International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(4s) 2026 pp. 346-360
https://doi.org/10.70917/ijcisim-2026-2520
Article

A CONCEPTUAL PERFORMANCE EVALUATION FRAMEWORK FOR BLOCKCHAIN-BASED HEALTHCARE INSURANCE FRAUD PREVENTION: COMPARATIVE INSIGHTS FROM THE ABHA DIGITAL HEALTH ECOSYSTEM

JASPREET KAUR[1], GAGANDEEP CHAWLA[2]

[1] University Institute of Computing, Chandigarh University
Jaspreet18aug@gmail.com
[2] University Institute of Computing, Chandigarh University
gagandeep.e12787@cumail.in

Abstract: Healthcare insurance fraud continues to impose substantial financial and operational burdens on healthcare providers, insurers, and government agencies, while undermining trust in digital health ecosystems. Although the Ayushman Bharat Health Account (ABHA) ecosystem has significantly improved health information accessibility and interoperability through standardized digital identities and consent-driven data sharing, it is not specifically designed to provide immutable, decentralized, and fraud-resistant insurance claim verification. Blockchain technology offers a promising alternative by enabling transparent transaction recording, tamper-resistant data management, automated claim validation through smart contracts, and end-to-end auditability. This study proposes a blockchain-based framework for healthcare insurance fraud prevention and develops a multidimensional performance evaluation model to compare the proposed architecture with the ABHA digital health ecosystem. The proposed framework integrates decentralized ledger technology, cryptographic security mechanisms, smart contracts, identity verification, and audit trails to enhance the integrity and transparency of healthcare insurance claim processing. A comprehensive evaluation framework is established using eight critical performance dimensions: security, transparency, fraud detection capability, data integrity, privacy preservation, transaction efficiency, scalability, and interoperability.
The comparative methodology is designed to assess the operational strengths and limitations of both architectures within healthcare insurance workflows while maintaining interoperability and regulatory compliance.
The study contributes to the literature in three significant ways. First, it presents a dedicated blockchain-enabled framework tailored to healthcare insurance fraud prevention rather than general health record management. Second, it introduces a multidimensional benchmarking model that enables systematic comparison between blockchain-based insurance processing and the ABHA digital health ecosystem. Third, it provides a foundation for future empirical validation and policy development by identifying standardized performance indicators for secure, transparent, and trustworthy digital health insurance systems. The proposed framework offers a scalable and privacy-preserving approach that can support next-generation healthcare insurance infrastructures and facilitate the adoption of decentralized technologies for fraud-resistant claim management.

Keywords: Blockchain, Healthcare Insurance Fraud Prevention, ABHA Digital Health Ecosystem, Smart Contracts, Digital Health, Performance Evaluation, Transparency, Data Integrity, Privacy Preservation, Healthcare Informatics

1. INTRODUCTION

The rapid digital transformation of healthcare systems has fundamentally altered the generation, exchange, and management of medical information across the world. The integration of electronic health records, digital identities, interoperable platforms, and intelligent healthcare services has improved healthcare accessibility and operational efficiency while creating new opportunities for data-driven decision-making and patient-centered care (Agbo et al., 2019; Hasselgren et al., 2020; Kasyapa & Vanmathi, 2024). However, the increasing digitization of healthcare financing and insurance processes has simultaneously introduced significant challenges related to data security, claim authenticity, privacy protection, and healthcare insurance fraud prevention (Ismail & Zeadally, 2021; Mahapatra & Sinha, 2024).

Healthcare insurance fraud represents one of the most critical threats to sustainable healthcare systems, generating substantial financial losses for governments, insurers, healthcare providers, and patients. Fraudulent activities include duplicate claims, identity theft, phantom billing, fabricated treatments, provider collusion, and unauthorized reimbursements that undermine the integrity of insurance mechanisms and reduce public confidence in digital healthcare infrastructures (Ismail & Zeadally, 2021). Traditional centralized claim-processing systems frequently encounter limitations associated with fragmented databases, delayed verification procedures, insufficient transparency, and restricted audit capabilities, thereby creating opportunities for fraudulent behavior and administrative inefficiencies (Casino et al., 2019; Saeed et al., 2022).

Blockchain technology has emerged as a transformative paradigm capable of addressing many of these challenges through decentralized data management, cryptographic security, immutable transaction records, and programmable smart contracts (Nakamoto, 2008; Christidis & Devetsikiotis, 2016; Zheng et al., 2018). Unlike conventional centralized architectures, blockchain systems distribute data validation responsibilities among multiple participants, ensuring that verified transactions cannot be modified without collective consensus. Smart contracts further enhance operational efficiency by automating predefined business rules, reducing human intervention, and minimizing opportunities for manipulation during insurance claim processing (Buterin, 2014; Christidis & Devetsikiotis, 2016).

The application of blockchain technology within healthcare has attracted considerable scholarly attention during the past decade. Existing research demonstrates its potential to improve electronic health record management, patient identity verification, healthcare interoperability, pharmaceutical supply chain monitoring, and secure medical data exchange (Kuo et al., 2017; Gordon & Catalini, 2018; Mayer et al., 2020). Frameworks such as MedRec and FHIRChain illustrate how decentralized architectures can support patient-centric healthcare systems while maintaining transparency and data integrity (Azaria et al., 2016; Zhang et al., 2018). Systematic reviews have further emphasized that blockchain technologies can strengthen trust among healthcare stakeholders through immutable audit trails and enhanced privacy-preserving mechanisms (Agbo et al., 2019; Hussien et al., 2019; Saeed et al., 2022).

Recent investigations have extended these applications toward healthcare insurance ecosystems, particularly in the context of fraud prevention and automated claim validation. Mahapatra and Sinha (2024) proposed a blockchain-enabled healthcare framework incorporating fraud detection mechanisms, demonstrating the potential of smart contracts for secure insurance workflows. Similarly, Kasyapa and Vanmathi (2024) highlighted the importance of addressing scalability, performance optimization, and security concerns when integrating blockchain solutions into healthcare environments. Contemporary research also indicates that combining blockchain technologies with trustworthy artificial intelligence principles can enhance transparency, accountability, and resilience within digital healthcare systems (Shinde et al., 2024).

In the Indian context, the Ayushman Bharat Digital Mission (ABDM) has established a comprehensive digital public infrastructure aimed at promoting interoperability and citizen-centered healthcare services. A central component of this initiative is the Ayushman Bharat Health Account (ABHA), which provides individuals with unique digital health identities that facilitate secure, consent-based access to medical records across healthcare providers (National Health Authority, 2022, 2023a). The ABHA ecosystem represents a significant advancement in healthcare digitization by enabling standardized data exchange and improving patient empowerment within the national healthcare landscape (National Health Authority, 2023b).

Despite these achievements, the ABHA ecosystem primarily focuses on health information accessibility and interoperability rather than specialized mechanisms for healthcare insurance fraud prevention. The existing architecture does not inherently incorporate decentralized consensus protocols, immutable transaction validation, or smart-contract-based automation specifically designed to authenticate insurance claims and prevent fraudulent activities. Consequently, there remains an opportunity to complement existing digital health infrastructures through

blockchain-enabled solutions that provide enhanced transparency, auditability, and security within healthcare insurance operations (Ismail & Zeadally, 2021; Mahapatra & Sinha, 2024).

Another important consideration concerns the ethical and governance implications of integrating advanced digital technologies into healthcare systems. International frameworks on trustworthy artificial intelligence and responsible innovation emphasize transparency, accountability, fairness, and human oversight as essential principles for digital health ecosystems (Floridi et al., 2018; Jobin et al., 2019; European Commission, 2019; World Health Organization, 2021). The National Institute of Standards and Technology (2023) similarly highlights risk management, trustworthiness, and governance as critical dimensions for emerging digital infrastructures. These principles are particularly relevant for blockchain-enabled healthcare insurance systems, where automated decision-making mechanisms must remain transparent, explainable, and aligned with regulatory requirements.

Although previous studies have explored blockchain applications in healthcare and insurance management, a significant research gap persists regarding systematic performance evaluations that compare blockchain-based fraud prevention architectures with established national digital health ecosystems such as ABHA. Most existing investigations emphasize technological implementation or conceptual benefits without developing multidimensional benchmarking frameworks capable of assessing operational performance across security, transparency, fraud detection, privacy preservation, transaction efficiency, scalability, and data integrity dimensions (Hasselgren et al., 2020; Kasyapa & Vanmathi, 2024). This limitation constrains evidence-based decision-making among policymakers, healthcare administrators, and technology developers seeking to adopt decentralized solutions within healthcare insurance environments.

To address this gap, the present study proposes a blockchain-based framework specifically designed for healthcare insurance fraud prevention and develops a comprehensive performance evaluation model to compare the proposed architecture with the ABHA digital health ecosystem. The evaluation framework incorporates eight critical dimensions, namely security, transparency, fraud detection capability, data integrity, privacy preservation, transaction efficiency, scalability, and interoperability. Through this multidimensional assessment, the study seeks to provide a systematic understanding of the strengths and limitations of both approaches within healthcare insurance claim management processes.

The study contributes to the literature in three important ways. First, it presents a dedicated blockchain-enabled framework tailored explicitly to healthcare insurance fraud prevention rather than general healthcare information management. Second, it introduces a multidimensional benchmarking model that facilitates structured comparison between decentralized insurance architectures and the ABHA ecosystem. Third, it establishes a conceptual foundation for future empirical investigations and policy development by identifying standardized performance indicators that support secure, transparent, and trustworthy healthcare insurance infrastructures.

The remainder of the article is organized as follows. Section 2 reviews the literature on blockchain technologies, healthcare insurance fraud, digital health ecosystems, and the ABHA framework. Section 3 presents the proposed blockchain-based fraud prevention framework and research methodology. Section 4 describes the performance evaluation model and comparative analysis procedures. Section 5 discusses the implications of the findings for healthcare policy and digital transformation initiatives. Finally, Section 6 concludes the study and outlines directions for future research.

1.1 Novelty of the Study

The novelty of this study lies in three interconnected contributions. First, it proposes a blockchain architecture specifically designed for healthcare insurance fraud prevention rather than general healthcare record management. Second, it introduces one of the first conceptual benchmarking frameworks comparing blockchain-enabled insurance validation mechanisms with India's ABHA digital health ecosystem. Third, it develops an integrated multidimensional evaluation model comprising security, transparency, fraud detection capability, data integrity, privacy preservation, transaction efficiency, scalability, and interoperability as standardized assessment indicators for future empirical investigations.

2. REVIEW OF LITERATURE

2.1 Blockchain Technologies in Healthcare

Blockchain technology has emerged as a promising solution for addressing challenges related to healthcare data security, interoperability, transparency, and patient-centered information management. The decentralized and immutable characteristics of blockchain enable secure information sharing among multiple stakeholders while

reducing risks associated with centralized databases (Nakamoto, 2008; Zheng et al., 2018). Previous studies have demonstrated that blockchain can improve electronic health record management, patient data ownership, and healthcare interoperability through trusted data exchange mechanisms (Kuo et al., 2017; Gordon & Catalini, 2018). Frameworks such as MedRec and FHIRChain further illustrate the potential of blockchain to support secure access control and standardized clinical data sharing within healthcare environments (Azaria et al., 2016; Zhang et al., 2018). Systematic reviews consistently report that blockchain enhances data integrity, transparency, and privacy protection, although scalability and implementation challenges remain important considerations (Agbo et al., 2019; Hussien et al., 2019; Saeed et al., 2022; Kasyapa & Vanmathi, 2024).

2.2 Smart Contracts and Healthcare Insurance Management

Smart contracts extend blockchain capabilities by enabling the automated execution of predefined business rules without relying on centralized intermediaries (Buterin, 2014; Christidis & Devetsikiotis, 2016). Within healthcare insurance systems, smart contracts can facilitate automated claim verification, treatment authentication, and reimbursement processing, thereby reducing administrative complexity and opportunities for manipulation. Existing studies indicate that smart-contract-based healthcare frameworks improve transparency, accountability, and operational efficiency through immutable transaction records and automated validation mechanisms (Yue et al., 2016; Mahapatra & Sinha, 2024). These features are particularly valuable for healthcare insurance ecosystems that require secure and trustworthy claim management processes.

2.3 Healthcare Insurance Fraud Prevention

Healthcare insurance fraud continues to generate significant financial losses and operational inefficiencies across healthcare systems. Common fraudulent practices include duplicate claims, identity misuse, phantom billing, and provider collusion (Ismail & Zeadally, 2021). Conventional claim-processing systems frequently suffer from limited transparency and insufficient audit capabilities, which create vulnerabilities within insurance workflows. Blockchain-based approaches address these limitations through decentralized verification mechanisms and immutable audit trails that strengthen accountability and transaction authenticity (Casino et al., 2019; Ismail & Zeadally, 2021). Recent studies further demonstrate that integrating fraud detection functionalities with blockchain infrastructures can enhance the security and reliability of healthcare insurance operations (Mahapatra & Sinha, 2024).

2.4 ABHA and Digital Health Ecosystems

The Ayushman Bharat Digital Mission (ABDM) represents a major digital transformation initiative aimed at promoting interoperability, secure data exchange, and citizen-centered healthcare services in India. The Ayushman Bharat Health Account (ABHA) provides individuals with unique digital identities that support consent-based access to healthcare information across providers (National Health Authority, 2022, 2023a). The digital health ecosystem has significantly improved standardized information exchange and patient empowerment within the national healthcare framework (National Health Authority, 2023b). However, the ABHA architecture primarily focuses on health information interoperability rather than specialized mechanisms for healthcare insurance fraud prevention. The absence of decentralized consensus protocols and smart-contract-based claim validation mechanisms presents opportunities for blockchain-enabled solutions to complement existing digital health infrastructures through enhanced transparency, auditability, and fraud resistance (Mahapatra & Sinha, 2024).

2.5 Research Gap

Existing literature has extensively examined blockchain applications in healthcare information management, electronic health records, and digital interoperability. Nevertheless, limited research has focused specifically on blockchain-enabled frameworks for healthcare insurance fraud prevention. Furthermore, systematic performance comparisons between blockchain-based insurance architectures and the ABHA digital health ecosystem remain largely unexplored. Standardized evaluation dimensions encompassing security, transparency, fraud detection capability, data integrity, privacy preservation, transaction efficiency, and scalability are also insufficiently addressed in current studies. To bridge these gaps, the present study proposes a blockchain-based healthcare insurance fraud prevention framework and develops a multidimensional performance evaluation model for comparative analysis with the ABHA digital health ecosystem.

3. RESEARCH OBJECTIVES, RESEARCH QUESTIONS, AND CONTRIBUTIONS

3.1 Research Objectives

The study is guided by the following objectives:

1. To develop a blockchain-based framework for healthcare insurance fraud prevention using decentralized ledger technologies and smart contracts.

2. To compare the proposed blockchain framework with the ABHA digital health ecosystem across multiple operational dimensions.

3. To establish a multidimensional performance evaluation model encompassing security, transparency, fraud detection capability, data integrity, privacy preservation, transaction efficiency, scalability, and interoperability.

4. To identify policy and implementation implications for secure, transparent, and trustworthy digital healthcare insurance systems.

3.2 Research Questions

The study seeks to answer the following research questions:

RQ1: How can blockchain technologies improve healthcare insurance fraud prevention compared with conventional digital health infrastructures?

RQ2: What performance differences exist between blockchain-based insurance architectures and the ABHA digital health ecosystem across critical evaluation dimensions?

RQ3: How can smart contracts and decentralized validation mechanisms contribute to secure, transparent, and trustworthy healthcare insurance claim management systems?

3.3 Contributions of the Study

The study makes four principal contributions to the literature and practice of digital healthcare insurance systems.

First, it develops a conceptual blockchain-based framework specifically designed for healthcare insurance fraud prevention through smart contracts, decentralized verification mechanisms, and immutable audit trails.

Second, it provides a structured conceptual benchmarking exercise between the proposed blockchain architecture and the ABHA-enabled digital health ecosystem within the Indian healthcare context.

Third, it establishes a multidimensional evaluation model encompassing security, transparency, fraud detection capability, data integrity, privacy preservation, transaction efficiency, scalability, and interoperability as integrated assessment criteria for healthcare insurance infrastructures.

Finally, the study offers policy and governance insights regarding the integration of decentralized technologies with national digital health initiatives, thereby supporting future empirical research and evidence-based digital health policymaking.

4. PROPOSED BLOCKCHAIN-BASED FRAMEWORK AND RESEARCH METHODOLOGY

4.1 Proposed Blockchain-Based Framework for Healthcare Insurance Fraud Prevention

The proposed framework employs a permissioned blockchain architecture to enhance transparency, security, and trust within healthcare insurance claim processing. The framework integrates healthcare providers, insurance

companies, patients, regulatory authorities, and claim auditors through a decentralized network that maintains immutable records of healthcare transactions and insurance activities.

The architecture consists of six major components: patient identity management, healthcare provider verification, smart-contract-based claim validation, decentralized ledger storage, cryptographic security mechanisms, and audit and compliance monitoring. Patient identities are authenticated using digital health identifiers that maintain interoperability with the Ayushman Bharat Health Account (ABHA) ecosystem while introducing decentralized verification mechanisms to strengthen claim authenticity and fraud prevention.

Healthcare providers submit treatment records and insurance claims through authenticated interfaces. Smart contracts automatically verify predefined eligibility conditions, treatment consistency, policy coverage, and duplicate claim detection before claim approval. The execution of these contracts reduces manual intervention and minimizes opportunities for fraudulent manipulation. Every validated transaction is permanently recorded within the blockchain ledger, thereby ensuring transparency, traceability, and non-repudiation throughout the insurance lifecycle (Buterin, 2014; Christidis & Devetsikiotis, 2016).

Cryptographic hashing and distributed consensus mechanisms further enhance data integrity by preventing unauthorized modifications to healthcare records and insurance transactions. Regulatory authorities and authorized auditors can access immutable audit trails to monitor compliance, investigate suspicious activities, and maintain accountability across participating stakeholders (Nakamoto, 2008; Yaga et al., 2019). The framework therefore complements existing digital health infrastructures by incorporating fraud-resistant mechanisms without compromising interoperability or privacy requirements.

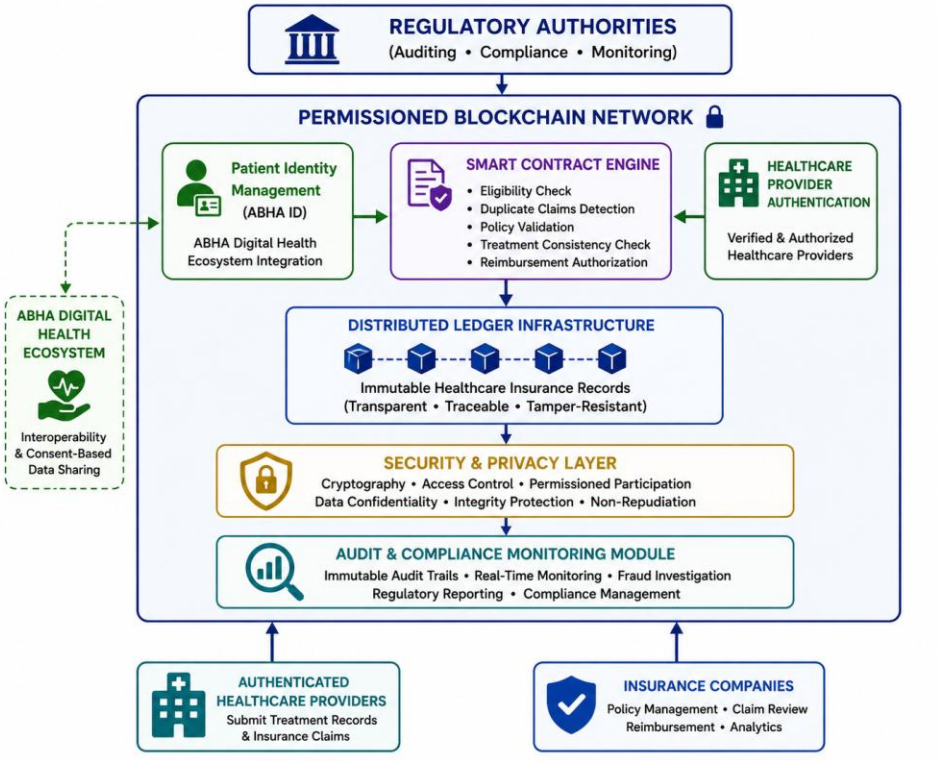

Figure 1: Proposed Permissioned Blockchain Framework for Healthcare Insurance Fraud Prevention Integrated with the ABHA Digital Health Ecosystem

4.2 Framework Components

The proposed architecture comprises the following functional modules:

Patient Identity Management Module: This component integrates digital identity verification mechanisms with ABHA-compatible identifiers to ensure secure authentication and eliminate identity-related insurance fraud.

Healthcare Provider Authentication Module: Authorized healthcare institutions participate as validated nodes within the blockchain network, ensuring that only legitimate medical providers can submit treatment information and insurance claims.

Smart Contract Engine: Automated business rules govern claim eligibility, policy verification, duplicate claim detection, reimbursement authorization, and exception handling, thereby reducing administrative delays and enhancing operational transparency.

Distributed Ledger Infrastructure: All validated transactions are recorded within an immutable blockchain ledger that supports secure data sharing, decentralized verification, and comprehensive audit capabilities.

Security and Privacy Layer: Cryptographic techniques, access control mechanisms, and permissioned participation policies preserve confidentiality while maintaining transparency and accountability across the healthcare insurance ecosystem.

Audit and Regulatory Monitoring Module: Immutable transaction histories facilitate real-time monitoring, fraud investigation, and regulatory compliance assessments by authorized governmental and insurance agencies.

Table 2: Functional Components of the Proposed Blockchain Framework

Component	Function	Fraud Prevention Contribution
Patient Identity Management	ABHA-compatible digital identity verification	Prevents identity misuse
Healthcare Provider Authentication	Validates authorized providers	Prevents fake providers
Smart Contract Engine	Automates claim validation	Detects duplicate claims
Distributed Ledger Infrastructure	Stores immutable transactions	Prevents record tampering
Security and Privacy Layer	Cryptography and access control	Protects confidentiality
Audit and Compliance Module	Regulatory monitoring	Supports fraud investigation

4.3 Research Methodology

The present study adopts a conceptual comparative research design to evaluate the effectiveness of the proposed blockchain-based healthcare insurance fraud prevention framework relative to the ABHA digital health ecosystem. The methodology emphasizes multidimensional performance assessment rather than empirical implementation, thereby providing a structured foundation for future validation studies.

The comparative analysis utilizes eight performance dimensions identified from previous blockchain and healthcare informatics research, namely security, transparency, fraud detection capability, data integrity, privacy preservation, transaction efficiency, scalability, and interoperability (Agbo et al., 2019; Hasselgren et al., 2020; Kasyapa & Vanmathi, 2024).These dimensions collectively capture the operational characteristics required for trustworthy healthcare insurance systems.

The study employs a conceptual benchmarking methodology to compare the theoretical capabilities of the proposed blockchain-based framework and the ABHA digital health ecosystem. The comparative assessment is derived from established findings in the blockchain, healthcare informatics, and digital governance literature rather than from empirical measurements or operational datasets. The ABHA ecosystem serves as the baseline digital health infrastructure because of its established role in promoting interoperability, digital identity management, and consent-based information exchange within India. The proposed blockchain framework is assessed according to its conceptual ability to enhance fraud resistance, decentralized verification, immutable auditability, and automated claim processing while maintaining compatibility with existing healthcare infrastructures. Consequently, the comparative analysis provides a theoretical foundation for future empirical validation rather than definitive performance measurements.

4.4 Performance Evaluation Dimensions

The comparative framework incorporates eight evaluation criteria:

1. Security: Protection against unauthorized access, cyberattacks, and data manipulation.

2. Transparency: Visibility and traceability of healthcare insurance transactions across stakeholders.

3. Fraud Detection Capability: Ability to identify duplicate claims, identity misuse, phantom billing, and unauthorized reimbursements.

4. Data Integrity: Preservation of accurate and immutable healthcare insurance records.

5. Privacy Preservation: Protection of sensitive patient information through controlled access mechanisms.

6. Transaction Efficiency: Speed and automation of claim verification and reimbursement processes.

7. Scalability: Capacity to support large-scale healthcare networks and increasing transaction volumes.

8. Interoperability: Ability to exchange and utilize healthcare and insurance information across heterogeneous digital platforms while maintaining compatibility with existing health information infrastructures, including the ABHA ecosystem.

These eight dimensions provide a standardized basis for systematically comparing blockchain-enabled healthcare insurance architectures with existing digital health ecosystems and contribute to future empirical investigations in healthcare informatics and digital governance.

5. PERFORMANCE EVALUATION FRAMEWORK AND COMPARATIVE ANALYSIS

5.1 Performance Evaluation Framework

The effectiveness of digital healthcare insurance infrastructures depends on their ability to maintain security, transparency, privacy, operational efficiency, and resistance to fraudulent activities. To facilitate a systematic assessment, the present study develops a multidimensional evaluation framework that compares the proposed blockchain-based architecture with the Ayushman Bharat Health Account (ABHA) digital health ecosystem. The evaluation criteria are derived from prior studies on blockchain applications in healthcare, digital trust, and healthcare informatics (Agbo et al., 2019; Hasselgren et al., 2020; Kasyapa & Vanmathi, 2024).

Eight performance dimensions are considered in the analysis: security, transparency, fraud detection capability, data integrity, privacy preservation, transaction efficiency, scalability, and interoperability. These dimensions collectively represent the technological and operational requirements of trustworthy healthcare insurance systems.

The ABHA ecosystem serves as the reference digital infrastructure because it provides standardized digital identities, consent-based information sharing, and interoperable healthcare services. However, its primary objective is healthcare data accessibility rather than insurance fraud prevention. In contrast, the proposed blockchain framework incorporates decentralized validation mechanisms, immutable transaction records, and smart-contract automation specifically intended to strengthen claim verification and reduce fraudulent activities.

5.2 Evaluation Dimensions

Security: Security refers to the capability of the system to protect healthcare information and insurance transactions against unauthorized access, tampering, and cyber threats. Blockchain networks employ cryptographic hashing and distributed consensus mechanisms that strengthen protection against malicious modifications, whereas centralized architectures depend primarily on institutional security controls (Yaga et al., 2019).

Transparency: Transparency measures the extent to which healthcare insurance transactions can be monitored, verified, and audited by authorized participants. Immutable ledgers provide complete transaction histories, thereby improving accountability and reducing information asymmetry among stakeholders (Casino et al., 2019).

Fraud Detection Capability: This dimension evaluates the ability of the system to identify duplicate claims, identity misuse, phantom billing, and unauthorized reimbursements. Smart contracts and decentralized validation procedures enhance fraud prevention by automating verification processes and eliminating single points of failure (Ismail & Zeadally, 2021; Mahapatra & Sinha, 2024).

Data Integrity: Data integrity reflects the preservation of accurate and consistent information throughout the insurance lifecycle. Blockchain immutability prevents retrospective modifications, thereby ensuring reliable medical and insurance records (Kuo et al., 2017).

Privacy Preservation: Healthcare systems must maintain confidentiality while enabling legitimate information sharing. Permissioned blockchain architectures support controlled access mechanisms that complement existing consent-based digital health infrastructures (Hasselgren et al., 2020).

Transaction Efficiency: Transaction efficiency represents the speed and effectiveness of insurance claim processing. Smart contracts reduce administrative delays by automating eligibility checks and reimbursement workflows (Christidis & Devetsikiotis, 2016).

Scalability: Scalability concerns the capability of the system to accommodate increasing numbers of users, institutions, and transactions. Although centralized platforms often provide high throughput, recent blockchain developments have introduced mechanisms that improve scalability while preserving decentralization (Kasyapa & Vanmathi, 2024).

Interoperability: Interoperability refers to the ability of healthcare systems to exchange and utilize information across heterogeneous platforms. The proposed framework is designed to maintain compatibility with ABHA digital identities and existing healthcare infrastructures while introducing decentralized insurance validation mechanisms.

5.3 Conceptual Benchmarking of the Proposed Framework and the ABHA Ecosystem

Table 1 presents a comparative evaluation of the proposed blockchain-based framework and the ABHA digital health ecosystem across the selected performance dimensions.

Conceptual Benchmarking Criteria

The comparative assessment presented in this study adopts a conceptual benchmarking approach based on theoretical characteristics reported in previous blockchain and healthcare informatics literature. Since the study does not involve empirical implementation or quantitative performance testing, the evaluation categories should be interpreted as qualitative indicators rather than numerical measurements.

The benchmarking scale is defined as follows:

- Very High: The architecture inherently provides strong support for the specified capability through its core design principles and technological mechanisms.
- High: The architecture provides substantial support for the capability, although certain limitations or dependencies may exist.
- Moderate: The capability is supported to a reasonable extent but relies primarily on institutional processes or external mechanisms rather than intrinsic technological features.
- Low: The capability receives limited support within the underlying architectural design.

These qualitative assessments are derived from existing theoretical and empirical findings in blockchain-enabled healthcare systems, digital health infrastructures, and healthcare insurance management studies (Agbo et al., 2019; Hasselgren et al., 2020; Saeed et al., 2022; Kasyapa & Vanmathi, 2024).

Table 2: Comparative Performance Evaluation of Blockchain-Based Insurance Framework and ABHA Ecosystem

Performance Dimension	Proposed Blockchain Framework	ABHA Digital Health Ecosystem
Security	Very High: Cryptographic protection and decentralized validation mechanisms	High: Centralized security controls and consent-based access management

Performance Dimension	Proposed Blockchain Framework	ABHA Digital Health Ecosystem
Transparency	Very High: Immutable transaction records and comprehensive audit trails	Moderate: Limited visibility within insurance claim processing activities
Fraud Detection Capability	Very High: Smart-contract automation and duplicate claim verification	Moderate: Relies primarily on institutional verification procedures
Data Integrity	Very High: Tamper-resistant distributed ledger architecture	High: Centralized database integrity mechanisms
Privacy Preservation	High: Permissioned access and cryptographic safeguards	Very High: Strong consent-driven information sharing policies
Transaction Efficiency	High: Automated claim validation and reimbursement processes	High: Efficient digital identity and healthcare information exchange
Scalability	Moderate to High: Dependent on blockchain implementation strategies	Very High: National-scale digital public infrastructure
Interoperability	High: Designed for compatibility with ABHA and existing health systems	Very High: Standardized healthcare data exchange framework

Note: The qualitative categories (Very High, High, Moderate, and Low) represent conceptual assessments derived from the theoretical characteristics and capabilities reported in existing literature and do not constitute empirical performance measurements.

The conceptual relationship between the proposed blockchain-enabled insurance layer and the existing ABHA digital health ecosystem is illustrated in Figure 2, highlighting their complementary roles in establishing a trustworthy healthcare insurance infrastructure.

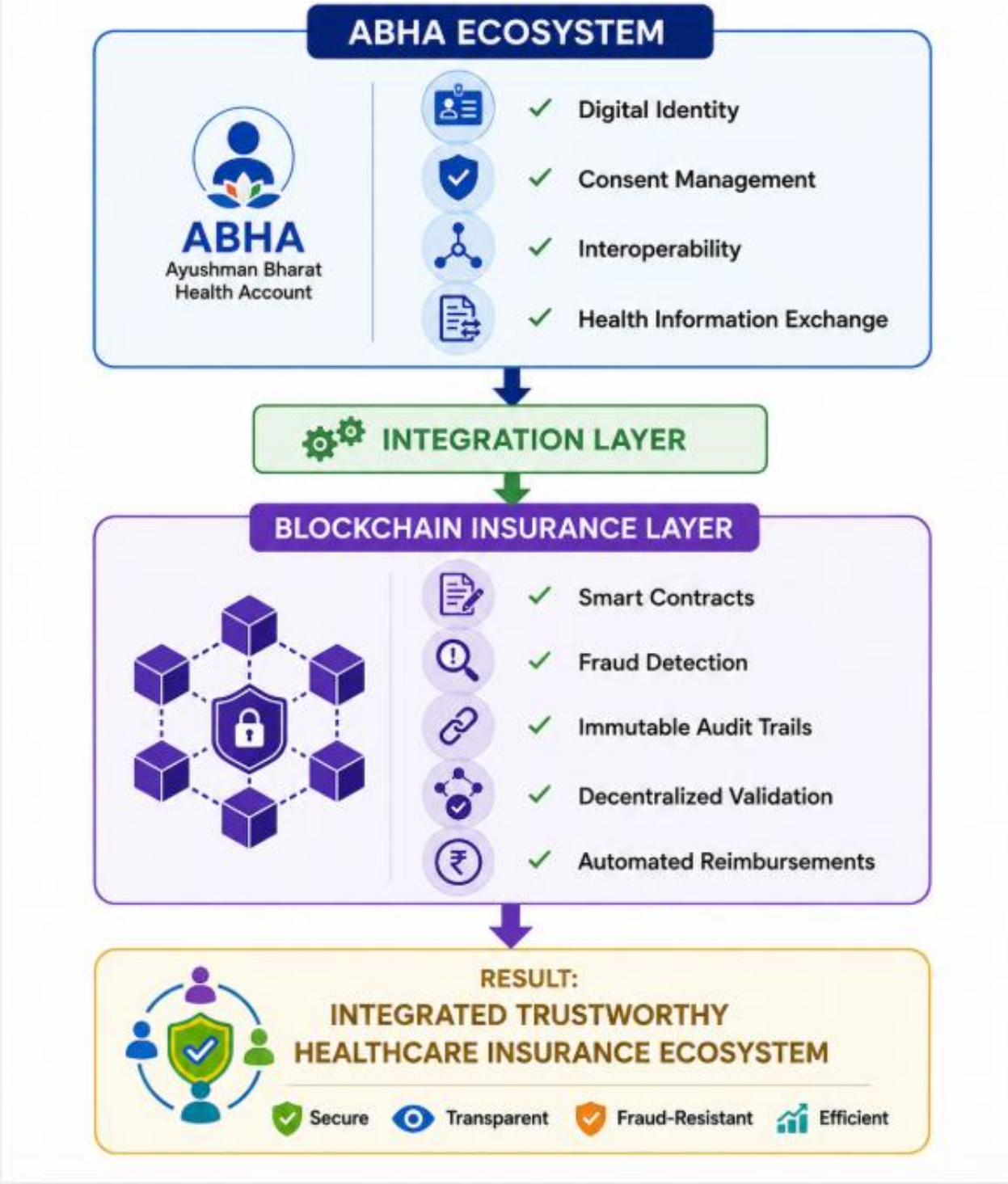

Figure 2: Conceptual Positioning of the Proposed Blockchain Framework Relative to the ABHA Digital Health Ecosystem

5.4 Discussion of Comparative Findings

Blockchain technologies may offer substantial theoretical advantages in fraud prevention, transaction traceability, and data integrity because of their decentralized and tamper-resistant characteristics. Empirical implementation studies are required to validate these anticipated benefits.

The ABHA ecosystem, in contrast, exhibits significant strengths in interoperability, digital identity management, and large-scale healthcare information exchange. Its consent-based architecture effectively protects patient privacy and supports standardized communication among healthcare providers. Nevertheless, its primary focus remains healthcare data accessibility rather than specialized insurance fraud mitigation mechanisms.

The analysis further suggests that blockchain technologies should not be considered replacements for existing digital health infrastructures. Instead, they may function as complementary layers that introduce secure insurance validation, decentralized auditing, and automated reimbursement controls while preserving interoperability with national digital health ecosystems. Such integration could facilitate the development of trustworthy, scalable, and fraud-resistant healthcare insurance environments.

Overall, the multidimensional evaluation framework developed in this study provides a structured basis for future empirical investigations and policy discussions concerning the adoption of blockchain technologies within healthcare insurance systems. The framework also contributes standardized performance indicators that may support comparative assessments across different digital health architectures and regulatory contexts.

6. DISCUSSION AND POLICY IMPLICATIONS

6.1 Discussion

The findings of the comparative evaluation indicate that blockchain technology possesses significant potential to strengthen healthcare insurance systems through decentralized verification, immutable transaction management, and automated claim-processing mechanisms. The proposed framework demonstrates particular advantages in fraud detection capability, transparency, and data integrity, which are critical requirements for trustworthy healthcare insurance environments. The incorporation of smart contracts enables the automatic execution of predefined insurance rules, thereby reducing administrative delays and limiting opportunities for fraudulent interventions within claim management processes (Christidis & Devetsikiotis, 2016; Mahapatra & Sinha, 2024).

The analysis further suggests that blockchain-based infrastructures can complement existing digital health ecosystems rather than replace them. The ABHA ecosystem has successfully established standardized digital identities, consent-driven information exchange, and interoperability among healthcare stakeholders. However, its primary orientation toward health information accessibility creates opportunities for additional technologies that specifically address insurance fraud prevention and transaction auditability. Integrating decentralized validation mechanisms with existing digital public infrastructure may therefore enhance both operational efficiency and institutional trust (National Health Authority, 2022; National Health Authority, 2023).

Another important observation concerns the role of immutable audit trails in supporting accountability across healthcare insurance networks. Traditional centralized systems frequently depend on institutional verification procedures that may be vulnerable to information asymmetries or delayed investigations. Blockchain ledgers provide permanent transaction histories that facilitate real-time monitoring, independent auditing, and transparent dispute resolution. These characteristics can improve stakeholder confidence and strengthen governance mechanisms within healthcare financing systems (Casino et al., 2019; Ismail & Zeadally, 2021).

Despite these advantages, practical implementation challenges require careful consideration. Blockchain scalability, computational efficiency, interoperability standards, and regulatory compliance remain important issues for large-scale healthcare deployments. Recent studies emphasize that permissioned blockchain architectures and optimized consensus mechanisms are essential for balancing security, privacy, and performance requirements within healthcare environments (Kasyapa & Vanmathi, 2024; Shinde et al., 2024). Consequently, future implementation strategies should prioritize technological compatibility with existing national digital health initiatives while maintaining robust fraud-prevention capabilities.

6.2 Policy Implications

The present study provides several implications for policymakers, healthcare administrators, insurance providers, and technology developers involved in digital health transformation initiatives.

First, national digital health policies should encourage the integration of blockchain-enabled insurance verification mechanisms with existing healthcare infrastructures. Rather than establishing independent systems, policymakers may consider interoperable models that combine ABHA-based digital identities with decentralized claim validation processes. Such integration can strengthen trust, improve accountability, and reduce fraudulent activities without disrupting current healthcare services.

Second, regulatory frameworks should establish standardized guidelines for smart-contract implementation within healthcare insurance ecosystems. Clear governance mechanisms concerning automated decision-making, dispute resolution, data ownership, and institutional responsibilities are necessary to ensure legal compliance and public acceptance. International principles relating to trustworthy digital technologies emphasize transparency, accountability, and human oversight as fundamental requirements for responsible innovation (Floridi et al., 2018; World Health Organization, 2021).

Third, healthcare organizations should invest in secure digital infrastructures that support cryptographic protection, permissioned access controls, and real-time auditing capabilities. These technological investments can enhance organizational resilience while facilitating more efficient insurance claim management processes. Training programs for healthcare professionals and insurance administrators are likewise essential to ensure effective adoption and operational sustainability.

Fourth, policymakers should encourage collaborative research initiatives involving academic institutions, healthcare providers, insurance companies, and governmental agencies. Empirical validation studies, pilot implementations, and large-scale performance assessments can provide evidence-based insights into the practical benefits and limitations of blockchain-enabled healthcare insurance systems. Such collaborative efforts would contribute to the development of scalable and context-sensitive digital health policies.

Finally, future digital health strategies should recognize that trustworthy healthcare ecosystems require an integrated approach encompassing technological innovation, ethical governance, privacy protection, and institutional accountability. Blockchain technologies, when appropriately aligned with existing public health infrastructures such as ABHA, may serve as enabling mechanisms for more transparent, secure, and fraud-resistant healthcare insurance environments.

6.3 Implications for Future Digital Health Ecosystems

The evolution of digital healthcare systems increasingly depends on the convergence of interoperability, trust, automation, and secure information management. The proposed framework illustrates how decentralized technologies can complement national digital health initiatives by introducing additional layers of verification and accountability within insurance operations. Future healthcare ecosystems may therefore adopt hybrid architectures that combine centralized service delivery with blockchain-based validation mechanisms to achieve both operational efficiency and institutional trust.

Such an approach can support sustainable healthcare financing, strengthen citizen confidence in digital services, and promote resilient healthcare infrastructures capable of addressing emerging technological and governance challenges. The insights generated by this study consequently provide a conceptual foundation for future innovations in healthcare insurance management and digital public health systems.

7. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

7.1 Conclusion

The increasing digitalization of healthcare services has created new opportunities for improving accessibility, interoperability, and patient-centered care, while simultaneously introducing challenges related to healthcare insurance fraud, data security, and transactional transparency. Although the Ayushman Bharat Health Account (ABHA) ecosystem has established an important digital foundation for healthcare information exchange in India, its primary emphasis remains on interoperability and consent-based data access rather than specialized mechanisms for fraud-resistant insurance claim verification.

This study proposed a blockchain-based framework specifically designed to strengthen healthcare insurance fraud prevention through decentralized validation, immutable transaction recording, cryptographic security, and smart-contract-driven automation. The framework was conceptually integrated with existing digital health infrastructures to preserve interoperability while enhancing transparency, accountability, and auditability within insurance claim processes.

A multidimensional performance evaluation model was developed to compare the proposed architecture with the ABHA digital health ecosystem across eight critical dimensions: security, transparency, fraud detection capability, data integrity, privacy preservation, transaction efficiency, scalability, and interoperability. The comparative analysis indicates that blockchain technologies offer substantial advantages in fraud prevention, transaction traceability, and data integrity because of their decentralized and tamper-resistant characteristics. At the same time, the ABHA

ecosystem demonstrates considerable strengths in large-scale interoperability, digital identity management, and consent-driven healthcare information exchange.

The findings suggest that blockchain-based healthcare insurance systems should be viewed as complementary technologies rather than direct replacements for existing digital public infrastructures. The integration of decentralized claim validation mechanisms with established healthcare ecosystems can support more trustworthy, efficient, and transparent insurance operations while maintaining regulatory compliance and patient privacy protections.

The study contributes to the literature in several ways. First, it presents a dedicated conceptual framework focused explicitly on healthcare insurance fraud prevention rather than general healthcare information management. Second, it introduces a standardized multidimensional evaluation approach for comparing blockchain-enabled insurance systems with national digital health ecosystems. Third, it provides theoretical and policy foundations that may guide future technological implementations, empirical investigations, and digital health governance strategies.

7.2 Future Research Directions

The present work adopts a conceptual and comparative perspective; therefore, several opportunities exist for future investigation and practical validation.

First, empirical studies should be conducted to implement prototype blockchain-based healthcare insurance platforms and evaluate their real-world performance using operational datasets from healthcare providers and insurance organizations. Such investigations can validate the effectiveness of smart contracts, decentralized verification mechanisms, and fraud detection processes under practical conditions.

Second, future research may employ quantitative methodologies to measure system performance across dimensions such as transaction throughput, computational efficiency, latency, scalability, and cost-effectiveness. Benchmarking studies involving multiple blockchain architectures, including permissioned and consortium networks, would provide deeper insights into implementation trade-offs within healthcare environments.

Third, advanced fraud analytics techniques incorporating artificial intelligence and machine learning can be integrated with blockchain infrastructures to support intelligent anomaly detection and predictive risk assessment. The combination of trustworthy AI principles with decentralized technologies may further enhance transparency, accountability, and explainability in automated healthcare insurance systems.

Fourth, comparative investigations involving digital health ecosystems from different countries would enrich understanding of how blockchain technologies can complement national healthcare infrastructures under varying regulatory and institutional conditions. Cross-country analyses could facilitate the development of internationally applicable frameworks for secure and interoperable healthcare insurance management.

Finally, future policy-oriented studies should examine legal, ethical, and governance considerations associated with smart contracts, digital identities, patient consent mechanisms, and data ownership within decentralized healthcare systems. Establishing comprehensive regulatory guidelines will be essential for ensuring responsible adoption and long-term sustainability of blockchain-enabled healthcare insurance solutions.

Overall, continued interdisciplinary collaboration among researchers, healthcare institutions, insurance providers, technology developers, and policymakers will be critical for realizing the full potential of blockchain technologies in creating transparent, secure, and fraud-resistant digital healthcare ecosystems.

Reference

1. Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. Healthcare, 7(2), 56. https://doi.org/10.3390/healthcare7020056
2. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25–30). IEEE.
3. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. https://ethereum.org/en/whitepaper/
4. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006
5. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
6. Engelhardt, M. A. (2017). Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. Technology Innovation Management Review, 7(10), 22–34. https://doi.org/10.22215/timreview/1111
7. European Commission. (2019). Ethics guidelines for trustworthy AI. European Commission.

8. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
9. Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. Computational and Structural Biotechnology Journal, 16, 224–230. https://doi.org/10.1016/j.csbj.2018.06.003
10. Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences: A scoping review. International Journal of Medical Informatics, 134, 104040. https://doi.org/10.1016/j.ijmedinf.2019.104040
11. Hussien, H. M., Yasin, S. M., Udzir, S. N. I., Zaidan, A. A., & Zaidan, B. B. (2019). A systematic review for enabling blockchain technology in healthcare application: Taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. Journal of Medical Systems, 43(10), 320. https://doi.org/10.1007/s10916-019-1445-8
12. Ismail, L., & Zeadally, S. (2021). Healthcare insurance frauds: Taxonomy and blockchain-based detection framework. IT Professional, 23(4), 36–43. https://doi.org/10.1109/MITP.2021.3071534
13. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2
14. Kasyapa, M. S. B., & Vanmathi, C. (2024). Blockchain integration in healthcare: A comprehensive investigation of use cases, performance issues, and mitigation strategies. Frontiers in Digital Health, 6, 1359858. https://doi.org/10.3389/fdgth.2024.1359858
15. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and healthcare applications. Journal of the American Medical Informatics Association, 24(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068
16. Mahapatra, S., & Sinha, D. (2024). Smart h-Chain: A blockchain based healthcare framework with insurance fraud detection. Transactions on Emerging Telecommunications Technologies, 35(4), e4911. https://doi.org/10.1002/ett.4911
17. Mayer, A. H., da Costa, C. A., & Righi, R. R. (2020). Electronic health records in a blockchain: A systematic review. Health Informatics Journal, 26(2), 1273–1288. https://doi.org/10.1177/1460458219866350
18. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
19. National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). U.S. Department of Commerce.
20. National Health Authority. (2022). Ayushman Bharat Digital Mission: Health data management policy. Government of India.
21. National Health Authority. (2023a). ABHA (Ayushman Bharat Health Account) official documentation. Government of India.
22. National Health Authority. (2023b). Ayushman Bharat Digital Mission strategy and implementation framework. Government of India.
23. OECD. (2019). OECD principles on artificial intelligence. OECD Publishing.
24. Roehrs, A., da Costa, C. A., & da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. Journal of Biomedical Informatics, 71, 70–81. https://doi.org/10.1016/j.jbi.2017.05.012
25. Saeed, H., Malik, H., Bashir, U., Ahmad, A., Riaz, S., Ilyas, M., Bukhari, W. A., & Khan, M. I. A. (2022). Blockchain technology in healthcare: A systematic review. PLOS ONE, 17(4), e0266462. https://doi.org/10.1371/journal.pone.0266462
26. Shinde, R., Patil, S., Kotecha, K., Potdar, V., Selvachandran, G., & Abraham, A. (2024). Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions. Transactions on Emerging Telecommunications Technologies, 35(1), e4884. https://doi.org/10.1002/ett.4884
27. Topol, E. (2019). Deep medicine: How artificial intelligence can make healthcare human again. Basic Books.
28. Vazirani, A. A., O'Donoghue, O., Brindley, D., & Meinert, E. (2019). Implementing blockchains for efficient health care: Systematic review. Journal of Medical Internet Research, 21(2), e12439. https://doi.org/10.2196/12439
29. Wood, G. (2014). Ethereum: A secure decentralized generalized transaction ledger. Ethereum Project Yellow Paper.
30. World Health Organization. (2021). Ethics and governance of artificial intelligence for health: WHO guidance. World Health Organization.
31. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview (NISTIR 8202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202
32. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10), 218. https://doi.org/10.1007/s10916-016-0574-6
33. Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. Computational and Structural Biotechnology Journal, 16, 267–278. https://doi.org/10.1016/j.csbj.2018.07.004
34. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647