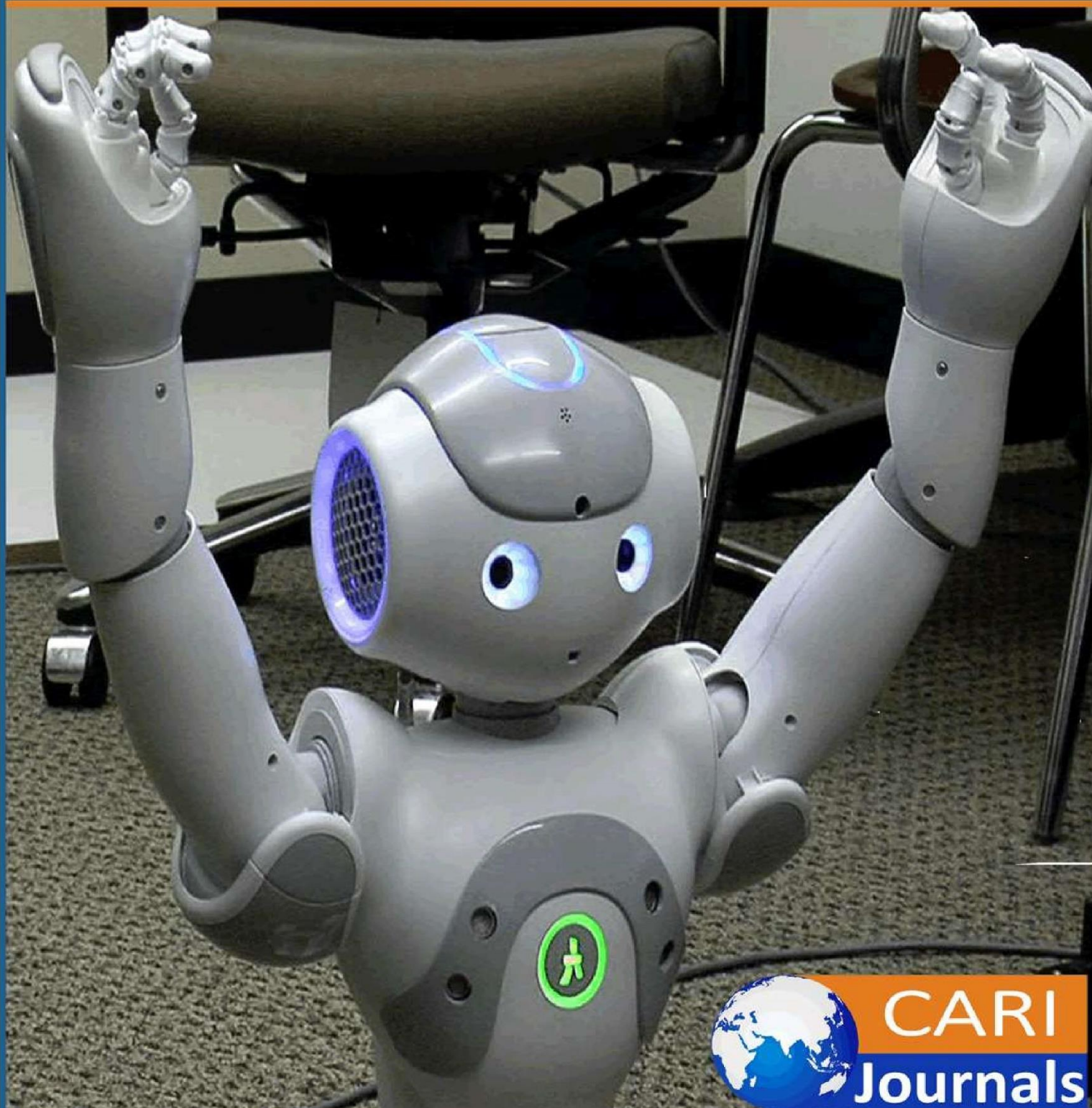
International Journal of
Computing and
Engineering
(IJCE)

Modernizing Healthcare Master Data Management (MDM): Harnessing Real-Time Processing, IoT, and Blockchain



International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 7, Issue No. 4, pp. 24 - 39, 2025
www.carijournals.org

Modernizing Healthcare Master Data Management (MDM): Harnessing Real-Time Processing, IoT, and Blockchain

Somnath Banerjee

IEEE Senior Member & Forbes Technology Council Member, NJ, USA.

https://orcid.org/0009-0003-0132-4218

Accepted: 22nd Apr, 2025, Received in Revised Form: 18th May, 2025, Published: 22nd Jun, 2025

Abstract

Purpose: This paper aims to propose a robust, future-ready master data management (MDM) architecture that addresses traditional MDM challenges by enhancing data accuracy, trust, and accessibility, while aligning with regulatory frameworks such as the 21st Century Cures Act and TEFCA.

Methodology: Employing a qualitative design-oriented approach, the study combines literature review, technical architecture modeling, and real-world case analyses. Key interoperability standards (HL7/FHIR), decentralized identity protocols (DIDs), and smart contract frameworks were analyzed. The proposed architecture was validated through five empirical case studies, including Estonia's blockchain-based national health system, and ICU telemetry streaming models. The architecture consists of four layers: IoT data ingestion, real-time stream processing (via Kafka and Flink), blockchain-based trust infrastructure, and a unified MDM layer.

Findings: The architecture addresses longstanding MDM pain points: reducing integration latency from hours to seconds, eliminating duplication through blockchain-backed identity management, and enhancing auditability with immutable ledgers. Key benefits include real-time anomaly detection, improved chronic care monitoring, and secure multi-organizational data sharing. Clinical use cases demonstrated timely updates to patient records and improved data reliability across institutions. Comparative analysis highlighted the architecture's ability to scale horizontally, support federated governance, and ensure compliance with both HIPAA and GDPR.

Unique contribution to theory, practice, and policy: The study advances theoretical understanding of MDM in the context of decentralized and high-frequency healthcare environments. Practically, it offers a modular, interoperable solution for healthcare IT leaders seeking to modernize legacy infrastructures. From a policy perspective, it outlines a path toward data-sharing frameworks that balance innovation, compliance, and patient autonomy. This research establishes a blueprint for secure, scalable, and intelligent MDM, contributing to the ongoing digital transformation of healthcare systems globally.

Keywords: *Healthcare, Master Data Management (MDM), IoT, Blockchain, Real-Time Processing.*

INTRODUCTION

Master Data Management (MDM) in healthcare refers to the organizational strategy and technology systems deployed to maintain a unified and authoritative source of critical business data, especially patient data, across disparate information systems. In the United States, MDM efforts often revolve around the Master Patient Index (MPI), which links fragmented records from multiple electronic health record (EHR) systems and ensures consistent patient identification. The primary goals are to eliminate duplicate records, minimize identification errors, and promote a unified clinical view that underpins accurate diagnoses, billing, and treatment decisions [1]. With the rapid digitalization of healthcare, traditional MDM systems are showing signs of strain.

Despite the growing adoption of EHRs and Health Information Exchanges (HIEs), traditional MDM continues to face enduring issues such as duplication rates ranging from 8% to 12% across U.S. hospitals, overlay errors, and integration latency [1, 2]. Batch-oriented systems fail to provide real-time alerts, creating lags that jeopardize safety and efficiency. Data stewards are often overburdened by manual reconciliation processes that do not scale with growing data volumes [3]. These constraints have only intensified with the post-HITECH Act expansion of digitized health data, which led to data fragmentation across providers, payers, and states [4].

The legacy MDM problems have become more acute with the advent of the Internet of Things (IoT) in healthcare. IoT is a network of interconnected medical wearables, sensors, and remote monitoring systems that generate high-frequency, streaming health data outside of traditional hospital infrastructure [3]. These real-time, decentralized data flows strain the capabilities of legacy MDM systems, which are often built for batch, infrequent updates [5]. Data flows from these decentralized patient devices also require new approaches to verify their authenticity and provenance as they move across different institutions and technological systems. Traditional MDM systems typically lack immutable audit trails or verifiable history, which undermines data provenance and stakeholder confidence in shared records [6].

To address traditional MDM challenges and meet the ever-evolving needs of digital healthcare, this paper proposes a next-generation approach to MDM that integrates real-time stream processing, IoT data ingestion, and a blockchain-based trust infrastructure. Real-time data frameworks (e.g., Apache Kafka, Apache Flink) can enable the continuous ingestion of streaming data, facilitating near-instant updates to master records. Meanwhile, incorporating blockchain technology adds a cryptographically verifiable layer of integrity and provenance to the data, while smart contracts and decentralized identifiers (DIDs) empower patients to control access and consent [7, 8].

This study has four primary objectives:

1. Explore the limitations of traditional MDM in supporting real-time IoT health data and establishing a trustworthy, blockchain-based audit trail.
2. Examine how IoT, real-time processing, and blockchain technologies can modernize healthcare MDM.
3. Propose an architecture that integrates IoT acquisition, streaming, and blockchain to modernize MDM deployments.
4. Analyze case studies that demonstrate practical applications and outcomes of this integrated model.

This work aligns with U.S. regulatory imperatives such as the 21st Century Cures Act and CMS Interoperability Rule, both of which demand enhanced data accessibility and trust [9, 10].

LITERATURE REVIEW

Theoretical Review

Master Data Management in Healthcare Contexts

Master Data Management (MDM) has traditionally served as the backbone of data accuracy and reconciliation within large healthcare systems. At its core, MDM seeks to ensure a "single source of truth" for key business entities such as patients, providers, and locations [1]. In U.S. healthcare, the primary vehicle for patient MDM is the Master Patient Index (MPI), which aggregates and links records across different EHR systems. However, typical MPI approaches suffer from batch processing inefficiencies, outdated probabilistic matching algorithms, and limitations in data governance that fail to address modern interoperability demands [11].

Challenges in Conventional MDM Systems

Legacy MDM platforms are often built on relational databases and centralized hub-and-spoke architectures, introducing latency and fragility in environments that now demand agility and decentralization [6]. The deterministic and demographic-based record matching used by most MPIs often yields false positives or duplicates, especially when dealing with common names, immigrants without standardized documentation, or pediatric records lacking identifiers. Manual stewardship workflows, while important for data accuracy, are not scalable in the era of big data and distributed health networks [3].

Additionally, current MDM implementations do not handle high-velocity data flows, such as those from continuous monitoring systems, effectively. These systems typically operate through periodic ETL (Extract-Transform-Load) processes which update master records once every few hours or

even daily. This causes critical latency that renders the data less useful—or even obsolete—in time-sensitive scenarios such as emergency care or intensive care monitoring [3].

The following figure illustrates a traditional Healthcare MDM implementation.

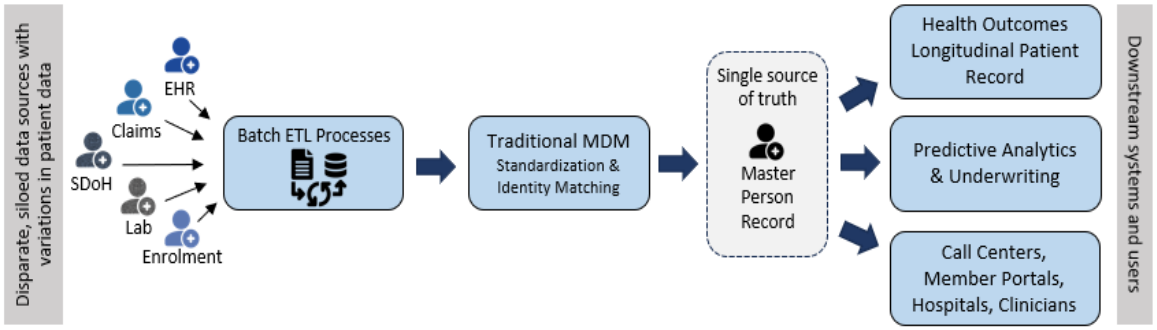


Figure 1: Traditional Healthcare MDM implementation

Emergence of IoT and Streaming Complexity

The Internet of Medical Things (IoT) has transformed the healthcare data landscape, introducing continuous telemetry from wearables, implantables, and smart home devices [12]. Devices like glucose monitors, blood pressure cuffs, and ECG patches provide granular, time-stamped health data that must be accurately attributed to the right patient in real time. Unfortunately, legacy MDM systems were not designed for ingestion or reconciliation of time-series data streams and thus pose a serious bottleneck to the promise of IoT-enabled personalized medicine [13].

Moreover, the location and contextual metadata from IoT streams add complexity to identity resolution. Patient-device pairing must be dynamic and verified securely, particularly in mobile or remote care settings. Without real-time integration, such data often lives outside clinical workflows, contributing to data silos and missed care opportunities [3, 6].

Blockchain for Trust and Data Provenance

Blockchain introduces a decentralized architecture to record, verify, and manage data events across distributed health systems. By using distributed ledgers and smart contracts, blockchain can replace traditional centralized identity registries with Decentralized Identifiers (DIDs) that are cryptographically linked to patient data sources [14, 15]. In this model, each event—whether it's a record update, identity assertion, or data access—is hashed and immutably recorded on the ledger, creating an auditable chain of custody [7].

Furthermore, smart contracts can be used to enforce consent management and role-based access control. Patients can authorize or revoke access to specific datasets in real time, and healthcare providers can query the ledger to verify consent without accessing the raw data itself [16]. Blockchain’s built-in transparency and security also reduce the risks of unauthorized access and

manipulation of sensitive health records [17].

Real-Time Data Integration through Streaming Platforms

Real-time stream processing frameworks such as Apache Kafka and Apache Flink are now critical components in modern healthcare data architectures [6]. Kafka provides a fault-tolerant, scalable pub-sub model that decouples data producers from consumers, enabling resilient ingestion pipelines for IoT data. Flink, meanwhile, supports event-time processing, windowing, and stateful transformations—features that are crucial for real-time MDM enrichment, patient matching, and anomaly detection [18].

Streaming systems allow data to be processed "in motion," reducing time-to-insight and eliminating the delay of batch cycles. When integrated with blockchain and MDM, they provide the foundation for an intelligent data orchestration platform capable of reconciling identities, verifying provenance, and updating longitudinal records in seconds [19].

Empirical Review

Estonia's National Health Infrastructure

Estonia's e-Health system [8] represents one of the earliest and most mature national implementations of blockchain in healthcare. Every citizen has a unique digital ID, and all health data access events are logged via a KSI blockchain [2]. This ensures complete auditability and empowers patients to monitor who accessed their records and when. Consent is granular, role-based, and governed through cryptographic policies. The system supports both primary care and specialty access across a federated national network, offering a blueprint for blockchain-based MDM at scale.

MIT's MedRec Project

The MedRec platform, developed by MIT Media Lab, is a decentralized record locator system built on Ethereum. Instead of storing data on-chain, MedRec logs pointers to data along with access metadata, controlled through smart contracts [7]. This architecture enables patients to manage access privileges across institutions and supports longitudinal health record portability. MedRec has influenced policy discussions and inspired decentralized MDM initiatives in academic and policy circles [16].

Smart ICU and Streaming Data Integration

In an ICU setting, continuous telemetry from bedside monitors must be captured, analyzed, and acted upon in near-real time. Mao Z, et al., 2023 [18] and Bhatia M, Sood SK., 2016 [20] describe intelligent ICU frameworks that combine device streaming with alerting engines and data provenance systems. Mao Z, et al., 2023 [18] extended this model using blockchain to validate the

source, integrity, and timeliness of each telemetry record, creating a tamper-proof environment for critical care analytics.

Remote Monitoring and Home-Based IoT

Patients with chronic conditions are increasingly using wearable devices and smart monitoring platforms to track symptoms and relay data to clinicians. Projects in Japan and Canada have demonstrated 20–30% reductions in hospital readmissions using real-time alerting systems [21]. Blockchain-enhanced frameworks—such as the tamper-proof mobile health architecture by Ichikawa et al., 2017 [22] —allow these home monitoring systems to function securely and efficiently outside traditional EHR environments.

Blockchain in Clinical Research and Trials

Beyond care delivery, blockchain is also being explored to improve data transparency in clinical trials. Nugent et al., 2016 [23] introduced smart contracts to record protocol adherence, consent, and data lineage in oncology research. These innovations demonstrate blockchain's potential to modernize trust and verification in both operational and investigational healthcare environments.

METHODOLOGY

This study employed a qualitative, design-oriented methodology to propose and evaluate an architecture for modernizing Master Data Management (MDM) in healthcare by integrating real-time processing, Internet of Things (IoT), and blockchain technologies. The methodology includes a literature-driven analysis, system design modeling, and validation through real-world case study comparisons.

Literature and Standards Review

The research began with a structured literature review focusing on the evolution of MDM in healthcare, the emergence of real-time data needs, and the promise of blockchain for data integrity and patient empowerment. Peer-reviewed studies, government publications, and industry white papers from authoritative sources (e.g., IEEE, FHIR/HL7, and ONC) were used to frame the technological and regulatory landscape [9, 10, 12, 24, 25].

Interoperability standards such as HL7/FHIR were referenced for structuring patient data exchange [12]. The W3C Decentralized Identifier (DID) standard was examined to ensure compatibility with self-sovereign identity models [14]. The ONC's Trusted Exchange Framework and Common Agreement (TEFCA) was studied as a policy backdrop to align the proposed architecture with national interoperability mandates [2, 9, 10].

Case Study Selection and Analysis

Empirical support for the architectural design was derived from the analysis of five case studies:

1. **Estonia's national blockchain-enabled health system**, which uses a KSI blockchain to secure data provenance [2, 8].
2. **MIT's MedRec**, an Ethereum-based system that offers patient-controlled access management [7].
3. **Smart ICU frameworks** integrating streaming data and blockchain logging to detect clinical deterioration in real time [18].
4. **Home-based chronic care pilots**, which combine Kafka pipelines and mobile consent via smart contracts [6, 12, 16, 22].
5. **Blockchain for clinical research auditing**, as explored by Nugent et al., 2016 [23].

These case studies informed both technical feasibility and architectural modularity.

Architecture Modeling

A layered architecture is proposed to align technology capabilities with clinical and operational MDM requirements. This architecture is modular – each layer can evolve (e.g., changing blockchain platform or streaming tech) without disrupting the others, thanks to well-defined interfaces. The architecture consists of:

1. **IoT Data Acquisition Layer**: Integrates structured and unstructured data from EHRs, wearables, and home-based sensors via secure device gateways [3].
2. **Real-Time Stream Processing Layer**: Employs Apache Kafka for ingestion and Apache Flink for enrichment, filtering, and dynamic identity matching [6].
3. **Blockchain Trust Layer**: Records immutable logs of data events, manages patient DIDs, and automates consent flows using smart contracts [14, 15, 16].
4. **Unified MDM/MPI Layer**: Maintains a reconciled, real-time master index with verified identity links (cross-verified with the blockchain ledger). The MDM layer exposes data to downstream applications using FHIR APIs [1, 3].

This model supports federated deployments and is compatible with both centralized hospital systems and decentralized regional networks.

The following figure illustrates the proposed four-layer modern MDM architecture.

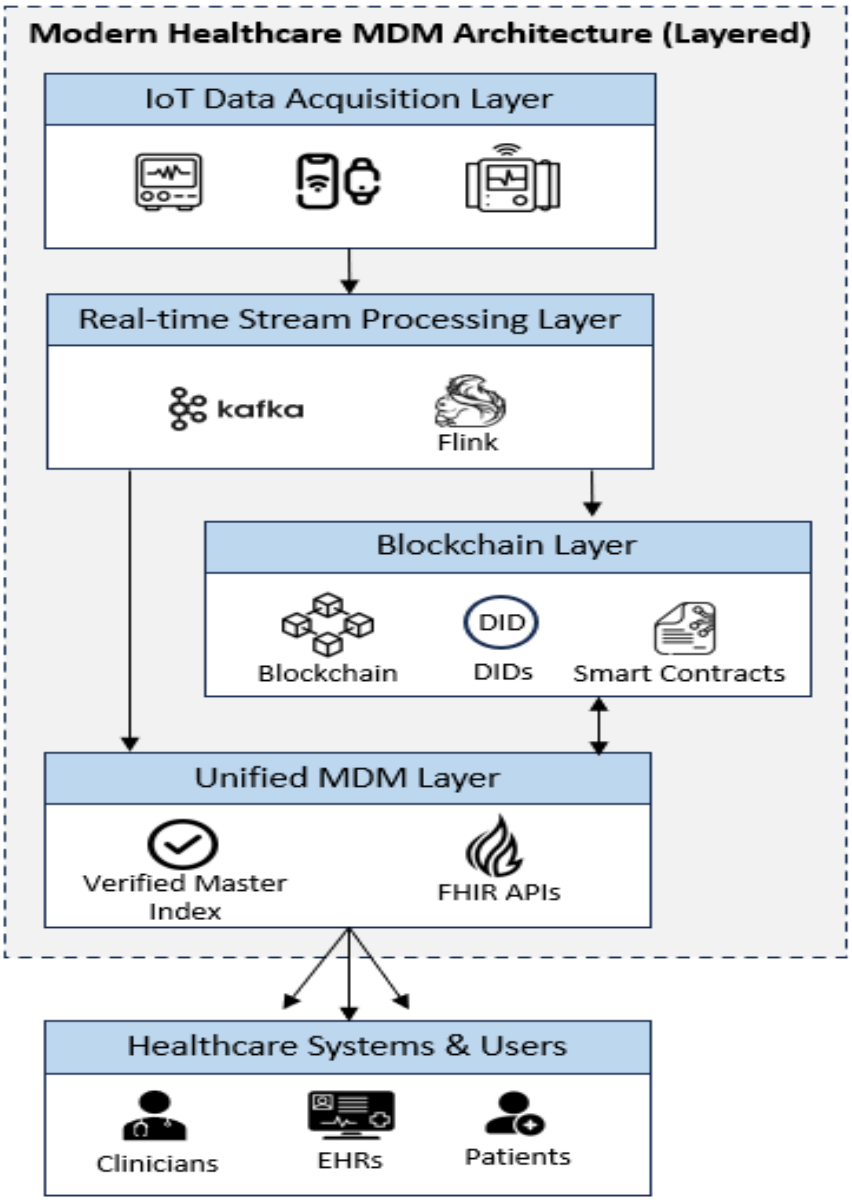


Figure 2: Proposed Modern MDM Architecture (four-layers)

Solution Alignment with the traditional MDM challenges

To ascertain that the proposed architecture addresses the traditional MDM challenges, each element of the architecture was mapped to one or more challenges.

- Kafka mitigates data latency.
- Flink supports real-time enrichment and matching.
- Blockchain addresses trust and consent gaps.

- DIDs eliminate centralized identity dependencies.

Together, these modules resolve existing limitations and prepare MDM for the demands of real-time, patient-centric healthcare.

FINDINGS

This section presents the data flow analysis and evaluation of the proposed four-layer MDM architecture, including the IoT data acquisition, stream processing, blockchain trust, and MDM/MPI unification layers. The evaluation is structured through hypothetical scenarios and empirical alignments with real-world use cases to illustrate how the proposed architecture mitigates traditional MDM limitations.

Validation of the Proposed Architecture through Data Flow Analysis

Below is a step-by-step data flow for a representative scenario: a wearable IoT device monitoring a cardiac patient and updating the master patient record in real-time, with blockchain ensuring trust.

Step 1: IoT Device Captures Data: A patient is wearing a smart heart monitor (an IoT ECG patch). The device continuously measures heart rate and rhythm. Suppose it detects an arrhythmia event at 10:02:00. The raw sensor data (heartbeat intervals, etc.) is generated on the device.

Step 2: Data Transmission via Gateway: The device is paired to the patient's smartphone (acting as an IoT gateway) or a home Wi-Fi hub. It immediately transmits the arrhythmia event data to the cloud IoT platform via a secure connection.

Step 3: Stream Processing and MDM Integration: The incoming data is routed to the streaming infrastructure (Kafka topic). A stream processing job picks up the message from the Kafka topic. This job knows the device's unique ID and looks up which patient it's linked to using a blockchain DID directory. It then enriches the event message and pushes this update to the MDM system's API. In the MDM database, the patient's record is updated with a new clinical data point. At the same time, business rules in the MDM might trigger an alert notification to that patient's cardiologist since a critical event was recorded.

Step 4: Blockchain Recording: Simultaneously, the stream processing pipeline or the MDM system itself submits a transaction to the blockchain network. This transaction might include a hash of the data. The purpose is to create an immutable event log. The blockchain consensus nodes validate and add this transaction to a new block. Now, there is a permanent, time-stamped record that the specific patient experienced an arrhythmia event at the recorded time. The MDM Master Patient Index can also be cross-verified with the DID on the blockchain ledger. The actual data (e.g., ECG waveform) remains stored in the MDM or a secure cloud storage, but anyone with

access to the blockchain (e.g., the hospital, patient) can later verify that an event was recorded and see the pointer to where the full data can be fetched (if authorized). If this patient goes to a different hospital in the future, that hospital's system could query the blockchain for the patient's record index and discover this event, then request details from the original source.

Step 5: Unified Data View for Users: A clinician (or the patient) using a portal or EHR interface queries the patient's record. Thanks to the integration, by 10:02:30 (perhaps within seconds of the event), the master patient record in the system now shows: *"Arrhythmia alert at 10:02 – source: wearableECG".* The cardiologist can see this in near real-time and might call the patient or advise immediate action. If the patient goes into an emergency room, the ER doctors pulling up the MPI will see this recent critical information, which could influence treatment (e.g., giving appropriate medications). This demonstrates the timeliness benefit – no manual entry was needed, no nightly batch job; it is essentially live updating of the patient's master data.

The following figure illustrates the data flow analysis described above.

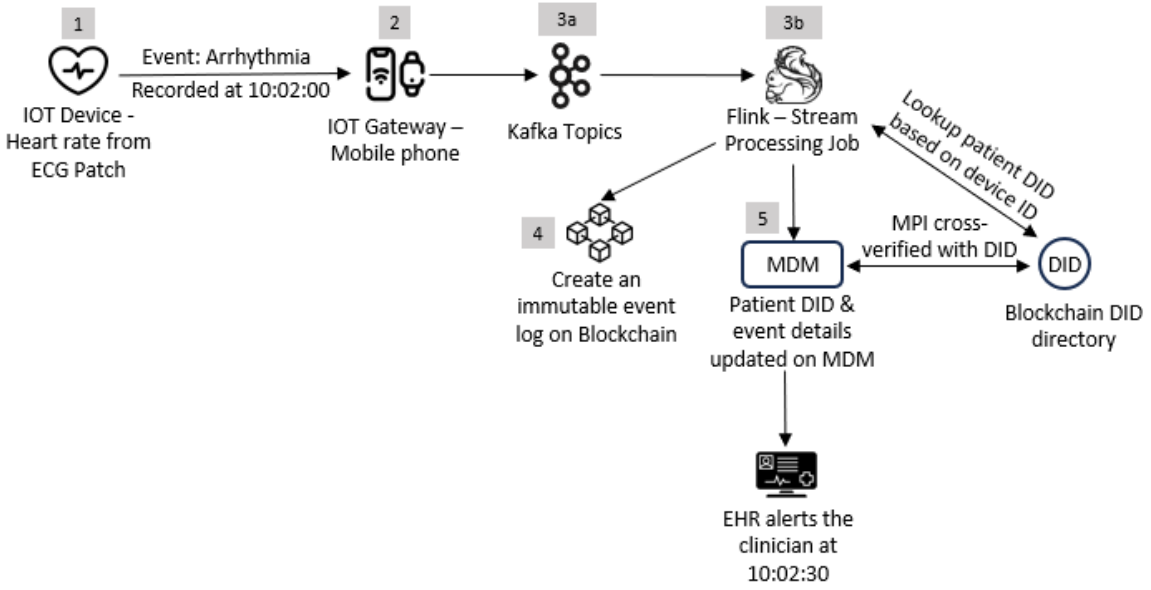


Figure 3: Proposed Modern MDM Architecture – Data Flow Analysis

This representative data flow highlights how timeliness, interoperability, and trust are woven into each transaction. The patient's device data flows quickly to those who need it (no silo), and the blockchain provides confidence and auditability (no blind trust in a central silo). It's worth noting that edge processing (not explicitly shown) could also take place: for example, the wearable or phone might run an AI algorithm locally to decide if an alert is significant before sending, to avoid false alarms. That would further improve efficiency and reduce noise in the MDM.

Validation of the Proposed Architecture through Empirical Use Case Analysis

When aligned with the following empirical use cases, the proposed MDM architecture demonstrates its effectiveness and advantages.

Use Case: Emergency Medical Response

In a trauma event, paramedics scan a QR code on the patient's ID tag or use a biometric sensor to access the patient's DID stored on a blockchain ledger. This DID links to MPI pointers and authorizes access to key health information: allergies, medication history, chronic conditions. As vitals are streamed via a secure edge gateway, Kafka ingests and Flink processes the data in real time. Alerts are generated if anomalies (e.g., low blood pressure + high lactate) are detected.

Before hospital arrival, the ER team can access updated patient history and current vitals. This preemptive readiness reduces treatment latency and risk of medical error [2, 18].

Blockchain ensures each data element is cryptographically logged and tied to the originating paramedic device and consent rule [22]. This contrasts sharply with legacy batch MDM systems that would only reconcile data post-admission.

Use Case: Smart ICU Integration

This use case demonstrates the ICU scenario where multiple telemetry devices stream data (e.g., ECG, BP, SpO_2) to Kafka topics. Flink joins these with contextual data (e.g., bed location, medication status) and runs predictive ML models to identify deterioration patterns (e.g., signs of sepsis). Blockchain is used to validate device authenticity and timestamp logs.

Each telemetry event is matched to the patient's DID, which links to a unified MDM record. Data lineage is preserved across shifts and departments, ensuring reliable handoffs and legal audit readiness [18, 20].

This model addresses ICU data fragmentation, a major limitation in conventional MDM, which often lacks real-time visibility and chain-of-custody for machine-generated data [6, 18].

Use Case: Remote Monitoring for Chronic Conditions

Patients with chronic illnesses (e.g., heart failure, diabetes) use home-based devices—like smart scales, BP monitors, and glucometers—that stream data daily to a hospital-run Kafka system [12]. Flink detects trends such as sudden weight gain (fluid retention) or erratic glucose levels and updates the MDM record with event tags.

Each update is hashed and recorded on a permissioned blockchain, including metadata (e.g., device ID, timestamp, DID). Smart contracts confirm the device's registration and patient's consent state

[16]. Clinicians are notified if intervention is warranted, often before symptoms worsen.

Real-world trials using similar architectures [21, 22] report reductions in readmissions and improved adherence to treatment plans.

Use Case: Federated Interoperability across Providers

A patient moves between a primary care clinic, imaging center, and emergency hospital over three months. Instead of relying on a centralized MPI, each institution operates a node in a permissioned blockchain consortium. The patient's DID links to data indexes stored off-chain (via pointers or FHIR resource URIs). Every time a system queries or updates the master record, the blockchain logs the event, verifying its origin and timestamp [2, 14].

Consent is enforced via smart contracts. For instance, lab data may be shared with the ER team but withheld from a payer until the patient explicitly approves access [7].

This federated model complies with TEFCA principles while preserving patient trust. Unlike centralized HIEs, it ensures that no single entity owns the full patient graph, solving a major political and technical hurdle in MDM scaling [16, 24].

Traditional MDM vs. Modern MDM – A Comparison

The following comparison table shows the key benefits of the modernized architecture.

Table 1: Traditional MDM vs. Modern MDM

Dimension	Traditional MDM	Proposed Modern MDM
Primary Data Sources	Hospital EHRs, billing, lab systems; IoT and patient data often excluded.	Includes EHRs plus IoT (wearables, sensors), health apps, and external streams.
Data Ingestion & Update Frequency	Nightly ETL, periodic interface messages; high latency.	Real-time streaming via Kafka/Flink; near-instant updates [6].
Architecture & Integration	Centralized hub-and-spoke with siloed systems; scaling is difficult.	Distributed architecture: edge IoT, event streaming, blockchain, and MDM hub. Scales horizontally [2].
Identity Management	Demographic matching with local IDs; high risk of duplicates [1].	Blockchain-based DIDs; cryptographic identity resolution; reduced duplication via consensus [2].
Data Quality & Trust	Managed by internal rules and data stewards; fragmented audit trails.	Enforced by smart contracts; blockchain ensures immutable, transparent audit trails. [7]
Interoperability	Limited; brittle HL7 v2/CDA interfaces; weak cross-org sharing [2].	Uses HL7 FHIR, blockchain for identity/data; supports patient-controlled data sharing [6, 7, 25]
Handling Data Volume & Variety	Focused on structured data; struggles with telemetry and unstructured inputs.	Supports high-volume IoT data; integrates structured/unstructured data via scalable platforms.
Governance & Compliance	Manual governance; HIPAA-focused; limited sharing due to breach concerns.	Smart contracts automate rules; blockchain auditability supports compliance (HIPAA, GDPR, Cures Act).

Challenges and Risks

While the findings are optimistic, there are also some challenges to consider.

Scalability: While Kafka and Flink scale horizontally, blockchain may introduce write bottlenecks. Layer-2 or hybrid architectures may be needed [17].

Interoperability Standards: Cross-chain data exchange remains under-defined. Unified APIs and smart contract formats are necessary for ecosystem success [19].

Governance: Blockchain nodes require federated governance, SLAs, and legal frameworks—these challenges are often underestimated [24].

Privacy: Even hashed data poses re-identification risks. Use of privacy-enhancing technologies like ZKPs is recommended [14].

Clinical Workflow Integration: Streaming systems must interface cleanly with EHRs and clinician dashboards. Poor UX can negate technological gains [3].

FUTURE RESEARCH RECOMMENDATIONS

Future studies should examine the impact of real-time MDM systems on clinical workflows, particularly in high-pressure environments such as intensive care units (ICUs) and emergency departments. This includes assessing whether these systems help clinicians make faster and more accurate decisions while reducing their workload. As healthcare data increasingly crosses national borders, it is important to explore how tools like blockchain, smart contracts, and decentralized identifiers (DIDs) can facilitate compliance with diverse regulations such as HIPAA in the U.S. and GDPR in the EU. Research should also examine how patients engage with self-sovereign identity solutions and digital consent tools, as well as the challenges they face, particularly in terms of usability and digital literacy. To ensure these systems are practical at scale, real-world testing in large, interconnected health networks is essential to evaluate performance under pressure and during system failures. Another area of interest is how well these MDM frameworks can provide clean, timely data to AI models used in clinical prediction, and whether that improves the accuracy and reliability of those models. Finally, the long-term ethical and security implications of using blockchain in healthcare must be carefully studied, particularly in terms of handling incorrect or outdated information, protecting patient privacy, and governing access and consent in a decentralized system.

CONCLUSION

With the rapid digitalization of healthcare, the modernization of Master Data Management (MDM) is not just a technological upgrade but a necessary organizational shift. This paper presents a

practical framework for a real-time, secure, and intelligent MDM system that brings together the strengths of IoT, streaming analytics, and blockchain. The proposed architecture directly addresses the shortcomings of traditional systems by enhancing interoperability and building trust in the reliability and timeliness of health information. Realizing this vision will depend on collaboration across multiple disciplines. Clinicians, IT experts, policymakers, and patients must collaborate to establish the standards that will guide this evolving ecosystem. Case studies from around the world show that such transformation is not only possible but already underway in some settings. As digital technologies continue to reshape healthcare, the core data infrastructure must also advance to keep pace. By adopting the strategies outlined in this paper, healthcare systems can manage patient data more effectively, leading to safer, more connected, and responsive care.

REFERENCES

1. Moore, S. (2022). *5 Challenges for Master Data Management in Healthcare*. Semarchy Blog. Available: https://semarchy.com/blog/important-mdm-concepts-for-healthcare-data/
2. Gagnon, M. L. (2018, October 30). Using Blockchain for a Nationwide Patient Index. *Healthcare Innovation*. Available: https://www.hcinnovationgroup.com/interoperability-hie/article/13030839/using-blockchain-for-a-nationwide-patient-index
3. Grode, J. (2023). *How to Leverage Internet of Things with Master Data Management. Stibo Systems Blog (Feb 14, 2023).* Available: https://www.stibosystems.com/blog/3-ways-to-master-your-iot-devices-and-data
4. HIPAA Journal. (2025). *What is the HITECH Act? 2025 Update. (Online article).* Available: https://www.hipaajournal.com/what-is-the-hitech-act/
5. Zheng P., Lau B (2024). Chapter Seven - Internet of things and data science methods for enhanced data processing. *Elsevier - Advances in Computers*. Volume 133, 2024, pp.181-199. Available: https://doi.org/10.1016/bs.adcom.2023.10.006
6. Kai Waehner. (2023, November 27). *The State of Data Streaming for Healthcare in 2023 with Apache Kafka and Flink*. Available: https://www.kai-waehner.de/blog/2023/11/27/the-state-of-data-streaming-for-healthcare-in-2023/
7. Ekblaw, A., Azaria, A., Halamka, J., & Lippman, A. (2017). *MedRec: Blockchain for Medical Data Access, Permission Management and Trend Analysis*. MIT Media Lab. Available: https://www.media.mit.edu/publications/medrec-blockchain-for-medical-data-access-permission-management-and-trend-analysis

8. e-Estonia Briefing Centre. (n.d.). *Estonia's e-Health Records: Smart, Secure, and Patient-Centric. e-estonia.com.* Available: https://e-estonia.com/solutions/e-health-2/e-health-records/
9. U.S. Office of the National Coordinator for Health Information Technology (ONC). (2021). *Trusted Exchange Framework and Common Agreement (TEFCA).* https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement
10. Zhuang Y, Zhang L (2024). Promoting TEFCA with Blockchain Technology: A Decentralized Approach to Patient-centered Healthcare Data Management. AMIA Annu Symp Proc. 2024 Jan 11;2023:824-833. PMID: 38222410; PMCID: PMC10785864. – TEFCA WITH BLOCKCHAIN
11. Gellert, G. A., Erwich, M. E., & Herdman, S. K. (2024). Challenges meeting 21st Century Cures Act patient identity interoperability and information blocking rules. *Journal of Healthcare Quality.* 2024 Sep-Oct 01;46(5):306-315. doi: 10.1097/JHQ.0000000000000446. PMID: 39197844
12. Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of Things for health care: A comprehensive survey. *IEEE Access*, *3*, 678–708. https://doi.org/10.1109/ACCESS.2015.2437951
13. Farahani, B., Firouzi, F., et al. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems. Volume 78, Part 2, 2018, pp. 659-676. Available: https://doi.org/10.1016/j.future.2017.04.036
14. Satybaldy, A., Hasselgren, A., & Nowostawski, M. (2022). Decentralized identity management for e-health applications: State-of-the-art and guidance for future work. *Blockchain in Healthcare Today, 5*. Available: https://doi.org/10.30953/bhty.v5.195
15. Dock.io (2025). Decentralized Identifiers (DIDs): The Ultimate Beginner's Guide. *Dock Blog*. Available: https://www.dock.io/post/decentralized-identifiers
16. Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association, 24*(6), 1211–1220. Available: https://doi.org/10.1093/jamia/ocx068

17. Vazirani AA, O'Donoghue O, Brindley D, Meinert E (2019). Implementing Blockchains for Efficient Health Care: Systematic Review J Med Internet Res 2019;21(2):e12439. Available: https://doi.org/10.2196/12439
18. Mao Z, Liu C, Li Q, Cui Y, Zhou F. (2023). Intelligent Intensive Care Unit: Current and Future Trends. Intensive Care Res. 2023 May 16:1-7. doi: 10.1007/s44231-023-00036-5. Available: https://link.springer.com/article/10.1007/s44231-023-00036-5
19. Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. (2018). Secure and Trustable Electronic Medical Records Sharing using Blockchain. AMIA Annu Symp Proc. 2018 Apr 16;2017:650-659. PMID: 29854130; PMCID: PMC5977675.
20. Bhatia M, Sood SK. (2016). Temporal Informative Analysis in Smart-ICU Monitoring: M-HealthCare Perspective. J Med Syst. 2016 Aug;40(8):190. doi: 10.1007/s10916-016-0547-9. Epub 2016 Jul 7. PMID: 27388507.
21. Roehrs, A., da Costa, C. A., da Rosa Righi, R., de Oliveira, K. S. F., & da Silva, V. F. (2017). Personal health records: A systematic literature review. *Journal of Medical Internet Research*, *19*(1), e13. Available: https://doi.org/10.2196/jmir.5876
22. Ichikawa, D., Kashiyama, M., & Ueno, T. (2017). Tamper-resistant mobile health using blockchain technology. *JMIR mHealth and uHealth*, *5*(7), e111. Available: Available: https://doi.org/10.2196/mhealth.7938
23. Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research*, *5*, 2541. Available: https://doi.org/10.12688/f1000research.9756.1
24. Gordon, W. J., Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Elsevier - Computational and Structural Biotechnology Journal*. Volume 16, 2018, pp. 224-230. Available: https://doi.org/10.1016/j.csbj.2018.06.003
25. HealthIT.gov (2024). Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR). *healthit.gov.* Available: https://www.healthit.gov/topic/standards-technology/standards/fhir