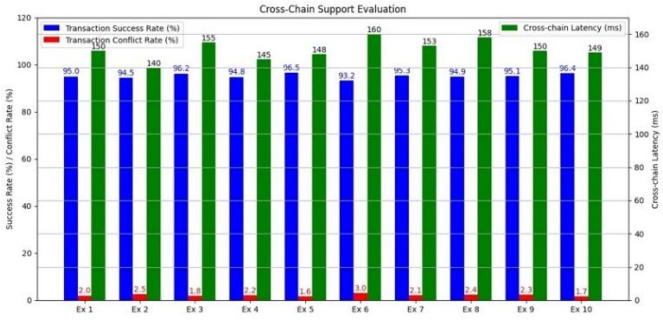

Fig. 8. Transaction success rate, conflict rate, and latency.

The system demonstrates a high cross-chain transaction success rate of approximately 95%, ensuring reliable interactions across different blockchain systems. The transaction conflict rate remains low, under 3%, indicating smooth data flow with minimal errors in cross-chain communication. Cross-chain latency averages around 150 milliseconds, allowing quick data access across blockchain networks and minimizing delays for healthcare providers requiring patient information from various sources.

H. Patient and Provider Satisfaction

Patient and provider satisfaction metrics, shown in Figure 9, provide insights into the system's usability, efficiency, and reliability from the perspective of end-users. High satisfaction scores indicate positive feedback from both patients and providers, reinforcing the system's effectiveness in real-world healthcare settings. Patient satisfaction scores range between 4 and 5 on a 5-point scale, reflecting a favorable view of the system's accessibility, data privacy, and ease of data retrieval. Provider satisfaction scores range from 3.5 to 4.5, suggesting that healthcare providers find the system beneficial for workflow efficiency, data accuracy, and accessibility, which enhances their productivity and decision-making capabilities.

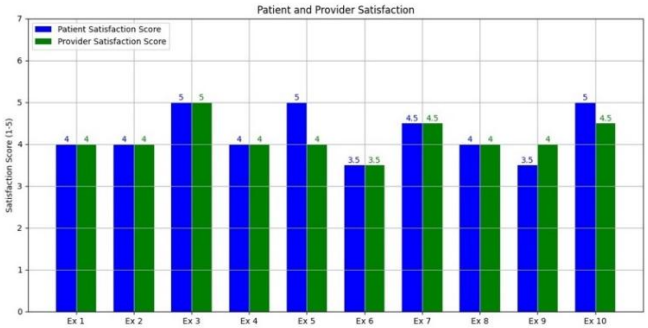

Fig. 9. Patient and service provider success score.

V. Conclusion and Future Work

This study demonstrates the potential of blockchain technology to address critical challenges in EHR interoperability by enhancing data security, privacy, and accessibility. The proposed blockchain-based framework BlockMed provides secure EHR exchange with translation of the standards i.e HL7 and FHIR using AI module. It is a decentralized approach to EHR management, ensuring compliance with contemporary standards and regulatory requirements like HIPAA while giving patients control over their own data. The integration of smart contracts further enhances the system by enforcing data sharing rules and maintaining accessibility without compromising privacy and data integrity. The BlockMed is proven to be secure and efficient after evaluation with the metrics i.e. Data Accuracy, Mapping Quality, Response Time, Latency, Interoperability Coverage, AI Model Efficiency, Consent and Security Management, Cross-Chain Support, Patient and Provider Satisfaction.

Despite these advancements, the real-world implementation of interoperable blockchain-based EHR systems remains limited, with few existing solutions that offer seamless data exchange across diverse healthcare platforms. This research contributes a foundational framework that can be expanded to develop scalable, interoperable EHR systems that meet the evolving needs of the healthcare industry. Future work should focus on real-world applications, addressing scalability issues, refining cross-chain support, and improving system performance under heavy data loads.

Overall, the study presents a promising path forward in the healthcare sector, leveraging blockchain to ensure secure, efficient, and interoperable EHR systems that can evolve with technological and regulatory developments. Further research and collaboration with healthcare providers and policymakers will be essential to fully realize the benefits of blockchain-based EHR interoperability. This study contributes a framework for blockchain-based EHR interoperability that adheres to HIPAA and HL7 standards, facilitating secure, cross-institutional patient data exchange. Future research should explore AI-driven data mapping to enhance translation accuracy between HL7 and FHIR standards and investigate cross-chain solutions to support data portability.

Acknowledgment

This work was supported by the Deanship of Scientific Research, the Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia under project KFU250655.

References

[1] F. A. Reegu, W. A. Bhat, A. Ahmad, and M. Z. Alam, "A review of importance of blockchain in IOT security," in AIP Conference Proceedings, 2023, vol. 2587, no. 1.

[2] A. A. Dar, F. A. Reegu, and G. Hussain, "Comprehensive Analysis of Enterprise Blockchain: Hyperledger Fabric/Corda/Quorom: Three Different Distributed Leger Technologies for Business BT - Mobile Radio Communications and 5G Networks," 2024, pp. 383–395.

[3] F. A. Reegu, S. Ayoub, A. A. Dar, G. Hussain, Y. Gulzar, and U. Fatima, "Building Trust: IoT Security and Blockchain Integration," in 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), 2024, pp. 1429–1434, doi: 10.23919/INDIACom61295.2024.10499070.

[4] A. A. Dar, F. A. Reegu, S. Ahmed, and G. Hussain, "Blockchain Technology and Artificial Intelligence based Integrated Framework for Sustainable Supply Chain Management System," in 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), 2024, pp. 1392–1397, doi: 10.23919/INDIACom61295.2024.10498149.

[5] A. A. Dar, F. A. Reegu, S. Ahmed, and G. Hussain, "Strategic Security Audit Protocol: Safeguarding Smart Home IoT Devices against Vulnerabilities," in 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), 2024, pp. 1386–1391, doi: 10.23919/INDIACom61295.2024.10498906.

[6] M. Z. Alam, F. Reegu, A. A. Dar, and W. A. Bhat, "Recent Privacy and Security Issues in Internet of Things Network Layer: A Systematic Review," Int. Conf. Sustain. Comput. Data Commun. Syst. ICSCDS 2022 - Proc., no. October, pp. 1025–1031, 2022, doi: 10.1109/ICSCDS53736.2022.9760927.

[7] A. A. Dar, M. Z. Alam, A. Ahmad, F. A. Reegu, and S. A. Rahin, "Blockchain Framework for Secure COVID-19 Pandemic Data Handling and Protection," Comput. Intell. Neurosci., vol. 2022, p. 7025485, 2022, doi: 10.1155/2022/7025485.

[8] X. Zhou, J. Liu, Q. Wu, and Z. Zhang, "Privacy Preservation for Outsourced Medical Data with Flexible Access Control," IEEE Access, vol. 6, pp. 14827–14841, 2018, doi: 10.1109/ACCESS.2018.2810243.

[9] M. English, S. Auer, and J. Domingue, "Block Chain Technologies & The Semantic Web : A Framework for Symbiotic Development," Comput. Sci. Conf. Univ. Bonn Students, pp. 47–61, 2016, doi: 10.1111/j.1364-3703.2010.00667.x.

[10] M. Al-Shabi and A. Al-Qarafi, "Improving blockchain security for the internet of things: challenges and solutions," Int. J. Electr. Comput. Eng., vol. 12, no. 5, pp. 5619–5629, 2022, doi: 10.11591/ijece.v12i5.pp5619-5629.

[11] M. Samaniego and R. Deters, "Blockchain as a Service for IoT," Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016, no. January 2020, pp. 433–436, 2017, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102.

[12] T. Alam, "Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges," Computers, vol. 12, no. 1, 2023, doi: 10.3390/computers12010006.

[13] G. Carter, H. Shahriar, and S. Sneha, "Blockchain-based interoperable electronic health record sharing framework," Proc. - Int. Comput. Softw. Appl. Conf., vol. 2, pp. 452–457, 2019, doi: 10.1109/COMPSAC.2019.10248.

[14] E. Lee, Y. Yoon, G. M. Lee, and T. W. Um, "Blockchain-based perfect sharing project platform based on the proof of atomicity consensus algorithm," Teh. Vjesn., vol. 27, no. 4, pp. 1244–1253, 2020, doi: 10.17559/TV-20200218052217.

[15] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," Expert Syst. Appl., vol. 154, 2020, doi: 10.1016/j.eswa.2020.113385.

[16] F. Bizzaro, M. Conti, and M. S. Pini, "Proof of Evolution: Leveraging blockchain mining for a cooperative execution of Genetic Algorithms," Proc. - 2020 IEEE Int. Conf. Blockchain, Blockchain 2020, pp. 450–455, 2020, doi: 10.1109/Blockchain50366.2020.00065.

[17] M. Du, Q. Chen, and X. Ma, "MBFT: A New Consensus Algorithm for Consortium Blockchain," IEEE Access, vol. 8, pp. 87665–87675, 2020, doi: 10.1109/ACCESS.2020.2993759.

[18] X. Fu, H. Wang, and P. Shi, "A survey of Blockchain consensus algorithms: mechanism, design and applications," Sci. China Inf. Sci., vol. 64, no. 2, pp. 1–15, 2021, doi: 10.1007/s11432-019-2790-1.

[19] F. M. Bublitz et al., "Disruptive technologies for environment and health research: An overview of artificial intelligence, blockchain, and internet of things," Int. J. Environ. Res. Public Health, vol. 16, no. 20, pp. 1–24, 2019, doi: 10.3390/ijerph16203847.

[20] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology," 2017.

[21] C. Mcfarlane, M. Beer, J. Brown, and N. Prendergast, "Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1.0," 2017.

[22] [A. Hossain, R. Quaresma, and H. Rahman, "Investigating factors influencing the physicians' adoption of electronic health record (EHR) in healthcare system of Bangladesh: An empirical study," Int. J. Inf. Manage., vol. 44, no. September 2018, pp. 76–87, 2019, doi: 10.1016/j.ijinfomgt.2018.09.016.

[23] F. A. Reegu et al., "Systematic Assessment of the Interoperability Requirements and Challenges of Secure Blockchain-Based Electronic Health Records," Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/1953723.

[24] R. Saripalle, C. Runyan, and M. Russell, "Using HL7 FHIR to achieve interoperability in patient health record," J. Biomed. Inform., vol. 94, p. 103188, Jun. 2019, doi: 10.1016/j.jbi.2019.103188.

[25] M. Farhadi, H. Haddad, and H. Shahriar, "Compliance Checking of Open Source EHR Applications for HIPAA and ONC Security and Privacy Requirements," pp. 704–713, 2019, doi: 10.1109/COMPSAC.2019.00106.

[26] Reegu Faheem, Zada Khan Wazir, Mohd Daud Salwani, Arshad Quratulain, and Armi Nasrullah, "A Reliable Public Safety Framework for Industrial Internet of Things (IIoT)," Proceeding - 2020 Int. Conf. Radar, Antenna, Microwave, Electron. Telecommun. ICRAMET 2020, pp. 189–193, Nov. 2020, doi: 10.1109/ICRAMET51080.2020.9298690.

[27] T. R. Vance and A. Vance, "Cybersecurity in the Blockchain Era," pp. 107–112, 2019.

[28] S. Niu, L. Chen, J. Wang, and F. Yu, "Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain," IEEE Access, vol. 8, pp. 7195–7204, 2020, doi: 10.1109/ACCESS.2019.2959044.

[29] N. Andola, Raghav, S. Prakash, S. Venkatesan, and S. Verma, "SHEMB: A secure approach for healthcare management system using blockchain," 2019 IEEE Conf. Inf. Commun. Technol. CICT 2019, 2019, doi: 10.1109/CICT48419.2019.9066237.

[30] S. Ayoub, Y. Gulzar, F. A. Reegu, and S. Turaev, Generating Image Captions Using Bahdanau Attention Mechanism and Transfer Learning, Symmetry (Basel)., vol. 14, no. 12, 2022, doi: 10.3390/sym14122681.