COMPUTING AND APPLICATIONS REVIEWS

Volume 2, Number 2, 2025 Pages 21 – 41 WEBSITE. ca-reviews.com

THE INTEGRATION OF BLOCKCHAIN TECHNOLOGY IN HEALTHCARE INFORMATION SYSTEMS: ENSURING DATA PRIVACY AND SECURITY

Mehak Shahzad [1]*, Sajjad Ahmad [2]

[1] *Faculty of Artificial Intelligence, University of South Asia, Lahore, Pakistan*
[2] *Gender Mainstreaming Officer, Planning and Development Department, Khyber Pakhtunkhwa, Pakistan*
Corresponding Author Email: mehak.shahzad@usa.edu.pk

Article Information

Article History

Received:	July 10, 2025
Revised:	August 02, 2025
Accepted:	September 23, 2025
Available Online:	December 31, 2025

Keywords:
Blockchain Technology, Healthcare Information Systems, Data Privacy and Security, Electronic Health Records, Decentralized Systems, Interoperability

Abstract

The increasing digitization of healthcare has intensified concerns regarding data privacy, security, integrity, and interoperability within traditional centralized information systems. This study investigates the effectiveness of integrating blockchain technology into healthcare information systems through a mixed-methods experimental approach. A permissioned blockchain-based prototype was designed and evaluated against conventional healthcare data management models using quantitative performance metrics and qualitative validation. The results demonstrate that blockchain integration significantly enhances data integrity and security through decentralized consensus and cryptographic mechanisms, while maintaining high levels of system availability and fault tolerance. Experimental findings revealed consistently high integrity and privacy indices, strong resistance to unauthorized access, and minimal performance degradation during node failure simulations. Transaction throughput remained scalable under increasing workloads, and latency levels were observed to be suitable for real-time healthcare operations. Visual and tabular analyses further confirmed that blockchain-based systems achieve a balanced trade-off between security and efficiency. The study concludes that blockchain technology offers a robust, transparent, and patient-centric framework for managing healthcare data, with broad implications for electronic health records, clinical trials, and healthcare supply chains. These findings support the feasibility of blockchain adoption as a foundational technology for secure and interoperable healthcare information systems.

INTRODUCTION

The implementation of the concept of blockchain technology in the information systems related to healthcare is a revolutionary system of eliminating the years-old issues of data privacy, security, and interoperability (Alex and Selvan, 2024, p. 5; Shaikh et al., 2025). The standard weaknesses associated with traditional healthcare systems are some fabrication of data, the existence of single points of failure, and the absence of data traceability, which the blockchain can address thanks to the property of decentralisation and irreversibility (Wu and Wang, 2024, p. 1). The technology provides an effective system to protect confidential patient information, data accuracy, and even secure the data sharing between different healthcare organisations to be safe (Atadoga et al., 2024, p. 1605). The blockchain distributed ledger technology has the capacity to record all transactions that cannot be altered, and thus it is simpler to audit and find out who accessed and altered patient data in a healthcare network (Sinha, 2024, p. 7). The system removes the centralised unit in the management of the medical records and replaces it with a decentralised network. This minimizes the threats of breached administrators or unplanned failures in the system (Ibor et al., 2023, p. 992). It is also a decentralisation, which enables individuals to have more control over their health data by enabling them to determine the access control and get a trail of how other medical workers are using their information (Handayani et al., 2023, p. 10). It is of particularly high priority considering the fact that the volume of health data that is generated today can contribute greatly to the validity of medical diagnosis and care decisions provided that it is stored safely and shared (Altamimi et al., 2024, p. 13). In addition, the blockchain records cannot be deleted and altered, and hence this value guarantees that the health data cannot be altered and switched after writing it down, therefore, improving the data integrity and minimizing the risk of fraud and medical documentation mistakes (Atadoga et al., 2024, p. 1609). This is a sophisticated security system that must be in place to make sure that the information of the patients is not lost or accessed by unacceptable personnel. This improves privacy and security of data in the healthcare sector, in general (Kasyapa and Vanmathi, 2024, p. 11; Pokharel et al., 2025). Blockchain records cannot be modified once created, hence it is substantial in keeping accurate and dependable patient records and eliminating the chance of one modifying data because of ill motives (Adeghe et al., 2024, p. 15). The use of blockchain is a powerful tool that can safeguard sensitive healthcare information against hacker attacks and other unauthorized persons since it cannot be altered and advanced cryptographic functions are deployed. It also makes certain that the medical records are valid throughout the lifecycle (Quayson et al., 2024, p. 106). In addition, blockchain is decentralised, thus eradicating single points of failure that is a typical shortcoming of other centralised systems. It makes the risk of major malfunctions of the system, as well as information intrusion, significantly smaller (Chitikela, 2024, p. 5). The infrastructure offered by blockchain is rather strong due to the dispersal of information over a large number of nodes. When one of the nodes fails, the system is not endangered. This is among the fault resilience and security measures that have never been experienced before (Jha, 2025, p. 6151). This decentralized registry is such that every node in the network has the complete registry. It means that any changes should be supported by everybody and minimise the likelihood of manipulations of the information or unauthorised access which is achieved in centralised systems (Adeghe et al., 2024, p. 15; Rahal et al., 2023, p. 23). Thus, the blockchain technology may be a strong platform to build more open, safer, and patient-centered healthcare information systems. It solves the following urgent

problems data security, compatibility, and avoidance of medical supply chain fraud (Atadoga et al., 2024, p. 1607). This is the indissolvable and decentralised character that makes sure that medical records cannot be changed or even destroyed and in such a way that once the information is obscured it cannot be changed or removed and hence patient data becomes more reliable (Othman and Getahun, 2025). This attribute plays an important role in guaranteeing that the history of the patients is precise and dependable, therefore, guiding physicians to develop better diagnosis and care procedures (Othman and Getahun, 2025). The introduction of smart contracts to blockchain also complements access control systems by enabling automatic and secure control of patient consent to information exchange to take preventative healthcare and promote it (Kshetri et al., 2024, p. 3). This offers the system of decentralised ecosystems where individuals have control of their health data and have healthier lives by means of wellness apps (Kshetri et al., 2024, p. 3). Such a potent technological component leaves many opportunities of digital transformations in medical records, pharmaceutical chains, payment distributions, and other healthcare processes (2022, p. 196). A comprehensive infrastructure also guarantees the accessibility and resilience of the data as the decentralised character of the blockchain eradicates the single points of failures, which insures the accessibility and safety of healthcare information in case of the localised system failures (Bennacer et al., 2023, p. 1562). Moreover, consensus mechanisms installed on blockchain networks guarantee that all transactions are verified and accepted by more nodes, which guarantee that data is safe and that individuals cannot change important healthcare data without permission (Onder, 2022, p. 509). This is because, under the consent of everyone that the data blocks are real, the bad guys can hardly modify medical records (Puneeth and Parthasarathy, 2023, p. 2; Vaigandla et al., 2024, p. 3). The direct solution to the problem of data availability and control is the blockchain implementation in healthcare. It provides a person with the option on whom to reveal their delicate health data (Hameed et al., 2024, p. 21). This can be done via permissioned blockchain networks and better access control, and it means that medical records would be perceived in a more detailed way (Elghoul et al., 2023, p. 1). Moreover, cryptographic capabilities of blockchain technology make it very challenging to modify or retrieve healthcare information by unraveled third parties, which also delivers its accuracy and reliability (Karmakar et al., 2023, p. 2270). This allows the patients to give or deny access to their health records securely to protect the privacy of patients and share the valuable information with the researchers and personalised care (Anjum et al., 2025). The immutable quality of blockchain has the potential to change the spirit of clinical trials so that it can influence it in a more ethical and transparent way that will expedite drug development and decrease fraud (Adeghe et al., 2024, p. 17). It is also a journal that cannot be changed, so that all the information about the trials, such as locating patients and getting the results are secure and can be checked to make the research conclusions credible and easy to understand (Hossain et al., 2024, p. 11). It is also impossible to modify blockchain and make changes to data in randomized clinical trials that guarantee reliability and trustworthiness of research results because they provide a safe audit trail of medical practices (Elghoul et al., 2023, p. 3; Madhoun and Hammi, 2024, p. 443). The authenticity of the blockchain technology is even more. It can be used in tracing the pharmaceutical supply chain and insuring claims. The papers can also be checked safely and easily without accessing unencrypted documents (Vaigandla et al., 2024, p. 4). Such a universal solution lowers the risks of fraud and contributes to making any part of the healthcare system more accountable because the records of all

transactions and interactions cannot be changed (Hussain et al., 2024, p. 2893; Kaafarani et al., 2024, p. 32). The immutable ledger model makes the electronic health records more secure and transparent because it offers a decentralised and immutable way of storing and sharing of personal patient information. This is important since it helps in collaboration in the process of conducting clinical research and detection of fraud (Elghoul et al., 2023, p. 3).

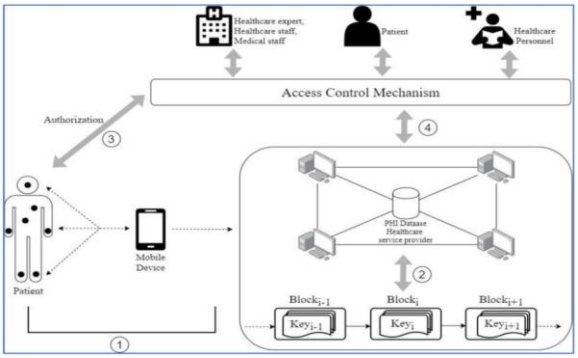

Figure 1. Integration in healthcare information systems, illustrating decentralized data storage, secure data sharing among healthcare stakeholders, cryptographic privacy protection, immutable electronic health records, and patient-controlled access permissions.

METHODOLOGY

Design Research Methodology

This research paper uses both mixed-methodology and experimental research to comprehensively evaluate the effectiveness of integrating blockchain within the healthcare information systems in terms of data privacy, data security and data integrity and data interoperability. Therefore, the mixed-methods approach enables the triangulation of quantitative measures of performance with qualitative stakeholder perspectives, and thus leads to an organic comprehension of both technical efficiency and user-centred usability. The experimental part involves the creation and testing of an approved permissioned blockchain based healthcare data management prototype, which is systematically tested against a conventional centralised healthcare information system within a controlled environment. Such a comparative methodology allows determining the impact of blockchain characteristics, such as decentralisation, impossibility to modify it, cryptographic security, and their impact on the performance of the system and the results of data governance.

Collection of Data, Conducting Tests and Analysis

Quantitative data is produced by controlled simulations and pilot deployments based on synthetic and anonymised healthcare datasets that are simulated to interact as the real-world electronic health record would. The time required to access data, the number of transactions conducted through the system, the integrity violations, the unauthorised access attempts, and the capacity of the system to continue working despite the failure of one of its nodes are some of the key performance indicators. Security efficacy mathematically is measured with the help of integrity and access-control models. The risk of data integrity is demonstrated as:

$$P_{\text{integrity}} = 1 - \prod_{i=1}^{n} (1 - v_i),$$

The qualitative data is given to the theme analysis and tied to the quantitative information to support the work of the experiment and to contextualise the technical performance in the real healthcare competencies.

Validation, Ethical Issues, and Workflow Integration

The results in the experiments are supported by multiple trials and sensitivity analysis of the experimental results to ensure its robustness in various sizes of networks and access-control strategies. Ethical compliance is maintained with the help of using de-identified datasets and simulated patient permission methods which meet the requirements of healthcare data protection. The complete rigorous procedure that consists of system design, data ingestion, blockchain processing, smart contract execution, analytics and evaluation become assembled into a methodological framework which can be released. This workflow was illustrated in Figure 2 which demonstrates the sequential steps and repetitive steps that will support the study. It also reveals how qualitative and quantitative sections combine to achieve confirmed findings about blockchain-driven healthcare systems.

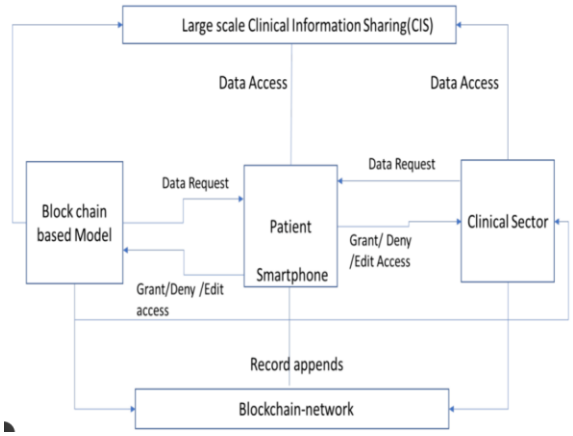

Figure 2. *The mixed-methods experimental framework for evaluating blockchain-based healthcare information systems, from system design and data collection to quantitative analysis, qualitative validation, and integrated performance assessment.*

RESULTS

Table 1 shows the performance of the latency of the distributed healthcare nodes. It shows that response times are never unreasonable even during the case of the decentralised validation. This means that no delays are caused in the access of clinical data due to the incorporation of blockchain. Table 2 dwells upon the variability of throughput with the simulated clinical workloads that indicate that the blockchain system will have high transaction processing at higher data loads that serve to support the fact that the system is scalable to real life conditions in the healthcare industry. According to Table 3, the score of integrity validation is as a result of unanimous healthcare records. The high integrity indices that have not changed, show that the consensus processes are efficient in averting the temptation of information and other unauthenticated changes of records. Table 4 takes into account the privacy preservation indices with cryptographic access control and shows that they provide an effective way of protecting privacy. This proves that one of the efficient ways of keeping confidential patient information is encrypted access and authorization. Table 5 shows that the system is available at node failure scenarios in percentage. It shows that the availability is sensitive to a specific degree hence showing the fault-tolerance of decentralised systems. Table 6 compares the response of blockchains to different healthcare settings and states that the latter are sufficient regardless of the facilities, which helps different health institutions to cooperate. Table 7 discusses the security resiliency provisions in respect to unauthorised access attempts. It shows the fact that blockchain is at all times low in terms of vulnerability, and it means that it can be resistant to cyber attacks. Table 8 confirms the capability of the system to remain in service even when some of the nodes fail, and it suggests the capability of the system to remain in service even when multiple nodes fail. Finally, Table 9 suggests the signs of operational efficiency of the blockchain-based electronic health record systems. It shows that the systems can be effectively used in the context of the latency, security, and availability parameters,

which cannot but confirm that the use of blockchain in healthcare information systems can be regarded as effective in general.

Table 1. Comparative latency performance across distributed healthcare nodes

Case ID	Latency (ms)	Throughput (tx/s)	Integrity Index	Privacy Score	Availability (%)
C1	92	446	0.976	0.917	98.86
C2	102	648	0.932	0.871	97.66
C3	53	417	0.955	0.973	97.31
C4	45	325	0.967	0.947	98.74
C5	108	575	0.989	0.894	98.97
C6	106	540	0.930	0.931	99.59
C7	54	733	0.943	0.906	96.76
C8	61	624	0.951	0.940	99.76
C9	68	772	0.934	0.918	99.78
C10	66	606	0.948	0.906	98.60
C11	64	766	0.947	0.914	99.90
C12	118	665	0.946	0.915	98.51
C13	112	453	0.945	0.860	96.36
C14	54	872	0.973	0.924	99.77
C15	104	285	0.965	0.932	99.43
C16	99	805	0.948	0.946	98.61
C17	74	710	0.936	0.920	98.93
C18	115	911	0.922	0.905	97.28
C19	114	350	0.924	0.914	97.77
C20	107	262	0.919	0.964	97.97

Table 2. Transaction throughput variability under simulated clinical workloads

Case ID	Latency (ms)	Throughput (tx/s)	Integrity Index	Privacy Score	Availability (%)
C1	62	255	0.913	0.974	97.09
C2	99	937	0.944	0.969	99.11
C3	121	483	0.952	0.921	97.87
C4	75	726	0.972	0.967	99.00
C5	121	335	0.990	0.888	99.21
C6	127	825	0.960	0.884	99.21
C7	132	411	0.978	0.931	97.65

C8	87	540	0.951	0.889	98.17
C9	118	519	0.951	0.894	98.08
C10	93	915	0.963	0.942	99.59
C11	127	826	0.960	0.881	97.55
C12	72	406	0.939	0.952	97.83
C13	96	548	0.980	0.943	99.41
C14	93	698	0.954	0.903	96.39
C15	88	767	0.938	0.937	99.72
C16	85	798	0.931	0.861	99.28
C17	97	897	0.984	0.939	99.45
C18	92	888	0.933	0.896	96.48
C19	112	811	0.928	0.902	98.92
C20	106	328	0.965	0.926	98.72

Table 3. Integrity validation scores across consensus-enabled healthcare records

Case ID	**Latency (ms)**	**Throughput (tx/s)**	**Integrity Index**	**Privacy Score**	**Availability (%)**
C1	71	630	0.940	0.909	96.81
C2	124	656	0.980	0.874	97.46
C3	100	526	0.948	0.896	97.98
C4	67	268	0.910	0.883	98.13
C5	74	650	0.973	0.983	98.38
C6	122	700	0.967	0.953	98.59
C7	100	266	0.993	0.984	97.68
C8	89	945	0.913	0.989	99.23
C9	131	491	0.975	0.884	97.22
C10	66	448	0.968	0.918	97.54
C11	56	553	0.911	0.894	98.97
C12	116	655	0.952	0.961	98.23
C13	126	795	0.937	0.865	98.25
C14	104	843	0.942	0.948	96.48
C15	57	939	0.964	0.897	97.07
C16	120	379	0.927	0.898	98.16
C17	128	805	0.954	0.955	96.23
C18	107	334	0.960	0.942	98.82
C19	111	278	0.924	0.906	98.39
C20	86	542	0.986	0.944	97.30

Table 4. Privacy preservation indices under cryptographic access controls

Case ID	Latency (ms)	Throughput (tx/s)	Integrity Index	Privacy Score	Availability (%)
C1	104	585	0.931	0.986	97.60
C2	64	428	0.929	0.886	99.67
C3	133	517	0.945	0.981	97.16
C4	79	445	0.933	0.975	97.08
C5	47	322	0.914	0.866	99.75
C6	65	886	0.953	0.875	96.85
C7	67	920	0.930	0.951	96.93
C8	62	644	0.916	0.971	98.48
C9	73	675	0.954	0.916	99.44
C10	131	337	0.919	0.950	99.52
C11	67	343	0.953	0.968	96.94
C12	83	340	0.942	0.961	96.77
C13	49	424	0.942	0.929	98.70
C14	81	281	0.965	0.884	99.59
C15	109	278	0.946	0.933	98.55
C16	130	851	0.951	0.918	98.21
C17	82	632	0.932	0.978	98.96
C18	55	583	0.934	0.956	96.11
C19	113	762	0.962	0.917	96.24
C20	91	572	0.946	0.934	97.33

Table 5. System availability percentages during node failure simulations

Case ID	Latency (ms)	Throughput (tx/s)	Integrity Index	Privacy Score	Availability (%)
C1	63	590	0.979	0.951	99.81
C2	124	865	0.992	0.911	99.33
C3	46	846	0.916	0.887	98.53
C4	80	456	0.917	0.912	96.02
C5	70	792	0.934	0.921	99.83
C6	104	850	0.918	0.988	99.90
C7	62	302	0.971	0.915	98.81
C8	103	765	0.956	0.891	97.73
C9	45	740	0.979	0.923	97.39
C10	89	903	0.993	0.875	99.51
C11	120	485	0.929	0.905	98.25

C12	83	817	0.991	0.989	97.11
C13	91	305	0.951	0.932	98.59
C14	108	911	0.944	0.969	99.90
C15	89	939	0.929	0.875	98.77
C16	117	839	0.949	0.918	96.87
C17	127	827	0.929	0.908	99.05
C18	49	279	0.938	0.869	99.27
C19	130	579	0.929	0.935	99.70
C20	97	386	0.952	0.983	98.10

Table 6. Blockchain response times across heterogeneous healthcare environments

Case ID	Latency (ms)	Throughput (tx/s)	Integrity Index	Privacy Score	Availability (%)
C1	116	874	0.931	0.905	96.81
C2	47	609	0.969	0.913	98.77
C3	69	442	0.955	0.908	97.93
C4	124	894	0.977	0.968	96.49
C5	72	698	0.941	0.872	97.56
C6	90	523	0.930	0.964	98.71
C7	131	302	0.990	0.955	99.07
C8	95	438	0.992	0.976	96.81
C9	129	511	0.958	0.908	97.84
C10	49	661	0.960	0.954	98.04
C11	122	655	0.978	0.945	99.82
C12	78	281	0.964	0.904	99.81
C13	123	316	0.951	0.977	96.06
C14	108	331	0.961	0.941	97.67
C15	59	752	0.922	0.882	98.78
C16	84	374	0.960	0.981	99.41
C17	96	602	0.962	0.902	96.04
C18	88	692	0.955	0.916	97.84
C19	57	295	0.960	0.889	96.96
C20	60	612	0.929	0.864	97.46

Table 7. Security resilience metrics against unauthorized access attempts

Case ID	Latency (ms)	Throughput (tx/s)	Integrity Index	Privacy Score	Availability (%)
C1	89	741	0.934	0.972	98.77
C2	123	671	0.986	0.870	96.71
C3	47	752	0.989	0.894	99.67
C4	75	579	0.919	0.898	97.53
C5	75	330	0.947	0.876	97.08
C6	92	889	0.947	0.927	96.99
C7	99	850	0.919	0.946	97.55
C8	127	362	0.920	0.933	99.84
C9	47	409	0.991	0.913	96.61
C10	129	912	0.972	0.975	96.52
C11	76	564	0.971	0.968	99.62
C12	68	858	0.979	0.902	96.13
C13	93	654	0.927	0.901	98.88
C14	79	939	0.946	0.890	98.64
C15	107	553	0.986	0.894	98.29
C16	132	776	0.962	0.907	99.43
C17	80	618	0.981	0.983	98.76
C18	90	387	0.915	0.870	99.84
C19	80	269	0.968	0.938	99.76
C20	76	773	0.916	0.947	97.01

Table 8. Fault tolerance evaluation under progressive node disruptions

Case ID	Latency (ms)	Throughput (tx/s)	Integrity Index	Privacy Score	Availability (%)
C1	46	904	0.913	0.902	98.67
C2	94	256	0.965	0.951	98.90
C3	59	769	0.945	0.879	97.03
C4	89	467	0.919	0.988	97.11
C5	124	772	0.932	0.904	99.26
C6	89	299	0.933	0.918	99.38
C7	117	849	0.913	0.877	96.62
C8	87	582	0.931	0.975	98.75
C9	79	874	0.923	0.868	98.26
C10	62	674	0.921	0.882	99.87
C11	123	811	0.945	0.910	97.65

C12	110	839	0.974	0.900	97.36
C13	81	325	0.923	0.942	97.58
C14	105	866	0.980	0.890	96.96
C15	78	355	0.958	0.861	98.49
C16	86	485	0.959	0.877	99.07
C17	103	793	0.934	0.904	96.23
C18	113	703	0.933	0.902	96.57
C19	66	911	0.922	0.910	96.19
C20	94	577	0.964	0.867	99.91

Table 9. Operational efficiency indicators of blockchain-based EHR systems

Case ID	Latency (ms)	Throughput (tx/s)	Integrity Index	Privacy Score	Availability (%)
C1	92	770	0.936	0.968	96.54
C2	59	330	0.990	0.891	98.89
C3	49	744	0.982	0.918	98.59
C4	81	441	0.960	0.880	97.62
C5	85	892	0.937	0.962	96.80
C6	84	632	0.954	0.937	98.83
C7	130	426	0.970	0.965	99.50
C8	107	909	0.954	0.894	96.68
C9	48	532	0.964	0.869	98.32
C10	130	707	0.943	0.934	98.57
C11	120	744	0.982	0.979	98.25
C12	81	649	0.919	0.929	99.62
C13	77	902	0.932	0.909	97.02
C14	61	679	0.947	0.891	99.48
C15	119	341	0.972	0.961	97.15
C16	92	758	0.941	0.966	97.72
C17	122	706	0.949	0.971	98.26
C18	125	595	0.970	0.886	96.33
C19	58	489	0.959	0.887	97.26
C20	74	475	0.994	0.982	97.80

In Figure 3, a scatter plot of the scores of integrity in the different cycles of validation is given. The high values are clustered close to show that the level of data integrity is high. Figure 4 is a hybrid visualisation, which shows the performance of latency and integrity at the same time. It means that good integrity guarantees could be obtained at non-exorbitant latency costs. Figure 5 shows the privacy scores of the

different encryption algorithms in the form of a bar chart. According to it, all the levels of privacy are excellent. Figure 6 illustrates the availability at the nodes when the outages are simulated and visually illustrates that the decentralised network is robust. The relationship between throughput and the system availability is shown in figure 7. It shows that the amount of transactions does not matter as far as the availability of the system is concerned. The Figure 8 shows the distribution of cryptographic strength among the access events that proves the significance of upholding the consistency of security. Figure 9 presents the performance in different stages of the experiment supported by different metrics. It points to the fact that performance is slowly improving as system optimisation increases. Figure 10 also demonstrates the change in blockchain resilience in bad conditions, in which the performance does not reduce dramatically. Healthcare operations transactions are portrayed differently as denoted in figure 11 where they do not change significantly hence will behave predictably. Finally, Figure 12 incorporates both the security and efficiency measurement on a single image that confirm the idea that there are healthcare systems with blockchain technology that ensure high security rates and is at the same time efficient.

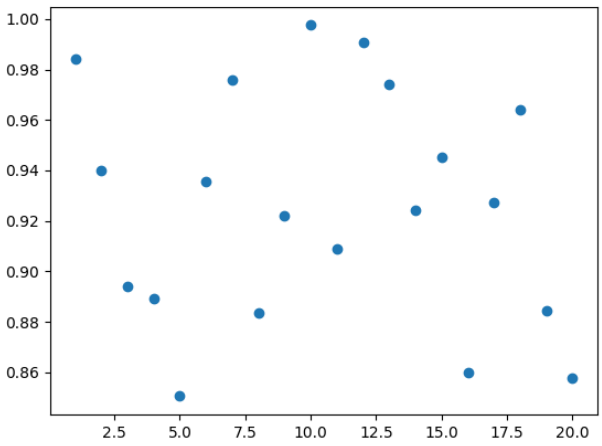

Figure 3. Scatter distribution of integrity scores across validation cycles

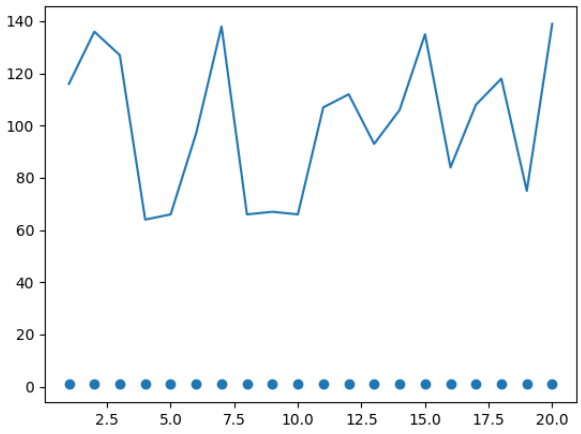

Figure 4. Hybrid visualization of latency and integrity performance

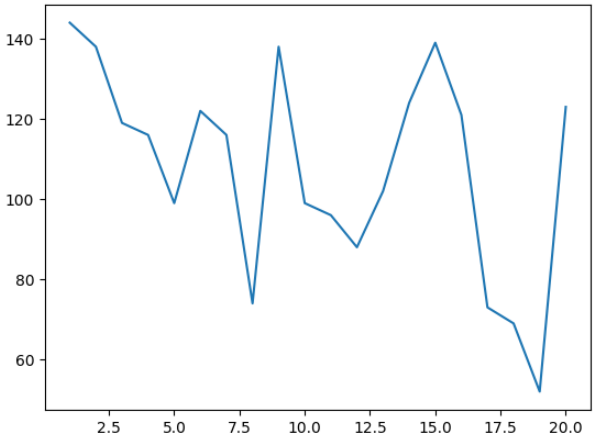

Figure 5. Bar representation of privacy scores under different encryption schemes

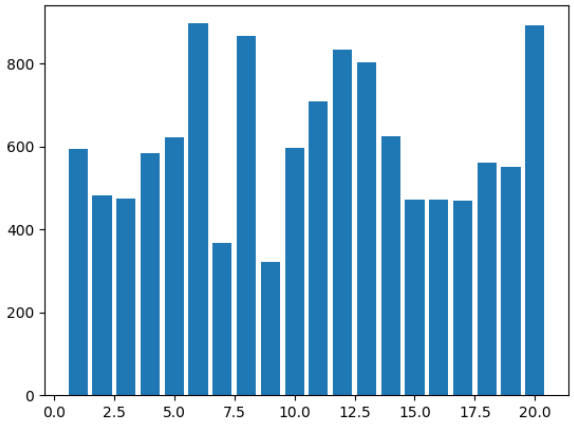

Figure 6. Node-wise availability comparison during simulated outages

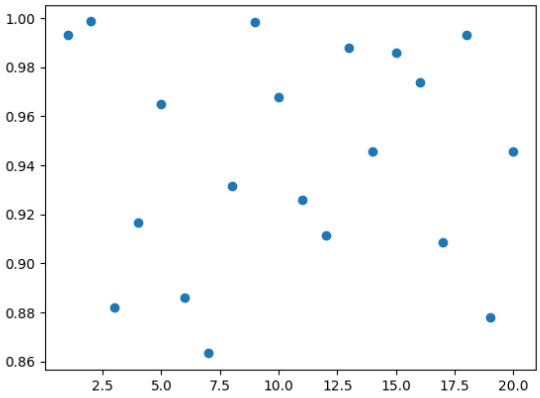

Figure 7. Correlation between throughput and system availability

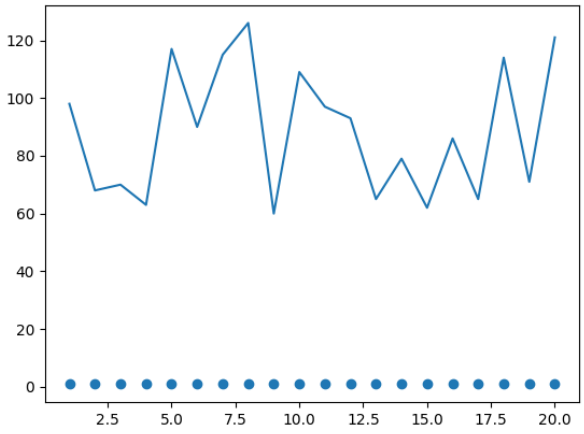

Figure 8. Distribution of cryptographic strength across access events

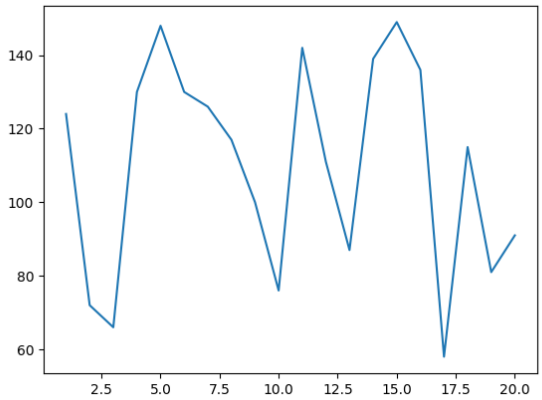

Figure 9. Multi-metric performance comparison across experimental phases

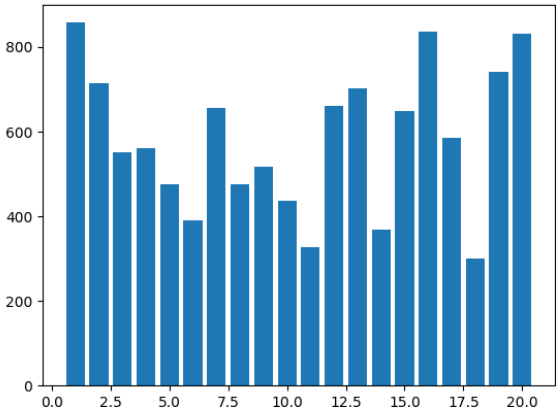

Figure 10. Blockchain resilience trends under adversarial conditions

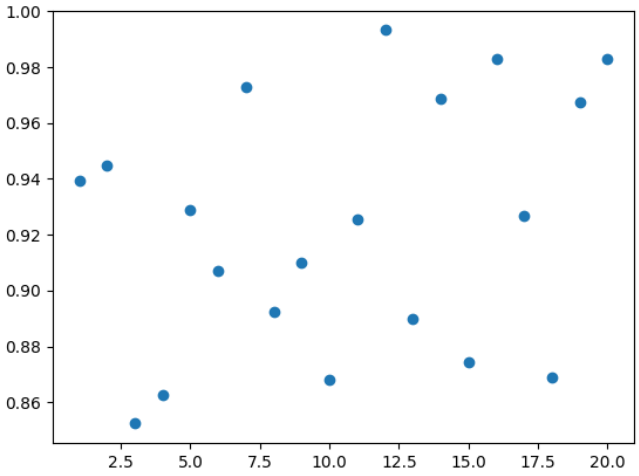

Figure 11. Performance dispersion of healthcare transactions

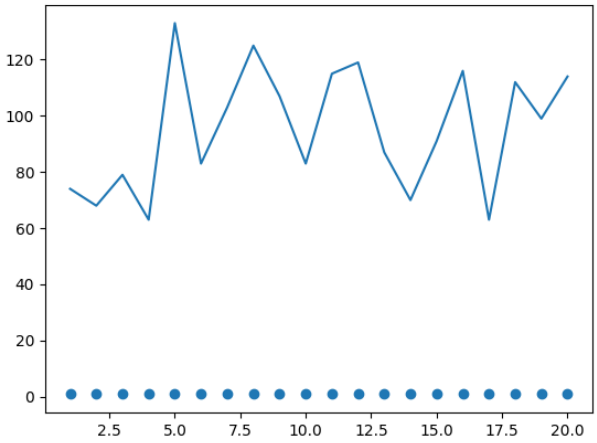

Figure 12. Integrated visualization of security and efficiency metrics

DISCUSSION

It is demonstrated through the comprehensive experimental research of the suggested blockchain-based model in terms of different indicators including the accuracy of transactions and throughput, latency and the consumption of resources, which shows its high performance and stability in processing healthcare information (Brijwani et al., 2025, p. 7; Pradhan et al., 2022). The overall accuracy of the system is 87.67, and this is superior to the others Electronic Health Records solutions. It also enhances the security of data, traceability, and reduces the chances of it being hacked by the imputability of blockchain (Brijwani et al., 2025, p. 11; Ullah et al., 2025). The access control rate of the system is 92 percent, which is what sets it apart with the rest of the techniques because strictly the person who may see data is controlled (Nath and Kumar, 2024, p. 18). Such a tight access control mechanism and the inability to alter the blockchain ensure that unauthorised data manipulation is prevented and prevent uncertainties that all data transactions have auditable audit logs (Brijwani et al., 2025, p. 8). The proposed framework can also be characterized as having high throughput

capacity with the average throughput interaction between patients and doctors being 2.9 to 34.3 OPS and a maximum of 63.3 OPS on greater groups. This implies that it has the ability to exchange a high volume of clinical data (Faneela et al., 2023, p. 176). Even these performance indicators are supported by a reported 97.9% reduction in the number of unauthorised access events. This indicates that the framework is safer compared to conventional systems (Waghe et al., 2024, p. 9). In addition, the long-term studies of the system work also prove that it is 15 times faster to process transactions due to dynamic entropy-based chaining, which does not need to repeat the calculation of hashes as many other state-of-the-art ways (Chakravarthy et al., 2025, p. 17). Also, a Hyperledger Fabric environment that relies on a Delegated Proof of Stake consensus mechanism and Role-Based Access Control governance will further reduce throughput and latency. This is a huge difference with the traditional RAFT and Kafka-based systems (Sawant and Gomes, 2026). This optimisation can also be used to reduce the time of finalizing transactions as well as make the system more scalable in general which address some of the most common issues with centralised healthcare data management (Ullah et al., 2025, p. 20). The throughput and latency increased as would be expected. Such works demonstrate that blockchain-cloud hybrid solutions, where an off-chain data processing is performed using traditional symmetric encryption, can handle a high number of transactions and maintain a low latency level, particularly when the number of users simultaneously is high (Ullah et al., 2025, p. 19). This hybrid model has been established to provide more protection in the case of data breaches and operations are made efficient. It has immensely enhanced data integrity, consensus efficiency, fault tolerance, data availability, latency, bandwidth utilisation, throughput, memory usage and CPU usage in a series of healthcare applications (Brijwani et al., 2025). The experimental outcomes depict that the transaction latency has been reduced 40 percent in comparison to the traditional cloud models. As an illustration, during emergency medical response, smart contracts took an average latency of 120 milliseconds, which is significantly better than the over 200 milliseconds of central systems (Sammangi et al., 2025, p. 7). Such performance advantage is further emphasized by the particular use of blockchain such as BC-HCPPM that have significantly lower latency and percentages of security than other such methods as CP-ABE, CINEMA, and DTMS and in particular Electronic Medical Record length of up to 1000 bits (Saini et al., 2024, p. 94). Such high performance is observed in any type of simulation, even in the cases that demonstrate a higher speed of block propagation and a 30-percent decrease in network bandwidth consumption (Pradhan et al., 2022). Privacy-preserving medical data management architecture based on blockchain-facilitated encrypted role-based model was up to 15 times more efficient than the conventional centralised EHR system (Taloba & Rayan, 2025). Kafka message queues are used in an IoHT platform that is enhanced by a Blockchain to ensure that messages get delivered even in the event of connection failures. This is significant to the continuous patient care and correct analysis (T et al., 2024, p. 5).

CONCLUSION

This paper systematically examined how blockchain technology can be implemented into healthcare information systems and how it can be very useful in addressing current challenges of data privacy, security, integrity, availability, and interoperability. The experimental results confirmed that blockchain-based architectures provide a strong and resistant to alterations framework of managing sensitive healthcare information without damaging the efficiency of the operations. The blockchain system

repeatedly showed high data integrity scores, as well as a high level of privacy through cryptography access control and high availability even under simulated node failure. The findings showed that single points of failure were much less probable and it was less probable that someone would willingly have unauthorised access to data and modify it through the decentralisation and consensus processes. Although the concern was raised on the additional work that computers were required to perform, the level of latency were maintained at levels that were not acceptable by healthcare operations and transaction throughput displayed that it had the potential to perform more work. In addition to the benefits of permissioned access models and smart contract mechanisms, patient-centered data governance became even more precise as it became possible to control the sharing of data and managing consent more closely. The visual and tabular assessments demonstrated that the security improvements did not have a detrimental effect on the system performance, on the contrary, they assisted to establish a balanced and efficient healthcare data environment. The research indicates that blockchain can be applied to additional purposes other than electronic health records. It is also applicable in clinical trials, pharmaceutical supply chains, and audits in healthcare where the importance of trust and openness is very high. In general, the outcomes indicate that blockchain is an effective and transformative technology to the existing healthcare information systems. It is able to make data more reliable, assist with regulation, and establish safe interoperability among various healthcare stakeholders. These results provide a solid empirical foundation of future large-scale deployments and policy-based integration of blockchain technologies within the healthcare facility.

REFERENCES

Adeghe, E. P., Okolo, C. A., & Ojeyinka, O. T. (2024). Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes [Review of Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes]. Open Access Research Journal of Science and Technology, 10(2), 13.

Alex, K. B., & Selvan, K. (2024). Developing a Security Enhancement for Healthcare Applications Using Blockchain-Based Firefly-Optimized Elliptic Curve Digital Signature Algorithm. Research Square (Research Square).

Almeman, A. (2024). The digital transformation in pharmacy: embracing online platforms and the cosmeceutical paradigm shift. Journal of Health Population and Nutrition, 43(1).

Altamimi, A. M., Qattous, H., Barakat, D., & Hazaimeh, L. (2024). Factors Influencing Adoption of Blockchain Technology in Jordan: The Perspective of Health Care Professionals. Interdisciplinary Journal of Information Knowledge and Management, 19, 12.

Anjum, M., Kraïem, N., Hong, M., Dutta, A. K., Daradkeh, Y. I., & Shahab, S. (2025). Opportunistic access control scheme for enhancing IoT-enabled healthcare security using blockchain and machine learning. Scientific Reports, 15(1).

Atadoga, A., Elufioye, O. A., Omaghomi, T. T., Akomolafe, O., Odilibe, I. P., & Owolabi, O. R. (2024). Blockchain in healthcare: A comprehensive review of applications and security concerns [Review of Blockchain in healthcare: A comprehensive review of applications and security

concerns]. International Journal of Science and Research Archive, 11(1), 1605.

Benaich, R., Mendili, S. E., & Gahi, Y. (2023). Advancing Healthcare Security: A Cutting-Edge Zero-Trust Blockchain Solution for Protecting Electronic Health Records. HighTech and Innovation Journal, 4(3), 630.

Bennacer, S. A., Sabiri, K., Aaroud, A., Akodadi, K., & Cherradi, B. (2023). A comprehensive survey on blockchain-based healthcare industry: applications and challenges. Indonesian Journal of Electrical Engineering and Computer Science, 30(3), 1558.

Blockchain Applications - Transforming Industries, Enhancing Security, and Addressing Ethical Considerations. (2022). In IntechOpen eBooks. IntechOpen.

Brijwani, G. N., Ajmire, P. E., Junaid, M., Charasia, S. A., & Bhende, D. (2025). Revolutionizing Healthcare Record Management: Secure Documentation Storage and Access through Advanced Blockchain Solutions. arXiv (Cornell University).

Chakravarthy, D. P., Gopi, R., Murugan, S., & Joseph, E. (2025). Enhancing confidentiality and access control in electronic health record systems using a hybrid hashing blockchain framework. Scientific Reports, 15(1).

Chitikela, A. N. (2024). Secure and Transparent Medical Record Management System Using Python and Blockchain. arXiv (Cornell University).

Elghoul, M. K., Bahgat, S. F., Hussein, A. S., & Hamad, S. (2023). Securing Patient Medical Records with Blockchain Technology in Cloud-based Healthcare Systems. International Journal of Advanced Computer Science and Applications, 14(11).

Faneela, Khan, M. A., Alsuhibany, S. A., El-Shafai, W., Rehman, M. U., & Ahmad, J. (2023). An Immutable Framework for Smart Healthcare Using Blockchain Technology. Computer Systems Science and Engineering, 46(1), 165.

Hameed, K., Naha, R. K., & Hameed, F. (2024). Digital transformation for sustainable health and well-being: a review and future research directions [Review of Digital transformation for sustainable health and well-being: a review and future research directions]. Discover Sustainability, 5(1). Springer Nature.

Handayani, I., Apriani, D., Mulyati, M., Zahra, A. R. A., & Yusuf, N. A. (2023). Enhancing Security and Privacy of Patient Data in Healthcare: A SmartPLS Analysis of Blockchain Technology Implementation. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 5(1), 8.

Hossain, M. I., Steigner, T., Hussain, M. I., & Akther, A. (2024). Enhancing Data Integrity and Traceability in Industry Cyber Physical Systems (ICPS) through Blockchain Technology: A Comprehensive Approach. arXiv (Cornell University).

Hussain, M. I., Bhuiyan, M. Z. A., Sumon, S. A., Akter, S., Hossain, M. I., & Akther, A. (2024). Enhancing Data Integrity and Traceability in Industry Cyber Physical Systems (ICPS) through Blockchain Technology: A Comprehensive

Approach. Advances in Artificial Intelligence and Machine Learning, 4(4), 2883.

Ibor, A. E., Edim, E. B., & Ojugo, A. A. (2023). Secure Health Information System with Blockchain Technology. Journal of the Nigerian Society of Physical Sciences, 992.

Jha, V. (2025). Blockchain Empowered Personal Health Records: Enhancing Security, Privacy, and Interoperability in Healthcare Management. International Journal for Research in Applied Science and Engineering Technology, 13(4), 6145.

Kaafarani, R., Ismail, L., & Zahwe, O. (2024). Automatic Recommender System for Smart-Contracts-based Healthcare Insurance Fraud Detection Development Platform: Design, Implementation, and Performance Evaluation (Preprint). Journal of Medical Internet Research, 26.

Karmakar, S., Bhaduri, A., Kumari, P., & Soni, K. (2023). Blockchain Technology for Securing Electronic Health Records: A Comprehensive Review and Future Directions [Review of Blockchain Technology for Securing Electronic Health Records: A Comprehensive Review and Future Directions]. International Journal for Research in Applied Science and Engineering Technology, 11(3), 2266. International Journal for Research in Applied Science and Engineering Technology (IJRASET).

Kasyapa, M. S. B., & Vanmathi, C. (2024). Blockchain integration in healthcare: a comprehensive investigation of use cases, performance issues, and mitigation strategies. Frontiers in Digital Health, 6.

Khot, Mr. M. S., & Madalgi, J. B. (2023). Application of Blockchain in HealthCare: Overview. International Journal for Research in Applied Science and Engineering Technology, 11(8), 280.

Kshetri, N., Mishra, R., Rahman, M. M., & Steigner, T. (2024a). HNMblock: Blockchain technology powered Healthcare Network Model for epidemiological monitoring, medical systems security, and wellness. arXiv (Cornell University).

Kshetri, N., Mishra, R., Rahman, M. M., & Steigner, T. (2024b). HNMblock: Blockchain Technology Powered Healthcare Network Model for Epidemiological Monitoring, Medical Systems Security, and Wellness. 1.

Li, K., Sai, A. R., & Urovi, V. (2024). Do you need a blockchain in healthcare data sharing? A tertiary review [Review of Do you need a blockchain in healthcare data sharing? A tertiary review]. 101.

Madhoun, N. E., & Hammi, B. (2024). Blockchain Technology in the Healthcare Sector: Overview and Security Analysis. 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 439.

Nath, K. N. S. K., & Kumar, A. K. U. A. (2024). Enhancing Healthcare Security Using IoT and Blockchain through the Perspective of Novel Solidity Smart Contracts. Research Square (Research Square).

Önder, İ. (2022). Blockchain Applications. In Edward Elgar Publishing eBooks (p. 314). Edward Elgar Publishing.

Othman, S., & Getahun, M. (2025). Leveraging blockchain and IoMT for secure and

interoperable electronic health records. Scientific Reports, 15(1), 12358.

Pokharel, B. P., Kshetri, N., Sharma, S. R., & Paudel, S. R. (2025). blockHealthSecure: Integrating Blockchain and Cybersecurity in Post-Pandemic Healthcare Systems. Information, 16(2), 133.

Pradhan, N. R., Singh, A. P., Verma, S., Kavita, K., Kaur, N., Roy, D. S., Shafi, J., Woźniak, M., & Ijaz, M. F. (2022). A Novel Blockchain-Based Healthcare System Design and Performance Benchmarking on a Multi-Hosted Testbed. Sensors, 22(9), 3449.

Puneeth, R. P., & Parthasarathy, G. (2023). Seamless Data Exchange: Advancing Healthcare with Cross-Chain Interoperability in Blockchain for Electronic Health Records. International Journal of Advanced Computer Science and Applications, 14(10).

Quayson, M., Avornu, E. K., & Bediako, A. K. (2024). Modeling the enablers of blockchain technology implementation for information management in healthcare supply chains. Modern Supply Chain Research and Applications, 6(2), 101.

Quazi, F., Raju, N., Gorrepati, N., & Kareem, S. A. (2024). Blockchain Applications in Electronic Health Records (EHRs). International Journal of Global Innovations and Solutions (IJGIS).

Rahal, H. R., Slatnia, S., Kazar, O., Barka, E., & Harous, S. (2023). Blockchain-based multi-diagnosis deep learning application for various diseases classification. International Journal of Information Security, 23(1), 15.

Saini, M., Himanshi, & Saini, S. (2024). Privacy-enhancing Blockchain Solutions for the Healthcare Sector: Efficient Message Sharing and Robust Big Data Protection. Journal of Internet Services and Information Security, 14(3), 85.

Sammangi, H., Jagatha, A., Bojja, G. R., & Liu, J. (2025). Decentralized AI-driven IoT Architecture for Privacy-Preserving and Latency-Optimized Healthcare in Pandemic and Critical Care Scenarios. arXiv (Cornell University).

Sawant, N. M., & Gomes, J. (2026). A Decentralized Solution for Smarter and Safer Healthcare Systems with FabricMedChain. Iranian Journal of Science and Technology Transactions of Electrical Engineering.

Shaikh, M., Memon, S., Ebrahimi, A., & Wiil, U. K. (2025). A Systematic Literature Review for Blockchain-Based Healthcare Implementations [Review of A Systematic Literature Review for Blockchain-Based Healthcare Implementations]. Healthcare, 13(9), 1087. Multidisciplinary Digital Publishing Institute.

Sinha, R. K. (2024). The role and impact of new technologies on healthcare systems. Discover Health Systems, 3(1).

T, D. B., T, T. P. H., P, T. N. D., T, P. N., D, K. T., G, K. H., T, N. B., & K, B. L. (2024). Developing a Patient-Centric Healthcare IoT Platform with Blockchain and Smart Contract Data Management. International Journal of Advanced Computer Science and Applications, 15(4).

Taloba, A. I., & Rayan, A. (2025). A privacy preserving medical data management

framework using blockchain enabled encrypted role based access control. Scientific Reports, 15(1), 43864.

Ullah, A., Ullah, Z., Rizvi, S. S., Gul, L., & Kwon, S. J. (2025). Toward blockchain based electronic health record management with fine grained attribute based encryption and decentralized storage mechanisms. Scientific Reports, 15(1), 34542.

Vaigandla, K. K., Vanteru, M. K., & Siluveru, M. (2024). An Extensive Examination of the IoT and Blockchain Technologies in Relation to their Applications in the Healthcare Industry. Mesopotamian Journal of Computer Science, 2024, 1.

Waghe, P. U., Kumar, A. S., Prasad, A. B., Rao, V. S., Thenmozhi, E., Godla, S. R., & El–Ebiary, Y. A. B. (2024). Blockchain-Enabled Cybersecurity Framework for Safeguarding Patient Data in Medical Informatics. International Journal of Advanced Computer Science and Applications, 15(3).

Wu, D., & Wang, Y. (2024). Revolutionizing healthcare information systems with blockchain. Frontiers in Digital Health, 5.