SCIENTIFIC CULTURE

SCIENTIFIC CULTURE, Vol. 12, No.5, (2026), pp. 260-274
Open Access. Online & Print

www.sci-cult.com
DOI: 10.5281/zenodo.20332248

BLOCKCHAIN-BASED SECURE FRAMEWORKS FOR HEALTHCARE DATA MANAGEMENT: A COMPUTER SCIENCE PERSPECTIVE

Ankush Dhiman[1*], Dr. Asma Rani[2], LNC. Prakash K[3], Anand Kumar Mishra[4], K. Hema[5], Dr. Susmita Biswas[6], Dr. Parmanand Prabhat[7]

[1]Department of Computer Science, Kurukshetra University, Kurukshetra, Haryana-136119, India, Orcid Id: 0009-0002-7843-7301, Email Id: Dhiman.ankush@outlook.com
[2]Assistant Professor, Department of Computer Science and Engineering, Dr. B. R. Ambedkar Institute of Technology, Sri Vijayapuram, Orcid Id: 0000-0001-6087-6248, Email Id: asma.sags@gmail.com
[3]Associate Professor, Department of Computer Science and Engineering (Data Science), CVR College of Engineering, Hyderabad, Telangana, Orcid Id: 0000-0002-0084-1331, Email Id: lncprakashk@gmail.com
[4]Assistant Professor, School of Engineering and Technology (UIET), CSJM University Kanpur, Uttar Pradesh, Orcid Id: https://orcid.org/0009-0009-7039-4088, Email Id: mishra.anand13@gmail.com
[5]Assistant professor, Department of Computer science engineering, Specialization in Machine learning, Koneru Laksmaiah Education Foundation bowrampet, Hyderabad, Email Id: k.hema@klh.edu.in
[6]Associate Professor, Department of Cyber Science & Technology, Specialization in Artificial Intelligence, Brainware University, Orcid Id: 0000-0002-6317-5620, Email Id: bi.susmita@gmail.com
[7]Assistant Professor, Department of Artificial Intelligence and Machine Learning, Specialization in Computer Science, Engineering BGS Institute of Technology, Adichunchanagiri University, Mandya District, Karnataka-571448, India, Orcid Id:0009-0004-6767-5130, Email Id: parmanandprabhat@bgsit.ac.in

Abstract
Healthcare data security management has become a major issue in the digital health environment due to the rapidly growing number of electronic health records, inter-medical devices, telemedicine services, and inter-institutional data exchange. The classic centralized systems usually face the same problems of being exposed to privacy, low interoperability, patient lacks control, single point failure, and not ability to audit. Blockchain has come up as a promising technology to overcome these constraints by means of decentralization, immutability, cryptographic verification and transparent recording of transactions. Another perspective that can be analyzed as a computer science is blockchain, which can be leveraged to achieve a more holistic security architecture that can be deployed to manage and maintain trustful healthcare information. The paper discusses secure systems that consist of blockchain and builds a layered architecture consisting of user, application, smart contract, blockchain and off-chain storage. The framework enables the management of encrypted records, control access through consent, audit trail that cannot be altered, and the sharing of data between the patients and the health care providers, laboratories, and health insurance companies in a secure manner. Analytical analysis demonstrates high integrity, auditability, access governance and interoperability performance as well as demonstrates practical constraints in scalability, computational overhead and complexity of integration. The results show that blockchain would best work within a hybrid system as opposed to an all-on-chain system. Authenticated, transparent and disseminated healthcare data management can be therefore strengthened with the well-organized blockchain frameworks that balance security, efficacy and practical applicability in the modern healthcare societies.

Keywords: *Blockchain; Healthcare Data Management; Data Security; Smart Contracts; Decentralized Systems*

1. Introduction

The fast health care digitalization has revolutionized the creation, storage, exchange and utilization of medical information in clinical decision making. The electronic health records, telemedicine systems, interconnected diagnostic devices and mobile health platforms have augmented the quantity and complexity of healthcare data and thus secure data management has become a key issue in the contemporary health

informatics. Since medical records include a lot of personal and clinical data which is sensitive, ineffectiveness of storing and sharing systems will directly influence patient privacy and institutional trust and continuity of care. Recent research has highlighted that the issue of healthcare data management has ceased to be solely a technical storage issue, and a more general difficulty that touches on confidentiality, integrity, traceability, and secure interoperability among various actors in healthcare (Tariq et al., 2020).

Traditional healthcare data management systems are traditionally centrally-based or institution-centric systems. Despite their popularity in use, such models are susceptible to fragmentation, limited interoperability, lack of transparency and susceptible to unauthorized access or tampering of data. Practically, patient records can be spread over hospitals, labs, insurance companies, and experts, posing significant challenges to achieve effective coordination. In case of systems that are not well integrated, healthcare providers might be subjected to delays in accessing all and authenticated information about a patient and the patients have very little control on the usage and sharing of their records. An overview of blockchain-enabled safe healthcare data sharing has revealed that these endemic vulnerabilities of the conventional systems still drive the quest to identify more trustworthy and decentralized methods of medical data sharing (Xi et al., 2022).

One potential technology that has emerged in this regard due to its decentralized nature, immutability, auditability, and capability to support cryptographic verification is blockchain. Blockchain makes it possible to validate records and have tamper-resistant transaction history, unlike traditional databases, which are highly reliant on central administrative control. In terms of computer science, these properties become particularly pertinent to the healthcare setting where numerous stakeholders need to access trusted information without invading the privacy. An initial study of data management in blockchain-based systems has revealed that blockchain can be viewed not only as a ledger, but as a more general architectural paradigm that encompasses governance, security logic and distributed trust, which are quite applicable to healthcare data management (Paik et al., 2019).

The use of blockchain in the healthcare field has already gone beyond mere speculation. A number of studies suggest safe blockchain-based systems to handle patient records, authorization of data access as well as supporting privacy-friendly healthcare transactions. To illustrate, a distributed architecture of a safe healthcare data management system demonstrated the ability of distributed architectures to reinforce trust, minimize unauthorized manipulation, and enhance more regulated information exchange among healthcare organizations (Taloba et al., 2021). Similarly, additional recent studies on the subject of secure blockchain-based healthcare record management have cemented the importance of combining ledger security with organized access controls and feasible aspects of system design (Al-Khasawneh et al., 2024). According to these studies, blockchain can offer a significant basis in the healthcare data protection when implemented into well-thought-out frameworks.

In spite of these developments the literature is still fragmented. A lot of research concentrates on the individual elements of records storage, integration of Internet of Medical Things, interoperability or access control, but not on how these aspects are to be integrated to make up a full secure system. Blockchain, cloud, and IoT-based patient-centric healthcare reference architecture has demonstrated the significance of semantic interoperability and coordination of systems, demonstrating that secure management of healthcare data cannot be achieved by an isolated technical solution; a coherent architecture is necessary, capable of balancing distributed storage, secure access, and functional integration across a wide range of healthcare settings (Gohar et al., 2022). This means that there is still a need of the framework level analysis which is explicitly based on the computer science principles.

In line with this, this paper will analyze secure frameworks of healthcare data management based on blockchain with a computer science approach. This paper aims at design logic, architectural elements and security applicability of such frameworks with specific reference to decentralization, access control, data integrity and its practical application in digital healthcare ecosystems. The research has four goals, namely, to investigate the key issues of security and privacy in healthcare data management, to discuss how blockchain can help to overcome the issues, to determine the key elements of the safe blockchain-based healthcare systems, and to compare and contrast their strengths and weaknesses. Through this, the paper attempts to contribute towards a systematic understanding of the possibility of deploying blockchain to realize secure healthcare data management, not based on individual application scenarios. The rest of the paper discusses the literature on the topic, outlines the theoretical background, the research design, structure of the framework, implications, limitations and future research directions.

2. Literature Review

The academic body of blockchain-based healthcare data management has been growing at an unprecedented pace and it can be attributed to the increasing demands of secure, transparent and distributed means of managing sensitive medical data. Initial framework-based research formed the technical basis upon which this direction was set and demonstrated that blockchain could be modified to suit healthcare settings as a tool of enhancing trust, integrity of records and accountability. The healthcare system design proposed by Chakraborty et al. (2019) emphasized the concept of blockchain being able to offer a structural alternative to the centralized medical data system since it offers an immutable record of transactions and exchangeable information with the possibility to be verified. This first engagement helped to lay the groundwork of blockchain, not as a storage platform, but as a security-oriented design to create a healthcare system.

Later researches shifted their focus to conceptual design to more practical healthcare architectures. Khubrania (2021) proposed a smart health model, which applies blockchain to highlight the benefits of decentralization of coordination of data in health services, especially where various participants must access records in a timely and trustworthy fashion. Similarly, Abbas et al. (2024) created a blockchain-based secured information management system to analyze health information within Internet of Medical Things settings, showing how blockchain can be utilized to enable healthcare ecosystems with continuous data generated by devices. Its importance lies in the fact that this work not only expands the scope of blockchain in terms of protecting records but also in the management of health data on a dynamic basis in interconnected and connected medical infrastructures.

The adoption of blockchain in collaboration with other enabling technologies has evolved into a significant tendency in the literature. The system that Azbeg et al. (2022) offered that integrates IoT, blockchain, and IPFS is BlockMedCare, which should be used to tackle the security of medical data management. Their research is significant in the sense that it acknowledges that blockchain might not be effective in managing the storage needs of large medical records and as such is supported by off-chain or distributed storage. The same hybridist approach is observed in the article by Rathee et al. (2020) who proposed a framework of multimedia data processing in IoT-healthcare based on blockchain technology. Their input demonstrates that healthcare data management is turning into a high volume and multimedia intensive information, and therefore needs models that can maintain security without compromising the processing feasibility. Continuing this vein, Taloba et al. (2023) introduced a blockchain-based hybrid platform of multimedia data processing in IoT-healthcare, which further supports the claim that healthcare data systems need to integrate blockchain with additional computational layers to be efficient and applicable in the real world.

The second significant theme in the literature is how the distributed computing paradigms can be used to enhance secure data management in healthcare. Ngabo et al. (2021) considered a security system of medical data using blockchain technology in a fog computing network of the Internet of Things. Their results are applicable as the use of fog-assisted healthcare systems lowers the latency and promotes local processing but ensures that there is strong security and coordinated trust. This implies that blockchain systems can be particularly useful in cases where healthcare information is generated and consumed at decentralized computers, as opposed to a central database.

In the literature, privacy and patient control are also key issues. Masood et al. (2024) came up with a blockchain-based system that is directly related to patient data privacy and security, indicating the necessity to provide patients with greater protection and allow them to have a more transparent control over their data. Their work is representative of a wider trend in healthcare data research to patient-centered security models where data sharing needs to be secure and responsible. Sun et al. (2022) implemented a secure storage system of medical records on a blockchain, in a more storage-oriented contribution, which showed that to maintain effective healthcare information management, special attention must be paid to the division between the content of the protected records and the blockchain protocols that ensure integrity and verification. This literature all points to the fact that privacy in healthcare blockchain systems is not an additional feature, but is a design requirement.

There are also other studies on how blockchain structures can be used to enable sophisticated and smart healthcare applications. An example of how blockchain can be incorporated into predictive and data-intensive medical processes is provided by Shynu et al. (2021), who came up with a blockchain-based secure application in healthcare to predict diabetic-cardio disease in the context of fog computing. This is remarkable as it links secure data management to clinical analytics, indicating that the next generation of the healthcare system

will have to be able to protect and intelligent use patient data. A more futuristic view is presented in Galety et al. (2025) that spoke about the medical data security and organization through built-in blockchain concepts in AI based Healthcare 6.0 architecture. According to their work, blockchain is likely to become an increasingly important part of future health care ecosystems that will be based on artificial intelligence, automation, and the highly interconnected digital services.

Another issue that reoccurs is lightweight and efficient security design. Mahajan and Junnarkar (2023) introduced a smart healthcare system, which combines lightweight elliptic curve cryptography with a private blockchain in processing multimedia medical data. The significance of this contribution is that it is focused on the practical issue of the burden of computations in healthcare systems, particularly when the resources are limited and speedy secure calculations are necessary. This kind of work reinforces the perception that the effectiveness of blockchain in healthcare should be not just based on theoretical security, but also implementation efficiency. In general, the literature under review demonstrates that blockchain has evolved since it was a theoretical approach to data security to a more general technology of healthcare data management. Current literature shows that it has been used in relevant areas to ensure secure sharing of records, privacy maintenance, hybrid storage, integration of IoT and fog, multimedia data processing and intelligent healthcare applications. Concurrently, the literature is still spread in the area of specific themes, which brings about the necessity of a more consolidated study of blockchain-based secure systems in terms of computer science.

3. Theoretical and Conceptual Foundation

This section lays the computer science foundation of the study through the connection of healthcare data security needs with the framework design that is blockchain-enabled. Data management in healthcare systems is not just about data storage and retrieval, it must also be confidential, data integrity, availability, authentication, authorization, and accountable. Due to the fact that medical records are read by various stakeholders, in a distributed environment, an effective framework should involve a combination of technical protection, reliable validation and controlled access. In this light, blockchain should not be interpreted as a database replacement, but rather as an architectural layer that is security-focused, capable of enabling verifiable, decentralized and policy-driven healthcare data management.

3.1 Security Principles in Healthcare Data Management

Information systems in the healthcare sector handle records which are very sensitive such as diagnoses, prescriptions, laboratory reports, and patient identifiers. This is why, any safe healthcare system should comply with fundamental information security principles. Confidentiality ensures that records are not disclosed to unauthorized individuals; integrity that medical data cannot be altered without any detection and availability that the data will be accessible when the clinical use is legitimate. Moreover, authentication is used to confirm the user identity, authorization is used to determine what actions can be performed and accountability logs the user who should have accessed or altered the data. The principles are particularly significant in healthcare, as incorrectness or unauthorized interference can have a direct impact on the treatment results. An electronic health record protection framework implemented using blockchain demonstrated that to have a secure healthcare system, tamper detection and reliable records history, rather than simple database access rules, are required (Faruk et al., 2022). In this way, security of data in healthcare should not be considered as an administrative task but as an architectural requirement.

3.2 Blockchain as a Security Architecture

Blockchain brings with it a decentralized system of validating and recording transactions and cutting off the reliance on one controlling force. Its primary theoretical advantages are immutability, auditability, traceability and distributed trust. These are particularly applicable in the field of healthcare where data commonly traverses hospitals, laboratories, physicians, insurers, and patients. A privacy-preserving healthcare system showed that blockchain can facilitate secure and trusted exchange of records by ensuring verifiable records of exchanges and minimizing the chances of possible covert alterations (Al Omar et al., 2017). The concept of blockchain should not, however, be understood as the only place where all the medical content will be stored. Big medical records and data constantly generated by devices should be managed out of the chain instead, and blockchain stores hashes, authorizations, and logs of transactions. In this regard, it performs a conceptual role of a trust and validation layer in a larger framework in healthcare.

3.3 Cryptographic Protection and Access Control
The cryptographic protection and fine-grained access control should also be included in a safe blockchain-based healthcare system. Encryption is used to ensure patient information is safe when storing and transmitting the information such as when the records are stored in off-chain repositories or when information is shared over semi-trusted networks. An in-house blockchain-based cryptographic system ensured the cryptographic techniques continue to be at the core of securing sensitive distributed data settings (Ghazal et al., 2022). Access control, in conjunction with encryption, defines access to healthcare records, who can view, modify, or share such records. Given that healthcare data cannot be publicly accessible to all stakeholders, the authorization should be in accordance with the roles and institutional policies as well as patient consent. The lattice-based access control combined with blockchain smart contracts has been shown to be valuable through research that showed the worth of structured, rule-based authorization in healthcare systems (Haritha and Anitha, 2023). Similarly, a model of decentralized self-managed access control has been suggested as a privacy-conscious model where permission logic can be audited, and less reliant on centralized gatekeeping (Saidi et al., 2022). Encryption and the control of access are the two keys to a safe healthcare system.

3.4 Conceptual Basis of the Proposed Framework
According to these principles, in this paper, a conceptual framework was proposed, where secure healthcare data management is developed based on four interacting functions, namely data protection, trust validation, access governance and distributed coordination. Data security is ensured by encryption and safe storage, trust verification by immutable logs based on blockchain, access control with smart contracts and permission policies, and distributed coordination enables various healthcare participants to communicate without the need to have one central point of control. An edge blockchain-based model of health data exchange demonstrated that healthcare systems tend to need increasingly layered architectures where processing, exchange, and validation are performed at various computational layers (Akkaoui et al., 2020). This goes in favor of the current research that blockchain is an appropriate security and trust foundation in a layered healthcare architecture. Table 1 provides an overview of the mapping of key healthcare security requirements to key elements of a blockchain-based framework.

Table 1. Mapping of Healthcare Security Requirements to Blockchain-Based Framework Components

Healthcare security requirement	Meaning in healthcare systems	Framework component
Confidentiality	Prevents unauthorized disclosure of patient records	Encryption and permissioned access
Integrity	Prevents undetected data alteration	Immutable ledger and hash verification
Availability	Ensures timely access for authorized care delivery	Distributed architecture and resilient storage
Authentication	Verifies legitimate users and entities	Identity verification mechanisms
Authorization	Controls permitted actions on records	Smart contracts and access policies
Accountability	Tracks user actions and transactions	Auditable blockchain logs

Figure 1 illustrates the conceptual structure of the proposed blockchain-based secure healthcare framework by showing the relationship between security requirements, blockchain trust mechanisms, cryptographic protection, and access governance.

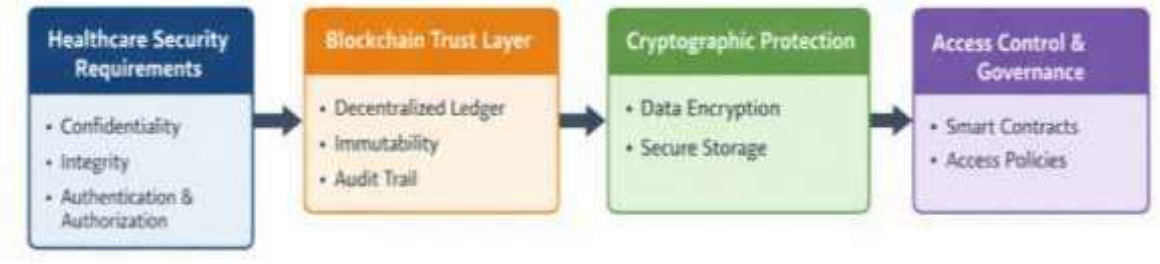

Figure 1. Conceptual foundation of the blockchain-based secure healthcare framework

4. Proposed Blockchain-Based Secure Framework for Healthcare Data Management

This part provides the suggested blockchain-realized safe model of healthcare data management. The framework has a computer science focus to overcome the key shortcomings of the traditional healthcare information systems especially centralized control, poor traceability, low patient control and susceptibility to unauthorized access. The suggested model is based on a layered approach whereby blockchain is the core of trust and verification, and smart contracts, cryptographic protection, as well as off-chain storage, facilitate the efficient and secure management of healthcare data. The framework will be used in settings that include patients, physicians, hospitals, and laboratories, insurance companies, and approved administrative bodies.

4.1 Framework Overview

The framework suggested is based on the idea that the healthcare data must be handled by means of a decentralization approach, controlled access, secure storage and auditable transactions. Instead of the medical records being stored on the blockchain, the framework divides the data into two parts: the secured healthcare content and blockchain-verified metadata. Delicate medical records are encrypted and stored in a safe off-chain storage system whereas the blockchain records hashes, transaction references, time-stamps, consent records, and access log records. This architecture ensures that there is less storage load and integrity and traceability are maintained.

The framework is institutionally coordinated and patient-centered. Patients will be at the heart of consent and data access, whereas hospitals and healthcare staff work on a permissible basis. Smart contracts control authentication, access requests, conditions of approval and audit logging. By so doing, the framework facilitates secure creation, retrieval, updating and sharing of records without necessarily having to depend on one central repository. Table 3 presents the outline of the structural make-up of the suggested framework.

Table 3. Architectural Layers of the Proposed Framework

Layer	Main entities/components	Core function
User Layer	Patients, physicians, hospitals, laboratories, insurers, regulators	Initiates and receives authorized healthcare transactions
Application Layer	EHR interface, mobile health portal, request management modules, dashboards	Provides user interaction and healthcare service access
Smart Contract Layer	Consent contract, access contract, audit contract, identity contract	Automates rules for validation, permissions, and logging
Blockchain Layer	Distributed ledger, transaction records, timestamps, hash references	Preserves integrity, immutability, and traceability
Storage Layer	Encrypted databases, cloud repositories, distributed file storage	Stores medical files and large healthcare records securely

The overall architectural structure of the framework is illustrated in **Figure 3**.

Figure 3. Layered architecture of the proposed blockchain-based secure healthcare framework

4.2 System Architecture

There are five layers that are built into the structure. The User Layer involves all actors that create, order, endorse or utilize healthcare data. The players in this include patients, physicians, hospitals, diagnostic labs, insurance agencies and regulators. All the participants are unique to the system based on pre-determined roles and access privileges.

Application Layer is the service interface between the users and the framework. It encompasses patient-facing applications, eHr portals, administrative dashboards, medical request interfaces, and patient-facing applications. This layer will handle requests, show healthcare information to verified users and send verified actions to the smart contract layer.

The core of the system is the rule-governance part, the Smart Contract Layer. It includes patient consent contracts, role based authorization, identity validation contracts and transaction auditing contracts. A smart contract ensures identity verification, access policy checks, and verifies whether an action is permitted or not when a healthcare actor requests access to a patient record. Any approvals, denials and modifications are automatically recorded.

The metadata of transactions, access logs, timestamps, permissions, and cryptographic hashes of healthcare files are placed in the Blockchain Layer. It keeps the history of transactions unchanged and can be subject to any appropriate change in the future. This layer guarantees that manipulation of records is not possible in a way that can go unnoticed.

Storage Layer is the location where the encrypted medical files themselves, such as patient histories, prescriptions, diagnostic reports and imaging outputs, are stored. As medical data can be huge and constantly changing, off-chain storage enhances the efficiency whereas the blockchain maintains a record of authenticity and history of access.

4.3 Working Mechanism of the Framework

The framework works in a series of data management. To begin with, a healthcare record is established by a hospital, a physician, a laboratory or a medical device. Secondly, the record is encrypted and saved in the secure storage layer. Third, the blockchain is written to with a cryptographic hash of the record, and metadata, including timestamp, identity of the creator, and a reference to storage. Fourth, when an access request is necessary by another authorized actor, an access request is made via the application layer. Fifth, smart contract makes its evaluations based on the request identity, role, consent status, and policy conditions. Sixth, upon meeting the necessary criteria, the request gets an access and vice versa. Seventh, all the requests, approvals, updates, and retrievals are documented in the blockchain ledger in the audit trail. Figure 4 represents the working process.

Figure 4. Workflow of secure healthcare data management in the proposed framework

4.4 Security Features of the Framework

The framework aims at meeting key healthcare security needs with built-in architectural controls. Access is granted by encryption and permission-based access with the aim of ensuring confidentiality. The integrity is ensured because the record hashes and transaction proofs are stored in the blockchain. The support of availability is the distributed access design and the resilient storage architecture. Before any transaction is carried out, authentication is done by identity verification procedures. During the process of authorization, smart contract rules based on user roles and consent conditions are implemented. Audit logs of everything that occurs in the system are immutable, and accountability is ensured. The association between security goals and framework mechanisms is summarized in Table 4.

Table 4. Security Mapping of the Proposed Framework

Security objective	Framework mechanism	Expected outcome
Confidentiality	Encryption and controlled permissions	Prevents unauthorized data disclosure
Integrity	Hash verification and immutable ledger	Detects unauthorized modification
Availability	Distributed access and secure storage	Supports timely data access
Authentication	Identity verification process	Confirms legitimate users
Authorization	Smart contract-based access rules	Restricts actions to approved entities
Accountability	Blockchain audit trail	Enables traceability and review

4.5 Role of Smart Contracts

The proposed framework will have smart contracts to undertake the central governance role. They automate rules of validation which would be otherwise based on manual institutional regulation or centralized administrative rationale. Consent smart contract is used to control the condition of consenting patients to share their data. An access contract defines the access rights of a user to a healthcare record (i.e. if a user can read, edit or move it). The events are recorded in an audit contract to be verified in the future. An identity contract is one that associates the roles with authorized actions of participants. The design enhances consistency, lessens policy ambiguity and enhances enforcement of rules among distributed healthcare entities.

4.6 Functional Advantages of the Framework

The suggested system has a number of benefits compared to traditional healthcare data systems. It decreases reliance on a single point of centralized control, enhances trust by having an unchangeable history of transactions, aids patients in gaining control over the data they access, and allows sharing of information with numerous institutions. It also balances the security and efficiency of operations by decoupling blockchain verification and off-chain storage. The model is thus appropriate in current healthcare settings where there is need to have secure coordination, distributed trust and controlled interoperability. In Table 5, a comparative overview of the functional benefits of the framework can be found.

Table 5. Functional Advantages of the Proposed Framework

Conventional limitation	Proposed framework response	Functional benefit
Centralized data dependency	Distributed blockchain validation	Reduces single-point failure
Weak auditability	Immutable transaction ledger	Improves traceability
Poor patient oversight	Consent-driven access logic	Strengthens patient control
Limited inter-organizational trust	Shared blockchain verification	Supports trusted exchange
Large record storage burden	Off-chain encrypted storage	Improves scalability and efficiency

In total, the proposed framework includes the layers design, governance of smart contracts, blockchain validation, and safe storage in a uniform way of managing healthcare data. It deals with the safeguarding of medical data as well as the orchestrating needed in distributed healthcare environments.

5. Analysis and Evaluation

Under this section, the proposed blockchain-based secure system will be evaluated in terms of security, functional suitability, system integrity, and its suitability in healthcare environments. It is discussed within the framework of computer science and the possibility to address the technical requirements of the modern data management in healthcare without falling victim to the key weaknesses of the traditional systems. The

framework is discovered to perform well in the integrity of data, auditability, distribution of trust, and controlled access, but has practical concerns with scalability, efficiency of storage, and complexity of implementation. The works on blockchain-based intelligent healthcare services have also shown that safe information platforms are more productive in cases when they are energized by effective protection systems and analytical service-based functionality (Bhattacharya et al., 2019).

5.1 Security Analysis

The suggested model helps to achieve some of the major security objectives in healthcare data management. The privacy is ensured by encryption and role access control based on smart contract. The off-chain sensitive records are kept and on-chain hashes, references, timestamps, and access logs are maintained, enhancing privacy and traceability.

A strong strength is integrity. Any record is associated with a blockchain hash that detects any illegal alterations. This is very essential in health care, where the accuracy in records directly influences clinical decisions. Accountability is also enhanced by blockchain since it has an auditable record of access, updates and verification points. Smart contracts and identity validation are used to implement authentication and authorization. Access policies are provided to various user groups, such as patients, physicians, hospitals, laboratories and insurers. The distributed verification and secure storage support availability, but, in practice, the performance depends on infrastructure and implementation. Table 6 summarizes the key security strengths.

Table 6. Security Evaluation of the Proposed Framework

Security dimension	Mechanism in the proposed framework	Analytical outcome
Confidentiality	Encryption and permissioned access	High protection against unauthorized disclosure
Integrity	Hash verification and immutable blockchain entries	Strong resistance to undetected tampering
Authentication	Identity validation before transaction execution	Supports legitimate user verification
Authorization	Smart contract-based access rules	Enables fine-grained control of permissions
Accountability	Immutable transaction and audit logs	Provides traceable record history
Availability	Distributed architecture with secure storage	Moderate to high, depending on deployment infrastructure

5.2 Comparative Analysis with Conventional Healthcare Systems

The offered framework will provide more transparency, verifiability, and confidence in the data processing in comparison with the centralized healthcare systems. The classical systems are based on the local databases and access rules specific to the institutions, which are effective inside but not outside the institution, with difficulties in sharing records across institutions. They also cause a single point of failure.

The suggested blockchain structure spreads validation and maintains an unchangeable list of important data transactions. This enhances auditing, exchange of records, patient awareness and trust. Patients will be in a better position to monitor the individuals that have accessed their information and all the approved and rejected activities will be registered forever.

Nonetheless, traditional systems might be quicker and easier locally. The centralized databases of hospitals tend to be more effective in addressing internal queries as compared to the permissioned blockchain workflows. Therefore, the suggested framework can best be applied to distributed healthcare and not serve as a complete substitute of the local systems. Table 7 provides the comparison between the traditional frameworks and the suggested one.

Table 7. Comparative Analysis of Conventional Systems and the Proposed Framework

Evaluation aspect	Conventional healthcare systems	Proposed blockchain-based framework
Control model	Centralized or institution-specific	Distributed and rule-governed

Data integrity	Vulnerable to hidden modification	Hash-linked and tamper-evident
Auditability	Often limited or fragmented	Strong and immutable
Trust management	Institution-dependent	Blockchain-verified
Patient oversight	Usually limited	Consent-based and transparent
Inter-organizational exchange	Often difficult	More secure and traceable
Scalability of file storage	High in local systems	Moderate with off-chain storage support
Operational simplicity	Higher in local deployment	More complex but more secure

The comparative profile of the two models can be visually presented in **Figure 5**.

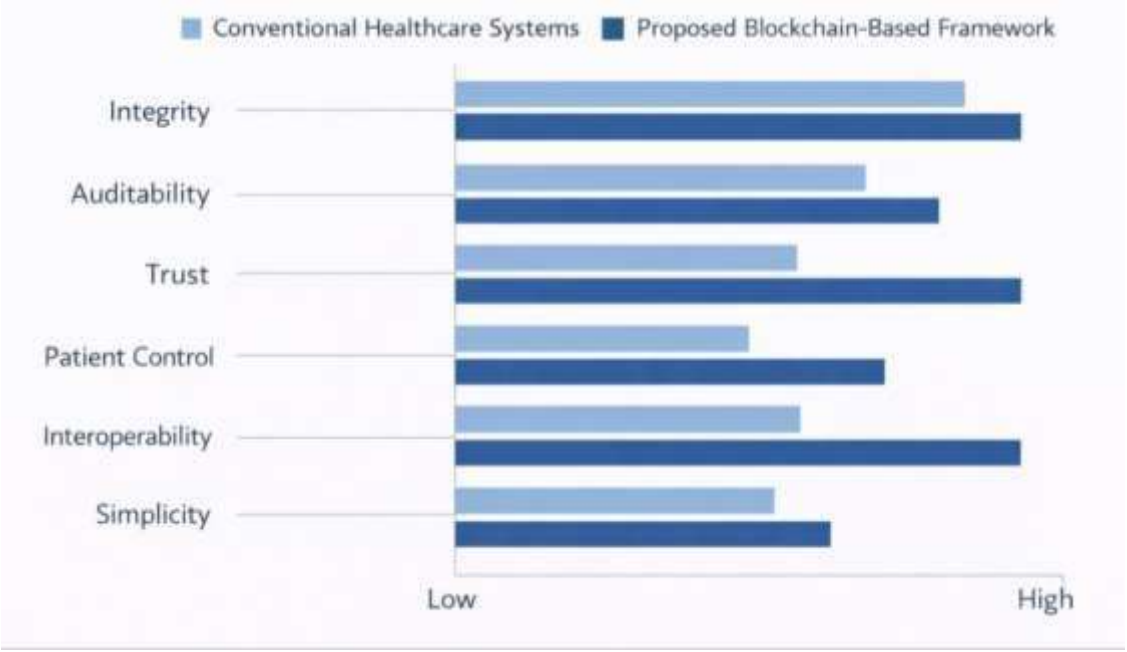

Figure 5. Comparative performance profile of conventional systems and the proposed framework

5.3 Interoperability and Data Management Efficiency

In healthcare, interoperability is necessary since the treatment of patients in most cases may require the input of multiple institutions. The suggested framework helps to achieve this, by decoupling data storage and verification. The blockchain does not store complete records on the blockchain, but rather just references, hashes and permission logs, which allow exchange of trusted information. This enhances coordination and also maintains the authenticity of data.

Off-chain storage is also beneficial to the framework. Repositories holding large files (e.g., diagnostic images, lab reports, multimedia records) are encrypted and blockchain records hold evidence of authenticity. This enhances storage efficiency and the security. But the actual interoperability is still subject to technical standards, common semantics and compatibility with the existing hospital systems. The framework is a safe base, yet to be successfully used by institutions necessitates institutional standardization. Table 8 summarizes an analysis of the operational performance.

Table 8. Operational Evaluation of the Proposed Framework

Operational criterion	**Assessment of the framework**	**Interpretation**
Interoperability support	High	Enables trusted exchange across multiple entities
Storage efficiency	Moderate to high	Improved through off-chain encrypted storage
Transaction transparency	High	All validated activities are recorded on-chain
Access management efficiency	High	Smart contracts automate permission logic
Real-time responsiveness	Moderate	Dependent on network and validation overhead
Integration complexity	Moderate to high	Requires coordination with existing healthcare systems

The efficiency profile of the framework may be illustrated in **Figure 6**.

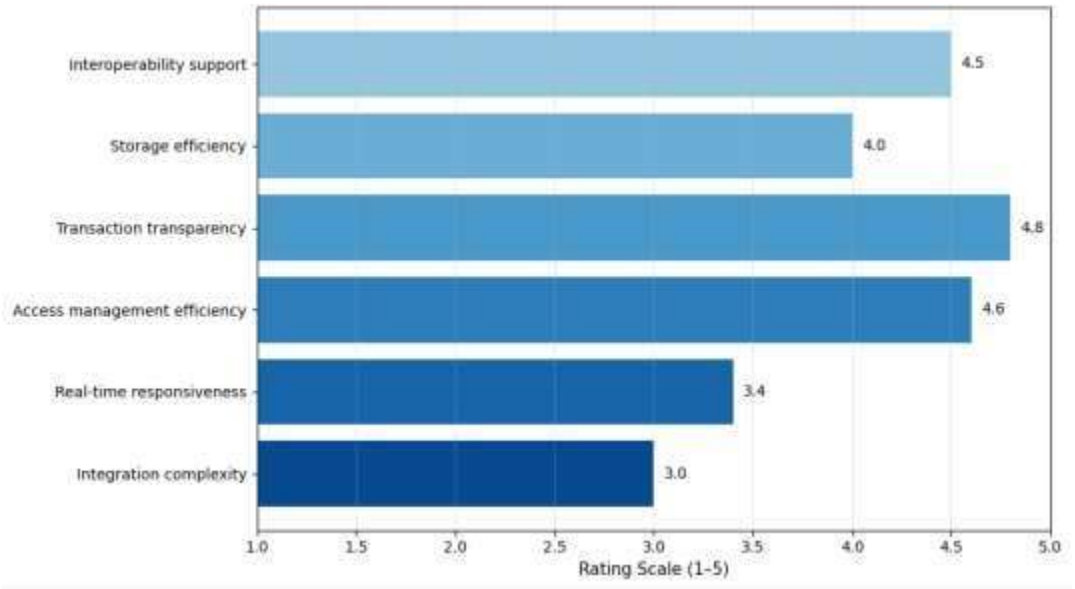

Figure 6. Operational evaluation of the proposed framework

5.4 Scalability and Deployment Constraints

Despite the strong performance of the framework in the areas of security and transparency, one of the main practical challenges is scalability. Healthcare systems produce copious amounts of structured and unstructured data, and heavy transaction loads can raise the latency and computation costs. Off-chain storage can be used to alleviate this load, yet efficient consensus, transaction processing, and network-architecture are required.

Deployment complexity is another limitation. The framework will need to coordinate the activities among institutions, integrate with the current health record systems, identity management, and consent on the access policy. Thus, although the framework provides a safe distributed architecture, the actual implementation performance lies in the fact that the implementation, organizational preparedness, and scalable infrastructure planning are vital in such a structure. Table 9 provides an overview of the key strengths and limitations.

Table 9. Strengths and Constraints of the Proposed Framework

Category	Major strengths	Main constraints
Security	Strong integrity, privacy, auditability, controlled access	Requires robust key and identity management
Architecture	Layered, modular, and suitable for distributed healthcare	More complex than local centralized systems
Data management	Off-chain storage improves efficiency	Integration with legacy systems may be difficult
Governance	Patient-centered and transparent	Policy standardization is required
Scalability	Better than fully on-chain systems	Still affected by validation overhead and transaction growth

A summary visualization of these strengths and constraints may be provided in **Figure 7**.

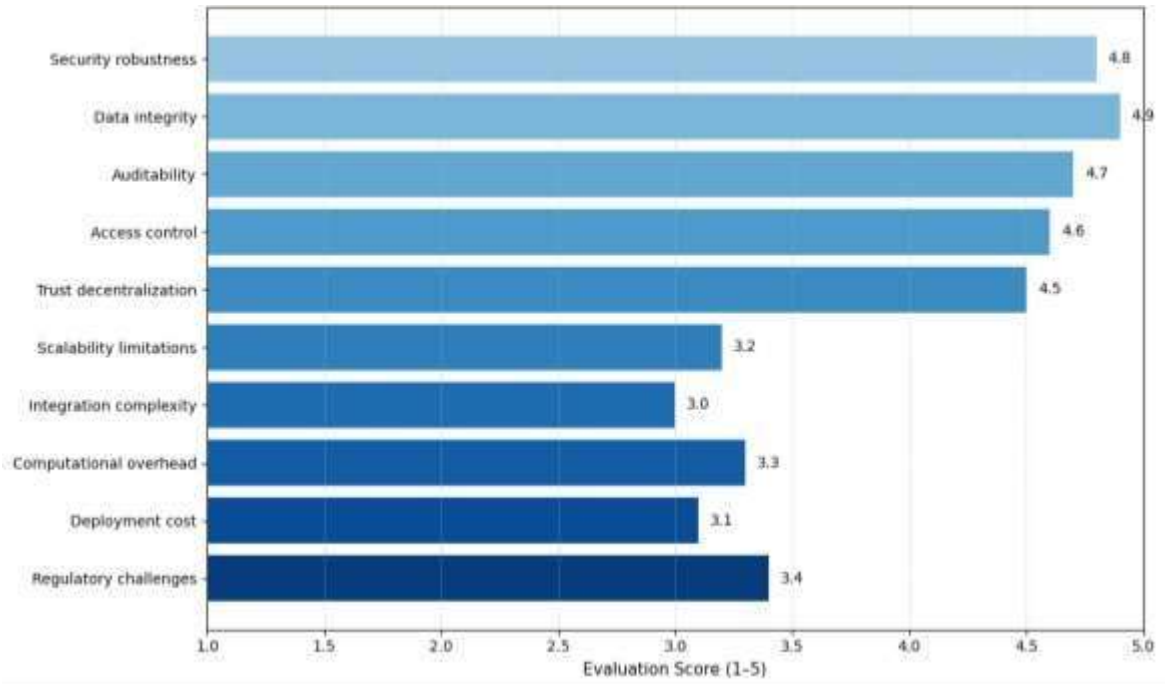

Figure 7. Strength–constraint balance of the proposed framework

In general, the analysis shows that the framework suggested offers a powerful security-based architecture to distributed data management of healthcare information. The key analytical strength of it is its ability to integrate immutable verification and smart contract-based access governance with an efficient off-chain storage into a unified framework. Although traditional systems can be still less complex in remote environments, the suggested framework is better suited to the modern healthcare ecosystems, where interoperability is secured, audit trail is trusted, and data governance is transparent and clear across various institutions.

6. Discussion

The results of the analysis and appraisal indicate that the proposed blockchain-based secure model offers a model of healthcare data management that is both technically compatible and practically feasible. This is what makes it add the most as it combines blockchain verification, smart contracts-based governance and off-chain encrypted storage into a single architecture. It is this stratified structure that led to the framework scoring well in integrity, auditability, access control and interoperability. In the context of computer science, the results indicate that healthcare data security would be most successful when these functions are not considered as independent mechanisms, but are implemented in the framework of coordinated mechanisms. In this regard, the framework meets one of the key shortcomings of most traditional systems wherein storage, access management and trust validation are frequently done in isolation and with minimal transparency.

One of the most significant results of the assessment is that the framework has a good performance in maintaining data integrity and traceability. Since healthcare records are associated with cryptographic hash values and authenticated by using immutable blockchain records, their unauthorized alteration is much easier to notice. This finding is of particular significance in the healthcare context, where the authenticity of the records directly influences the clinical reliability and decision-making. The result aligns with the research by Al-Khasawneh et al. (2024), which contended that secure blockchain systems of healthcare records can be valuable due to the ability to preserve the records and create auditable audit trails. The current paradigm depicts the same idea and its excellent scores on analytics in integrity and auditability indicate that blockchain can do more than just store security; it can also create a responsible account of all significant healthcare data incidents.

Access governance and patient-centered control were also done adequately by the framework. This finding is important since healthcare security is not just maintained by the ability to block external attacks, but also the control of legitimate access by the physicians, hospitals, laboratories and insurers. The proposed model will make access management a programmable and auditable process with the help of smart contracts. This minimizes discrepancy in the manner of granting

and registering permissions. This interpretation can be compared to the survey conducted by Villarreal et al. (2023), which pointed out that blockchain in healthcare is the most useful to be provided with security in addition to transparent and interoperable control measures. The present results support that opinion by demonstrating that patient oversight, logic of authorization and immutable auditability can collaborate in a consistent workflow.

The other strength that the framework enjoyed was interoperability. This model enables safe exchange, between heterogeneous healthcare actors, in which medical files are stored off-chain and only metadata, hashes and transaction proofs are stored on-chain without scaling to high utilization levels of the blockchain itself. This hybrid architecture applies especially to practical healthcare systems, in which all the storage on-chain would not be effective. The result is consistent with the work by Dalal et al. (2023), who have shown that secure Internet of Medical Things architectures require the coordination of the multiple layers of the architecture rather than the use of a single technical element. The current framework facilitates this understanding by showing that blockchain would best work as a trust and validation layer as a part of a larger healthcare data ecosystem.

At the same time, in the analysis, one can see that there are no practical constraints that vanish as a result of technical benefits. The lower scores in real time responsiveness and ease of integration suggest that blockchain-based healthcare systems continue to have the overhead of validation, complexity of deployment, and integration requirements. This is a very important finding due to the absence of overly idealized vision of blockchain adoption. The best frameworks are the distributed trust, record integrity and accountability, and the implementation of such a framework needs effective system design and scalable infrastructure to be successful. This finding correlates with Haque et al. (2024) who also noted that lightweight consensus and efficiency-focused engineering is needed to implement scalable blockchain-based data management. It also lends credence to the wider arguments of Haddad et al. (2022) who discovered that the best way to use blockchain is complementary with other technologies and not as a solution in itself. Likewise, Rahman et al. (2020) determined that the use of blockchain in healthcare systems is improved when it is used to coordinate securely in intelligent and distributed health settings.

These results have significant implications. They postulate that blockchain is not likely to displace the traditional databases, but a security architecture that best applies with off-chain storage, formal access controls, and distributed control. This paper is limited by the conceptual and analytic nature of the paper because it does not contain the real-world implementation or benchmarking of the hospital level. Subsequent research will focus on implementation-based validation, e.g., latency testing, scalability testing, smart contract testing and integration with IoMT and AI-enabled healthcare services. Overall, the discussion proves that the suggested framework is an effective example of a safe healthcare data management framework, and, simultaneously, it becomes clear that scalability, complexity, and reality of the deployment are the areas of concern in the further work.

Conclusion

This study examined blockchain-based secure frameworks for healthcare data management from a computer science perspective and showed that blockchain can provide a strong architectural foundation for addressing major weaknesses in conventional healthcare information systems. The proposed framework improves data integrity, auditability, controlled access, and distributed trust through blockchain verification, smart contracts, and off-chain encrypted storage. By separating secure record storage from ledger-based validation, the framework offers a practical balance between security, traceability, and operational efficiency for modern healthcare environments involving multiple institutions and stakeholders. The analysis also showed that blockchain is most effective when implemented as part of a layered and hybrid architecture rather than as a stand-alone storage solution. At the same time, challenges such as scalability, computational overhead, system integration, and regulatory compatibility remain important considerations for practical deployment. Future research may extend this computer science-oriented framework to direct medical applications by integrating it with clinical decision support, remote patient monitoring, and personalized care systems. Such expansion could support the medical field through more secure, interoperable, and patient-centered healthcare delivery. Overall, blockchain has strong potential to transform healthcare data management when supported by careful design and implementation.

References

1. Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2024). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Personal and ubiquitous computing*, *28*(1), 59-72.
2. Akkaoui, R., Hei, X., & Cheng, W. (2020). EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange. *IEEE access*, *8*, 113467-113486.
3. Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017, December). Medibchain: A blockchain based privacy preserving platform for healthcare data. In *International conference on security, privacy and anonymity in computation, communication and storage* (pp. 534-543). Cham: Springer International Publishing.
4. Al-Khasawneh, M. A., Faheem, M., Alarood, A. A., Habibullah, S., & Alzahrani, A. (2024). A secure blockchain framework for healthcare records management systems. *Healthcare Technology Letters*, *11*(6), 461-470.
5. Azbeg, K., Ouchetto, O., & Andaloussi, S. J. (2022). BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egyptian informatics journal*, *23*(2), 329-343.
6. Bhattacharya, P., Tanwar, S., Bodkhe, U., Tyagi, S., & Kumar, N. (2019). Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications. *IEEE transactions on network science and engineering*, *8*(2), 1242-1255.
7. Chakraborty, S., Aich, S., & Kim, H. C. (2019, February). A secure healthcare system design framework using blockchain technology. In *2019 21st international conference on advanced communication technology (ICACT)* (pp. 260-264). IEEE.
8. Dalal, S., Lilhore, U. K., Simaiya, S., Sharma, A., Jaglan, V., Kumar, M., ... & Rana, A. K. (2023). Original Research Article A Blockchain-based secure Internet of Medical Things framework for smart healthcare. *Journal of Autonomous Intelligence*, *6*(3), 401-423.
9. Faruk, M. J. H., Shahriar, H., Saha, B., & Barek, A. (2022). Security in electronic health records system: Blockchain-based framework to protect data integrity. In *Blockchain for cybersecurity in cyber-physical systems* (pp. 125-137). Cham: Springer International Publishing.
10. Galety, M. G., Tan, K. T., Kshirsagar, P. R., & Polamuri, S. R. (2025). Medical data security and effective organization using integrated Blockchain principles in AI-based healthcare 6.0 infrastructures. *Discover Computing*, *28*(1), 162.
11. Ghazal, T. M., Hasan, M. K., Abdullah, S. N. H. S., Bakar, K. A. A., & Al Hamadi, H. (2022). Private blockchain-based encryption framework using computational intelligence approach. *Egyptian Informatics Journal*, *23*(4), 69-75.
12. Gohar, A. N., Abdelmawgoud, S. A., & Farhan, M. S. (2022). A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT. *IEEE access*, *10*, 92137-92157.
13. Haddad, A., Habaebi, M. H., Islam, M. R., Hasbullah, N. F., & Zabidi, S. A. (2022). Systematic review on ai-blockchain based e-healthcare records management systems. *IEEE access*, *10*, 94583-94615.
14. Haque, E. U., Shah, A., Iqbal, J., Ullah, S. S., Alroobaea, R., & Hussain, S. (2024). A scalable blockchain based framework for efficient IoT data management using lightweight consensus. *Scientific Reports*, *14*(1), 7841.
15. Haritha, T., & Anitha, A. (2023). Multi-level security in healthcare by integrating lattice-based access control and blockchain-based smart contracts system. *IEEE Access*, *11*, 114322-114340.
16. Khubrania, M. M. (2021). A framework for blockchain-based smart health system. *Turkish Journal of Computer and Mathematics Education*, *12*(9), 2609-2614.
17. Mahajan, H. B., & Junnarkar, A. A. (2023). Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing. *Multimedia Tools and Applications*, *82*(28), 44335-44358.
18. Masood, I., Daud, A., Wang, Y., Banjar, A., & Alharbey, R. (2024). A blockchain-based system for patient data privacy and security. *Multimedia Tools and Applications*, *83*(21), 60443-60467.
19. Ngabo, D., Wang, D., Iwendi, C., Anajemba, J. H., Ajao, L. A., & Biamba, C. (2021). Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. *electronics*, *10*(17), 2110.
20. Paik, H. Y., Xu, X., Bandara, H. D., Lee, S. U., & Lo, S. K. (2019). Analysis of data management in blockchain-based systems: From architecture to governance. *Ieee Access*, *7*, 186091-186107.
21. Rahman, M. A., Hossain, M. S., Islam, M. S., Alrajeh, N. A., & Muhammad, G. (2020). Secure and provenance enhanced internet of health things framework: A blockchain managed

federated learning approach. *Ieee Access*, *8*, 205071.
22. Rathee, G., Sharma, A., Saini, H., Kumar, R., & Iqbal, R. (2020). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimedia Tools and Applications*, *79*(15), 9711-9733.
23. Saidi, H., Labraoui, N., Ari, A. A. A., Maglaras, L. A., & Emati, J. H. M. (2022). DSMAC: Privacy-aware Decentralized Self-Management of data Access Control based on blockchain for health data. *IEEE Access*, *10*, 101011-101028.
24. Shynu, P. G., Menon, V. G., Kumar, R. L., Kadry, S., & Nam, Y. (2021). Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing. *IEEE Access*, *9*, 45706-45720.
25. Sun, Z., Han, D., Li, D., Wang, X., Chang, C. C., & Wu, Z. (2022). A blockchain-based secure storage scheme for medical information. *EURASIP Journal on Wireless Communications and Networking*, *2022*(1), 40.
26. Taloba, A. I., Elhadad, A., Rayan, A., Abd El-Aziz, R. M., Salem, M., Alzahrani, A. A., ... & Park, C. (2023). A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. *Alexandria Engineering Journal*, *65*, 263-274.
27. Taloba, A. I., Rayan, A., Elhadad, A., Abozeid, A., Shahin, O. R., & Abd El-Aziz, R. M. (2021). A framework for secure healthcare data management using blockchain technology. *International Journal of Advanced Computer Science and Applications*, *12*(12).
28. Tariq, N., Qamar, A., Asim, M., & Khan, F. A. (2020). Blockchain and smart healthcare security: a survey. *Procedia Computer Science*, *175*, 615-620.
29. Villarreal, E. R. D., García-Alonso, J., Moguel, E., & Alegría, J. A. H. (2023). Blockchain for healthcare management systems: A survey on interoperability and security. *IEEE access*, *11*, 5629-5652.
30. Xi, P., Zhang, X., Wang, L., Liu, W., & Peng, S. (2022). A review of Blockchain-based secure sharing of healthcare data. *Applied Sciences*, *12*(15), 7912.