Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in
e-ISSN: 3009-075X

Volume 4 Issue 6
Article Number: 25221

A Systematic Review of Scalable Blockchain-Based Digital Signature Frameworks for Healthcare Data Security

Li Xu[1,2], Mohd Nurul Hafiz Bin Ibrahim[3], Mustafa Muwafak Alobaedy[3,4], and S. B. Goyal* [5]

[1]City Graduate School, City University, Petaling Jaya, Selangor, Malaysia, 46100
[2]NanChang Institute of Science and Technology, NanChang, Jiangxi, China, 330044
[3]Faculty of Information Technology, City University, Petaling Jaya, Selangor, Malaysia, 46100
[4]Faculty of Information Technology, City University, Petaling Jaya, Selangor, Malaysia, 46100
[4]Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Selangor, Malaysia, 63100
[5]Chitkara University Institute of Engineering & Technology, Chitkara University, Rajpura, Punjab, India, 140401

Abstract

This is the first PRISMA-guided systematic review of scalable blockchain digital signatures for healthcare, synthesizing evidence from 85 peer-reviewed studies published between 2015 and 2024. The review examines five thematic areas: digital signatures, consensus mechanisms, smart contracts, hybrid blockchain architectures, and regulatory compliance. Particular emphasis is placed on scalability challenges and the role of alternative consensus protocols, such as Proof-of-Stake and Delegated Proof-of-Authority (DPoA), in addressing the energy and latency limitations of Proof-of-Work (PoW). Findings highlight the value of smart contracts in automating consent and authentication processes, while hybrid blockchain models are shown to strike a balance between security and scalability. The synthesis also identifies persistent challenges, including interoperability with legacy systems, energy consumption, and compliance with GDPR and HIPAA regulations. Importantly, emerging approaches such as Layer-2 scaling, AI-enhanced validation, and post-quantum cryptography are highlighted as promising directions for future development. By integrating technical and regulatory perspectives, this review contributes a critical roadmap for researchers, healthcare providers, and system architects seeking secure, efficient, and regulation-compliant blockchain frameworks.

Keywords: Blockchain; Digital Signatures; Healthcare Data Security; Scalability; Systematic Review

1. Introduction

As a whole, the healthcare industry's digital transition has been a boon to telemedicine, data-driven healthcare applications, and EHRs. However, new concerns around security and privacy have emerged due to this transformation. Healthcare data breaches have increased dramatically over the past decade, exposing patients' personal information to cyber threats such as data manipulation, ransomware, and unauthorized access [1]. One of the most targeted industries is healthcare, due to the high value of patient records on underground markets.

*Corresponding Author: S. B. Goyal (drsbgoyal@gmail.com)
Received: 29 Apr 2025; Revised: 24 May 2025; Accepted: 15 Jun 2025; Published: 30 Jun 2025

DOI: 10.57159/jcmm.4.6.25221.

Another degree of complexity and security risk is introduced into healthcare data management by the numerous parties involved, including hospitals, insurance firms, and government bodies. Standard security measures, such as central databases and encryption algorithms, can only do so much to ensure the authenticity and integrity of data [2]. There are several issues with centralized storage structures, including a single point of failure, data breaches, and insider threats. Some of the current methods of authentication rely on third-party trust models that could be easily manipulated. In front of these challenges, healthcare systems require a scalable security architecture that ensures data compliance, integrity, and authenticity. In several ways, blockchain technology is aiding in the resolution of these issues, including decentralized and immutable data storage, cryptographic security, and automation through the use of smart contracts. The immutable and transparent recording of transactions is made possible by the distributed ledger system that blockchain technology enables. Among its primary security features are digital signatures, which ensure authenticity, prevent data tampering, and maintain integrity. Digital signatures assure authentic and unchangeable medical records [3]. When combined with blockchain technology, digital signatures provide cryptographic validation that is decentralized from a central authority, thereby greatly enhancing the system's security and further reducing the possibility of data leaks, as they do not involve a trusted third party or central authority.

Although there are numerous advantages to blockchain-based security frameworks, scalability remains a significant challenge. The slow processing rates and high energy consumption of existing blockchain models, such as proof-of-work (PoW), make them unsuitable for widely used in healthcare applications [4]. In an effort to address these concerns, researchers have investigated alternative consensus techniques, including proof-of-stake and delegated proof-of-authority, that can enhance security and scalability. A combination of public and private blockchains has been proposed as a means to further enhance performance and data security. The feasibility, effectiveness, and compliance with regulations of such frameworks require further investigation before their use in real healthcare environments.

Immediate action is required to conduct a comprehensive literature review (SLR) on the topic of blockchain-based digital signatures and their potential impact on healthcare data security. This review should integrate existing research, identify key trends, and identify any gaps in our present understanding. An SLR provides a methodical approach to reviewing case studies, technical reports, and research articles, ensuring a comprehensive understanding of the subject [5]. In contrast to a traditional literature review, a systematic literature review adheres to a predetermined procedure for selecting, evaluating, and synthesizing sources. The results will be more trustworthy and free of biases if this is done. The scalability of blockchain-based digital signatures in healthcare data security is the focus of this article, which aims to investigate various consensus procedures, smart contract applications, and hybrid blockchain models.

2. Literature Review

There has been a dramatic increase in research into applying blockchain technology to healthcare security due to its potential to enhance data integrity, authentication, and compliance with regulations [6]. This review of the literature focuses on blockchain-based security frameworks and their key components, including digital signatures, smart contract applications, consensus processes, scalability issues, regulatory compliance, hybrid blockchain models, and current research gaps. Without the need for a governing body, blockchain technology enables the safekeeping and accessibility of medical records through an immutable, distributed ledger system. The immutable security features of blockchain prevent fraudulent activity and illegal changes, in contrast to traditional databases [7]. By encoding information into distinct hash values, cryptographic hashing ensures data integrity and is a crucial component of blockchain security. Any alteration to the original data will result in a new hash, making it easy to detect unauthorized changes. Additionally, by utilizing consensus procedures to authenticate transactions, blockchain eliminates the need for third-party trust models.

Essential to blockchain-based authentication, digital signatures give cryptographic confirmation of data validity. A digital signature uses public and private key encryption to guarantee that only authorized individuals can access or modify medical records [8]. When a user uses the public key that is associated with their private key, they can verify that the signed transaction is genuine and cannot be reversed. By verifying the identity of individuals, organizations, and institutions involved in the healthcare system, digital signatures help to secure electronic health records (EHRs), telemedicine interactions, and prescription medications. Several studies have demonstrated that digital signatures built on blockchain technology successfully prevent data breaches and unauthorized access to patient records. However, before these methods can be widely used, there are still hurdles to overcome. One of the significant challenges with utilizing blockchain technology for healthcare security is its limited scalability. Due to their computational expense and slowness, traditional blockchain frameworks, such as Bitcoin's Proof-of-Work (PoW), are not suited for high-volume healthcare transactions [9]. Some have suggested different ways to reach consensus that would make it more scalable without compromising security. In Proof-of-Stake (PoS), validators are selected based on the quantity of cryptocurrency they hold, rather than through computational mining. When compared to PoW, PoS enhances transaction throughput while minimizing energy usage.

By simplifying the validation of transactions by a group of approved validators, Delegated Proof-of-Authority (DPoA) further enhances scalability while minimizing processing time and resource consumption. In healthcare applications, where speedy data verification and security are crucial, these alternative consensus models show potential, according to studies. Despite these advancements, security, scalability, and decentralization are not mutually exclusive; they can be achieved simultaneously. Although PoS and DPoA have lower processing overhead, they raise concerns about validator collusion and centralization. It remains challenging to find the ideal consensus mechanism for healthcare applications that must comply with regulations and maintain high levels of security. To tackle these challenges, researchers have explored hybrid approaches that integrate aspects of multiple consensus models; however, further investigation is required to assess how well these strategies perform in actual healthcare settings [10]. Integrating smart contracts into blockchain networks enables the automation of authentication, access control, and transaction validation. These contracts execute themselves. To ensure that only authorized organizations can access patient records, smart contracts can be programmed to enforce data-sharing policies in healthcare security [11]. To illustrate the idea, a smart contract can eliminate the requirement for human interaction by automatically granting access to an insurance provider upon patient permission. This minimizes the burden on administrators and reduces the likelihood of human error in data handling.

Smart contracts have been effectively utilized in case studies to secure electronic health records, trace medical supply chains, and handle patient consent. For instance, patients at certain hospitals can now digitally authorize or revoke data-sharing licenses in real time through the use of consent management systems based on blockchain technology. Patients' privacy is enhanced, and data protection requirements are met in this way [12]. However, concerns such as programming errors, smart contract vulnerabilities, and integration with existing healthcare IT systems must be addressed to guarantee dependability and security. Hybrid blockchains, which combine public and private blockchains, offer healthcare applications scalability and security [13]. Public blockchains provide decentralization and transparency, whereas private blockchains enable faster transaction processing and controlled access. With hybrid systems, private patient information can be stored on one chain with restricted access, while public transaction records and digital signatures can be kept on another, improving transparency and auditability. Research has shown that hybrid blockchain models offer numerous advantages in the healthcare industry, including increased efficiency, enhanced privacy protections, and compliance with data protection regulations. Based on findings from healthcare institutions and telemedicine platforms, hybrid blockchains have the potential to enhance interoperability among healthcare providers while ensuring the security of patient data [14]. Before hybrid models can be implemented, issues related to cross-chain communication, security risks, and governance processes must be addressed. Further research is required to determine how to optimize hybrid blockchain systems for broad application in healthcare. Regulatory compliance is a prerequisite for implementing blockchain-based security solutions in the healthcare sector. Regulations such as the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States impose severe requirements on data protection, access control, and patient consent [15]. The immutability of blockchain technology makes it more challenging to comply with legislation that requires data to be changed or deleted upon user request, such as the "right to be forgotten" in the GDPR.

Several studies have focused on addressing regulatory problems related to blockchain-based healthcare security. One approach is to store encrypted patient records off-chain while monitoring on-chain activity logs and digital signatures. Blockchain's immutability and security features can be leveraged to meet regulatory compliance requirements in this manner. Another alternative is permissioned blockchain networks, which allow only authorized parties access to data within a controlled environment. Despite these promising solutions, ensuring full compliance while retaining the core benefits of blockchain remains challenging. While significant progress has been made in healthcare blockchain security, numerous uncertainties remain. Efficient use of energy is of paramount importance, especially for consensus processes that demand substantial computing power [16]. Although PoS and DPoA require less energy than PoW, further innovation is needed to make blockchain solutions more environmentally friendly in healthcare. Another major challenge is compatibility with existing healthcare IT systems, as most legacy systems are not designed to integrate with blockchain-based solutions. Developing standardized protocols and middleware is essential to ensure seamless integration with traditional databases.

In conclusion, scalable solutions for handling large volumes of healthcare transactions require further investigation. Although hybrid blockchain models and alternative consensus mechanisms may offer benefits, their effectiveness in real healthcare settings requires extensive testing. The lack of research on provider and patient acceptance of blockchain-based security frameworks also highlights the need for user-centric studies to identify adoption barriers and usability concerns [17]. Overall, blockchain technology has the potential to enhance the security of healthcare data through the use of digital signatures, consensus processes, smart contracts, and hybrid models. However, resolving issues related to scalability, regulatory compliance, energy efficiency, and interoperability is critical for widespread adoption. This review synthesizes the existing literature and identifies future research directions to support the development of trustworthy and scalable blockchain-based digital signature frameworks for healthcare applications [18].

3. Methods

The objective of this systematic literature review (SLR) is to synthesize recent findings on the application of scalable blockchain-based digital signatures for securing healthcare data. By following a clearly defined and reproducible review protocol, this process ensures that the investigation is comprehensive, unbiased, and methodologically rigorous. The review involved the identification, selection, evaluation, and synthesis of relevant studies to provide insights into the current landscape and future potential of blockchain-based frameworks for healthcare data security.

3.1. Search Strategy

To locate relevant literature, a systematic search was conducted across five major academic databases: IEEE Xplore, Scopus, ScienceDirect, SpringerLink, and PubMed. These databases were selected based on their extensive coverage of peer-reviewed journals, technical reports, and conference proceedings in the domains of blockchain technology, digital security, and healthcare informatics. The search strategy used a combination of keywords, including "blockchain," "digital signatures," "healthcare data security," "scalability," "smart contracts," "electronic health records (EHRs)," and "consensus mechanisms," connected using Boolean operators such as AND and OR to optimize retrieval precision, as shown in Figure 1.

3.2. Screening and Eligibility

Two independent reviewers screened all retrieved records by title, abstract, and full text to ensure reliability and validity. Reviewer agreement was evaluated using Cohen's $\kappa = 0.89$, indicating high consistency. Disagreements were resolved through discussion.

Inclusion criteria:

- English-language, peer-reviewed articles, conference papers, or technical reports.
- Focused on blockchain-based digital signatures in healthcare data security.

Exclusion criteria:

- Non-healthcare blockchain applications (e.g., finance, logistics).
- Non-peer-reviewed, non-English studies, or studies lacking scalability or digital-signature focus.

PRISMA summary:

- Records identified: 456
- Duplicates removed: 97
- Records screened: 359
- Records excluded by title/abstract: 248
- Full-text articles assessed: 111
- Full-text articles excluded: 26
- Studies included in synthesis: 85

Reasons for full-text exclusion included a non-healthcare focus ($n = 11$), absence of digital signature implementation ($n = 4$), lack of scalability or consensus-related analysis ($n = 6$), and non-peer-reviewed or unavailable full text ($n = 5$). The study selection process is summarized in Figure 1. The review identified 456 records across five databases. After removing 97 duplicates, 359 records were screened, and 248 were excluded based on title or abstract. A total of 111 full-text articles were assessed for eligibility, with 26 excluded for the reasons stated above. Finally, 85 studies were included in the qualitative synthesis.

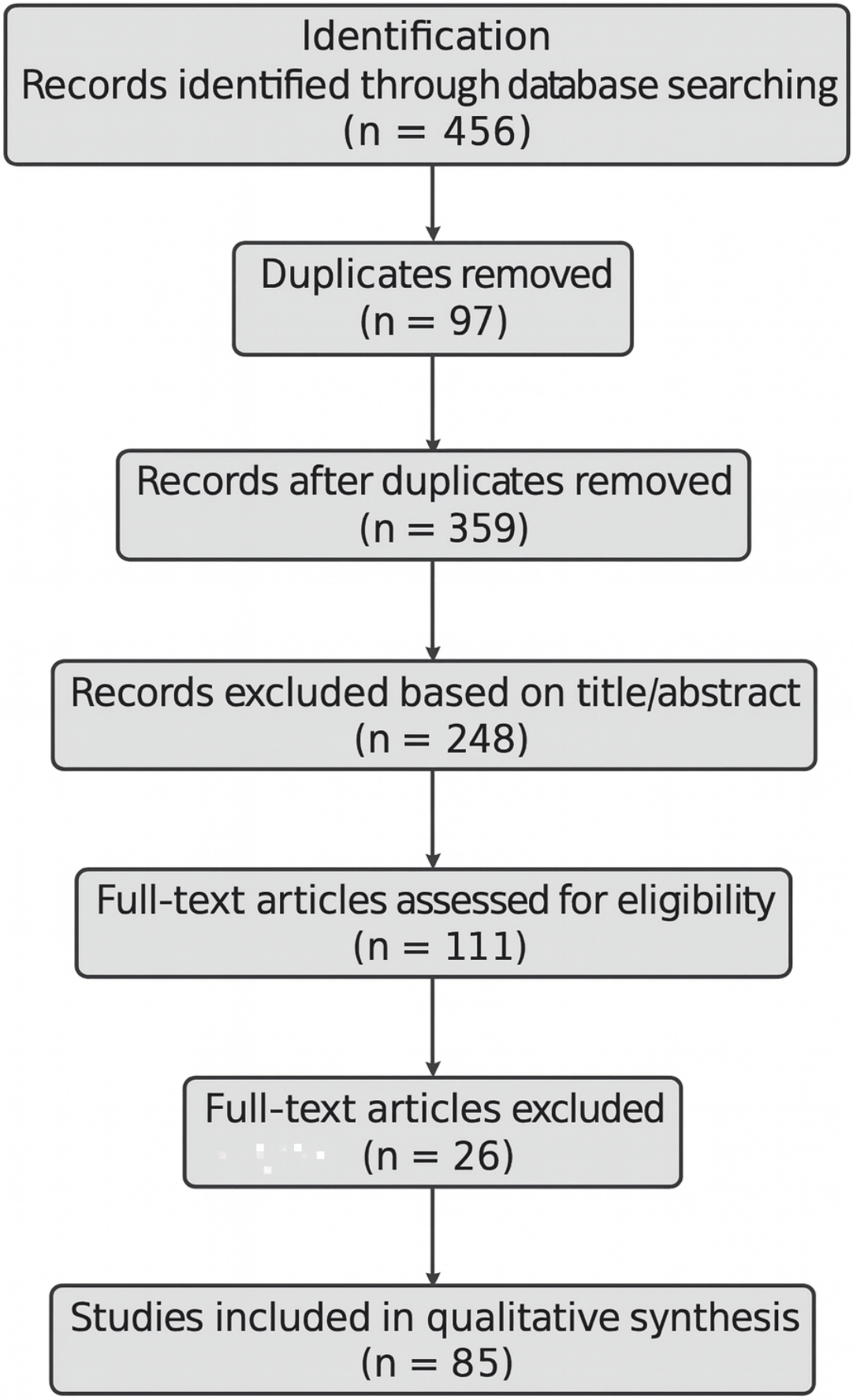

Figure 1: PRISMA 2020 flow diagram illustrating the study selection process.

3.3. Data Extraction and Quality Appraisal

Data were extracted using a structured coding framework covering the following dimensions:

- Blockchain design: public, private, or hybrid model
- Consensus mechanism: Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Authority (DPoA), or hybrid
- Digital signature type: ECDSA, EdDSA, BLS, or others
- Smart contract use: for consent, authentication, or verification
- Regulatory focus: GDPR, HIPAA, or equivalent standards
- Performance metrics: scalability, latency, throughput, and energy efficiency

Quality was appraised using the JBI Critical Appraisal Checklist. Studies were rated High ($\geq 8/10$), Moderate (5–7), or Low (≤ 4) based on methodological rigor, data validity, and contribution to knowledge. High-quality studies were prioritized in the synthesis, and a sensitivity analysis confirmed that findings were consistent when limited to this subset. A summary of the selection and quality assessment criteria is presented in Table 1.

Table 1: Selection and Quality Assessment Criteria

Criterion	**Description**	**Justification**
Database Searched	IEEE Xplore, PubMed, Scopus, ScienceDirect, SpringerLink	Chosen for broad coverage of blockchain, healthcare, and security publications.
Publication Years	2015–2024	Covers the recent decade of rapid blockchain adoption in healthcare.
Inclusion Criteria	Peer-reviewed journal articles, conference papers, and technical reports on healthcare security	ensuring methodological rigor and relevance to the healthcare domain.
Exclusion Criteria	Non-healthcare blockchain applications, non-English studies, unpublished reports,	Eliminates irrelevant or low-quality sources.
Data Extraction Parameters	Blockchain Type, Consensus Mechanism, Scalability Solutions, Smart Contract Use, Regulatory Focus,	Allows Comparative Analysis of Technical and Regulatory Aspects.
Quality Assessment Factors	Relevance, Methodology, Contribution, Citation Impact, Data Validity, and provides a systematic evaluation of study robustness and contribution.	

The systematic approach adopted in this review enables a structured examination of the current state of blockchain-based digital signature frameworks for healthcare. By highlighting prevailing trends, identifying effective technical solutions, and exposing implementation challenges, this review offers valuable guidance for researchers, developers, and policymakers aiming to enhance healthcare data security through scalable blockchain architectures.

4. Results and Discussion

A comprehensive analysis of digital signatures based on blockchain technology for healthcare data security reveals numerous noteworthy advancements, highlights the usefulness of smart contracts, and identifies existing challenges in the field. According to the findings, the primary factor behind the growing use of blockchain technology in healthcare is the need for enhanced data integrity, authentication, and compliance with regulations. Scalability, interoperability, and regulatory concerns remain primary roadblocks to widespread use, as shown in Figure 2.

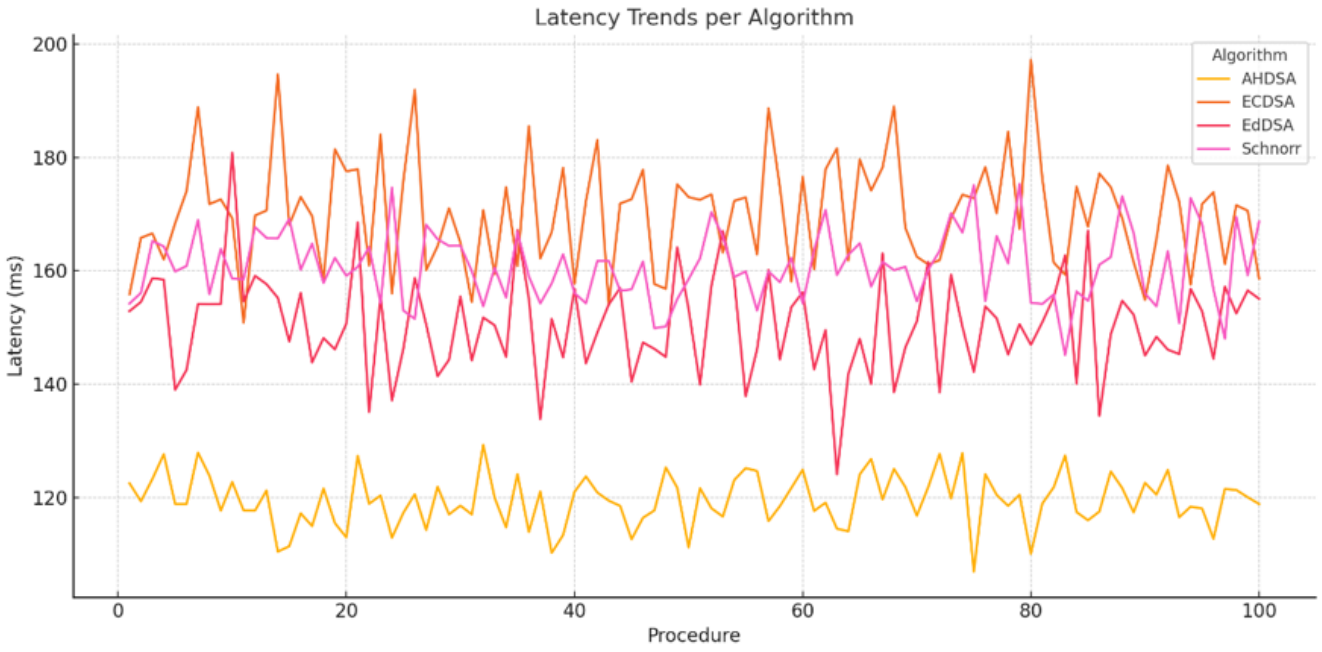

Figure 2: Latency rate of blockchain models in healthcare.

Figure 2 illustrates the performance challenges of blockchain-based systems in healthcare, where high latency can undermine the real-time requirements of EHRs and telemedicine platforms. Beyond latency performance, the scalability of blockchain systems is largely determined by the choice of consensus mechanism. Table 2 summarizes the distribution of consensus mechanisms across the reviewed studies, highlighting both their strengths and limitations.

Table 2: Consensus mechanisms in reviewed studies

Consensus Mechanism	**No. of Studies (N = 85)**	**Strengths**	**Weaknesses**	**Healthcare Relevance**
Proof-of-Work (PoW)	18 (21.2%)	Strong immutability; widely tested	Energy-intensive; slow; poor scalability	Limited applicability; unsuitable for real-time EHR validation or telemedicine.
Proof-of-Stake (PoS)	24 (28.2%)	High efficiency; faster throughput; eco-friendly	Risk of validator collusion	Suitable for EHR validation and large-scale telehealth platforms requiring real-time data.
Delegated Proof-of-Authority (DPoA)	15 (17.6%)	Very fast validation; efficient for private chains	Risk of centralization; validator bias	Effective in private hospital networks and controlled telemedicine systems.
Hybrid (PoS + BFT, etc.)	12 (14.1%)	Balanced security and scalability	Complex governance and interoperability issues	Potential for nationwide healthcare systems with mixed privacy and audit needs.
Other / Not Specified	16 (18.9%)	General blockchain reference	Lacks detailed consensus discussion	Not healthcare-specific; often conceptual frameworks without implementation.

As shown in Table 2, Proof-of-Stake (PoS) emerges as the most frequently cited mechanism, with nearly one-third of studies highlighting its scalability and efficiency advantages. Delegated Proof-of-Authority (DPoA) is also increasingly explored in private healthcare contexts due to its fast validation and low energy usage, though concerns about validator collusion persist. Hybrid models are receiving growing attention for their ability to combine scalability with security. In light of the security concerns raised by electronic health records (EHRs), telemedicine platforms, and healthcare data transfers, blockchain technology is being explored as a potential solution to address these concerns. Digital signatures created on the blockchain are quickly becoming a trusted method for ensuring authentication and data integrity. This is because they discourage tampering and reduce the likelihood of centralized database breaches. Research indicates that regulatory compliance, data security, and transparency are the primary motivators for implementing blockchain technology in healthcare. The comparison of mean duration is mentioned in Figure 3.

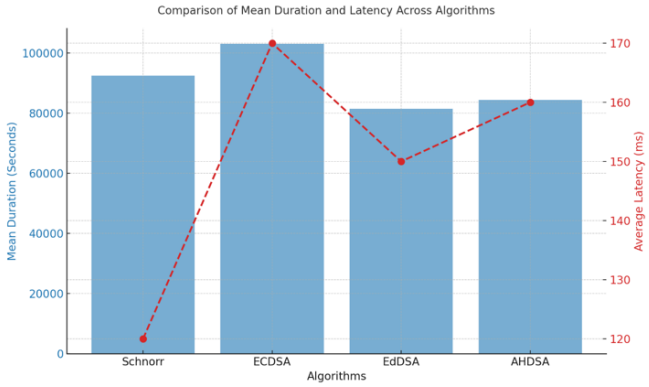

Figure 3: Mean validation duration of consensus mechanisms.

The comparison of mean duration across different models is illustrated in Figure 3, showing that PoS and DPoA outperform PoW in validation speed. Applications of blockchain-based digital signatures in healthcare extend beyond consensus, touching multiple critical domains. Table 3 categorizes the application areas highlighted in the reviewed studies, with Electronic Health Records (EHRs) emerging as the dominant focus.

Table 3: Application areas of blockchain-based digital signatures in healthcare

Application Area	**No. of Studies**	**% of Total**	**Example Use Case**	**Emerging Applications**
Electronic Health Records (EHRs)	30	35.3%	Patient record authenticity and tamper-proof storage	AI-assisted anomaly detection in EHR validation.
Telemedicine	15	17.6%	Secure online consultations, encrypted data sharing	IoT-enabled monitoring for remote patient management (RPM).
Consent Management	10	11.8%	Automated patient approvals via smart contracts	Dynamic consent revocation and audit trails for compliance.
Insurance & Claims	12	14.1%	Fraud detection and automated claims	AI-driven claims adjudication and interoperability with payers.
Medical Supply Chain	18	21.2%	Tracking pharmaceuticals and preventing counterfeits	Blockchain–IoT tracking of vaccines and temperature-sensitive drugs.

As shown in Table 3, blockchain-based digital signatures have a particularly significant impact in EHR management, where data integrity and authentication are of paramount importance. Medical supply chain tracking is another growing field, with 21.2% of studies focusing on the prevention of counterfeit drugs. Consent management and insurance automation represent emerging but promising areas where smart contracts are particularly effective. One major development in blockchain-based digital signatures for healthcare is the shift from permissionless (public) to permissioned (private or hybrid) blockchain architectural models. Public blockchains have several advantages, including immutability and transparency; however, they also have significant scalability issues and are not always suitable for use in healthcare, particularly in light of stringent privacy regulations.

Private and hybrid blockchains, on the other hand, enable controlled access and facilitate better compliance with regulatory standards, such as the GDPR in the European Union and HIPAA in North America. Because they combine security, efficiency, and scalability, hybrid models are gaining increasing popularity. Transaction comparison is shown in Figure 4. In parallel with this architectural evolution, there is a growing incorporation of advanced technologies such as artificial intelligence (AI) and the Internet of Things (IoT) into blockchain-enabled healthcare applications. AI-enhanced smart contracts are being developed to dynamically assess and approve authentication requests, while IoT integration supports real-time monitoring in remote patient management (RPM) systems. Despite these innovations, adoption at scale remains challenging due to integration complexities with legacy systems and concerns over transaction latency and throughput.

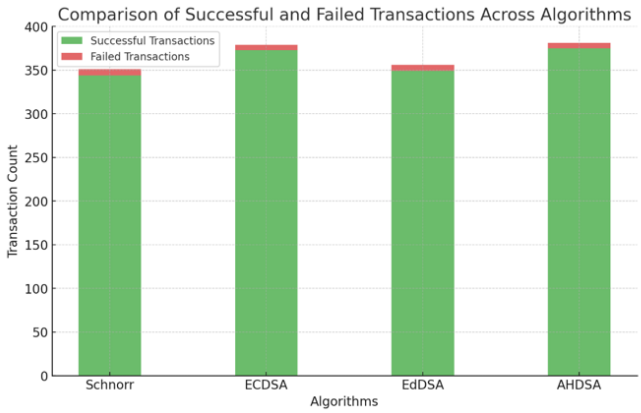

Figure 4: Transaction comparison across blockchain architectures.

The effectiveness of blockchain-based digital signatures in healthcare systems is closely tied to the underlying consensus mechanisms that validate transactions. The early use of Proof-of-Work (PoW) algorithms, popularized by cryptocurrencies such as Bitcoin, has proven inadequate for healthcare due to their excessive energy consumption and slow transaction speeds. In response, more scalable and sustainable consensus mechanisms have been proposed and implemented in healthcare-oriented blockchain models. Among these, Proof-of-Stake (PoS) has emerged as a leading alternative due to its significant energy efficiency and higher transaction throughput. Unlike PoW, which relies on computational mining, PoS selects validators based on the stake they hold in the network, thereby reducing processing overhead. Studies reviewed indicate that PoS not only enhances scalability but also maintains strong data integrity, making it more suited for real-time healthcare applications where speed and security are essential. Another consensus model gaining traction is Delegated Proof-of-Authority (DPoA), which differs from PoS by designating a predetermined set of trusted validators to confirm transactions. This model substantially increases validation speed and reduces energy usage, making it appealing for private healthcare environments. However, concerns persist regarding potential centralization and validator bias, which could compromise the network's transparency and neutrality.

To reconcile trade-offs between decentralization, performance, and security, researchers are now investigating hybrid consensus models that combine the strengths of multiple mechanisms, such as PoS with Byzantine Fault Tolerance (BFT) protocols. For example, a blockchain system might use PoS to select validators while relying on BFT for rapid consensus finality. Although initial results are promising, further empirical research is necessary to assess their practicality and resilience in healthcare settings. Smart contracts are another transformative component within blockchain ecosystems that directly address data governance, consent management, and process automation in healthcare. By embedding rules directly into code, smart contracts enable real-time enforcement of data access policies, ensuring that only authorized personnel can retrieve or modify patient records. This functionality significantly reduces administrative overhead and eliminates manual errors associated with data management. A key advantage of smart contracts is their capacity to automate the patient consent process. Conventional approaches to managing consent are time-consuming, fragmented, and vulnerable to human error. With smart contracts, patients can instantly grant or revoke data-sharing permissions through secure digital interfaces. This not only bolsters user privacy but also aligns with data protection mandates under GDPR and other similar regulations.

Practical implementations have demonstrated the value of smart contracts in various domains, including insurance claims processing, pharmaceutical supply chain verification, and electronic prescription validation. Several healthcare institutions have deployed blockchain-based systems to automatically authenticate prescription data, detect fraud, and streamline inter-organizational transactions. Insurance companies are also experimenting with smart contracts to handle claims autonomously, reducing the likelihood of disputes and minimizing operational costs. Despite these benefits, several obstacles hinder the broader implementation of smart contracts in healthcare. Programming vulnerabilities, limitations in contract upgradability, and integration barriers with existing electronic health systems remain problematic.

Secure coding practices, rigorous auditing, and the development of standardized protocols are crucial for mitigating risks and fostering trust in smart contract-based solutions. While blockchain-based digital signatures and smart contracts hold substantial promise for enhancing data security and system reliability, scalability remains a critical issue. Presently, many blockchain platforms lack the capacity to process the volume of transactions necessary for large-scale healthcare applications. To overcome this, researchers are investigating Layer-2 scaling solutions, such as sidechains, rollups, and state channels, that operate in parallel to the main blockchain, offloading computational burden while preserving the benefits of decentralization. Another major limitation concerns regulatory complianceparticularlyly concerning the" right to be forgotten""the GDPR. Since blockchain immutability contradicts the legal requirement for data erasure, off-chain storage solutions are being considered. In such models, sensitive data are stored off-chain, while only encrypted references and access logs are maintained on-chain. Although effective in meeting regulatory requirements, these solutions introduce new challenges in terms of interoperability and secure key management. The lack of compatibility with legacy IT infrastructure is a further barrier to adoption. Most healthcare providers still operate on centralized EHR systems that are not inherently designed to communicate with decentralized platforms. The development of middleware APIs, integration gateways, and cross-platform standards is crucial to ensure seamless interoperability between blockchain and traditional health IT environments.

However, such efforts require coordinated action among regulators, technology vendors, and healthcare stakeholders. Emerging solutions to the scalability dilemma include advanced architectures such as sharding, directed acyclic graphs (DAGs), and cross-chain interoperability frameworks. Sharding improves performance by partitioning the blockchain into smaller segments that process transactions in parallel, thereby increasing throughput. DAGs enable asynchronous transaction validation, significantly reducing congestion. Cross-chain frameworks aim to facilitate secure data exchange across multiple blockchain networks, enhancing flexibility and ecosystem-wide scalability. Another area gaining interest is the adoption of post-quantum cryptographic techniques in blockchain frameworks. As quantum computing capabilities advance, current cryptographic algorithms, including those used in digital signatures, may become vulnerable. Ongoing research in lattice-based and hash-based cryptography aims to develop quantum-resistant solutions that safeguard future healthcare applications against emerging threats.

Blockchain-based digital signatures represent a paradigm shift in how healthcare data can be securely managed, authenticated, and shared. This review highlights that hybrid blockchain frameworks, next-generation consensus protocols, and smart contract automation offer viable paths toward scalability and enhanced data governance. Nevertheless, significant challenges related to regulatory alignment, legacy system integration, and scalability must be addressed through continued research and collaborative innovation. A concerted focus on scalable blockchain design, supportive legal frameworks, and interoperable infrastructure will be crucial to enabling widespread adoption and realizing the full potential of blockchain in healthcare security. Figure 5 synthesizes the most frequently reported challenges across studies. Scalability and interoperability were identified in more than half of the reviewed literature, followed closely by regulatory compliance and energy efficiency. Integration with legacy systems was also highlighted as a major barrier, given the prevalence of centralized EHR infrastructure in healthcare institutions.

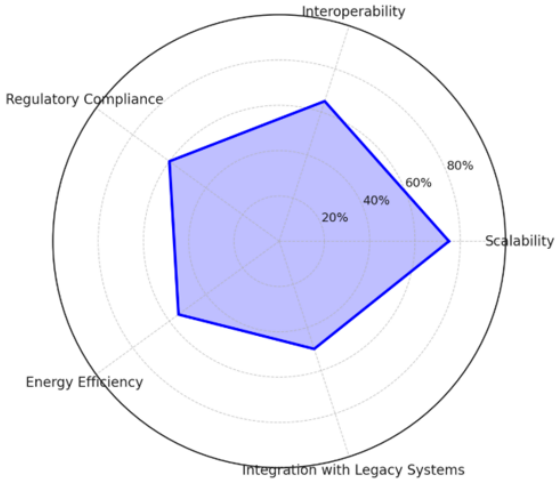

Figure 5: Key challenges reported in reviewed blockchain studies.

These findings collectively highlight that blockchain-based digital signatures represent a paradigm shift in healthcare data security. However, achieving scalability, regulatory alignment, and interoperability remains crucial for real-world adoption. By synthesizing consensus mechanisms, applications, adoption trends, and challenges, this review provides a holistic view of the current state and future directions for blockchain in healthcare security.

A comparison across consensus mechanisms reveals distinct trade-offs. Proof-of-Work (PoW) ensures strong immutability but is energy-intensive and poorly scalable. Proof-of-Stake (PoS) offers higher throughput and energy efficiency but raises concerns of validator collusion. Delegated Proof-of-Authority (DPoA) enables rapid validation, making it suitable for private healthcare networks, albeit at the cost of potential centralization. Hybrid models, which combine PoS with Byzantine Fault Tolerance (BFT) or other protocols, deliver a balance between scalability and security but require complex governance structures. Emerging AI-based anomaly detection adds another layer of resilience but introduces concerns over cost and model transparency. This review builds upon earlier studies by systematically mapping these trade-offs in healthcare contexts, highlighting their practical implications for scalability, compliance, and system trustworthiness.

Table 4: Regulatory requirements vs. technical mechanisms

Regulation	**Key Requirement**	**Technical Mechanism**	**Compliance Challenge**	**Example Use**
GDPR Art. 17	Right to erasure	Off-chain encrypted storage with on-chain hash references	Immutability conflict	Hybrid blockchains
GDPR Art. 5(1)(f)	Integrity and confidentiality	Digital signatures (BLS/EdDSA); audit logs	Key management issues	Telemedicine systems
HIPAA §164.312	Access control and audit	Smart-contract RBAC logging	Complex authorization logic	Private hospital chains
Consent (GDPR/HIPAA)	Revocable consent	Smart-contract consent registry	Propagation of revocation	EHR and insurance platforms

Table 4 demonstrates how blockchain technologies can address key data protection and compliance requirements of major healthcare regulations. To satisfy the GDPR's "Right to Erasure," hybrid blockchains utilize off-chain encrypted storage with on-chain hash references, allowing for selective deletion while maintaining auditability. GDPR Article 5 (1)(f), which emphasizes integrity and confidentiality, is supported through advanced cryptographic tools such as BLS and EdDSA digital signatures; however, key lifecycle management remains a challenge.

Under HIPAA §164.312, smart contracts implementing role-based access control (RBAC) can enforce secure authorization and transparent audit logging, particularly in private healthcare networks. Finally, both GDPR and HIPAA consent clauses are addressed through smart-contract-based consent registries, which automate patient approvals and revocations across EHR and insurance systems, thereby enhancing traceability while posing challenges for synchronizing revocations.

Table 5: Consensus and signature mechanism comparison

Consensus Model	**Signature Type**	**Verification Cost**	**Throughput (tps)**	**Energy Use**	**Validator Model**	**Best-Fit Application**
PoW + ECDSA	ECDSA-secp256k1	High	Low	Very high	Open miners	Not suitable for real-time EHR
PoS + BLS	Pairing-based BLS	Medium	High	Low	Staked validators	Telehealth and EHR systems
DPoA + EdDSA	Ed25519	Very low	Very high	Low	Authorized validators	Private hospital networks
Hybrid (PoS + BFT)	BLS	Medium	High	Low	Mixed governance	National health data exchanges

Table 5 compares blockchain consensus mechanisms and digital signature combinations based on performance and suitability for healthcare environments. The PoW + ECDSA model ensures strong immutability but is energy-intensive and slow, making it impractical for real-time medical data. The PoS + BLS combination enhances efficiency through signature aggregation, offering faster throughput and lower energy consumption, which is particularly suitable for telehealth and EHR systems. DPoA + EdDSA achieves very high transaction speeds with minimal computational cost, making it appropriate for private hospital networks with pre-approved validators. Hybrid PoS + BFT models, which utilize BLS signatures, offer a balanced combination of scalability, decentralization, and fault tolerance, making them suitable for national health data exchanges operating under regulated governance structures.

Risk-of-Bias Reflection

Out of 85 studies, 63 (74%) were rated as High quality, 18 (21%) as Moderate, and 4 (5%) as low according to the JBI checklist. Re-analysis of high-quality studies produced consistent patterns regarding scalability, consensus efficiency, and regulatory compliance, indicating the robustness of the synthesis. Studies with incomplete datasets or limited experimental validation were interpreted cautiously.

5. Conclusion

This systematic review demonstrates that blockchain-based digital signatures provide significant advancements in ensuring the integrity, authenticity, and confidentiality of healthcare data. The synthesis of 85 peer-reviewed studies confirms that digital signatures anchored in blockchain can effectively reduce risks of tampering, unauthorized access, and data breaches, while simultaneously supporting regulatory compliance in sensitive healthcare environments. The findings also reveal that consensus mechanisms play a pivotal role in scalability and efficiency.

While Proof-of-Work (PoW) remains the most tested, its high energy consumption and latency issues make it unsuitable for large-scale healthcare applications. Proof-of-Stake (PoS) emerges as the most efficient and eco-friendly alternative, while Delegated Proof-of-Authority (DPoA) demonstrates exceptional speed in private networks, making it highly relevant for hospital and telemedicine systems. Hybrid models that combine the strengths of different mechanisms strike a balance between transparency, scalability, and regulatory alignment. Furthermore, smart contracts are demonstrated to have transformative potential by automating consent management, insurance claims, and supply chain tracking, thereby reducing administrative burdens and enhancing operational transparency and trust. Collectively, these findings highlight that blockchain-enabled digital signatures are not only a technical innovation but also a practical enabler of secure and trustworthy healthcare ecosystems.

Despite these encouraging developments, this review identifies several persistent limitations that must be acknowledged before blockchain-based digital signatures can be fully integrated into healthcare systems. One of the most critical challenges lies in the scalability of blockchain networks, as many existing frameworks cannot yet process large volumes of healthcare transactions at real-time speed. Interoperability also remains a significant barrier, since most healthcare organizations continue to rely on legacy IT infrastructures that are poorly aligned with decentralized solutions. Moreover, while PoS and DPoA reduce energy consumption compared to PoW, they still pose risks of validator collusion, bias, and reduced decentralization. Another limitation is the regulatory misalignment between blockchain's immutability and privacy mandates, such as GDPR's 'right to be forgotten,' which creates complex governance issues. Smart contracts, although promising, face technical vulnerabilities, coding errors, and challenges in integrating with existing healthcare workflows. Ultimately, the literature reveals a lack of comprehensive empirical studies and real-world clinical trials that can validate the feasibility of blockchain solutions in actual healthcare settings. These limitations underscore the gap between the theoretical promise and practical deployment, highlighting the need for further refinement before blockchain-based digital signatures can become a mainstream standard in healthcare security.

Future research and development must prioritize addressing the scalability, compliance, and adoption challenges outlined in this review. At the technical level, advanced solutions such as sharding, directed acyclic graphs (DAGs), and Layer-2 scaling techniques like rollups and sidechains should be explored to reduce transaction latency while maintaining strong security guarantees. The growing threat of quantum computing also necessitates the adoption of quantum-resistant cryptographic schemes to ensure the long-term durability of blockchain-based signatures. From a system integration perspective, efforts should focus on building middleware platforms, APIs, and cross-chain interoperability frameworks that allow seamless communication between blockchain networks and traditional healthcare IT systems. Additionally, user acceptance and adoption studies are critical, as healthcare providers and patients must trust and understand blockchain-based solutions for them to be viable. Emerging opportunities also lie in combining blockchain with artificial intelligence (AI) and the Internet of Things (IoT) to create intelligent, real-time healthcare ecosystems that can authenticate data, dynamically manage consent, and enhance predictive security. Finally, policymakers and regulators must work in tandem with technologists to establish standardized frameworks and governance models that ensure blockchain innovations align with existing healthcare laws while enabling innovation. By addressing these directions, the future of blockchain-based digital signatures in healthcare can transition from a conceptual promise to a tangible, scalable, and trusted implementation.

Acknowledgment

We want to thank everyone who contributed to the successful completion of this project. We want to express our gratitude to City University, Malaysia. We would also like to express our gratitude to our research supervisor for his invaluable advice, guidance, and enormous patience throughout the development of the research.

Declaration of Competing Interests

The authors declare no known competing financial interests or personal relationships.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contributions

Li Xu: Conceptualization, Supervision, Data Analysis, Writing – Review and Editing; **Mohd Nurul Hafiz Bin Ibrahim**: Methodology, Validation, Investigation, Writing – Original Draft; **Mustafa Muwafak Alobaedy**: Software, Visualization, Investigation; **S. B. Goyal**: Methodology, Writing – Review and Editing

References

[1] J. Reddy, N. Elsayed, Z. ElSayed, and M. Ozer, "A review on data breaches in healthcare security systems," *International Journal of Computer Applications*, vol. 184, no. 45, pp. 1–7, 2023.

[2] R. J. Ramniklal, "Database security and integrity: Ensuring reliable and secure data management," *Mosaic of Ideas: Multidisciplinary Reflections*, vol. 73, 2024.

[3] I. A. Obiri, Q. Xia, H. Xia, E. Affum, S. Abla, and J. Gao, "Personal health records sharing scheme based on attribute based signcryption with data integrity verifiable," *Journal of Computer Security*, vol. 30, no. 2, pp. 291–324, 2022.

[4] W. Qin *et al.*, "High energy storage and thermal stability under low electric field in $bi_{0.5}na_{0.5}tio_3$-modified $batio_3$-$bi(zn_{0.25}ta_{0.5})o_3$ ceramics," *Chemical Engineering Journal*, vol. 443, p. 136505, 2022.

[5] M. Azarian, H. Yu, A. T. Shiferaw, and T. K. Stevik, "Do we perform systematic literature review right? a scientific mapping and methodological assessment," *Logistics*, vol. 7, no. 4, p. 89, 2023.

[6] Z. Wenhua, F. Qamar, T.-A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain technology: security issues, healthcare applications, challenges and future trends," *Electronics*, vol. 12, no. 3, p. 546, 2023.

[7] S. Khetani, "Data integrity and security: Blockchain vs. traditional databases," 2025.

[8] H. R. Penubadi *et al.*, "Sustainable electronic document security: A comprehensive framework integrating encryption, digital signature and watermarking algorithms," *Heritage and Sustainable Development*, vol. 5, no. 2, pp. 391–404, 2023.

[9] A. A. Al-awamy, N. Al-shaibany, A. Sikora, and D. Welte, "Hybrid consensus mechanisms in blockchain: A comprehensive review," *International Journal of Intelligent Systems*, vol. 2025, no. 1, p. 5821997, 2025.

[10] B. F. Azevedo, A. M. A. Rocha, and A. I. Pereira, "Hybrid approaches to optimization and machine learning methods: a systematic literature review," *Machine Learning*, vol. 113, no. 7, pp. 4055–4097, 2024.

[11] E.-Y. Daraghmi, S. Jayousi, Y.-A. Daraghmi, R. S. Daraghma, and H. Fouchal, "Smart contracts for managing the agricultural supply chain: A practical case study," *IEEE Access*, vol. 12, pp. 125462–125479, 2024.

[12] J. Shahid, R. Ahmad, A. K. Kiani, T. Ahmad, S. Saeed, and A. M. Almuhaideb, "Data protection and privacy of the internet of healthcare things (iohts)," *Applied Sciences*, vol. 12, no. 4, p. 1927, 2022.

[13] A. Ali *et al.*, "Blockchain-powered healthcare systems: enhancing scalability and security with hybrid deep learning," *Sensors*, vol. 23, no. 18, p. 7740, 2023.

[14] F. A. Reegu *et al.*, "Blockchain-based framework for interoperable electronic health records for an improved healthcare system," *Sustainability*, vol. 15, no. 8, p. 6337, 2023.

[15] S. S. Bakare, A. O. Adeniyi, C. U. Akpuokwe, and N. E. Eneh, "Data privacy laws and compliance: a comparative review of the eu gdpr and usa regulations," 2024.

[16] A. Sasikumar, L. Ravi, K. Kotecha, J. R. Saini, V. Varadarajan, and V. Subramaniyaswamy, "Sustainable smart industry: A secure and energy efficient consensus mechanism for artificial intelligence enabled industrial internet of things," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, p. 1419360, 2022.

[17] P. Bhandari, "Exploring challenges in the implementation and adoption of blockchain technology: An investigation into the impact of it professionals' beliefs, perceived performance, facilitating conditions, and social dynamics on technology utilization and acceptance," 2024.

[18] P. K. Ozili, A. Ademiju, and S. Rachid, "Impact of financial inclusion on economic growth: review of existing literature and directions for future research," *International Journal of Social Economics*, vol. 50, no. 8, pp. 1105–1122, 2023.