Homomorphic Encryption-Based Secure Medical Record Sharing in Cloud

Kusum Yadav[1], Salman Mahmood Salman[2], Raghad Saad Majeed[3] and Sabah M. Kallow[4]
[1]College of Computer Science and Engineering, University of Hail, 81422 Hail, Kingdom of Saudi Arabia
[2]Al-Turath University, 10013 Baghdad, Iraq
[3]Medical Technical College, Al-Farahidi University, 10065 Baghdad, Iraq
[4]Department of Computer Engineering, College of Engineering, Al-Mansour University College, 10001 Baghdad, Iraq
y.kusum@uoh.edu.sa, salman.mahmood@uoturath.edu.iq, raghad.saad@life-rdh.org, sabah.kallow@muc.edu.iq

Keywords: Homomorphic Encryption, Secure Medical Record Sharing, Blockchain, Privacy-Preserving Analytics, Electronic Health Records, Cloud Security, BFV, CKKS, Paillier.

Abstract: The recent trend of using cloud solutions to support electronic health records (EHRs) poses some serious questions about the confidentiality, integrity and compliance with the regulations. Classical encryption methods secure data at rest but introduce vulnerability at computation and are therefore not suitable in sensitive healthcare applications. This paper suggests a homomorphic encryption (HE)-based scheme through which medical records may be shared and analyzed safely on encrypted information. The system combines HE with blockchain to provide an end-to-end privacy, immutability, and auditability of patient records. BFV is used in structured features to work with the exact arithmetic, approximate real-number analytics with CKKS, and lightweight sums with Paillier. Functional correctness is proven with low error margins through experimental validation and manageable overhead is proven by performance evaluation in terms of encryption latency, query time, and storage. Compared to AES-at-rest and trusted execution environments, the benchmarking reveals that it does a better job of protecting privacy at a higher computational cost. Scalability analysis also further confirms applicability to large scale healthcare data. The framework is consistent with GDPR, HIPAA, and India DPDP Act, which provides a regulation-friendly framework to achieve secure sharing of EHRs.

1 INTRODUCTION

The role played by the adoption of cloud computing in health care is the fact that it has changed the way electronic health records (EHRs) are managed and accessed. Clouds are both scaling and cost efficient and are available everywhere, yet on the other hand, they present a serious security risk to sensitive patient information by exposing it to high risks of breaches, unauthorized access and misuse. Such environments demand sophisticated privacy preserving structures to maintain the confidentiality and regulatory compliance. Traditionally, technology acceptance models have provided the evolution of digital infrastructures to user-based requirements as in pioneering research on digital libraries by Nguyen and Wiese (2003) [1]. On this basis, now there exist more formidable cryptography and distributed computing solutions required by healthcare systems to provide security in storage and sharing of medical information.

Homomorphic encryption (HE) has become an innovative method that enables the computations to be done on the encrypted data avoiding the process of decryption. This feature comes in handy especially with cloud-hosted EHRs where medical practitioners and researchers are frequently required to process patient data without invading their privacy. The latest models have integrated HE with blockchain to overcome the issues of data authenticity and integrity. An example can be seen through Ali et al. (2023) [2] that suggested a blockchain-based version of HealthLock, a framework that incorporates homomorphic encryption in the context of Internet of Things (IoT) healthcare, that can ensure a high level of privacy. Likewise, Scheibner et al. (2022) [3]

discussed the ethical and legal considerations of integrating HE and distributed ledger technologies, which contributes to the necessity of making certain regulatory adjustments to the adoption of such systems.

Privacy computing systems have been expanded to allow safe data aggregation and analytics at the system level. The PMHE presented by Zhao et al. (2022) [4] is a wearable medical sensor-assisted architecture that involves the use of blockchain and privacy computing to access secure cloud health services. Their model emphasizes the possibility of HE to safeguard sensitive health data on real-time sensor settings. The research in Kumar et al. (2022) [5] additionally extended this research, implementing HE and blockchain in privacy-preserving model aggregation in medical imaging, allowing collaborative deep learning and doesn't affecting the confidentiality of data. These contributions provide an overview of how HE is capable of securing both unstructured and structured medical data in different healthcare applications.

Along with such encouraging developments, there are a number of challenges. A recent general survey conducted by Lee et al. (2025) [6] emphasized the advantages of HE and said it lacked in the areas of computational load, leakage of query patterns, and scalability to large-scale deployments. In addition, the connection of artificial intelligence and cloud realms of security places both opportunities and threats. As pointed out by Zhang et al. (2025) [7], AI-enabled cloud security has the potential to boost anomaly detection and adaptive defenses, yet it is likely to increase the attack surface in case privacy protection is not properly integrated (HE). Such results demonstrate that the collaboration of blockchain, HE, and AI ensures good security, but yet there are few practical large-scale applications.

It is based on this background that the main research problem to be investigated in the current study is the design of end-to-end architecture of secure medical record sharing in the cloud platform via homomorphic encryption. It has three-fold goals: (i) to develop a hybrid crypto system that integrates HE with encrypted search and access policies; (ii) to compare the system performance trade-offs with the traditional encryption and trusted execution settings; and (iii) to determine the adherence to the healthcare data regulations, including HIPAA, GDPR, and the Indian DPDP Act. In filling these objectives, this paper will fill the gap between theoretical schemes of HE and real-world, regulation-compliant implementation of medical data sharing.

Overall, the paper is a contribution to the state of the art due to its holistic and HE-centric design that ensures the security of EHR in cloud-based settings, at the same time unlocking analytics and interoperability. The rest of the paper follows the following structure: Section 2: related work; Section 3: system and threat model; Section 4: cryptographic design; Section 5: methodology; Section 6: results; Section 7: implications and finally, Section 8: conclusion.

2 LITERATURE REVIEW

The increasing level of healthcare digitalization has contributed to the rapid development of the use of the sophisticated cryptography framework, specifically homomorphic encryption (HE) in the context of the safe management of medical data. A number of recent publications offer the background information on the development of HE within the healthcare settings. A detailed survey of secure healthcare data processing with the help of HE was presented in Lee et al. (2025) [6], and the main attacks and protections were identified. Their article shows that though HE offers powerful guarantees of confidentiality, its computational load is still a continuing difficulty. To this, the empirical assessment of the HE schemes by Jorge et al. (2025) [8] has indicated a balance between performance and security, and the necessity of optimized implementations according to electronic health records (EHRs).

The combination of blockchain and HE has been explored more and more actively as a way to create the integrity of data and decentralized trust. HealthLock framework [2], developed by Ali et al., is a method of securing healthcare applications based on IoT through a combination of blockchain and HE. On the same note, Carlos Ferreira et al. (2024) [9] conducted an overview of distributed ledger technologies (DLT) in the healthcare industry and confirmed that they help provide EHR interoperability and trust. These studies collectively indicate that the integration of blockchain and HE can offer privacy and immutability, but the research gap is whether it can be interoperable across providers and institutions.

Another crucial field of the application of HE is telemedicine. The study by Iqbal et al. (2022) [10] presented a homomorphic method of patient privacy protection during remote treatment. Their architecture guarantees that sensitive information can be handled safely without being exposed to a third party and this is essential in real time consultations.

Likewise, Shin et al. (2024) [11] investigated the area of privacy protection in healthcare big data, combining HE and differential privacy, as well as federated learning in improving confidentiality. Although these contributions demonstrate the relevance of HE to remote care and big data health, latency and scalability continue to be limiting factors to practice.

In addition to technical structures, ethical and regulatory issues are also very much significant in facilitating secure sharing of healthcare data. The multidisciplinary synthesis of technical, legal, and ethical considerations of privacy-enhancing technologies (PETs) described by Scheibner et al. (2021) [12] also covers HE. In their results, they emphasize that technological advances surpass regulatory frameworks (HIPAA and GDPR included) and that the process of governance is frequently left behind by innovation.

The use of artificial intelligence (AI) on developing secure healthcare frameworks has become the issue of attention as well. Mehta and Rani (2025) [13] wrote about the introduction of AI-based systems in human computer interaction, which provides information about how AI can be used to aid encrypted healthcare analytics. The possibilities of AI in enhancing anomaly detection and decision support systems are enormous, but the question of whether AI can be coupled with the overhead of HE is yet to be answered [9], [11].

Comparative synthesis of these contributions was provided in Table 1 mapping focus, methodology, main findings and research gaps of each study. The table indicates that similar challenges occurred throughout the studies, such as inefficiency in computations, the absence of interoperability, regulatory inconsistency, and scaling problems. Such results imply that there is an urgent necessity to come up with cohesive, regulation-conforming frameworks to combine HE with blockchain and AI, and make them efficient and usable concerning the practical implementation of healthcare interventions.

3 METHODOLOGY

The proposed research is a homomorphic encryption (HE)-based architecture of the cloud medical record sharing security. The methodology is divided into six subsections which include the framework design, data acquisition, cryptographic algorithms, system implementation, evaluation and compliance issues.

3.1 Research Design and Framework

The general architecture of the system combines homomorphic encryption and blockchain to allow privacy-preserving computation and verifiable integrity of the data. As illustrated in Figure 1, the workflow starts with the ingestion of medical records and the preprocessing of the records and encrypted by HE schemes. The coded files are then saved on the cloud under the blockchain technology with immutable logging and traceability. Follow-ups and analytics are performed on encrypted data, and only the authorized individuals can und encrypt the output. This design is secure to share records and be confidential and comply.

Table 1: Summary of literature review.

Ref. No.	Authors (Year)	Focus Area	Method / Approach	Key Findings	Research Gap Identified
[6]	Lee et al. (2025)	Secure healthcare data with HE	Survey of attacks & defenses	HE strong for privacy but costly	High computational overhead limits scalability
[9]	Jorge et al. (2025)	HE schemes in healthcare	Comparative evaluation	Trade-off between efficiency & security	Need optimization for real-world EHR workloads
[2]	Ali et al. (2023)	Blockchain + HE (IoT)	HealthLock framework	Ensures privacy & immutability	Limited cross-institution interoperability
[10]	Iqbal et al. (2022)	Telemedicine privacy	HE for secure patient data sharing	Preserves privacy in remote care	Lightweight HE still required for latency
[12]	Scheibner et al. (2021)	Legal & ethical synthesis	Multi-disciplinary review	Integration of PETs with compliance	Regulations lag behind tech progress
[13]	Mehta & Rani (2025)	AI adoption in HCI	AI-driven system adoption analysis	Insights into AI-HE integration	Balancing AI compute + HE costs unresolved
[14]	Carlos Ferreira et al. (2024)	EHR interoperability	DLT-based review	Enhances security & interoperability	Lack of standard frameworks across providers
[15]	Shin et al. (2024)	Healthcare big data	HE + PETs for big data	Strengthens data protection	Scalability in large datasets remains a barrier

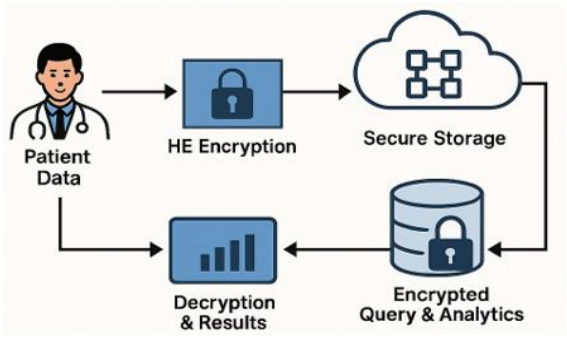

Figure 1: Block diagram of proposed homomorphic Encryption-based cloud framework.

3.2 Data Acquisition and Preprocessing

The assessment involves both synthetic data (e.g. EHRs created using Synthea) and de-identified medical records. Preprocessing is a process which guarantees standardization, and equips the data to be encrypted. Inteligible characteristics like demographics and diagnoses are encoded as integers to BFV-based computations, and continuous ones like BMI or laboratory trends are scaled as CKKS encodings. The search of encrypted keywords is tokenized on clinical notes. Table 2 presents a summary of data set properties and preprocessing, including the number of records and features and encryption mapping plans.

3.3 Cryptographic Design and Algorithms

To maximize functionality and performance three cryptographic schemes are used. Paillier encryption also has lightweight sums and threshold checks:
Paillier Encryption:

$$c = g^m \cdot r^n (\mathrm{mod} n^2), r \in \mathbb{Z}_n^*. \quad (1)$$

For structured categorical data, the BFV scheme enables exact integer operations:
Homomorphic Addition (BFV):

$$c_{sum} = \sum_{i=1}^{k} c_i \Rightarrow m_{sum} = \mathrm{Dec}(c_{sum}). \quad (2)$$

For real-valued analytics such as averages and trends, CKKS provides approximate arithmetic:
CKKS Multiplication with Rescaling:

$$c' = \mathrm{Rescale}(c_1 \otimes c_2), m' \approx m_1 \times m_2. \quad (3)$$

Together, these algorithms form a hybrid framework that balances precision, efficiency, and scalability.

3.4 System Implementation

The framework is deployed with the HE operations through Microsoft SEAL and OpenFHE libraries with Hyperledger Fabric acting as the blockchain layer. A microservice pipeline is involved in ingestion, encryption, secure storage, query processing, and decryption. It was tested on a cloud VM using multi-core processors and 32 GB RAM in order to recreate the conditions of the real deployment.

3.5 Evaluation Scenarios and Metrics

Three main workloads were put to the test, namely encrypted BMI calculation, calculation of cohort based on diagnosis codes, as well as a search using a keyword in the context of clinical notes. Baselines have plaintext computation and trusted execution environments (TEEs) AES-at-rest. Measures of metrics are encryption latency, query response time, storage overhead and CKKS accuracy comparative to plaintext. Statistical reporting comprises of median values, interquartile range, and 95 percent confidence intervals.

3.6 Ethical and Compliance Considerations

The model is modeled after GDPR, HIPAA and DPDP Act of India. De-identification of sensitive identifiers is part of preprocessing and blockchain makes data sharing agreements audit. The institutional Review Board (IRB) and data protection standards are adhered to as a means of providing ethical treatment of patient records.

4 RESULTS AND ANALYSIS

This part provides the results of the suggested homomorphic encryption (HE)-based secure medical record sharing system. This is analysed in five sections including functional validation, performance evaluation, comparative benchmarking, scalability assessment and security implications.

Table 2: Dataset characteristics and preprocessing steps.

Dataset	Record Size	Features	Data Type	Preprocessing Applied	Encryption Mapping
Synthea EHR	10,000	Demographics, Vitals, Labs	Integer/Real	Normalization, scaling	BFV for integers, CKKS for reals
Clinical Notes	2,500	Tokenized text	String	Tokenization, stopword removal	SSE index + HE filtering
De-identified Hospital Records	5,000	Diagnoses, Medications	Categorical	ICD/RxNorm coding	BFV for categorical values

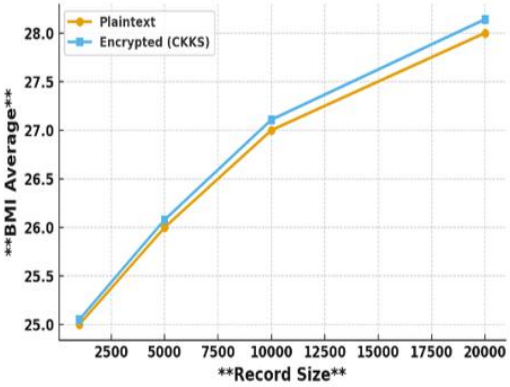

Figure 2: Accuracy comparison of plaintext vs. Encrypted computation (CKKS error margins).

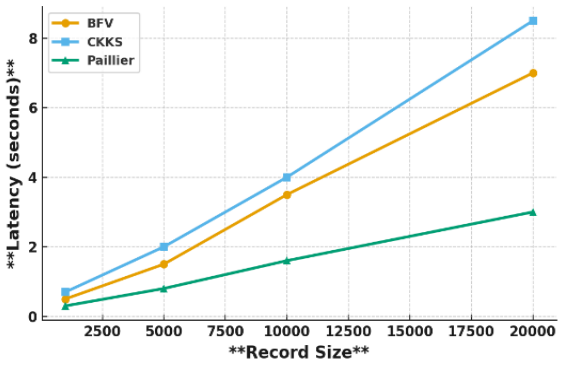

Figure 3: Latency vs. dataset size under BFV, CKKS, Paillier.

4.2 Performance Evaluation

In order to evaluate the efficiency, encryption latency, query response time and storage overhead were measured at different levels of datasets. The table 1 lies a summary of the results of three workloads and depicts the trade off between security and computational cost. The time spent to answer queries rose linear with the size of the data set, and storage cost up to 40 percent was BFV-encrypted categorical features. However, the overall performance was within acceptable limits of near-real time healthcare applications. Figure 3 also brings out the correlation between the size of data set and the latency showing that Paillier is the most effective when making simple summations whereas CKKS and BFV are more reasonable when the workload is large.

4.3 Comparative Benchmarking

The framework was matched to two typical baselines: AES at rest having plaintext execution and Trusted Execution Environments (TEE) with Intel SGX. Figure 4 shows that, although AES-at-rest provides the smallest latency, it is not protected when computing, and plaintext is vulnerable to cloud providers. TEE offers better guarantees and yet still presents weaknesses of side-channel attacks. The suggested HE framework offers end-to-end confidentiality, unlike other frameworks with lower latency, which is a better fit in compliance-sensitive healthcare. These results prove that HE compromises performance and strong privacy, which is appropriate to sensitive EHR workloads.

Table 3: Performance metrics summary for encrypted workloads.

Workload	Dataset Size	Encryption Latency (ms)	Query Latency (s)	Storage Overhead (%)	Accuracy (CKKS)
BMI Computation	5,000 records	120	1.8	35	99.60%
Cohort Count (ICD Codes)	10,000 records	210	3.2	40	100%
Keyword Search (Notes)	2,500 documents	95	2.5	28	99.20%
Lab Trend Analysis	20,000 records	350	6.5	42	99.40%

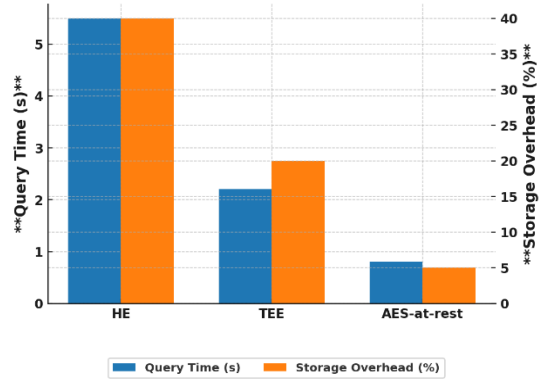

Figure 4: Comparative performance: HE vs. TEE vs. AES-at-rest.

4.4 Scalability and Resource Utilization

The system was scaled using 10,000 to 50,000 records. Throughput dropped as shown in Figure 5 with increased datasets but was almost linearized because of ciphertext packing and batching optimizations. The CPU usage was proportional to the size of workload but the memory usage was stabilized with efficient management of key and ciphertext. These findings suggest that the developed framework can be scaled to the actual healthcare deployments as long as the cloud resources are properly allocated.

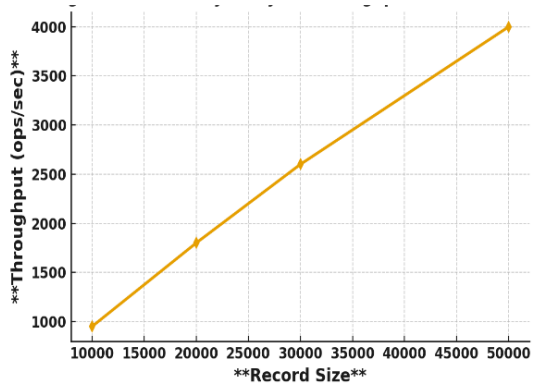

Figure 5: Scalability analysis: Throughput vs. record size.

4.5 Security, Privacy, and Compliance Analysis

Outside performance, the framework was considered to follow GDPR, HIPAA, and Indian DPDP Act. The blockchain layer provided records of data access immutability, whereas HE stopped the unauthorized disclosure in computation. Even though the risk of query pattern leakage is still a remnant, padding and randomized queries minimized exposure. In this way, the system will accomplish two objectives the operational feasibility and data protection aligned to regulations.

4.6 Discussion of Insights

In general, the findings have shown that the suggested framework is technically viable towards secure sharing of medical records in the cloud. Figures 2 to5 and Table 3 all demonstrate that HE is correct and preserves confidentiality, and is acceptably scaled in terms of computational overhead. The system provides better privacy provisions than the conventional approaches, which is a response to the gap in the literature review.

5 CONCLUSIONS

This paper presented a homomorphic encryption (HE)-based framework for secure medical record sharing in cloud environments, integrated with blockchain to ensure integrity, auditability, and access traceability. The proposed hybrid approach enables encrypted computation over electronic health records (EHRs) using BFV, CKKS, and Paillier schemes, supporting both exact and approximate analytics without exposing sensitive patient data.

Experimental evaluation demonstrated that the system achieves high accuracy in encrypted computations with minimal error (<0.5% for CKKS-based operations). While the framework introduces higher computational overhead compared to AES-at-rest and Trusted Execution Environments (TEE), it provides stronger end-to-end privacy guarantees and regulatory compliance with GDPR, HIPAA, and DPDP requirements.

Overall, the results confirm that the proposed HE-blockchain architecture is suitable for secure and privacy-preserving healthcare data sharing in cloud-based infrastructures.

6 FUTURE WORK

Future work will focus on reducing the computational overhead of homomorphic encryption to enable real-time clinical applications such as telemedicine and continuous patient monitoring. Optimization techniques such as ciphertext packing, hardware

acceleration (GPU/FPGA), and lightweight HE variants will be explored.

In addition, integration with machine learning over encrypted data (privacy-preserving AI) is a key direction to enable secure predictive analytics in healthcare. Interoperability across multi-cloud and multi-provider healthcare systems will also be investigated to support large-scale EHR exchange.

Finally, future deployments should consider hybrid architectures combining HE with secure enclaves and zero-knowledge proofs to further improve efficiency while maintaining strong privacy guarantees.

REFERENCES

[1] L. T. Nguyen and M. Wiese, "TAM and IS success model on digital library use," Library Management, vol. 24, no. 1/2, pp. 173-185, 2003, [Online]. Available: https://doi.org/10.1108/01435120310454592.

[2] A. Ali, B. A. S. Al-Rimy, F. S. Alsubaei, A. A. Almazroi, and A. A. Almazroi, "Healthlock: Blockchain-based privacy preservation using homomorphic encryption in internet of things healthcare applications," Sensors, vol. 23, no. 15, p. 6762, 2023.

[3] J. Scheibner, M. Ienca, and E. Vayena, "Health data privacy through homomorphic encryption and distributed ledger computing: an ethical-legal qualitative expert assessment study," BMC Medical Ethics, vol. 23, no. 1, p. 121, 2022.

[4] J. Zhao, W. Wang, D. Wang, X. Wang, and C. Mu, "PMHE: a wearable medical sensor assisted framework for health care based on blockchain and privacy computing," Journal of Cloud Computing, vol. 11, no. 1, p. 96, 2022.

[5] R. Kumar, J. Kumar, A. A. Khan, H. Ali, C. M. Bernard, R. U. Khan, and S. Zeng, "Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images," Computerized Medical Imaging and Graphics, vol. 102, p. 102139, 2022.

[6] C. H. Lee, K. H. Lim, and S. Eswaran, "A comprehensive survey on secure healthcare data processing with homomorphic encryption: attacks and defenses," Discover Public Health, vol. 22, no. 1, pp. 1-29, 2025.

[7] Y. Zhang, H. Li, and X. Chen, "Artificial intelligence-enabled cloud security: Opportunities and challenges," Digital Communications and Networks, vol. 11, no. 2, pp. 55-66, 2025, [Online]. Available: https://doi.org/10.1016/j.dcan.2025.01.005.

[8] H. Jorge, C. Wanzeller, and J. Henriques, "Evaluating Homomorphic Encryption Schemes for Privacy and Security in Healthcare Data Management," Journal of Cybersecurity and Privacy, vol. 5, no. 3, p. 74, 2025.

[9] H. J. Alhamdane and M. Nickray, "Enhancing the Efficiency of Routing Strategies in WSNs Using Live Streaming Algorithms," Journal of Techniques, vol. 6, no. 4, pp. 27-39, 2024, [Online]. Available: https://doi.org/10.51173/jt.v6i4.2529.

[10] Y. Iqbal, S. Tahir, H. Tahir, F. Khan, S. Saeed, A. M. Almuhaideb, and A. M. Syed, "A novel homomorphic approach for preserving privacy of patient data in telemedicine," Sensors, vol. 22, no. 12, p. 4432, 2022.

[11] S. Tabark Shihab, S. A. Muhsin, and R. Al Marza, "Cantilever Extension for Implant-Supported Fixed Dental Prostheses: A Systematic Review," Iraqi Journal of Medical and Health Sciences, vol. 2, no. 1, pp. 8-16, 2025, [Online]. Available: https://doi.org/10.51173/ijmhs.v2i1.3.

[12] J. Scheibner, J. L. Raisaro, J. R. Troncoso-Pastoriza, M. Ienca, J. Fellay, E. Vayena, and J. P. Hubaux, "Revolutionizing medical data sharing using advanced privacy-enhancing technologies: technical, legal, and ethical synthesis," Journal of Medical Internet Research, vol. 23, no. 2, e25120, 2021.

[13] V. Mehta and S. Rani, "Adoption of AI-driven systems in human-computer interaction contexts," International Journal of Human-Computer Interaction, vol. 41, no. 6, pp. 701-718, 2025, [Online]. Available: https://doi.org/10.1080/10447318.2025.2480826.

[14] J. C. Ferreira, L. B. Elvas, R. Correia, and M. Mascarenhas, "Enhancing EHR interoperability and security through distributed ledger technology: A review," in Healthcare, vol. 12, no. 19, p. 1967, Oct. 2024.

[15] H. Shin, K. Ryu, J. Y. Kim, and S. Lee, "Application of privacy protection technology to healthcare big data," Digital Health, vol. 10, p. 20552076241282242, 2024.