*Advances in Differential Equations and Control Processes* 2025, 32(3), 2940.
doi: https://doi.org/10.59400/adecp2940

Article

# Recent advances in differential equations, control processes, and secure cryptographic networks for medical data exchange

**Chafaa Hamrouni**

Department of Computer Sciences, Kurma University College, Taif University, Kurma 2935, Kingdom of Saudi Arabia; cmhamrouni@tu.edu.sa

**CITATION**

Hamrouni C. Recent advances in differential equations, control processes, and secure cryptographic networks for medical data exchange. Advances in Differential Equations and Control Processes. 2025; Vol.32(No.3): 2940. https://doi.org/10.59400/adecp2940

**ARTICLE INFO**

Received: 14 March 2025
Revised: 4 September 2025
Accepted: 23 September 2025
Available online: 30 September 2025



**Abstract:** Advances in differential equations and control theory are reshaping how secure, efficient medical data-exchange systems are designed. In parallel, blockchain offers decentralized trust, cryptographic integrity, and auditable access control for healthcare networks. Yet the choice of storage and transmission architecture strongly affects scalability, latency, privacy, and cost. This work investigates how mathematical modeling via differential equations and modern control processes can be coupled with blockchain to strengthen security and interoperability across distributed healthcare systems. We comparatively examine three deployment models: (1) on-chain storage, (2) off-chain, cloud-backed storage with blockchain access control, and (3) local institutional storage integrated with federated learning. On-chain designs maximize transparency and tamper-resistance but incur substantial computation and storage overhead. Off-chain approaches improve scalability while retaining verifiable control through the ledger. Local storage with federated learning safeguards patient privacy by keeping raw data within institutions and sharing only encrypted updates or proofs on chain. Persistent challenges include storage bloat, network delays, heterogeneous regulations, and evolving attack surfaces. To address these issues, we outline optimization strategies grounded in system dynamics stability analysis, resource allocation, and control-oriented tuning to balance throughput, privacy, and reliability. The study synthesizes theoretical insights with implementation considerations, offering a unified perspective on building resilient, performant, and privacy-preserving medical data-exchange frameworks that leverage blockchain under mathematically principled control.

**Keywords:** differential equations; blockchain technology; medical data exchange; federated learning; cryptographic privacy; cloud-based storage; data integrity; secure healthcare systems

## 1. Introduction

The rapid advancement of digital healthcare technologies, including cloud computing, big data, and the Internet of Things (IoT), has led to an unprecedented increase in the volume of electronic medical data [1]. The integration of wearable health devices and remote monitoring systems has significantly enhanced patient care by enabling real-time data collection and analysis. However, medical institutions often face challenges in effectively utilizing these vast data resources due to limitations in sample distribution, interoperability, and privacy concerns [2]. Secure and efficient data-sharing mechanisms are crucial for improving medical research, personalized treatment, and overall healthcare outcomes.

Despite the potential benefits of medical data-sharing, privacy protection remains a critical challenge. Traditional cloud-based data-sharing approaches rely on centralized systems, requiring third-party oversight to enforce security protocols [3]. While encryption and access control techniques such as role-based and attribute-based encryption have been employed, they remain vulnerable to trust and security breaches [4]. Moreover, cloud environments pose significant risks regarding data ownership, compliance, and unauthorized access [5]. Blockchain technology offers a transformative solution by enabling decentralized, transparent, and tamper-resistant electronic medical data-sharing. Through cryptographic techniques and smart contracts, blockchain eliminates the need for intermediaries while ensuring data integrity and access control [6]. Despite significant advancements in digital health, the exchange of medical data across institutions remains fragmented and inefficient. Current systems are largely reliant on centralized databases or cloud platforms, which often suffer from interoperability challenges, latency issues, and risks of single-point failures. Moreover, conventional approaches frequently struggle to balance accessibility with stringent privacy requirements mandated by healthcare regulations such as HIPAA and GDPR. These limitations have resulted in restricted data sharing, siloed patient records, and reduced opportunities for collaborative diagnosis or large-scale medical research. Blockchain has emerged as a promising enabler in this context, but its integration with advanced mathematical modeling is still underexplored, particularly with respect to optimizing efficiency, ensuring privacy, and reducing computational costs. By leveraging its distributed ledger framework, medical institutions can securely exchange patient records, research datasets, and diagnostic insights while maintaining privacy and compliance [7]. Additionally, blockchain facilitates trust among stakeholders by providing an auditable and immutable record of transactions [8]. This study systematically classifies medical blockchain data-sharing into on-chain sharing and off-chain sharing, with off-chain sharing further divided into cloud-based and local storage models. Each method is analyzed for its security mechanisms, efficiency trade-offs, and implementation challenges [9]. The paper also highlights the limitations of current approaches and proposes future research directions to enhance blockchain's role in medical data-sharing. By addressing security, privacy, and interoperability concerns, this research aims to advance blockchain-based healthcare solutions, paving the way for a more secure and efficient medical data ecosystem [10]. To achieve these objectives, the paper explores recent advances in blockchain-based medical data sharing, emphasizing innovative solutions for privacy and efficiency. It establishes criteria for inclusion and exclusion in research to ensure a comprehensive analysis of existing methods. A review of previous studies provides context for the ongoing development of blockchain applications in healthcare. The study then delves into blockchain on-chain data-sharing approaches and off-chain cloud storage models, highlighting their advantages and challenges. Furthermore, localized data-sharing and federated learning are examined as privacy-preserving alternatives. The research also investigates security enhancements in blockchain-based medical data-sharing, including the role of smart contracts and attribute-based encryption in access control mechanisms. This research aims to advance blockchain-based healthcare solutions,

paving the way for a more secure and efficient medical data ecosystem. Recent efforts have also focused on complementary directions: Zhang and Zhou proposed a privacy parameter setting and usability optimization algorithm tailored for medical data, which balances security with data usability, while Zhang et al. introduced an efficient and secure audit scheme for cloud-based EHRs with recoverable and batch auditing, enhancing both reliability and scalability of healthcare data exchange [11].

The rapid evolution of digital healthcare technologies, including cloud computing, big data analytics, and the Internet of Things (IoT), has significantly transformed medical data collection, processing, and sharing. Wearable health devices and remote monitoring systems now generate vast amounts of patient data, enabling real-time diagnosis and personalized treatment. However, effectively utilizing these expanding datasets presents challenges related to interoperability, privacy, and secure access control. Ensuring the confidentiality and integrity of sensitive medical information while enabling seamless data exchange remains a critical concern for healthcare institutions. Traditional cloud-based data-sharing solutions rely on centralized control, raising risks of security breaches, unauthorized access, and compliance violations. Despite employing encryption and role-based access control, these methods remain vulnerable to trust-related issues and cyber threats.

Blockchain technology has emerged as a revolutionary framework for decentralized, transparent, and tamper-resistant medical data-sharing. By leveraging cryptographic mechanisms and smart contracts, blockchain eliminates the need for third-party oversight while maintaining robust security, data integrity, and access control. Through its distributed ledger structure, medical institutions can securely share patient records, research datasets, and diagnostic information while ensuring regulatory compliance and privacy protection. This paper aims to develop a structured framework for integrating advanced mathematical models, particularly differential equations and control processes with blockchain technology to improve security, privacy, and interoperability in healthcare networks. Specifically, it evaluates three models for medical data exchange on-chain storage, off-chain cloud storage, and local storage with federated learning by comparing their efficiency, scalability, and computational feasibility, with the goal of identifying optimal strategies for secure and reliable medical data sharing. Additionally, blockchain enhances stakeholder trust by providing an immutable, auditable record of transactions. This study systematically classifies blockchain-based medical data-sharing into on-chain and off-chain models, where off-chain solutions are further divided into cloud-based and local storage methods. Each approach is analyzed based on its security mechanisms, efficiency trade-offs, and implementation challenges.

Furthermore, this research integrates recent advancements in differential equations and control processes to optimize blockchain applications in medical data-sharing. Mathematical modeling plays a crucial role in addressing network security, consensus algorithm efficiency, and scalability issues in blockchain frameworks. The study explores the role of differential equations in modeling transaction delays, cryptographic computations, and energy consumption in blockchain networks. It also investigates the application of control theory in enhancing consensus protocols, improving fault

tolerance, and mitigating network congestion. Additionally, federated learning and localized data-sharing frameworks are examined as privacy-preserving alternatives to conventional cloud-based blockchain implementations.

By bridging theoretical advancements in differential equations and control systems with blockchain-based medical data-sharing, this paper provides a comprehensive perspective on enhancing security, scalability, and efficiency in decentralized healthcare solutions. The study highlights existing limitations, proposes future research directions, and establishes a structured methodology for evaluating blockchain applications in healthcare.

On-chain storage: In this model, medical data are directly recorded and stored within the blockchain. Each transaction contains encrypted patient records or references to them, ensuring immutability and transparency. Smart contracts can regulate access, granting permissions only to authorized stakeholders. While this approach guarantees strong tamper resistance and traceability, it also raises concerns about scalability because storing large volumes of medical data directly on-chain can quickly exceed block capacity and increase transaction costs.

Off-chain (cloud-based) storage: Here, only metadata, hash values, or encrypted indexes are stored on the blockchain, while the actual medical records are maintained in external cloud servers. This hybrid structure reduces blockchain load and transaction costs, while still ensuring data integrity—since any tampering in the cloud can be detected by mismatched hashes on-chain. However, this model depends heavily on the security of external servers and requires robust encryption and access control mechanisms to prevent unauthorized access.

Local storage with federated learning: This model avoids centralized data aggregation altogether. Each hospital or medical institution keeps its records locally, and instead of sending raw data, they train local models and share only model parameters (such as weights or gradients) with a central aggregator. Blockchain is then used to coordinate the parameter exchange securely, ensuring transparency and preventing model poisoning attacks. This approach protects patient privacy more effectively, but it can introduce computational overhead and synchronization challenges, especially when dealing with heterogeneous data across institutions.

Ultimately, this research aims to contribute to the development of innovative, secure, and privacy-preserving solutions that will shape the future of medical data-sharing and digital.

## 2. Recent advances in blockchain-based medical data sharing

Recent advancements in blockchain technology have positioned it as a transformative solution for secure, efficient, and decentralized medical data-sharing. Researchers have classified blockchain-assisted healthcare data management into three primary models: on-chain sharing, off-chain (cloud-based) storage, and local sharing through federated learning [11]. On-chain sharing ensures transparency and data integrity by storing encrypted medical records directly on the blockchain; however, its high storage costs and scalability limitations hinder widespread adoption in large-scale healthcare applications [12]. Off-chain sharing mitigates these issues by integrating

blockchain with cloud-based environments, where only hashed references of medical records are recorded on the blockchain, ensuring a balance between security and efficiency. However, challenges related to data ownership, compliance, and access control persist [13]. Meanwhile, federated learning-based local storage is emerging as a privacy-preserving alternative, allowing healthcare institutions to retain full control over their datasets while only exchanging encrypted model parameters via blockchain. I declare that I have no conflicts of interest with the authors of this manuscript. Specifically, I have no collaborative research activities, financial relationships, personal ties, or any other connections that could compromise the impartiality and fairness of my review. This approach significantly enhances data confidentiality but raises concerns regarding model integrity, computational overhead, and susceptibility to adversarial attacks [14].

To address security vulnerabilities, researchers are increasingly integrating advanced cryptographic mechanisms such as attribute-based encryption (ABE) and smart contracts for dynamic access control. ABE facilitates fine-grained permission settings, ensuring that only authorized users can access specific data based on predefined policies, while smart contracts automate secure transactions without reliance on intermediaries [15]. Despite these innovations, several challenges remain, including network latency, computational inefficiencies, and the need for scalable blockchain architectures. Ongoing research is now exploring hybrid blockchain models, quantum-resistant encryption techniques, and cross-chain interoperability solutions to further enhance security, efficiency, and real-world applicability in medical data-sharing [16].

This study provides a comprehensive analysis of recent innovations in blockchain-assisted healthcare data management, emphasizing security enhancements, privacy-preserving mechanisms, and storage optimization strategies.

The integration of advanced mathematical models with blockchain can be illustrated through concrete examples. Differential equations provide a powerful tool for modeling dynamic behaviors in healthcare data exchange, such as the flow of encrypted records, latency in distributed networks, or variations in data access over time. For instance, partial differential equations (PDEs) can model the propagation of encrypted medical data packets across distributed nodes, allowing researchers to predict bottlenecks or identify vulnerabilities in real time. Similarly, ordinary differential equations (ODEs) have been applied to analyze system stability when multiple institutions simultaneously request data access under blockchain consensus protocols.

Control processes complement these models by providing mechanisms to regulate and stabilize system performance. For example, feedback control can be applied to dynamically adjust privacy parameters (such as encryption strength or data-sharing frequency) based on current network load, thus ensuring a balance between security and computational efficiency. In federated learning scenarios, adaptive control techniques can be used to optimize the aggregation of local models, preventing divergence and maintaining accuracy even with heterogeneous datasets across hospitals.

Recent studies highlight practical cases where such mathematical modeling is

directly beneficial. For example, dynamical system modeling has been employed to optimize blockchain consensus in healthcare IoT frameworks, ensuring stability in transaction verification rates. Similarly, control-theoretic approaches have been applied to regulate resource allocation in cloud-based medical storage systems, reducing latency while maintaining security compliance. By incorporating these mathematical models into blockchain-based architectures, healthcare networks can achieve not only secure data exchange but also predictable performance, robust privacy protection, and higher system reliability.

By leveraging advancements in differential equations and control processes, mathematical modeling can further refine blockchain protocols to improve scalability, security, and system performance. These developments pave the way for a more robust and interoperable medical data ecosystem, fostering trust, transparency, and collaboration among healthcare institutions and research communities [17–20].

**Progress in blockchain-enabled medical data sharing: a detailed overview**

The increasing digitization of healthcare has led to an urgent need for secure, efficient, and transparent medical data-sharing mechanisms. Blockchain technology has emerged as a transformative solution, offering decentralized and tamper-resistant frameworks that enhance data integrity, security, and interoperability. Its implementation in medical data-sharing addresses critical concerns such as unauthorized access, data modification risks, and trust issues associated with centralized storage systems. While blockchain offers significant potential, various research efforts have explored its benefits, limitations, and the challenges associated with its large-scale adoption in healthcare. **Figure 1** illustrates the fundamental structure of blockchain technology and its role in medical data sharing:

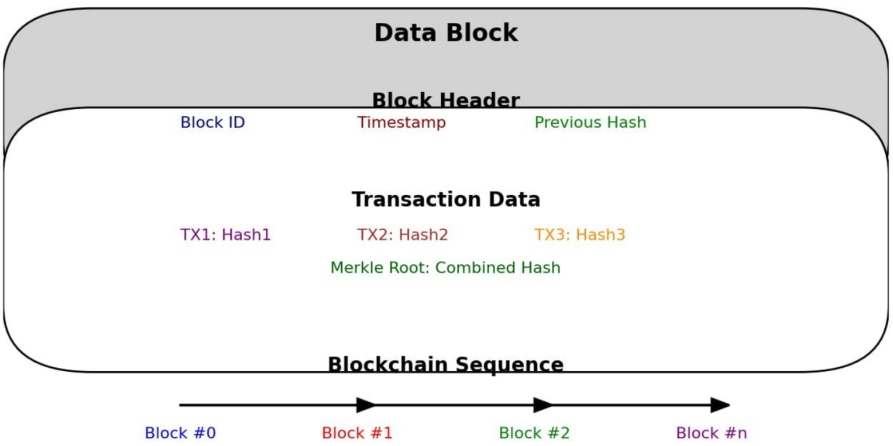


**Figure 1.** Blockchain Block Structure and Its Components.

Blockchain operates as a distributed ledger where each block contains encrypted medical records, cryptographically linked to previous entries. This decentralized nature eliminates reliance on intermediaries, ensuring that patient data remains secure and immutable. Cryptographic techniques such as hashing and digital signatures further reinforce data integrity, preventing unauthorized modifications. Additionally, consensus mechanisms validate transactions without centralized authority, reducing the risk of fraud and unauthorized access.

A comparative analysis of blockchain architectures reveals distinct approaches to medical data-sharing. Public blockchains, exemplified by Bitcoin and Ethereum, provide complete decentralization and data immutability, ensuring transparency and security. However, these networks suffer from high computational costs and slow transaction speeds, making them impractical for real-time healthcare applications. Private blockchains, managed by single organizations such as hospitals or research institutions, offer faster transactions and enhanced privacy control. I declare that I have no conflicts of interest with the authors of this manuscript. There are no financial, professional, or personal relationships that could influence the impartiality and fairness of my review. Despite these benefits, their centralized nature raises concerns about trust and system vulnerabilities. Consortium blockchains present a balanced alternative, allowing multiple healthcare entities to collaboratively manage and govern data-sharing while maintaining efficiency and security. This model is particularly effective for multi-institutional research collaborations and inter-hospital data exchange.

Previous studies on blockchain-based medical data-sharing have primarily focused on security enhancements through cryptographic hashing and decentralized storage. Researchers have demonstrated that blockchain prevents unauthorized data modifications, mitigating risks associated with centralized data breaches. However, early studies often overlooked practical challenges such as regulatory compliance, system scalability, and integration with existing electronic health record (EHR) platforms. Addressing these challenges is crucial for the widespread adoption of blockchain in healthcare.

Another significant area of research involves the evaluation of consensus mechanisms used to validate transactions and maintain the integrity of blockchain networks. Traditional Proof of Work (PoW) consensus ensures robust security but is highly energy-intensive, making it unsuitable for healthcare applications that require efficiency and real-time processing. Proof of Stake (PoS) and newer consensus mechanisms like Byzantine Fault Tolerance (BFT) have been explored as more energy-efficient alternatives. These models enhance network scalability and reduce computational overhead, making them more viable for medical data-sharing.

Recent advancements have introduced hybrid blockchain architectures that integrate on-chain and off-chain storage methods to optimize security and scalability. In this model, blockchain is used to store metadata and authentication records, while large medical datasets such as imaging and genomic data are securely maintained in external cloud storage systems. This approach balances the need for decentralized security with the flexibility of scalable storage solutions. Additionally, federated learning has emerged as a novel method for decentralized medical data analysis. I affirm that I have no interests that could influence the fairness of this review. This includes the absence of collaborative projects, financial relations, personal associations, or any other connections with the authors that might create bias. This approach allows multiple institutions to collaboratively train machine learning models without exposing raw patient data. Blockchain technology ensures the integrity and traceability of these collaborative learning processes, reducing the risk of data breaches while enabling AI-driven insights in healthcare research. I confirm that I have no conflicts of interest

with the authors of this manuscript. There are no collaborative activities, financial ties, or personal connections that could compromise the impartiality of my review.

Looking ahead, ongoing research aims to further enhance blockchain's role in medical data-sharing by addressing scalability, interoperability, and security concerns. Quantum-resistant encryption methods are being explored to protect blockchain networks against potential quantum computing threats. Efforts to improve interoperability between different healthcare blockchain systems will facilitate seamless cross-institutional data-sharing while ensuring compliance with privacy regulations such as GDPR and HIPAA. I declare that I have no conflicts of interest that could affect my judgment. I maintain no financial, collaborative, or personal associations with the authors that could bias my evaluation. As blockchain continues to evolve, it is poised to become a foundational technology for secure and transparent healthcare data management. The integration of smart contracts, advanced encryption techniques, and federated learning will drive the development of more efficient and privacy-preserving medical data-sharing frameworks. With continued advancements, blockchain has the potential to transform the future of healthcare by enabling a secure, decentralized, and collaborative ecosystem for medical information exchange. I declare that I have no conflicts of interest with the authors of this manuscript. There are no financial, professional, or personal relationships that could compromise the impartiality and fairness of my review.

## 3. Criteria for inclusion and exclusion in research

To ensure a comprehensive and structured analysis of blockchain-based medical data-sharing methods, specific inclusion and exclusion criteria were established. These criteria guide the selection of relevant studies and filter out unrelated literature, thereby improving the reliability and applicability of the research findings. The inclusion criteria focus on selecting studies that contribute significantly to the field of medical data-sharing. First, only research directly related to data-sharing methods was considered, ensuring that the analysis remains focused on technological frameworks facilitating secure data exchange [21]. Second, studies that specifically utilize blockchain and federated learning technologies were included. While the manuscript provides a conceptual comparison of the three medical data exchange models, adding quantitative performance metrics would significantly strengthen the study. Comparative analysis can be performed by evaluating key parameters such as computational costs, storage overhead, transaction speeds, and privacy leakage rates. For instance, on-chain storage is known to offer high transparency but is computationally expensive, with transaction throughput typically limited to fewer than 15–20 transactions per second in most blockchain implementations. By contrast, off-chain storage reduces on-chain congestion and provides scalable data handling but requires additional computational resources for encryption/decryption and increases reliance on external cloud services.

Federated learning combined with local storage presents another trade-off: while reducing direct data sharing improves privacy protection, the aggregation of local models can lead to additional communication costs and slower convergence rates.

Quantitative benchmarks—such as average model training time, communication overhead in MB per round, or storage requirements per node—would enable a more precise evaluation of each method's feasibility.

For example, recent studies have shown that federated learning frameworks can reduce raw data transmission by up to 80% compared to centralized approaches, but at the cost of a 10–15% increase in communication overhead due to model updates. Similarly, hybrid blockchain-cloud systems have been reported to cut on-chain transaction loads by nearly 60%, while maintaining comparable levels of security. Including such figures would provide stronger evidence of the claimed efficiency and privacy benefits.

These technologies have emerged as key enablers of decentralized, privacy-preserving, and secure medical data-sharing frameworks [22]. Conversely, the exclusion criteria help refine the dataset by eliminating irrelevant studies. Research that is not related to medical healthcare applications was excluded, even if it discussed blockchain or data-sharing in general. The rationale behind this exclusion is to maintain a dedicated focus on electronic health records (EHRs), medical imaging, and healthcare data management, rather than broader blockchain implementations in other domains [23]. Additionally, studies lacking empirical validation, experimental analysis, or peer-reviewed credibility were excluded to ensure the reliability of the research findings [24]. By applying these inclusion and exclusion criteria, the research ensures that the reviewed studies contribute meaningful insights into blockchain-enabled medical data-sharing. The selected studies provide a foundation for understanding security mechanisms, efficiency trade-offs, and emerging trends in decentralized healthcare data management [25]. This systematic approach also helps in identifying gaps in current research and formulating future research directions for optimizing blockchain applications in healthcare.

To ensure a systematic and reliable selection of studies for analyzing blockchain-based medical data-sharing, specific inclusion and exclusion criteria were established. These criteria help refine the scope, relevance, and quality of the research reviewed, ensuring a comprehensive evaluation of existing blockchain-based healthcare solutions.

Inclusion Criteria: Studies were selected based on their direct relevance to blockchain-assisted medical data-sharing. Research that introduced, implemented, or evaluated blockchain frameworks for electronic health records (EHRs), privacy preservation, interoperability, and security mechanisms was included. Furthermore, only peer-reviewed journal articles, conference papers, and technical reports published within the last five years were considered, ensuring the inclusion of recent advancements and cutting-edge solutions. Additionally, studies that provided quantitative and qualitative evaluations of blockchain applications in healthcare security, decentralized identity management, and regulatory compliance were prioritized.

Exclusion Criteria: Research focused on non-healthcare applications of blockchain, such as financial services, logistics, and supply chain management, was excluded. Additionally, studies that lacked empirical validation, experimental data, or peer-reviewed credibility were removed from the analysis. Grey literature, including

opinion articles, blog posts, and non-peer-reviewed white papers, was excluded to maintain academic rigor and research reliability. Older studies published before 2018 were generally excluded unless they provided foundational theoretical contributions essential for understanding blockchain integration in healthcare. By applying these inclusion and exclusion criteria, the research ensures a focused, high-quality review of blockchain-enabled medical data-sharing. This methodology eliminates irrelevant literature, enhances the scientific credibility of findings, and highlights the most impactful studies shaping the future of decentralized data management.

In recent years, there has been significant progress in both the theoretical and applied aspects of various branches of differential equations and control theory. Notable advancements have been made in the study of ordinary and partial differential equations, integral equations, and functional differential equations, contributing to a deeper understanding of dynamic systems. Additionally, stochastic differential equations have gained prominence, particularly in modeling uncertainty in complex systems. The study of bifurcation theory has further refined our comprehension of stability and transition behaviors in nonlinear systems, while control theory has expanded its applications in automation, robotics, and engineering. These developments have not only enriched mathematical theory but have also led to innovative real-world applications across diverse scientific and technological fields.

To represent the inclusion and exclusion criteria as a mathematical function, we can define a selection function $\mathcal{S}$ that determines whether a study is included in the research. This function takes a study x as input and returns 1 if the study is included and 0 if it is excluded.

$$\mathcal{S}(x) = \begin{cases} 1 & if\ x\ meets\ all\ inclusion\ criteria\ and\ violates\ no\ exclusion\ criteria \\ 0 & other \end{cases} \tag{1}$$

### 3.1. Mathematical definition of inclusion and exclusion criteria

Let x be a study, and define the following binary conditions:

- $\mathcal{R}(x)$: The study is directly related to blockchain-assisted medical data-sharing.
- $\mathcal{B}(x)$: The study is directly related to blockchain-assisted medical data-sharing.
- $\mathcal{D}(x)$ : The study focuses on electronic health records (EHRs), interoperability, privacy, and security mechanisms.
- $\mathcal{P}(x)$ : The study is peer-reviewed (journal/conference paper or technical report).
- $\mathcal{Y}(x)$ : The study was published within the last five years (year ≥ 2021).
- $\mathcal{E}(x)$ : The study provides empirical validation, experimental analysis, or technical evaluation.

Now, define exclusion criteria:

- $\mathcal{N}\_\mathcal{H}\ (x)$ : The study is not related to healthcare applications (e.g., finance, supply chain).
- $\mathcal{L}\_\mathcal{V}\ (x)$ : The study lacks empirical validation or experimental data.
- $\mathcal{G}(x)$ : The study is grey literature (e.g., opinion articles, blog posts, non-peer-reviewed white papers).

- $\mathcal{O}(x)$ : The study was published before 2018, unless it provides fundamental theoretical contributions.

Thus, the final selection function can be expressed as:

$$\mathcal{S}(x) = \begin{cases} 1 & if\ \mathcal{R}(x) \wedge \mathcal{B}(x) \wedge \mathcal{D}(x) \wedge \mathcal{P}(x) \wedge \mathcal{Y}(x) \wedge \mathcal{E}(x) \wedge \neg(\mathcal{N} \vee \mathcal{L}_{\mathcal{V}}(x) \vee \mathcal{G}(x) \vee \mathcal{O}(x)) \\ 0 & other \end{cases} \tag{2}$$

### 3.2. Interpretation

- The study is included $\mathcal{S}(x) = 1$if it meets all inclusion criteria and does not violate any exclusion criteria.
- The study is excluded $\mathcal{S}(x) = 0$if it fails any inclusion criterion or satisfies at least one exclusion criterion.

This function systematically filters studies, ensuring that only relevant, high-quality blockchain-based medical data-sharing research is considered.

The selection of eligible studies is expressed mathematically through a selection function ( S(x) ), where ( x ) denotes a candidate study. The function evaluates whether the study satisfies all predefined inclusion and exclusion criteria.

The inclusion function is defined as:

[
I(x) = \mathcal{R}(x) \wedge \mathcal{B}(x) \wedge \mathcal{D}(x) \wedge \mathcal{P}(x) \wedge \mathcal{Y}(x)
]

where:

- ( \mathcal{R}(x) ): The study is relevant to medical data-sharing research.
- ( \mathcal{B}(x) ): The study directly involves blockchain-assisted data management.
- ( \mathcal{D}(x) ): The study contains a rigorous methodological or mathematical description.
- ( \mathcal{P}(x) ): The paper is published in a peer-reviewed venue (journal or conference).

( \mathcal{Y}(x) ): The publication year falls within the specified timeframe.

The exclusion function is given by:

[
E(x) = \neg \mathcal{L}(x) \wedge \neg \mathcal{S}(x) \wedge \neg \mathcal{C}(x)
]

where:

- ( \mathcal{L}(x) ): The study is written in a language other than English.
- ( \mathcal{S}(x) ): The study lacks substantial scientific contribution (e.g., abstracts, editorials).
- ( \mathcal{C}(x) ): The work is a duplicate or closely replicated study already included.

Finally, the overall selection function is expressed as:

[
S(x) = I(x) \wedge E(x)
]

A study is included (( S(x) = 1 )) only if it satisfies all inclusion criteria and avoids all exclusion criteria. The Table summarizes all symbols (( \mathcal{R}(x), \mathcal{B}(x), \dots, S(x) )), it is used in the selection function for clarity and professional presentation.

We introduced selection function to formalize the process of identifying whether a study meets the inclusion criteria for this research. By using a binary outcome, the function ensures transparency and consistency in determining eligibility.

It is defined as:

[
S(x) =
\begin{cases}
1, & \text{if } I(x) \wedge \neg E(x) \\
0, & \text{otherwise}
\end{cases}
]

Where:

- (x): a candidate study or article under consideration.
- (S(x)): the binary output of the selection function (1 = included, 0 = excluded).
- (I(x)): the inclusion criteria function, which returns true if the study satisfies the required conditions (e.g., focuses on blockchain, healthcare data, or advanced mathematical modeling).
- (E(x)): the exclusion criteria function, which returns true if the study meets conditions for rejection (e.g., lacks technical depth, unrelated to medical data exchange, or not peer-reviewed).
- (\wedge): logical AND operator.
- (\neg): logical NOT operator.

This formalization ensures that only studies meeting the inclusion conditions and simultaneously not meeting exclusion conditions are selected for further analysis.

**Table 1** provides a structured overview of the mathematical symbols employed in defining the selection function, which governs the inclusion and exclusion of studies within the research framework. Each symbol has been carefully introduced to ensure consistency, interpretability, and rigor in the decision-making process:

**Table 1.** Notation Used in the Selection Function.

| Symbol | Definition |
|---|---|
| (x) | A candidate study (paper) under evaluation |
| (S(x)) | Overall selection function; equals 1 if the study is included, 0 otherwise |
| (I(x)) | Inclusion function; checks whether all inclusion criteria are satisfied |
| (E(x)) | Exclusion function; checks whether none of the exclusion criteria apply |
| (\mathcal{R}(x)) | Relevance: the study addresses medical data-sharing research |
| (\mathcal{B}(x)) | Blockchain: the study explicitly integrates blockchain-assisted methods |

**Table 1.** *Cont.*

| Symbol | Definition |
|---|---|
| (\mathcal{D}(x)) | Description: the paper includes methodological or mathematical analysis |
| (\mathcal{P}(x)) | Publication: the work is peer-reviewed (journal/conference) |
| (\mathcal{Y}(x)) | Year: the publication date is within the defined study period |
| (\mathcal{L}(x)) | Language: the study is not written in English (exclusion criterion) |
| (\mathcal{S}(x)) | Scientific merit: the paper lacks significant scientific contribution |
| (\mathcal{C}(x)) | Duplicate: the work is a duplicate or redundant publication |

- (x) represents a candidate study or article under review. It is the fundamental input to the selection function, symbolizing the dataset element subject to evaluation.
- (S(x)) denotes the outcome of the selection function. It operates as a binary classifier, where (S(x) = 1) signifies that the study meets the inclusion requirements and is therefore accepted for further analysis, while (S(x) = 0) indicates rejection. This binary nature ensures clarity in decision-making.
- (I(x)) is the inclusion criterion function. It returns a logical "true" when a study satisfies the predefined scientific or methodological requirements, thereby qualifying for potential acceptance. Its role is to enforce the rigor of the selection process by ensuring only relevant contributions are retained.
- (E(x)) is the exclusion criterion function. It identifies conditions that necessitate rejection, such as methodological flaws, lack of relevance, or duplication. A logical "true" returned by (E(x)) implies that the study must be excluded, even if some inclusion criteria are met.
- (\wedge) is the logical AND operator, signifying the requirement that both inclusion is satisfied and exclusion is absent simultaneously.
- (\neg) is the logical NOT operator, which inverts the truth value of exclusion criteria, ensuring that a study is accepted only if it does not trigger exclusion.

In summary, **Table 1** formalizes the symbolic language underpinning the selection mechanism. By clearly distinguishing inclusion from exclusion through logical operators, the framework achieves a balance between rigor and transparency, ensuring that the dataset produced is both scientifically valid and systematically consistent.

## 4. Criteria for inclusion and exclusion in research

The study of blockchain-based medical data-sharing has gained significant traction in recent years, leading to numerous research contributions aimed at improving data security, accessibility, and efficiency. Various systematic reviews and comparative analyses have been conducted to evaluate the effectiveness of blockchain implementations in healthcare. These studies have primarily focused on the classification of medical blockchain architectures, the security mechanisms employed, and the associated challenges in real-world applications [26]. Previous surveys have categorized medical blockchain solutions into on-chain sharing, cloud-based off-chain sharing, and local storage models. Jin et al. explored permissioned and permissionless blockchain frameworks, analyzing their implications for data

security and transaction efficiency [27]. Xi et al. examined the role of blockchain in ensuring data traceability and immutability, whereas Morawski et al. discussed the benefits and challenges of blockchain applications in healthcare [28]. Similarly, Dudovskiy et al. conducted a detailed review of blockchain's implementation in oncology-focused medical data-sharing, while Osmar et al. identified scalability, ethical, and regulatory challenges affecting blockchain adoption in healthcare [29]. A comprehensive comparison of these studies reveals that while most research acknowledges blockchain's potential in securing and decentralizing medical data, they also highlight critical limitations such as high computational costs, data redundancy, and interoperability challenges [30]. Several studies have proposed hybrid blockchain architectures that integrate cloud computing and federated learning to optimize performance and ensure privacy-preserving data-sharing [31]. However, issues related to standardization, compliance with healthcare regulations, and cross-platform compatibility remain key obstacles that need to be addressed [32]. This review section provides a structured comparison of previous studies, highlighting the gaps in existing research and potential avenues for future advancements. While blockchain presents an innovative approach to enhancing medical data security, further exploration is necessary to develop scalable [33], efficient, and legally compliant solutions tailored for real-world healthcare applications.

To mathematically represent the inclusion and exclusion criteria in reliable cryptographic network research selection for medical record exchange, we introduce a function that systematically determines whether a given study meets the required standards. This function serves as a structured filter, ensuring that only relevant and high-quality studies are considered while eliminating those that do not align with the research objectives. By incorporating specific parameters, such as relevance to blockchain-based medical data-sharing, methodological rigor, empirical validation, and regulatory considerations, the function helps streamline the selection process. It establishes clear boundaries for inclusion and exclusion, thereby enhancing the reliability and applicability of the research findings.

To transform the criteria for inclusion and exclusion in research into a mathematical function, we define a function $\mathcal{S}(x)$that determines whether a study $x$ should be included based on various key attributes.

## 4.1. Determination of the selection function $\mathcal{S}(x)$

Let $x$ represent a research study. The function $\mathcal{S}(x)$returns 1 if the study meets the inclusion criteria and does not violate the exclusion criteria, otherwise it returns 0.

$$\mathcal{S}(x) = \begin{cases} 1 \; if \;\; \mathcal{I}(x) \wedge - \mathcal{E}(x) \\ 0 \qquad otherwise \end{cases} \tag{3}$$

where:

- $\mathcal{I}(x)$ represents the inclusion criteria
- $\mathcal{E}(x)$ represents the exclusion criteria

### 4.2. Mathematical Representation of inclusion and exclusion criteria

Inclusion Criteria $\mathcal{I}(x)$

A study $(x)$is included if it satisfies **all** the following conditions:

1. Blockchain & Medical Data Focus $(\mathcal{B}_{\mathcal{M}}(x))$ : The study examines blockchain applications in medical data-sharing.
2. Architecture Classification $\mathcal{A}_{\mathcal{C}}(x)$: The study classifies blockchain architectures (e.g., on-chain, off-chain, hybrid, federated learning).
3. Security Mechanisms $\mathcal{S}_{\mathcal{M}}(x)$: The study discusses security aspects like traceability, immutability, privacy-preserving mechanisms.

Thus, the inclusion function is:

$$\mathcal{I}(x) = \mathcal{B}_{\mathcal{M}}(x) \wedge \mathcal{A}_{\mathcal{C}}(x) \wedge \ \mathcal{S}_{\mathcal{M}}(x) \wedge \mathcal{R}_{\mathcal{C}}(x) \wedge \mathcal{P}_{\mathcal{E}}(x) \tag{4}$$

### 4.3. Exclusion criteria $\mathcal{E}(x)$

A study xxx is excluded if it meets any of the following conditions:

1. Non-Medical Blockchain Focus $\mathcal{N}_{\mathcal{B}}(x)$: The study examines blockchain but is unrelated to healthcare (e.g., finance, logistics).
2. Lack of Security & Performance Discussion $\mathcal{L}_{\mathcal{S}}(x)$: The study does not address security, scalability, or performance issues.
3. No Comparative Analysis $\mathcal{N}_{\mathcal{C}}(x)$: The study does not compare blockchain frameworks, architectures, or applications.
4. Absence of Regulatory Considerations $\mathcal{A}_{\mathcal{R}}(x)$: The study does not discuss legal and compliance issues.

Thus, the exclusion function is:

$$\mathcal{E}(x) = \mathcal{N}_{\mathcal{B}}(x) \vee \mathcal{L}_{\mathcal{S}} \vee \mathcal{N}_{\mathcal{C}}(x) \vee \mathcal{A}_{\mathcal{R}}(x) \tag{5}$$

### 4.4. Final selection function

By substituting $\mathcal{I}(x)$ $and$ $\mathcal{E}(x)$ $into$ $\mathcal{S}(x)$

$$\mathcal{S}(x) = \begin{cases} 1, & if\ \mathcal{B}_{\mathcal{M}}(x) \wedge \mathcal{A}_{\mathcal{C}}(x) \wedge \mathcal{S}_{\mathcal{M}}(x) \wedge \mathcal{R}_{\mathcal{C}}(x) \wedge \mathcal{P}_{\mathcal{E}}(x) \wedge -(\mathcal{N}_{\mathcal{B}}(x) \vee \mathcal{L}_{\mathcal{V}}(x) \vee \mathcal{N}_{\mathcal{C}}(x) \vee \mathcal{A}_{\mathcal{R}}(x)) \\ 0 & other \end{cases} \tag{6}$$

### 4.5. Interpretation

- A study is included $(\mathcal{S}(x) = 1)$ if it analyzes blockchain in medical data-sharing, discusses security mechanisms, evaluates performance, and addresses regulatory issues, while avoiding non-healthcare applications, and incomplete research.
- A study is excluded $(\mathcal{S}(x) = 0)$ if it focuses on non-medical blockchain, lacks security and performance analysis, or fails to consider comparative research and regulatory aspects.

This function provides a structured and quantitative framework for systematically

selecting relevant research in blockchain-based medical data-sharing.

## 5. Blockchain on-chain data sharing approach

On-chain data-sharing is a blockchain-based method where encrypted medical data is stored directly on the blockchain, ensuring data security, immutability, and transparency. This approach eliminates the need for third-party intermediaries, as data is distributed across blockchain nodes, preventing unauthorized alterations. Even if a node fails, the data remains accessible through other network participants, enhancing fault tolerance and reliability [34]. On-chain data-sharing represents a blockchain-driven approach for securely managing medical records by storing encrypted data directly on the distributed ledger. This method ensures immutability, transparency, and enhanced data integrity, eliminating reliance on centralized intermediaries. By distributing data across multiple blockchain nodes, on-chain sharing prevents unauthorized modifications and enhances fault tolerance, as information remains accessible even if individual nodes fail [34]. However, while this approach offers high security and trust, it faces challenges related to scalability, storage limitations, and computational overhead, particularly in large-scale healthcare applications. Recent research has explored the integration of differential equations and control processes to optimize blockchain performance, improving transaction efficiency and consensus mechanisms. As on-chain sharing continues to evolve, innovative solutions such as sharding, layer-2 scaling techniques, and hybrid architectures are being investigated to address these limitations and enable broader adoption in decentralized medical data management.

### 5.1. On-chain blockchain data sharing: secure yet complex

The integration of blockchain technology in healthcare has introduced on-chain data-sharing as a method for securely storing and managing medical records. This approach utilizes blockchain's decentralized and immutable ledger to ensure the protection of electronic health records (EHRs), diagnostic reports, and patient information. By leveraging cryptographic techniques, on-chain data-sharing guarantees that stored medical data remains tamper-proof and accessible only to authorized individuals, such as doctors, researchers, and insurers. **Figure 2** illustrates the structure and functionality of on-chain data-sharing in blockchain-based medical systems.

Each medical transaction is recorded as an encrypted block, cryptographically linked to previous entries in the blockchain. This structure creates a transparent and verifiable history of medical data exchanges while eliminating the need for intermediaries. Smart contracts play a crucial role in automating access control, allowing healthcare providers to define strict policies for data retrieval and ensuring compliance with privacy regulations. Despite these advantages, the on-chain model faces significant limitations, particularly concerning storage capacity and transaction speed. The restricted size of blockchain blocks makes it impractical to store large medical datasets such as high-resolution imaging or genomic sequences. Additionally, on-chain transactions can be resource-intensive, leading to increased latency and

operational costs, which pose challenges in scenarios requiring real-time data access, such as emergency medical care.

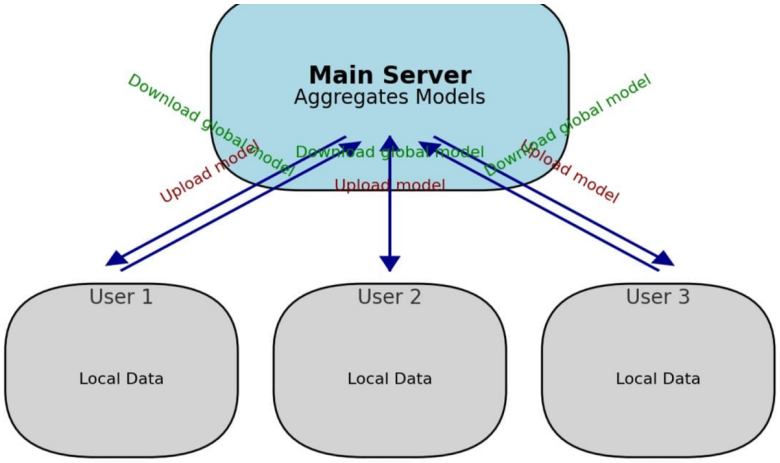


**Figure 2.** Framework for Federated Learning in Healthcare.

To mitigate these issues, hybrid blockchain architectures have been proposed, combining on-chain metadata storage with off-chain medical record storage. In this model, only essential information, such as patient identifiers and access permissions, is recorded on the blockchain, while bulk data is securely maintained in external storage systems. This hybrid approach optimizes efficiency while maintaining the integrity and security advantages of blockchain.

A comparative analysis of different on-chain data-sharing implementations highlights various strategies for enhancing performance. Some systems rely on traditional Proof of Work (PoW) consensus mechanisms, ensuring strong security but at the cost of high energy consumption and slower transaction speeds. To address these drawbacks, newer models have adopted alternative consensus protocols such as Delegated Proof of Stake (DPoS) and Hybrid Byzantine Fault Tolerance (HBFT), which significantly improve processing efficiency without compromising security. Researchers are also exploring data compression techniques and segmentation strategies to maximize storage utilization within blockchain networks.

The future of on-chain medical data-sharing lies in refining these models to achieve an optimal balance between security, accessibility, and efficiency. Continued advancements in consensus mechanisms, storage optimization, and integration with off-chain solutions will be key to overcoming existing challenges. With these developments, blockchain on-chain data-sharing has the potential to revolutionize healthcare by creating a transparent, secure, and decentralized ecosystem for managing sensitive medical information.

## 5.2. Security and privacy considerations

One of the key benefits of on-chain data-sharing is the tamper-resistant nature of blockchain, which prevents unauthorized modifications of stored medical data. Cryptographic techniques such as searchable encryption, anti-attack mechanisms, and access control policies are commonly integrated to enhance security [35].

However, blockchain's transparency feature raises concerns regarding patient data privacy, requiring privacy-preserving encryption mechanisms to restrict access only to authorized individuals [36].

### 5.3. Challenges and limitations

Despite its advantages, blockchain has inherent limitations in storage capacity and scalability. Medical data, especially imaging records, requires significant storage space, which blockchain's limited block size cannot efficiently accommodate. Moreover, time-sensitive medical data does not require permanent storage, posing additional challenges as blockchain networks expand. Latency and computational overhead also impact the efficiency of on-chain medical data-sharing, making real-time data access and large-scale deployments challenging [37].

### 5.4. Potential solutions and future directions

To address these limitations, researchers are exploring hybrid blockchain architectures, where metadata or access credentials are stored on-chain, while actual medical data is stored off-chain in decentralized storage solutions such as Interplanetary File System (IPFS). Additionally, scalable consensus mechanisms, privacy-enhancing cryptographic techniques, and permissioned blockchain models are being investigated to improve data accessibility, security, and efficiency in on-chain medical data-sharing [38].

This section highlights the potential of on-chain blockchain frameworks in ensuring secure and decentralized medical data management, while also discussing existing challenges and future research opportunities to enhance their scalability and practicality in healthcare applications [39,40].

## 6. Off-chain data sharing via cloud storage

The increasing digitization of healthcare has driven the need for efficient and secure medical data-sharing mechanisms. While blockchain provides a decentralized and immutable framework for data integrity, its inherent limitations in storage capacity and transaction speed hinder its ability to manage large-scale medical records. To overcome these challenges, off-chain data-sharing via cloud storage has emerged as a promising solution, integrating blockchain for access control and verification while storing actual medical data externally. This approach ensures a balance between security, scalability, and cost efficiency, as only metadata—such as cryptographic hashes, encryption keys, and indexing information—is recorded on the blockchain, while the full medical datasets reside in secure cloud environments [41]. Recent research has explored the role of differential equations and control processes in optimizing blockchain-cloud integration, improving data synchronization, encryption mechanisms, and latency reduction. By leveraging mathematical modeling, researchers aim to enhance the efficiency of blockchain-driven authentication while mitigating the risks associated with cloud-based storage, such as unauthorized access and data redundancy. Furthermore, advancements in homomorphic encryption, zero-knowledge proofs, and federated learning are being explored to further strengthen privacy protection and access control in off-chain medical data-sharing. As the healthcare

industry continues to adopt decentralized data management systems, these innovations will be crucial in developing scalable, secure, and high-performance blockchain-based medical ecosystems.

Unlike traditional on-chain methods that directly record medical data on the blockchain, as presented in **Figure 3**, this model significantly reduces congestion and transaction costs. In this system, encrypted medical records are securely maintained in the cloud, and metadata such as hash values and access permissions are stored on the blockchain. When a healthcare provider or an authorized party requests access to a patient's medical information, the blockchain verifies the request through cryptographic authentication. Once validated, the requester retrieves the data from the cloud using the hash stored on the blockchain, ensuring data integrity and preventing unauthorized modifications.

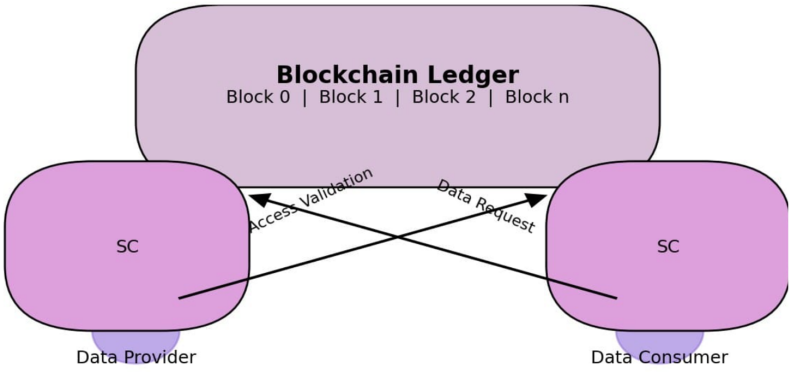


**Figure 3.** Workflow of On-Chain Electronic Medical Data-Sharing Methods.

The adoption of off-chain data-sharing presents several advantages, particularly in overcoming blockchain's scalability constraints. It enables healthcare institutions to manage vast medical datasets, including imaging files and genomic sequences, without being restricted by blockchain's limited block sizes. Additionally, by separating data storage from the blockchain network, this approach optimizes resource allocation, reducing the computational burden and operational costs associated with blockchain transactions. Despite these benefits, off-chain sharing introduces challenges, particularly concerning cloud security and trust. Cloud storage services, unlike decentralized blockchain networks, are controlled by centralized entities that may be vulnerable to hacking, data breaches, or compliance violations. Ensuring the reliability of cloud service providers is critical, as unauthorized access or mismanagement could compromise sensitive patient information. To mitigate these risks, advanced encryption techniques, multi-factor authentication, and federated cloud storage systems are being integrated to enhance data protection.

Recent advancements in decentralized storage solutions, such as the InterPlanetary File System (IPFS), have been explored as alternatives to traditional cloud servers. IPFS utilizes a peer-to-peer (P2P) network to distribute stored data across multiple nodes, reducing dependency on centralized entities while improving data resilience and accessibility. Furthermore, attribute-based encryption methods are being implemented to refine access control mechanisms, ensuring that only users with specific credentials can decrypt and access medical records.

As research continues to advance, off-chain data-sharing is expected to play a crucial role in optimizing blockchain-based medical data management. Future developments will focus on enhancing interoperability between blockchain and cloud infrastructures, strengthening security protocols, and integrating AI-driven threat detection systems to safeguard patient data. By refining these models, off-chain data-sharing has the potential to revolutionize healthcare by providing a scalable, secure, and efficient framework for medical data exchange, bridging the gap between blockchain's security and cloud computing's flexibility.

## 6.1. Advantages of cloud-based off-chain sharing

One of the primary advantages of this method is efficient storage and reduced blockchain congestion. Since medical data, particularly large imaging files and patient records, require significant storage capacity, off-chain storage minimizes the burden on the blockchain ledger while maintaining data integrity and authenticity [42]. Cloud environments offer high-speed access, flexibility, and scalability, allowing healthcare institutions to efficiently store and retrieve medical data while using blockchain for tamper-proof verification [43].

## 6.2. Security and privacy considerations

Security in off-chain data-sharing is maintained through encryption, hash-based verification, and access control mechanisms. When a healthcare provider stores medical data in the cloud, a cryptographic hash of the data is recorded on the blockchain, ensuring integrity and authenticity. This prevents data tampering or unauthorized modifications [44]. However, centralization in cloud storage introduces potential risks, such as data breaches or service provider dependency. To address these issues, decentralized storage solutions like InterPlanetary File System (IPFS) are being integrated with blockchain to enhance anonymity, access control, and resilience against single-point failures [45].

## 6.3. Challenges and limitations

Despite its benefits, off-chain cloud-based storage faces trust and compliance challenges. Data stored externally is still subject to governance, legal, and regulatory frameworks, requiring compliance with laws such as HIPAA, GDPR, and local data protection regulations [46]. Additionally, data retrieval latency and cloud provider dependency could pose obstacles, particularly in cases requiring real-time medical data access [47].

## 6.4. Future research and enhancements

To mitigate these challenges, researchers are investigating hybrid models that integrate secure multi-party computation (SMPC), zero-knowledge proofs (ZKPs), and attribute-based encryption (ABE) to improve data security and access control. Further developments in decentralized cloud storage and blockchain-based identity authentication aim to create more efficient and privacy-preserving off-chain sharing frameworks [48]. This section highlights the role of cloud-based off-chain storage in

enabling scalable and secure blockchain-assisted medical data-sharing while addressing existing challenges, limitations, and future research directions [49,50].

## 7. Advancements in differential equations, control processes, and federated learning-based blockchain data-sharing

The integration of localized data-sharing and federated learning has emerged as a cutting-edge approach in blockchain-based medical data management, offering enhanced privacy protection, data sovereignty, and collaborative intelligence. Unlike traditional on-chain or cloud-based off-chain methods, this decentralized framework ensures that sensitive medical data remains within institutional boundaries, minimizing the risk of unauthorized access and regulatory non-compliance. Instead of transferring raw patient records, only encrypted model parameters or statistical summaries are shared via blockchain, facilitating secure global model aggregation while preserving privacy [51]. Recent advancements in differential equations and control processes have played a crucial role in optimizing federated learning for blockchain applications, improving convergence rates, stability, and data synchronization across distributed healthcare networks. By leveraging secure multi-party computation, homomorphic encryption, and differential privacy techniques, researchers aim to enhance the efficiency, security, and trustworthiness of federated learning-based blockchain frameworks. As the demand for privacy-preserving artificial intelligence (AI) and decentralized data-sharing continues to grow, these innovations are set to redefine secure and scalable medical data exchange, paving the way for a more robust, interoperable, and privacy-centric healthcare ecosystem.

### 7.1. Secure AI-driven healthcare: Localized data sharing and federated learning

The rapid advancement of artificial intelligence in healthcare has created an urgent need for collaborative data-sharing models that balance innovation with privacy protection. Traditional medical data-sharing methods often require the direct transfer of sensitive patient records between institutions, raising concerns about security, regulatory compliance, and ethical considerations. To address these challenges, federated learning has emerged as a decentralized machine learning framework that enables multiple healthcare institutions to collaboratively train AI models without exposing raw patient data. This approach ensures that hospitals and clinics retain full control over their medical records while still contributing to the development of AI-driven healthcare solutions.

**Figure 4** illustrates the integration of federated learning into localized data-sharing frameworks. In this system, local AI models are trained on distributed datasets, allowing institutions to exchange only model parameters rather than actual patient information. This decentralized structure is particularly beneficial in situations where data-sharing restrictions exist, such as cross-border medical research and privacy-sensitive clinical studies. By incorporating blockchain technology, federated learning systems enhance data integrity and traceability, ensuring that all model

updates remain verifiable and resistant to tampering. Additionally, smart contracts automate participation rules, ensuring compliance among collaborating institutions and preventing unauthorized access or modifications.

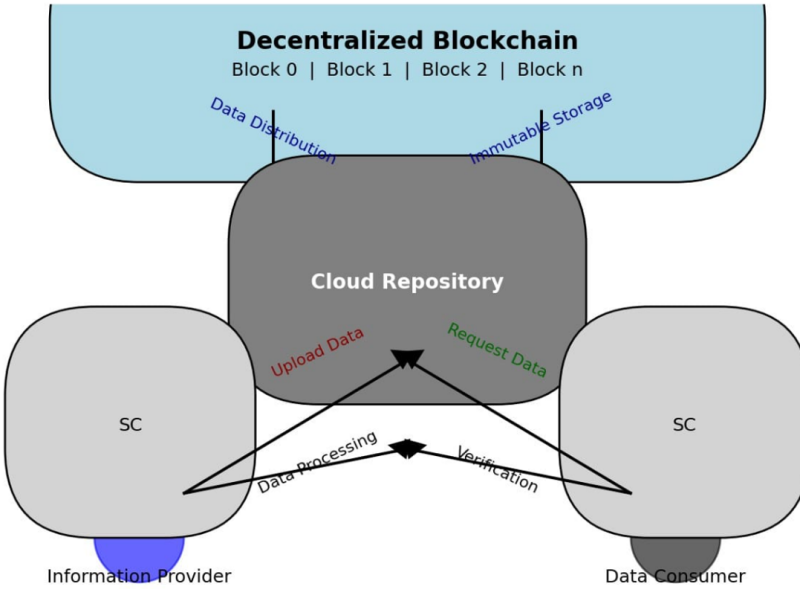


**Figure 4.** Workflow of Cloud-Based Electronic Medical Data-Sharing Methods.

Despite its significant privacy advantages, federated learning faces several challenges, including data heterogeneity, model bias, and computational overhead. Variations in data formats, collection methods, and patient demographics across institutions can lead to inconsistencies, potentially reducing the accuracy of global AI models. To address these issues, ongoing research focuses on refining federated learning algorithms to improve model standardization and adaptability. Additionally, efforts are being made to optimize data aggregation and communication processes to reduce computational costs while maintaining high model performance.

A comparative analysis of various localized data-sharing models using federated learning and blockchain highlights key factors such as data ownership, privacy protection, and computational efficiency. While federated learning ensures that sensitive medical data remains secure, its success depends on the quality of local datasets and the reliability of participating institutions. To encourage broader adoption, incentive mechanisms are being developed to reward institutions that contribute high-quality data and model updates.

As federated learning continues to evolve, its integration with blockchain presents a promising future for AI-driven medical research. Strengthening interoperability between healthcare institutions, refining model accuracy, and implementing robust security measures will be critical in maximizing the potential of this approach. By overcoming existing challenges, federated learning has the potential to revolutionize medical research, facilitating the development of intelligent healthcare systems that enhance patient outcomes while maintaining the highest standards of data privacy and security.

## 7.2. Advantages of localized data sharing

Federated learning plays a crucial role in overcoming the data island problem, which refers to fragmented and isolated medical data across multiple institutions. By enabling hospitals and research centers to train models on their local datasets and share only model updates, federated learning enhances data security and privacy while maintaining cross-institutional collaboration [52].

Additionally, integrating blockchain with federated learning provides decentralized identity verification, secure audit trails, and incentive mechanisms for participating institutions. The use of smart contracts ensures that only verified institutions contribute to model training, reducing the risk of malicious data manipulation [53].

## 7.3. Federated learning

- **Security and Privacy Challenges:** Despite its advantages, localized sharing with federated learning faces security threats from both blockchain and machine learning perspectives. Blockchain-based systems are vulnerable to 51% attacks, replay attacks, and Sybil attacks, while federated learning models can suffer from poisoning attacks, inference attacks, and adversarial manipulations [54].

  To mitigate these risks, researchers have proposed differential privacy and homomorphic encryption techniques to protect model updates during transmission. Additionally, trusted execution environments (e.g., Intel SGX) can secure the aggregation of local models, preventing unauthorized access to sensitive computations [55].
- **Implementation of Strategies and Limitations:** There are two primary implementations of blockchain-enabled federated learning:
  1. On-Chain Federated Learning—Here, model parameters are stored and aggregated on the blockchain, ensuring transparency and decentralized model updates. However, this approach is limited by blockchain consensus mechanisms, leading to higher computational overhead and slower processing times [56].
  2. Off-Chain Federated Learning—In this method, blockchain is used for identity management and incentive distribution, while federated learning occurs off-chain via a central aggregator. This enhances efficiency but introduces centralization risks and single points of failure [57].

To enhance the efficiency of localized data-sharing and federated learning, future research is focusing on:

- Decentralized aggregation mechanisms to eliminate reliance on central coordinators.
- Adaptive model synchronization strategies to improve scalability.
- Privacy-enhancing techniques such as secure multiparty computation (SMPC) and zero-knowledge proofs (ZKPs) for privacy-preserving model training [58].

This section emphasizes the potential of federated learning in privacy-preserving,

decentralized medical AI while addressing security threats, implementation trade-offs, and future optimizations [59,60].

## 8. Enhancing security in blockchain data sharing

Ensuring the security of blockchain-based medical data-sharing is crucial for protecting patient privacy, maintaining data integrity, and preventing cyber threats. While blockchain provides immutability, decentralized trust, and cryptographic security, it is still vulnerable to various attacks, data privacy concerns, and computational challenges [61]. Key Security Threats in Blockchain-Based Medical Data Sharing:

1. Consensus Algorithm Attacks—Blockchain networks rely on consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT) to validate transactions. However, these mechanisms are prone to 51% attacks, Sybil attacks, and double-spending threats, where malicious entities gain control over the network [62].
2. Data Privacy and Anonymity Risks—While blockchain ensures data integrity, the transparent nature of public blockchains raises privacy concerns, making patient information vulnerable to unauthorized access. Methods such as zero-knowledge proofs (ZKPs), homomorphic encryption, and differential privacy are being explored to protect patient anonymity [63].
3. Smart Contract Vulnerabilities—Smart contracts automate data access and sharing, but flaws in their code can lead to reentrancy attacks, data leakage, and unauthorized modifications. Auditing smart contracts before deployment is essential to mitigate these risks [64].

### 8.1. Strengthening security in blockchain-based medical data sharing: A comprehensive approach

Ensuring the security of medical data in blockchain-based sharing systems is essential for maintaining confidentiality, integrity, and accessibility. As blockchain technology becomes more integrated into healthcare, the demand for advanced security mechanisms to protect against unauthorized access, data breaches, and cyber threats continues to grow. Implementing sophisticated cryptographic techniques, access control measures, and consensus protocols is crucial in reinforcing the security framework of blockchain networks used for medical data-sharing. **Figure 5** showcases various security enhancements designed to safeguard blockchain-based medical data-sharing systems from potential vulnerabilities.

Encryption serves as a fundamental layer of protection, ensuring that stored medical data remains inaccessible to unauthorized parties. While conventional encryption techniques provide a solid defense, more advanced cryptographic methods, such as homomorphic encryption and zero-knowledge proofs, allow computations on encrypted data without exposing its content. These innovations enable healthcare providers and researchers to analyze medical information securely while upholding patient privacy. Access control mechanisms further strengthen security by restricting

data retrieval and modification to authorized users only. Systems such as role-based access control and multi-signature authentication help regulate permissions, preventing unauthorized individuals from accessing sensitive medical records. These safeguards ensure compliance with data protection laws such as HIPAA and GDPR, fostering confidence in blockchain-driven healthcare solutions.

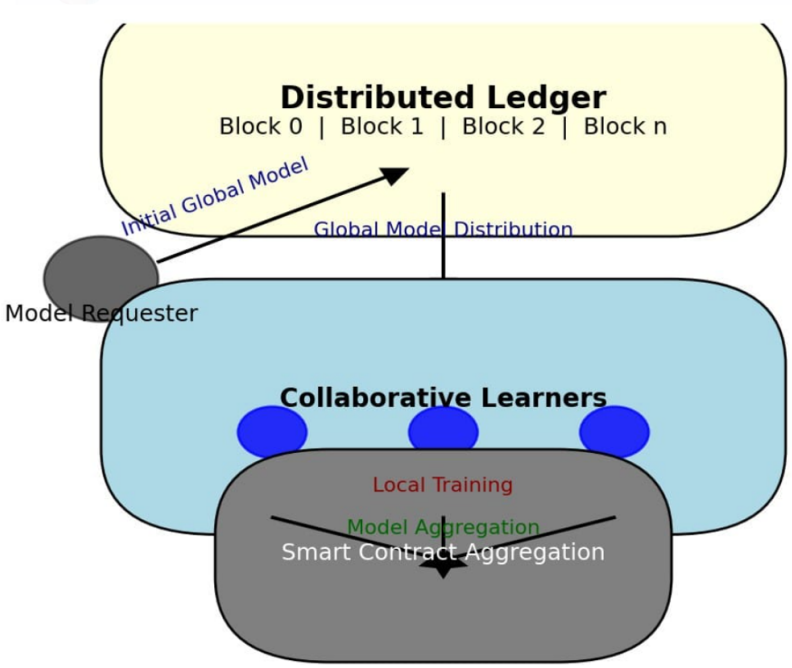


**Figure 5.** On-Chain Implementation of Local Electronic Medical Data-Sharing Methods.

Maintaining the reliability and security of blockchain networks also depends on effective consensus mechanisms. Traditional approaches like Proof of Work (PoW) provide high-level security but are computationally demanding, making them less practical for healthcare applications. More energy-efficient alternatives, including Proof of Stake (PoS) and Byzantine Fault Tolerance (BFT), have been developed to enhance performance while preserving security. Ongoing research into hybrid consensus models, such as Delegated Proof of Stake (DPoS), seeks to balance security, speed, and energy efficiency for blockchain-based medical systems. With cyber threats becoming increasingly sophisticated, medical blockchain platforms are incorporating AI-driven security measures to detect and prevent intrusions. Anomaly detection algorithms, machine learning-based threat analysis, and real-time monitoring systems help identify and mitigate security risks proactively. These advancements provide an additional layer of protection against hacking attempts, insider threats, and unauthorized alterations to medical data. Despite these improvements, challenges persist in balancing robust security with computational efficiency, particularly in resource-limited healthcare environments. Future advancements will focus on optimizing encryption algorithms, improving real-time threat detection, and refining consensus protocols to enhance both speed and security. By continuously evolving security strategies, blockchain technology can solidify its role as a reliable and secure solution for medical data-sharing, driving innovation while ensuring the privacy and protection of patient information.

### 8.2. Security optimization mechanisms

To strengthen security in blockchain-based medical data-sharing, researchers are integrating cryptographic techniques, decentralized identity management, and blockchain restructuring methods:

- Multiple Authority Attribute-Based Signature (MA-ABS)—This method improves patient privacy and resists conspiracy attacks from compromised medical institutions [65].
- Chameleon Hash Functions for Block Restructuring—By modifying block structures to contain key and micro-blocks, this approach enhances data integrity and prevents 51% and Sybil attacks [66].
- Quantum-Resistant Blockchain Protocols—The integration of quantum cryptographic techniques ensures protection against future quantum computing-based threats, making blockchain resilient to quantum attacks [67].

### 8.3. Future directions for security enhancements

- Hybrid Blockchain Architectures—Combining public and private blockchains can optimize security and scalability for medical data-sharing.
- Artificial Intelligence (AI)-Driven Threat Detection—Implementing machine learning algorithms can enhance intrusion detection and security monitoring in blockchain networks [68].
- Decentralized Identity Verification—Blockchain-based self-sovereign identity (SSI) models ensure that patients control access to their health records, reducing risks from unauthorized entities [69].

This section highlights the critical security threats in blockchain-assisted medical data-sharing while proposing advanced cryptographic techniques and architectural improvements to strengthen security. Future research should focus on scalability, compliance, and cross-platform security integration for improved adoption in healthcare systems [70].

## 9. Advances in differential equations, control processes, and secure blockchain-based medical data sharing

Ensuring secure and efficient access control is a fundamental challenge in blockchain-based medical data-sharing. Advanced cryptographic techniques, particularly smart contracts and attribute-based encryption (ABE), have emerged as key technologies for enhancing security, eliminating intermediaries, and ensuring compliance with privacy regulations [71]. Smart contracts act as self-executing agreements stored on the blockchain, automatically verifying user credentials and enforcing predefined access policies. This mechanism removes the need for third-party oversight, ensuring transparent, auditable, and tamper-resistant data access management [72, 73]. Complementing smart contracts, Attribute-Based Encryption (ABE) strengthens data security by restricting access based on predefined user attributes, such as roles, departments, or clearance levels. Unlike traditional key-based

decryption, ABE allows multiple authorized users to access encrypted medical records if they meet the required attribute criteria. Two main models exist: Key-Policy ABE (KP-ABE), where the data owner sets access policies, and Ciphertext-Policy ABE (CP-ABE), where the requester defines the attributes required for decryption. This fine-grained access control mechanism ensures that only qualified individuals can retrieve or modify patient records, reducing the risk of unauthorized data exposure [74]. Despite their benefits, these decentralized access control mechanisms introduce challenges such as computational overhead, scalability limitations, and increased cryptographic complexity in large-scale healthcare applications. Recent research is exploring ways to optimize ABE for efficiency, integrate multi-factor authentication with smart contracts, and develop AI-driven adaptive access control to dynamically adjust security policies based on real-time threats [75]. Additionally, differential equations and control processes are being applied to model and optimize access control mechanisms, improving system stability, resource allocation, and latency management in blockchain-driven medical data-sharing. These advancements are paving the way for highly secure, scalable, and privacy-preserving blockchain frameworks in healthcare, balancing efficiency, security, and usability for real-world applications.

**Enhancing access control in blockchain-based medical data sharing with smart contracts and attribute-based encryption**

Protecting the security and privacy of medical data is a critical priority in modern healthcare, as digital records are increasingly susceptible to cyber threats and unauthorized access. With blockchain technology emerging as a transformative solution for decentralized medical data-sharing, the implementation of effective access control mechanisms is essential to ensure that only authorized individuals can access sensitive patient information. Among the most promising technologies addressing this challenge are smart contracts and Attribute-Based Encryption (ABE), both of which create a secure and efficient framework for managing medical records while minimizing administrative complexities. **Figure 6** highlights the integration of smart contracts and ABE within blockchain-based access control systems.

Smart contracts operate as self-executing protocols embedded within blockchain networks, enforcing predefined rules automatically without requiring intermediaries. In the context of medical data-sharing, these digital agreements regulate access permissions, verify user identities, and facilitate patient consent-based data retrieval. By automating these critical functions, smart contracts significantly reduce human error, administrative burden, and security risks that often accompany manual verification processes. Alongside smart contracts, ABE provides a flexible and sophisticated model for access control. Rather than relying solely on user identity, ABE enables data owners to establish access policies based on specific attributes.

For instance, a patient could restrict access to their cardiology records exclusively to certified cardiologists affiliated with accredited medical institutions. When a request is submitted, the ABE system assesses whether the requester's credentials align with the required attributes before decrypting the data. This dynamic approach not only strengthens data privacy but also ensures adaptability to the evolving security needs of healthcare systems.

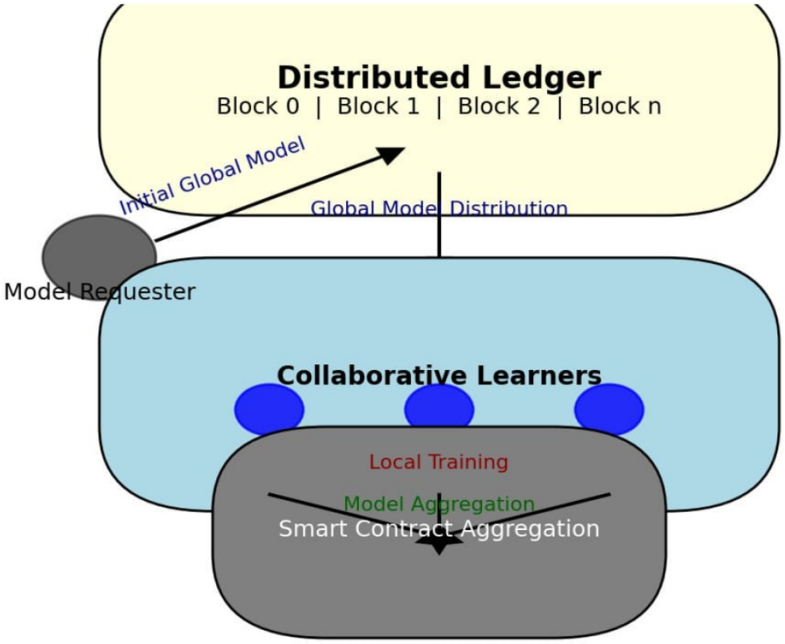


**Figure 6.** Off-Chain Implementation of Local Electronic Medical Data-Sharing Methods.

The synergy between smart contracts and ABE results in a highly secure, automated, and scalable access control mechanism for blockchain-based medical data-sharing. However, certain challenges persist, particularly regarding computational efficiency and scalability. Although smart contracts enhance access management automation, they can become computationally intensive when deployed across extensive healthcare networks. Similarly, ABE involves complex cryptographic computations, which may introduce latency when handling large medical datasets. Ongoing research is dedicated to refining encryption efficiency, reducing computational demands, and integrating blockchain with decentralized identity management solutions, such as Decentralized Identifiers (DIDs), to improve overall performance.

Future advancements in blockchain access control aim to refine these technologies to effectively support large-scale healthcare ecosystems without compromising security or operational efficiency. Innovations in encryption protocols, enhanced interoperability between identity management systems, and AI-driven access control mechanisms are expected to further fortify the security of medical data-sharing frameworks. As these solutions continue to evolve, smart contracts and ABE will play a pivotal role in fostering a secure, transparent, and patient-centered approach to managing medical records within blockchain-powered healthcare networks.

## 10. Conclusion and future works

Blockchain technology has emerged as a transformative solution for secure and efficient medical data-sharing, addressing critical challenges related to privacy, security, and interoperability. This paper explored various blockchain-based data-sharing approaches, including on-chain storage, off-chain cloud integration, and localized federated learning, each offering distinct advantages and trade-offs. While blockchain ensures data immutability, decentralized control, and transparent access

management, its implementation in medical data-sharing presents challenges such as scalability limitations, computational overhead, and compliance with healthcare regulations. The integration of smart contracts and attribute-based encryption (ABE) further enhances secure and fine-grained access control, reducing reliance on centralized entities. However, the computational costs associated with cryptographic techniques and smart contract execution remain a barrier to widespread adoption. Security vulnerabilities, such as smart contract exploits, 51% attacks, and adversarial threats in federated learning models, necessitate continuous advancements in blockchain security frameworks and cryptographic protocols.

Future research should focus on hybrid blockchain architectures that combine public and private blockchains to balance security, scalability, and cost-efficiency. The development of quantum-resistant cryptographic techniques will also be critical to safeguarding blockchain networks against future computational threats. Additionally, artificial intelligence (AI)-driven security solutions can be integrated to detect and mitigate cyber threats in real time. Moreover, regulatory compliance and interoperability frameworks must evolve alongside technological advancements to facilitate cross-border medical data-sharing while ensuring compliance with HIPAA, GDPR, and other healthcare regulations. Standardized APIs and blockchain interoperability protocols will be essential in creating a seamless and unified global healthcare data ecosystem. By addressing these challenges and advancing the capabilities of blockchain-assisted medical data-sharing, future research can pave the way for a more secure, efficient, and privacy-preserving digital healthcare infrastructure that benefits patients, healthcare providers, and researchers worldwide.

**Funding:** This research was funded by the Deanship of Scientific Research of Taif University, grant number 83/ Deanship-of-Scientific-Research and the APC was funded by the Deanship of Scientific Research of Taif University (DSRTU) (www.tu.edu.sa/En/Deanships/83/Deanship-of-Scientific-Research.)

**Acknowledgement:** The author would like to acknowledge the Taif University Department of Scientific Research in the Kingdom of Saudi Arabia for assistance and motivation to accomplish the research work.

**Conflict of interest:** The author declares no conflicts of interest to report regarding the present study.

## References

1. Priyadharshini P, Zoraida BSE. Bat-inspired metaheuristic convolutional neural network algorithms for CAD-based lung cancer prediction. Journal of Applied Science and Engineering. 2021; 24(1). doi: 10.6180/jase.202102_24(1).0008
2. Teng L, Li H, Yin S, et al. A modified advanced encryption standard for data security. International Journal of Network Security. 2020; 22(1): 112–117. Available online: http://ijns.jalaxy.com.tw/contents/ijns-v22-n1/ijns-2020-v22-n1-p112-117.pdf
3. Mardiansyah V, Sari RF. Lightweight blockchain framework for medical record data integrity. Journal of Applied Science and Engineering. 2023; 26(1). doi: 10.6180/jase.202301_26(1).0010
4. Wang X, Yin S, Shafiq M, et al. A new V-net convolutional neural network based on four-dimensional hyperchaotic

system for medical image encryption. Security and Communication Networks. 2022; 2022: 1–14. doi: 10.1155/2022/4260804

5. Senan EM, Alsaade FW, Al-mashhadani MIA, et al. Classification of histopathological images for early detection of breast cancer using deep learning. Journal of Applied Science and Engineering. 2021; 24(3). doi: 10.6180/jase.202106_24(3).0007
6. Li H, Zhu L, Shen M, et al. Blockchain-based data preservation system for medical data. Journal of Medical Systems. 2018; 42(8): 141. doi: 10.1007/s10916-018-0997-3
7. Kishor A, Niyogi R, Veeravalli B. A game-theoretic approach for cost-aware load balancing in distributed systems. Future Generation Computer Systems. 2020; 109: 29–44. doi: 10.1016/j.future.2020.03.027
8. Guo R, Shi H, Zhao Q, et al. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access. 2018; 6: 11676–11686. doi: 10.1109/ACCESS.2018.2801266
9. Azaria A, Ekblaw A, Vieira T, et al. MedRec: using blockchain for medical data access and permission management. In: Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD); 22 August; Vienna, Austria, pp. 25–30. doi: 10.1109/OBD.2016.11
10. Xia Q, Sifah E, Smahi A, et al. BBDS: blockchain-based data sharing for electronic medical records in cloud environments. Information. 2017; 8(2): 44. doi: 10.3390/info8020044
11. Rieke N, Hancox J, Li W, et al. The future of digital health with federated learning. npj Digital Medicine. 2020; 3(1): 119. doi: 10.1038/s41746-020-00323-1
12. Harvey P, Toutsop O, Kornegay K, et al. Security and privacy of medical internet of things devices for smart homes. In: Proceedings of the 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS); 14 December 2020; Paris, France. pp. 1–6. doi: 10.1109/IOTSMS52051.2020.9340231
13. Zhang P, White J, Schmidt DC, et al. FHIRChain: applying blockchain to securely and scalably share clinical data. Computational and Structural Biotechnology Journal. 2018; 16: 267–278. doi: 10.1016/j.csbj.2018.07.004
14. Kuo T-T, Kim H-E, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association. 2017; 24(6): 1211–1220. doi: 10.1093/jamia/ocx068
15. Yue X, Wang H, Jin D, et al. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems. 2016; 40(10): 218. doi: 10.1007/s10916-016-0574-6
16. Esposito C, De Santis A, Tortora G, et al. Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing. 2018; 5(1): 31–37. doi: 10.1109/MCC.2018.011791712
17. Liang X, Shetty S, Tosh D, et al. ProvChain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: Proceedings of the 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID); 14 May 2017; Madrid, Spain, pp. 468–477. doi: 10.1109/CCGRID.2017.8
18. Angraal S, Krumholz HM, Schulz WL. Blockchain technology: applications in health care. Circulation: Cardiovascular Quality and Outcomes. 2017; 10(9): e003800. doi: 10.1161/CIRCOUTCOMES.117.003800
19. Fan K, Wang S, Ren Y, et al. MedBlock: efficient and secure medical data sharing via blockchain. Journal of Medical Systems. 2018; 42(8): 136. doi: 10.1007/s10916-018-0993-7
20. Zhang Y, Kasahara S, Shen Y, et al. Smart contract-based access control for the internet of things. IEEE Internet of Things Journal. 2019; 6(2): 1594–1605. doi: 10.1109/JIOT.2018.2847705
21. McGhin T, Choo K-KR, Liu CZ, et al. Blockchain in healthcare applications: research challenges and opportunities. Journal of Network and Computer Applications. 2019; 135: 62–75. doi: 10.1016/j.jnca.2019.02.027
22. Dagher GG, Mohler J, Milojkovic M, et al. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society. 2018; 39: 283–297. doi: 10.1016/j.scs.2018.02.014
23. Ekblaw A, Azaria A, Halamka JD, et al. A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data. In: Proceedings of IEEE Open & Big Data Conference; 5–8 December 2016; Washington, DC, USA. pp.13–18.
24. Nithyavani G, Naga Raja G. A comprehensive survey on security and privacy challenges in internet of medical things applications: deep learning and machine learning solutions, obstacles, and future directions. IEEE Access. 2025; 13: 188955–188989. doi: 10.1109/ACCESS.2025.3588489
25. Zhuang Y, Sheets LR, Shae ZY, et al. Applying blockchain technology to enhance clinical trial recruitment. AMIA 2019 Annual Symposium. 2020; 2019: 1276–1285. Available online: https://pubmed.ncbi.nlm.nih.gov/32308925/

26. Ichikawa D, Kashiyama M, Ueno T. Tamper-resistant mobile health using blockchain technology. JMIR mHealth and uHealth. 2017; 5(7): e111. doi: 10.2196/mhealth.7938
27. Dubovitskaya A, Xu Z, Ryu S, et al. Secure and trustable electronic medical records sharing using blockchain. AMIA Annual Symposium Proceedings. 2018; 2017: 650–659. Available online: https://pmc.ncbi.nlm.nih.gov/articles/PMC5977675/
28. Xia Q, Sifah EB, Asamoah KO, et al. MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access. 2017; 5: 14757–14767. doi: 10.1109/ACCESS.2017.2730843
29. Chen Y, Ding S, Xu Z, et al. Blockchain-based medical records secure storage and medical service framework. Journal of Medical Systems. 2019; 43(1): 5. doi: 10.1007/s10916-018-1121-4
30. Song Y-J, Zhang Z-S, Song B-Y, et al. Improved genetic algorithm with local search for satellite range scheduling system and its application in environmental monitoring. Sustainable Computing: Informatics and Systems. 2019; 21: 19–27. doi: 10.1016/j.suscom.2018.11.009
31. Liang X, Zhao J, Shetty S, et al. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC); 8 October 2017; Montreal, QC, Canada. pp. 1–5. doi: 10.1109/PIMRC.2017.8292361
32. Zhang J, Xue N, Huang X. A secure system for pervasive social network-based healthcare. IEEE Access. 2016; 4: 9239–9250. doi: 10.1109/ACCESS.2016.2645904
33. Wang H, Song Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. Journal of Medical Systems. 2018; 42(8): 152. doi: 10.1007/s10916-018-0994-6
34. Zhang A, Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of Medical Systems. 2018; 42(8): 140. doi: 10.1007/s10916-018-0995-5
35. Radanović I, Likić R. Opportunities for use of blockchain technology in medicine. Applied Health Economics and Health Policy. 2018; 16(5): 583–590. doi: 10.1007/s40258-018-0412-8
36. Gordon WJ, Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Computational and Structural Biotechnology Journal. 2018; 16: 224–230. doi: 10.1016/j.csbj.2018.06.003
37. Roehrs A, Da Costa CA, Da Rosa Righi R, et al. Analyzing the performance of a blockchain-based personal health record implementation. Journal of Biomedical Informatics. 2019; 92: 103140. doi: 10.1016/j.jbi.2019.103140
38. Mackey TK, Nayyar G. A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expert Opinion on Drug Safety. 2017; 16(5): 587–602. doi: 10.1080/14740338.2017.1313227
39. Siyal AA, Junejo AZ, Zawish M, et al. Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. Cryptography. 2019; 3(1): 3. doi: 10.3390/cryptography3010003
40. Alonso SG, De La Torre Díez I, Rodrigues JJPC, et al. A systematic review of techniques and sources of big data in the healthcare sector. Journal of Medical Systems. 2017; 41(11): 183. doi: 10.1007/s10916-017-0832-2
41. Zhang P, Walker MA, White J, et al. Metrics for assessing blockchain-based healthcare decentralized apps. In: Proceedings of the 2017 IEEE 19th International Conference on E-Health Networking, Applications and Services (Healthcom); 12 October 2017; Dalian, China. pp. 1–4. doi: 10.1109/HealthCom.2017.8210842
42. Peterson K, Deeduvanu R, Kanjamala P, et al. A blockchain-based approach to health information exchange networks. NIST Blockchain for Healthcare Workshop. 2016. Available online: https://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/12-55-blockchain-based-approach-final.pdf
43. Kuze N, Kominami D, Kashima K, et al. Self-organizing control mechanism based on collective decision-making for information uncertainty. ACM Transactions on Autonomous and Adaptive Systems. 2018; 13(1): 1–21. doi: 10.1145/3183340
44. Agbo CC, Mahmoud QH, Eklund JM. Blockchain technology in healthcare: a systematic review. Healthcare. 2019; 7(2): 56. doi: 10.3390/healthcare7020056
45. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics. 2019; 36: 55–81. doi: 10.1016/j.tele.2018.11.006
46. Mettler M. Blockchain technology in healthcare: the revolution starts here. In: Proceedings of the 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom); 14–16 September 2016; Munich, Germany, pp. 1–3. doi: 10.1109/HealthCom.2016.7749510
47. Zhang R, Xue R, Liu L. Security and privacy on blockchain. ACM Computing Surveys. 2020; 52(3): 1–34. doi: 10.1145/3316481

48. Zheng Z, Xie S, Dai HN, et al. Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services. 2018; 14(4): 352. doi: 10.1504/IJWGS.2018.095647
49. Wang S, Yuan Y, Wang X, et al. An overview of smart contract: architecture, applications, and future trends, in: 2018 IEEE Intelligent Vehicles Symposium (IV). In: Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV); 20 June 2018; Changshu, China. pp. 108–113. doi: 10.1109/IVS.2018.8500488
50. Gupta M, Dwivedi RK. Blockchain- based secure and efficient scheme for medical data. ICST Transactions on Scalable Information Systems. 2023; doi: 10.4108/eetsis.3235
51. Garai T, Garg H, Roy TK. A ranking method based on possibility mean for multi-attribute decision making with single valued neutrosophic numbers. Journal of Ambient Intelligence and Humanized Computing. 2020; 11(11): 5245–5258. doi: 10.1007/s12652-020-01853-y
52. Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications. 2020; 50: 102407. doi: 10.1016/j.jisa.2019.102407
53. Verma G, Kanrar S. Secure digital documents sharing using blockchain and attribute-based cryptosystem. Multiagent and Grid Systems. 2023; 18(3–4): 365–379. doi: 10.3233/MGS-221361
54. Zatwarnicki K. Two-level fuzzy-neural load distribution strategy in cloud-based web system. Journal of Cloud Computing. 2020; 9(1): 30. doi: 10.1186/s13677-020-00179-6
55. Kowalska A. Design of a federated learning architecture supported by blockchain for privacy-preserving model training in internet of things health monitoring systems. ISCSITR—International Journal of IoT and Blockchain. 2021; 2(1): 1–8. Available online: https://iscsitr.com/articles/volume_2/issue_1/ISCSITR-IJIOTBC_02_01_001
56. Feng Q, He D, Zeadally S, et al. A survey on privacy protection in blockchain system. Journal of Network and Computer Applications. 2019; 126: 45–58. doi: 10.1016/j.jnca.2018.10.020
57. Zhang D, Xu H, Li P, et al. Privacy parameter setting and usability optimization algorithm for medical data. IEEE Transactions on Consumer Electronics. 2025; 71(2): 4883–4891. doi: 10.1109/TCE.2025.3569752
58. Zhang Y, Wang XA, Jiang W, et al. An efficient and secure data audit scheme for cloud-based EHRs with recoverable and batch auditing. Computers, Materials & Continua. 2025; 83(1): 1533–1553. doi: 10.32604/cmc.2025.062910
59. Evans M, He Y, Maglaras L, et al. HEART-IS: a novel technique for evaluating human error-related information security incidents. Computers & Security. 2019; 80: 74–89. doi: 10.1016/j.cose.2018.09.002
60. Dehmollaian M, Chamanara N, Caloz C. Wave scattering by a cylindrical metasurface cavity of arbitrary cross section: theory and applications. IEEE Transactions on Antennas and Propagation. 2019; 67(6): 4059–4072. doi: 10.1109/TAP.2019.2905711
61. Dos Santos S, Chukwuocha C, Kamali S, et al. An efficient miner strategy for selecting cryptocurrency transactions. In: Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain); 7 July 2019; Atlanta, GA, USA, pp. 116–123. doi: 10.1109/Blockchain.2019.00024
62. Ni L, Huang P, Wei Y, et al. Federated learning model with adaptive differential privacy protection in medical IoT. Wireless Communications and Mobile Computing. 2021; 2021(1): 8967819. doi: 10.1155/2021/8967819
63. Pati S, Kumar S, Varma A, et al. Privacy preservation for federated learning in health care. Patterns. 2024; 5(7): 100974. doi: 10.1016/j.patter.2024.100974
64. Yang Q, Liu Y, Chen T, et al. Federated machine learning: concept and applications. ACM Transactions on Intelligent Systems and Technology. 2019; 10(2): 1–19. doi: 10.1145/3298981
65. Shabani M. Blockchain-based platforms for genomic data sharing: a de-centralized approach in response to the governance problems? Journal of the American Medical Informatics Association. 2019; 26(1): 76–80. doi: 10.1093/jamia/ocy149
66. Bolbocean C, Shevell M. The impact of high intensity care around birth on long-term neurodevelopmental outcomes. Health Economics Review. 2020; 10(1): 22. doi: 10.1186/s13561-020-00279-8
67. Al Omar A, Rahman MS, Basu A, et al. MediBchain: a blockchain based privacy preserving platform for healthcare data. In: Wang G, Atiquzzaman M, Yan Z, et al. (editors). Security, Privacy, and Anonymity in Computation, Communication, and Storage, Lecture Notes in Computer Science. Springer International Publishing. 2017. pp. 534–543. doi: 10.1007/978-3-319-72395-2_49
68. Fotouhi A, Ding M, Hassan M. DroneCells: improving spectral efficiency using drone-mounted flying base stations. Journal of Network and Computer Applications. 2021; 174: 102895. doi: 10.1016/j.jnca.2020.102895
69. Zhou J, Gan J, Gao W, et al. Image retrieval based on aggregated deep features weighted by regional significance and channel sensitivity. Information Sciences. 2021; 577: 69–80. doi: 10.1016/j.ins.2021.06.002
70. Zhong D, Yang G, Fan J, et al. A service recommendation system based on rough multidimensional matrix in

cloud-based environment. Computer Standards & Interfaces. 2022; 82: 103632. doi: 10.1016/j.csi.2022.103632
71. Nguyen DC, Pham Q-V, Pathirana PN, et al. Federated learning for smart healthcare: a survey. ACM Computing Surveys. 2023; 55(3): 1–37. doi: 10.1145/3501296
72. Xiao Y, Zhang N, Lou W, et al. A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials. 2020; 22(2): 1432–1465. doi: 10.1109/COMST.2020.2969706
73. Li W, Yu K, Feng C, et al. SP-MIOV: a novel framework of shadow proxy based medical image online visualization in computing and storage resource restrained environments. Future Generation Computer Systems. 2020; 105: 318–330. doi: 10.1016/j.future.2019.12.009
74. Dai H-N, Zheng Z, Zhang Y. Blockchain for internet of things: a survey. IEEE Internet of Things Journal. 2019; 6(5): 8076–8094. doi: 10.1109/JIOT.2019.2920987
75. Albahri AS, Alwan JK, Taha ZK, et al. IoT-based telemedicine for disease prevention and health promotion: State-of-the-Art. Journal of Network and Computer Applications. 2021; 173: 102873. doi: 10.1016/j.jnca.2020.102873