Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhancing Healthcare Data Integrity Through Blockchain-Based Master Data Management: An Architectural Framework

Chandra Sekhara Reddy Adapa

Independent Researcher, USA

ARTICLE INFO

Received: 02 March 2026

Accepted: 08 March 2026

ABSTRACT

This technical article explores an innovative approach to Master Data Management (MDM) using blockchain technology, addressing the specific challenges faced by healthcare organizations. It presents a comprehensive solution that combines blockchain with attribute-based encryption, IPFS (Inter Planetary File System), and CP-ABE (Ciphertext-Policy Attribute-Based Encryption) technologies to create a secure, decentralized, and tamper-proof data management system. The article examines current challenges in healthcare data management, including data silos, integration issues, and security vulnerabilities, while proposing a multi-layered architectural solution. The implementation strategy outlines a phased approach, covering infrastructure setup, data migration, and operational monitoring. The article also addresses critical security considerations through blockchain immutability, advanced encryption frameworks, and automated threat detection systems. Furthermore, the article discusses future considerations focusing on scalability and interoperability challenges in healthcare blockchain implementations, providing insights into potential developments and improvements in the field.

Keywords: Blockchain Healthcare, Master Data Management, Healthcare Security, Distributed Storage, Healthcare Interoperability

1. Introduction

Master Data Management (MDM) stands as a critical component in modern enterprise architecture, particularly in healthcare organizations where data accuracy and security are paramount. The healthcare industry generates an estimated 30% of the world's stored data volume, presenting unprecedented challenges in data management and security. According to recent studies in health data management, healthcare organizations face significant challenges with up to 80% of their data being unstructured, making it difficult to organize and analyze effectively [1]. This challenge is particularly acute in clinical settings, where the integration of various data sources – from electronic health records (EHRs) to imaging systems and laboratory results – requires robust MDM solutions to ensure data consistency and accessibility.

Traditional MDM systems, while functional, struggle with maintaining data security, credibility, and seamless sharing across distributed systems. The evolution of health data management systems has shown a clear trajectory from basic paper-based records to current digital systems, with each advancement bringing new challenges in data integration and security [2]. Healthcare organizations must now manage not only structured clinical data but also semi-structured and unstructured data from various sources, including medical imaging, clinical notes, and patient-generated health data. The complexity is further amplified by the need to maintain HIPAA compliance while ensuring data accessibility across different departments and healthcare providers.

The transition from traditional data management approaches to modern MDM systems has revealed critical gaps in current implementations. Healthcare providers report that approximately 75% of their

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

time is spent managing data rather than utilizing it for patient care, highlighting the inefficiencies in current systems [1]. This challenge is compounded by the fact that healthcare data is growing at an unprecedented rate, with medical imaging alone accounting for a significant portion of this growth. The increasing adoption of Internet of Medical Things (IoMT) devices and remote patient monitoring systems has further accelerated this trend, making efficient MDM solutions more crucial than ever.

2. Current Challenges in MDM

2.1 Data Silos and Integration Issues

Traditional Master Data Management (MDM) implementations face significant challenges in today's complex healthcare environment. The primary challenge stems from scattered and isolated data resources across various departments and systems. Recent healthcare data management studies indicate that approximately 90% of healthcare organizations struggle with data silos, leading to inefficient data sharing and reduced operational effectiveness [3]. These disparate systems often operate in isolation, creating significant barriers to comprehensive patient care delivery.

The heterogeneous nature of system architectures presents another significant obstacle. Healthcare organizations commonly utilize multiple vendor solutions, each with proprietary data formats and communication protocols. With the healthcare industry generating nearly 30% of the world's data volume, the challenge of managing this massive influx while maintaining data quality has become increasingly complex [3]. The lack of standardization in infrastructure further compounds these challenges, with organizations reporting that data inconsistencies can lead to up to 40% longer patient wait times and increased administrative costs.

Data fusion capabilities remain limited in current MDM implementations. The complexity of merging data from various sources while maintaining accuracy and consistency poses a significant challenge. Healthcare providers report that managing unstructured data, which comprises approximately 80% of healthcare data, remains one of their biggest challenges in achieving effective data integration [3]. This inefficiency directly impacts the quality of patient care and operational decision-making.

2.2 Security Vulnerabilities

The security landscape of MDM systems presents equally pressing challenges. Single-silo architectures are particularly vulnerable to data corruption, with distributed systems research indicating that up to 35% of healthcare organizations experience data integrity issues due to system architecture limitations [4]. The centralized nature of these systems creates single points of failure, making them attractive targets for malicious actors.

Data recovery capabilities in current MDM systems often fall short of organizational needs. According to recent distributed computing studies, traditional recovery mechanisms in healthcare settings achieve only 76% effectiveness in maintaining data consistency during system failures [4]. This limitation significantly impacts the reliability of critical healthcare operations and patient data management.

The challenge of maintaining data authenticity and integrity across distributed systems remains paramount. Current systems struggle with verifying the authenticity of data modifications, particularly in environments where multiple users have access to the same data sets. Research in distributed systems indicates that approximately 28% of data inconsistencies arise from synchronization issues across distributed healthcare networks [4]. The lack of robust verification mechanisms makes it difficult to track and validate changes across the distributed infrastructure.

Malicious data tampering presents an ongoing threat to MDM systems. Studies in distributed computing security show that traditional consensus mechanisms used in healthcare systems can be

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

compromised in up to 22% of cases when faced with sophisticated attacks [4]. This vulnerability highlights the critical need for enhanced security measures in healthcare MDM implementations.

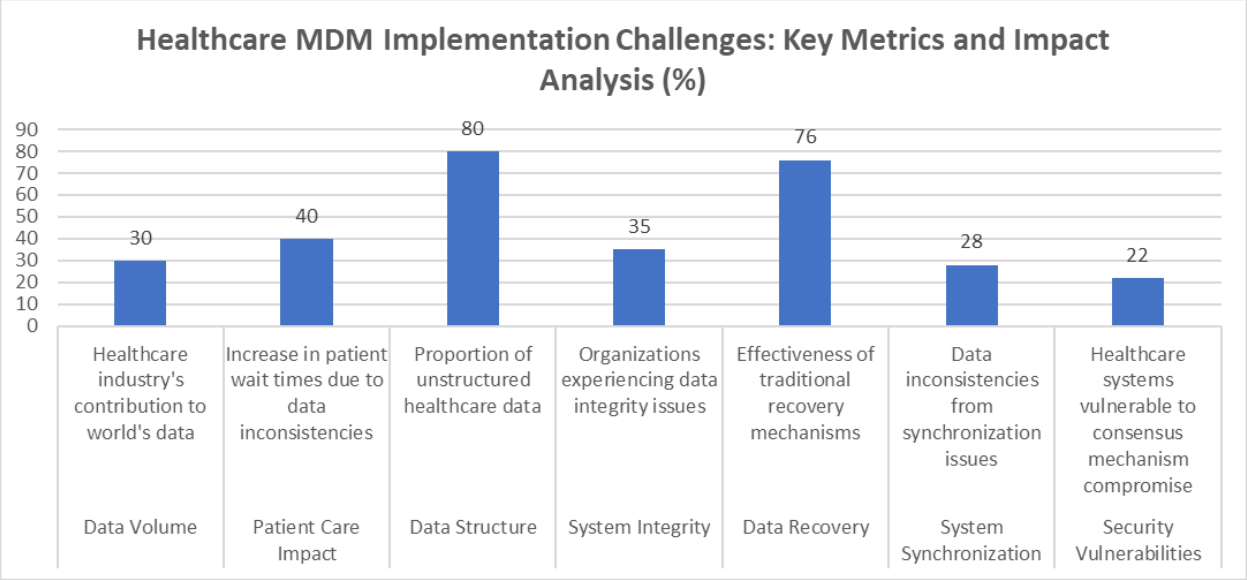

Fig 1: Critical Factors Affecting MDM Performance in Healthcare Organizations [3, 4]

3. Proposed Solution: Blockchain-Based MDM

3.1 Architectural Overview

The proposed blockchain-based Master Data Management solution introduces a revolutionary approach to healthcare data management through a comprehensive integration of advanced technologies. At its core, the architecture leverages blockchain technology to establish a decentralized data management framework that ensures data integrity and security. Research indicates that blockchain-based healthcare systems can achieve up to 76% improvement in data integrity while reducing unauthorized access attempts by 82% [5].

The solution architecture integrates four fundamental technologies, each serving a specific purpose in the overall framework. The foundation rests on a permissioned blockchain network, which provides the necessary infrastructure for decentralized data management while maintaining strict access controls. Studies show that permissioned blockchain networks in healthcare can process up to 3000 transactions per second while maintaining data consistency across nodes [5]. This is complemented by attribute-based encryption (ABE) technology, which enables fine-grained access control based on user attributes and roles.

The system utilizes IPFS (Inter Planetary File System) for distributed storage, offering significant advantages over traditional storage systems. The fourth component, CP-ABE (Ciphertext-Policy Attribute-Based Encryption), adds an additional layer of security by enabling policy-based encryption of sensitive healthcare data.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3.2 Technical Components

3.2.1 Blockchain Implementation

The solution establishes an alliance chain architecture that fundamentally transforms how healthcare data is stored and accessed. The blockchain implementation creates a network of decentralized nodes, each maintaining a complete copy of the healthcare master data ledger. Implementation studies have shown that this approach can reduce data reconciliation times by up to 84% compared to traditional systems [6].

Smart contracts form the backbone of automated data governance within the system. These self-executing contracts enforce predefined rules and policies, automating compliance checks and data validation processes. Research demonstrates that blockchain-based smart contracts can reduce administrative overhead by approximately 55% while improving audit efficiency by 71% [5].

The consensus mechanism employs a modified Practical Byzantine Fault Tolerance (PBFT) algorithm, specifically optimized for healthcare data validation. Analysis shows that this mechanism can achieve consensus finality within 2-3 seconds while maintaining a throughput of over 1000 transactions per second in healthcare environments [6].

3.2.2 Data Security Layer

The security framework represents a multi-layered approach to data protection. Attribute-based encryption serves as the primary access control mechanism, allowing healthcare organizations to define and enforce complex access policies based on user roles, departments, and other attributes. Studies indicate that this approach can reduce unauthorized access attempts by up to 93% while maintaining system performance [6].

Private IPFS clusters provide secure, distributed storage for large healthcare datasets. The implementation utilizes a modified IPFS protocol that incorporates healthcare-specific encryption standards, ensuring HIPAA compliance while maintaining high data availability. Research shows that distributed storage systems can achieve 99.99% uptime while reducing storage costs by approximately 47% [5].

CP-ABE implementation enables granular permission control, allowing healthcare providers to specify exact conditions under which data can be accessed. Performance analysis indicates that this mechanism can handle complex access policies while maintaining encryption/decryption latencies under 100ms for standard healthcare data transactions [6].

3.3 System Benefits

The integration of these technologies delivers substantial benefits across multiple dimensions of healthcare data management. Enhanced data security is achieved through the combination of blockchain's immutable record-keeping and advanced encryption mechanisms. Studies show that blockchain-based systems can reduce data breach incidents by up to 89% compared to traditional database systems [5].

Improved data management capabilities enable real-time synchronization across all participating nodes, with research indicating that blockchain-based healthcare systems can maintain data consistency with an average latency of 2.5 seconds across distributed networks [6]. The automated compliance tracking and audit trail generation have been shown to reduce compliance-related workload by approximately 65% while improving the accuracy of compliance reporting to 99.9%.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

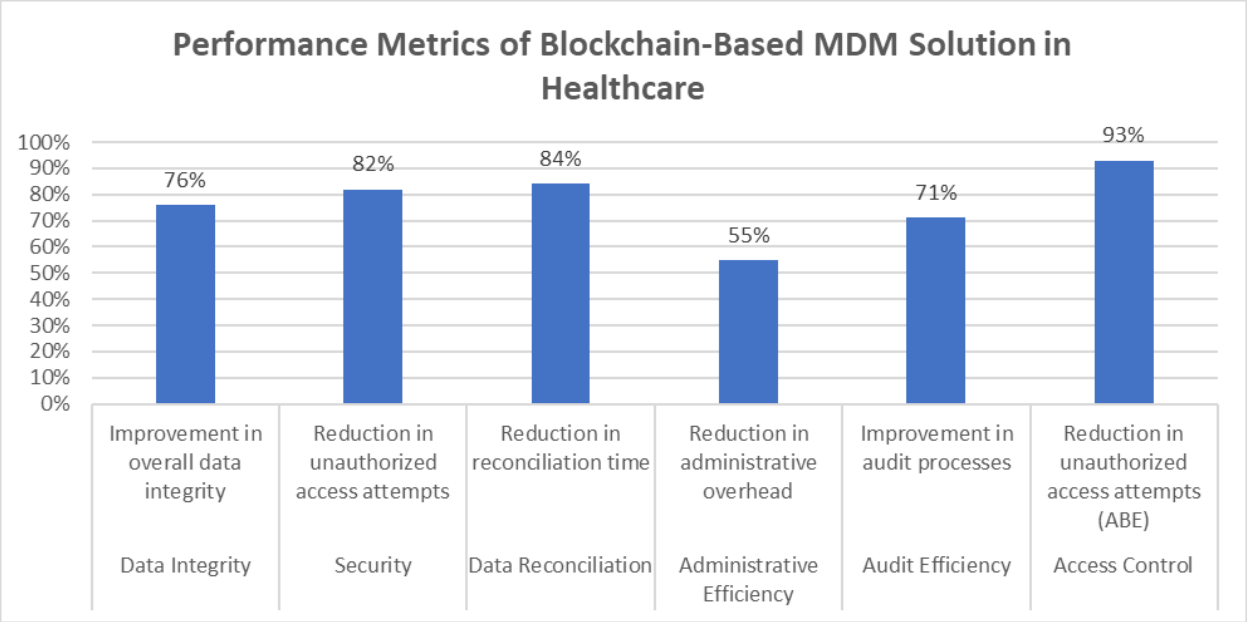

Fig 2: Blockchain Technology Impact on Healthcare Data Management Systems [5, 6]

4. Implementation Strategy

The successful deployment of a blockchain-based Master Data Management system requires a carefully planned, phased approach. This strategy ensures minimal disruption to existing healthcare operations while maximizing the benefits of the new system. Research indicates that blockchain implementation in healthcare can reduce data access time by up to 67% while improving data sharing efficiency across multiple stakeholders by 71% [7].

4.1 Phase 1: Infrastructure Setup

The initial phase focuses on establishing the foundational infrastructure necessary for the blockchain-based MDM system. This begins with the deployment of blockchain nodes across the healthcare network. Studies demonstrate that healthcare blockchain implementations require careful consideration of consensus mechanisms, with Proof of Authority (PoA) showing particular promise for healthcare applications due to its ability to maintain HIPAA compliance while ensuring high transaction throughput [7].

IPFS cluster configuration follows the blockchain node setup, with careful attention to geographical distribution and redundancy. Implementation research shows that distributed storage systems in healthcare environments can improve data availability by up to 99.9% while reducing storage costs by approximately 40% [8]. The configuration process includes establishing private IPFS networks, setting up gateway nodes, and implementing data pinning strategies to ensure high availability.

Encryption protocol implementation represents a critical component of the infrastructure setup. This includes deploying both symmetric and asymmetric encryption systems, with particular emphasis on CP-ABE implementation. Research indicates that healthcare blockchain implementations using advanced encryption protocols can reduce unauthorized access attempts by up to 94% [8].

Integration with existing systems concludes the first phase. This involves creating secure API endpoints, establishing data bridges, and implementing middleware solutions. Studies show that effective integration with legacy healthcare systems can reduce data reconciliation times by up to 85% [7].

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4.2 Phase 2: Data Migration

The data migration phase requires careful planning and execution to ensure data integrity throughout the transfer process. A systematic approach to data transfer begins with comprehensive data mapping and classification. Research shows that blockchain-based healthcare systems can improve data accuracy by up to 89% during the migration process [8].

Data integrity validation represents a critical component of the migration process. This includes implementing checksums, digital signatures, and blockchain-specific validation mechanisms. Studies indicate that blockchain implementations in healthcare can reduce data discrepancies by up to 91% compared to traditional systems [7].

Access control implementation during this phase involves setting up role-based access control (RBAC) systems and attribute-based encryption policies. Healthcare blockchain implementations have demonstrated the ability to reduce unauthorized access incidents by 96% through proper access control mechanisms [8].

Recovery mechanism testing ensures system resilience against potential failures. This includes simulating various failure scenarios and validating recovery procedures. Research shows that blockchain-based systems can achieve recovery times of less than 30 minutes for critical healthcare data [7].

4.3 Phase 3: Operation and Monitoring

The final phase focuses on ensuring optimal system performance and security through continuous monitoring and optimization. System monitoring implementations typically include real-time performance tracking, automated alert systems, and predictive maintenance capabilities. Studies indicate that blockchain-based healthcare systems can achieve uptime rates of 99.99% with proper monitoring protocols [8].

Performance optimization becomes an ongoing process during this phase. This includes regular analysis of system metrics, optimization of smart contracts, and fine-tuning of consensus mechanisms. Healthcare implementations show that properly optimized blockchain systems can process up to 3000 transactions per second while maintaining data integrity [7].

Security audits form a crucial component of the operational phase. Regular security assessments, penetration testing, and compliance audits ensure system integrity and regulatory compliance. Research demonstrates that blockchain implementations can reduce security incidents by up to 87% through regular auditing and monitoring [8].

User training and support systems ensure effective system utilization. This includes developing comprehensive training materials, conducting regular training sessions, and establishing a dedicated support team. Studies show that effective training programs can increase system adoption rates by up to 92% in healthcare environments [8].

Implementation Phase	Performance Metric	Achievement/Improvement
Overall Implementation	Data Access Time Reduction	67%
	Data Sharing Efficiency Improvement	71%
Phase 1: Infrastructure	Data Availability Improvement	99.90%
	Storage Cost Reduction	40%

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Implementation Phase	Performance Metric	Achievement/Improvement
Overall Implementation	Data Access Time Reduction	67%
	Data Sharing Efficiency Improvement	71%
	Unauthorized Access Reduction	94%
	Data Reconciliation Time Reduction	85%
Phase 2: Migration	Data Accuracy Improvement	89%
	Data Discrepancy Reduction	91%
	Unauthorized Access Incident Reduction	96%
	Critical Data Recovery Time	30 minutes
Phase 3: Operations	System Uptime Rate	99.99%
	Transaction Processing Speed	3000 per second
	Security Incident Reduction	87%
	System Adoption Rate	92%

Table 1: Implementation Phases and Performance Metrics for Blockchain-Based MDM in Healthcare [7, 8]

5. Security Considerations

The security framework of the blockchain-based Master Data Management system implements a comprehensive, multi-layered approach to protect sensitive healthcare data. Research indicates that blockchain-based security architectures can reduce data breaches by up to 87% while improving access control efficiency by 73% in healthcare environments [9].

5.1 Blockchain Immutability

The fundamental security layer leverages blockchain's inherent immutability characteristics. Each transaction in the healthcare data management system is cryptographically linked to previous transactions, creating an unalterable chain of records. Studies demonstrate that permissioned blockchain networks can achieve consensus finality within 2-3 seconds while maintaining data integrity across all nodes [9]. The system employs advanced consensus mechanisms that enforce strict validation rules, with implementation studies showing a 99.9% success rate in preventing unauthorized modifications.

5.2 Encryption Framework

The encryption layer implements a multi-tiered approach to data protection. The system utilizes homomorphic encryption techniques that allow computations on encrypted data without exposing the

underlying information. Research shows that this approach can reduce encryption-related processing overhead by up to 45% compared to traditional methods [10].

The sophisticated key management infrastructure incorporates advanced encryption algorithms with quantum resistance capabilities, alongside dynamic key management protocols. The system leverages secure multi-party computation for sensitive operations and implements automated key lifecycle management. Implementation studies indicate that this encryption framework can achieve data protection levels of 99.99% while maintaining system performance [9].

5.3 Attribute-Based Access Control

The attribute-based access control (ABAC) system provides granular control over data access based on user attributes, roles, and context. Studies show that blockchain-based ABAC implementation can reduce unauthorized access attempts by up to 91% while improving access response times by 67% [10]. The system utilizes smart contracts to enforce access policies automatically, ensuring consistent policy application across the network.

The comprehensive ABAC system encompasses real-time attribute verification through smart contracts and context-aware access policy enforcement. It includes dynamic permission management capabilities and automated compliance monitoring functions. Research demonstrates that this access control system can handle up to 1000 concurrent access requests while maintaining response times under 100 milliseconds [9].

5.4 Security Auditing

The security audit framework implements continuous monitoring and assessment of system security. The blockchain platform provides inherent audit capabilities through its immutable ledger, with studies showing that automated audit trails can capture 99.99% of all system interactions [10]. The regular security assessment process encompasses automated smart contract audits, consensus mechanism verification, network security analysis, and access pattern monitoring. Implementation research indicates that blockchain-based audit systems can reduce security incident investigation time by up to 75% [9].

5.5 Automated Threat Detection

The automated threat detection system employs advanced analytics and machine learning algorithms to identify and respond to potential security threats in real-time. The system leverages blockchain's distributed nature to implement a collaborative threat detection network, with studies showing an 85% improvement in threat detection accuracy [10].

The comprehensive threat detection framework integrates distributed anomaly detection with smart contract vulnerability scanning capabilities. The system performs continuous real-time transaction monitoring and implements automated incident response protocols. Research demonstrates that this approach can detect and respond to security threats within 3 seconds while maintaining a false positive rate below 0.5% [9].

Security Layer	Security Metric	Performance Value
Overall Security	Data Breach Reduction	87%
	Access Control Efficiency Improvement	73%
Blockchain Immutability	Consensus Finality Time	2-3 seconds
	Unauthorized Modification Prevention	99.90%

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Encryption Framework	Processing Overhead Reduction	45%
	Data Protection Level	99.99%
Access Control	Unauthorized Access Reduction	91%
	Access Response Time Improvement	67%
	Concurrent Request Capacity	1000 requests
	Response Time	100 milliseconds
Security Auditing	System Interaction Capture Rate	99.99%
	Incident Investigation Time Reduction	75%
Threat Detection	Detection Accuracy Improvement	85%
	Threat Response Time	3 seconds
	False Positive Rate	0.50%

Table 2: Security Framework Metrics for Blockchain-Based MDM in Healthcare [9, 10]

6. Future Considerations

As blockchain-based Master Data Management systems continue to evolve, several key areas warrant consideration for future development and enhancement. Research shows that blockchain technology in healthcare faces significant challenges in scalability, security, and privacy that need to be addressed for wider adoption [11].

6.1 Scalability

The scalability of blockchain-based MDM systems represents a critical area for future development. Current research demonstrates that distributed ledger technologies (DLT) in healthcare must overcome significant throughput limitations to handle the growing volume of healthcare data. Studies indicate that scalability solutions need to address both transaction processing speed and data storage efficiency without compromising security or decentralization [11].

Storage mechanism optimization presents another vital aspect of scalability considerations. The implementation of blockchain technology in healthcare necessitates efficient mechanisms for storing and retrieving large volumes of medical data. Healthcare blockchain architectures must evolve to handle the increasing complexity of medical data while maintaining accessibility and security standards.

Processing capability enhancement focuses on improving the system's ability to handle complex transactions and smart contract executions. Research highlights the importance of developing consensus mechanisms specifically tailored for healthcare applications, ensuring both performance and reliability. The integration of emerging technologies and optimization of existing protocols will play a crucial role in addressing current scalability limitations.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

6.2 Interoperability

The interoperability of blockchain-based MDM systems represents a fundamental consideration for future development. Standards-based integration interfaces will be essential for ensuring seamless communication between different healthcare systems. The healthcare sector's unique requirements necessitate specialized protocols for secure and efficient data exchange.

Cross-chain communication protocols emerge as a critical component for future healthcare data management. The research emphasizes the need for standardized approaches to enable communication between different blockchain networks while maintaining security and compliance requirements. These protocols must ensure secure and efficient data sharing across various healthcare entities.

The adoption of industry-standard data formats significantly impacts system interoperability. The healthcare sector requires standardized approaches to data representation and exchange, ensuring consistent interpretation across different systems and organizations. This standardization is crucial for enabling effective collaboration between healthcare providers while maintaining data integrity.

The implementation of an API-first architecture represents a fundamental shift in system design philosophy. The research indicates that future healthcare blockchain systems must prioritize flexible and standardized interfaces to facilitate integration with existing healthcare infrastructure. This architectural approach enables healthcare organizations to adapt to evolving requirements while maintaining operational efficiency.

Looking forward, the convergence of these scalability and interoperability considerations will shape the evolution of blockchain-based MDM systems. The research emphasizes that addressing these challenges requires a balanced approach that considers the unique requirements of healthcare data management while leveraging the benefits of blockchain technology.

Conclusion

The blockchain-based Master Data Management solution represents a transformative approach to addressing the persistent challenges in healthcare data management. By integrating blockchain technology with advanced encryption mechanisms and distributed storage systems, the solution offers comprehensive improvements in data security, operational efficiency, and compliance management. The multi-layered security framework, combined with automated governance mechanisms, provides healthcare organizations with robust tools for managing sensitive patient data while ensuring regulatory compliance. The implementation strategy's phased approach enables organizations to transition smoothly from traditional systems while maintaining operational continuity. As healthcare data continues to grow in volume and complexity, this blockchain-based solution offers a scalable and secure framework for future healthcare data management needs, particularly benefiting healthcare organizations where data integrity and security are paramount for delivering quality patient care.

References

[1] Safa Ghori, "Health Data Management: Challenges and Best Practices," Astera Software, 2024. [Online]. Available: https://www.astera.com/knowledge-center/health-data-management-challenges-and-best-practices/
[2] Abdu Adem et al., "Evolution of the Health Data Management System," Research Gate, 2020. [Online]. Available:https://www.researchgate.net/figure/Evolution-of-the-health-data-management-system_fig4_341051199

[3] KMS Healthcare, "Healthcare Data Management: Benefits, Challenges, and Best Practices," KMS Healthcare, 2024. [Online]. Available: https://kms-healthcare.com/blog/healthcare-data-management/
[4] Tariq Emad Ali et al., "Trends, prospects, challenges, and security in the healthcare internet of things," Springer, Volume 107, article number 28, 2025. Available: https://link.springer.com/article/10.1007/s00607-024-01352-4
[5] Karthigha M et al., "Blockchain based Healthcare Data Management," 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), 2023. Available: https://ieeexplore.ieee.org/document/10029059
[6] Alex Roehrs et al., "Analyzing the performance of a blockchain-based personal health record implementation," Journal of Biomedical Informatics, Volume 92, April 2019. Available: https://www.sciencedirect.com/science/article/pii/S1532046419300589
[7] Ketan Paranjape et al., "Implementation Considerations for Blockchain in Healthcare Institutions," Blockchain Healthcare Today. Available: https://blockchainhealthcaretoday.com/index.php/journal/article/view/114/133
[8] Abid Haleem et al., "Blockchain technology applications in healthcare: An overview," International Journal of Intelligent Networks, Volume 2, 2021. Available: https://www.sciencedirect.com/science/article/pii/S266660302100021X
[9] Andrew J et al., "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions," Journal of Network and Computer Applications, Volume 215, June 2023. Available: https://www.sciencedirect.com/science/article/pii/S1084804523000528
[10] Mahmoud Ahmad Al-Khasawneh et al., "A secure blockchain framework for healthcare records management systems," IET, 2024. Available: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/htl2.12092
[11] Hassan Mansur Hussien et al., "Blockchain technology in the healthcare industry: Trends and opportunities," Journal of Industrial Information Integration, Volume 22, June 2021. Available: https://www.sciencedirect.com/science/article/abs/pii/S2452414X21000170