

Blockchain-Based Data Provenance Architecture for IoMT-based Healthcare Systems

Ravishankar Borgaonkar¹[0000-0003-2874-3650], Andrea Neverdal Skytterholm¹,
and Guillaume Bor

SINTEF Digital, Strindvien 4, Trondheim Norway
{ravi.borgaonkar, andrea.skytterholm}@sintef.no

Abstract. The healthcare sector increasingly relies on personal Internet of Medical Things (IoMT) devices for clinical decision-making and research. However, low-cost consumer devices introduce fundamental trust challenges. IoMT devices such as smartwatches and smart rings are prone to cyberattacks and data manipulation due to trade-offs between security, cost, and performance. This paper addresses the challenge of establishing verifiable data provenance for health information from inherently untrusted personal IoMT devices. We present a two-layer security architecture that decouples device trust from data trust by anchoring provenance at the mobile application layer rather than at potentially compromised device endpoints. Our design separates device trust from data trust, enabling provenance assurance even when endpoints are untrusted. Our approach leverages Hyperledger Fabric to maintain immutable and distributed provenance records, enabling transparent data lifecycle tracking across organizational boundaries. The architecture integrates privacy-preserving authentication mechanisms, including national electronic identification systems, and fine-grained access controls through organizational channels and private data collections. A proof-of-concept implementation supports multi-organizational networks with comprehensive operations for dataset registration, modification, deletion, querying, and history retrieval. Our results demonstrate that trustworthy and auditable health data exchange can be achieved across healthcare and research institutions while preserving privacy and ensuring regulatory compliance without requiring inherent trust in the underlying devices.

Keywords: Blockchain · Data Provenance · Internet of Medical Things · Healthcare Data · Trust · IoMT security

1 Introduction

The proliferation of Internet of Medical Things (IoMT) devices has transformed healthcare delivery and patient monitoring paradigms. These connected medical devices, ranging from wearable fitness trackers and continuous glucose monitors to smart blood pressure cuffs and portable ECG sensors, enable numerous opportunities for personalized medicine, remote patient monitoring, and large-scale health research [1, 2]. The benefits extend beyond individual patient care:

IoMT technologies facilitate early disease detection, enable real-time health status tracking, reduce hospital readmission rates, and empower patients to actively participate in their own health management [3, 4]. From a societal perspective, IoMT ecosystems hold promise to relieve pressure on healthcare infrastructures by enabling predictive analytics, optimizing the allocation of medical resources, and expanding access to health-monitoring capabilities—especially in rural or underserved areas where traditional medical infrastructure is limited [1, 5].

However, as healthcare organizations increasingly rely on device-generated data for critical medical decisions and research applications [1], the need for robust mechanisms to trace, authenticate, and verify the origin and journey of this data becomes paramount. Data sourced from IoMT devices must be auditable in a trustworthy manner regarding their provenance, operational status, and collection circumstances before being utilized for clinical or research purposes. This requirement becomes particularly critical in scenarios where IoMT device-generated data is shared across organizational boundaries—for instance, when patient data is contributed to medical research studies or exchanged between healthcare providers—requiring transparent auditing, negotiated authorization involving both patients and healthcare organizations (such as hospitals, clinics, or national healthcare authorities), and verifiable custody tracking throughout the data lifecycle.

Blockchain and distributed ledger technologies offer promising tools for establishing auditable, tamper-evident data trails in multi-stakeholder healthcare ecosystems [6]. However, a fundamental challenge emerges: establishing trustworthy provenance for data originating from inherently untrusted and insecure IoMT devices. Personal IoMT devices—particularly low-cost, consumer-grade wearables and sensors—are frequently vulnerable to cyber-attacks, data manipulation, and unauthorized access due to fundamental trade-offs between security implementation costs, device performance constraints, and manufacturing economics. These devices typically lack robust security controls, operate with limited computational resources, exist in physically accessible environments where tampering is feasible, and frequently receive inadequate security updates throughout their operational lifetime [7, 8].

This paper addresses a fundamental challenge: establishing trustworthy data provenance for health information from inherently insecure personal IoMT devices. Rather than attempting to secure untrustworthy devices, we investigate how architectural frameworks can enable verifiable data provenance despite originating from potentially compromised sources. Our central research question is: How can healthcare ecosystems establish auditable data trails for information from non-regulated personal IoMT devices, enabling safe cross-organizational sharing while preserving patient privacy? We focus on personal IoMT devices that are privately purchased, non-prescribed, and operate outside formal healthcare channels. These consumer devices, including smartwatches, fitness trackers, and smart rings, are low-cost, non-regulated, and non-standardized, making them difficult to integrate with official patient health records. In Norwegian healthcare, for example, such devices cannot currently contribute to official pa-

tient journals due to absent certification, quality assurance, and provenance verification mechanisms. Our key contribution is an architecture that decouples device trust from data trust, demonstrating that healthcare systems can safely leverage patient-generated data from untrusted endpoints through robust provenance mechanisms anchored at controllable trust points.

Our investigation encompasses the design of a provenance layer security architecture that separates the trust establishment layer from the potentially untrusted device layer, leveraging the mobile application as a practical trust anchor. The architecture integrates several key technical components: lightweight cryptographic mechanisms appropriate for resource-constrained environments, privacy-preserving authentication and authorization protocols (including OAuth-based identity verification that protects patient anonymity), and permissioned blockchain technology based on Hyperledger Fabric for maintaining immutable, distributed provenance records.

Our key contributions are the following:

- A practical two-layer provenance architecture designed for personal and unregulated IoMT devices that establishes trust at the mobile application layer rather than relying on insecure device endpoints.
- An integrated blockchain-based framework utilizing Hyperledger Fabric that provides immutable provenance recording, fine-grained multi-organizational access controls, and privacy-preserving authentication mechanisms suitable for cross-organizational health data sharing scenarios.
- Design patterns for coordinating provenance protocols with authorization and negotiation mechanisms, enabling patient-controlled data sharing where provenance information supports informed consent and access control decisions across healthcare organizations and research institutions.
- A proof-of-concept implementation and evaluation demonstrating the feasibility of establishing auditable, trustworthy health data exchange for data originating from consumer-grade personal IoMT devices, with practical insights for real-world deployment in healthcare systems.

This work distinguishes itself by proposing a deployable, standards-aligned framework bridging mobile authentication and blockchain-based provenance, enabling trustable health data exchange without requiring inherent trust in IoMT devices themselves.

The remainder of this paper is organized as follows: Section 2 reviews related work in IoMT security, data provenance systems, and blockchain applications in healthcare. Section 3 presents our two-layer security architecture and detailed design rationale. Section 4 describes the technical implementation of our Hyperledger Fabric-based provenance framework, including chaincode design and network configuration. Section 5 presents experimental evaluation results and performance analysis. Section 6 discusses practical deployment considerations, limitations, and real-world applicability. Section 7 concludes and outlines future research directions.

2 Background

In this section, we begin by outlining the requirements of IoMT devices, highlighting key security challenges and clarifying the assumptions we make about IoMT devices, along with their justification based on discussions with our Norwegian healthcare partners. We then examine the concept of device and data provenance in the IoMT context, emphasizing its importance for trustworthy healthcare applications. Finally, we review related work on data provenance in healthcare, with particular attention to blockchain-based approaches and their potential role in ensuring integrity, transparency, and accountability.

2.1 IoMT in healthcare and security challenges

The increasing use of personal Internet of Medical Things (IoMT) devices plays a pivotal role in modern healthcare by enabling continuous monitoring and large-scale collection of personal health data. As these devices generate and transmit highly sensitive medical information, the need for robust security mechanisms becomes paramount to ensure data confidentiality, integrity, and availability. IoMT device security operates across multiple layers—hardware, software, and communication—requiring protection mechanisms that safeguard the device from vulnerabilities and prevent unauthorized access or tampering. This includes secure boot processes, strict access control policies, and encryption-based protection. Equally important is the end-to-end security of communication links between devices and backend systems, achieved through robust encryption, mutual authentication, and intrusion detection to mitigate risks of interception or data manipulation by malicious actors [1, 2, 6].

Despite the importance of security, ensuring comprehensive protection for IoMT devices remains a complex challenge. Many devices operate under severe resource constraints—limited power, memory, and processing capacity—which make traditional cryptographic and security frameworks unsuitable [7]. Strong security mechanisms designed for general-purpose computing platforms cannot easily be adapted to such constrained environments. Moreover, the absence of universal standards for low-cost IoT and medical devices has led to inconsistent security implementations across the ecosystem [5]. For instance, consumer-grade wearables such as fitness trackers or smartwatches vary significantly in the level of security control they provide, often prioritizing cost and performance over resilience. These disparities highlight the need for consistent, lightweight, and scalable security frameworks specifically tailored to IoMT devices [6, 7].

2.2 Device and Data Provenance in IoMT

There is no single, universally accepted definition of data provenance, as the term’s meaning often depends on the context and application domain. In the context of our work in this paper, we define data provenance as a record describing the entities, processes, and conditions involved in producing, transferring, or modifying a dataset, thereby enabling authenticity, trust, and reproducibility [9]. This definition aligns well with the IoMT domain, where establishing

transparent and verifiable data trails is essential for ensuring the reliability of patient-generated health information, as illustrated in Figure 1.

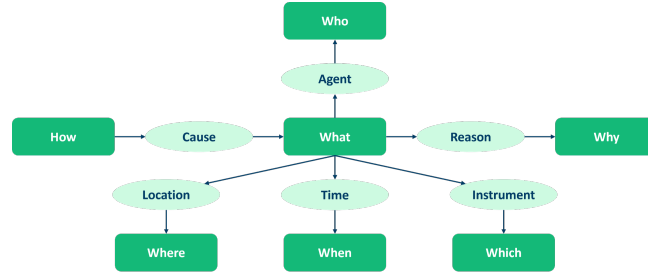


Fig. 1: W7 model illustrating a concept of data provenance (Adapted from [10])

Healthcare datasets generated by personal medical devices, whether used by clinicians for patient care or by researchers for scientific studies must be trustworthy and reliable. Data integrity directly affects clinical outcomes and research validity. As highlighted by prior studies on clinical data trust, "the correct data is collected from the right patient and that aggregated, computed, and visualized data are accurate representations of this original data" [11]. Hence, provenance mechanisms become vital for ensuring traceability, accountability, and transparency in data handling across diverse healthcare stakeholders.

Building upon these principles, in this paper, we adopt data provenance as a key mechanism to establish trust in metadata associated with patient-generated IoMT datasets. Provenance tracking enables documentation of critical lifecycle events—such as dataset registration, updates, and deletions—thereby ensuring comprehensive understanding of each dataset’s origin and evolution. This provenance-based approach strengthens confidence in IoMT data authenticity, providing a foundation for reliable clinical decision-making and medical research.

2.3 Blockchain and Hyperledger Fabric

This section outlines the technologies underpinning the data provenance layer, focusing on blockchain and its cryptographic advantages for ensuring trust and integrity. According to NIST, blockchain is a decentralized database of cryptographically signed transactions grouped into linked blocks, providing immutability and tamper resistance through network consensus [15]. Several studies have demonstrated blockchain’s effectiveness in data provenance: Sigwart et al. applied Ethereum smart contracts for IoT provenance [12], Abdullah and Dongfang developed immutable provenance services [13], and Aravind et al. proposed a blockchain platform for secure data tracking [14]. These works show blockchain’s potential to establish transparent and auditable data trails across multi-stakeholder systems.

For healthcare applications, we adopt a permissioned blockchain model suited to regulated domains. Unlike permissionless systems, permissioned blockchains

restrict participation to verified entities. We utilize Hyperledger Fabric, an enterprise-grade framework for building private distributed ledgers [16]. Fabric supports our provenance goals through distributed availability, immutable records, auditable transparency, and privacy via channels and private data collections. Its permissioned membership ensures authenticated, accountable participation among healthcare providers and researchers.

3 Data Sharing and Provenance Challenges in IoMT Ecosystems

In this section, we discuss three specific scenarios in which data sharing can be happened from IoMT in healthcare ecosystem for both research and diagnostic purpose. These three scenarios indicate associated data provenance challenges in terms of security and privacy.

3.1 IoMT Data Sharing Scenarios

This section examines three scenarios for sharing health data generated by personal IoMT devices—those not provided by healthcare authorities—with healthcare or research entities. While these scenarios vary according to national regulations, we use the Norwegian healthcare system as our reference framework for envisioning data sharing methods.

Scenario S1: Direct Manual Submission In the first scenario, data subjects directly submit their personal health data to health authorities, typically through an online platform. For example, a patient maintaining a personal health journal manually records details about their medical history, current health status, medications, and other relevant information, then uploads this data to the healthcare system.

Scenario S2: Device-to-Gateway Transmission The second scenario, illustrated in Figure 2, involves a wearable device connected to either a dedicated mobile application or a home gateway. Health data collected by the wearable device—such as activity levels or vital signs—is transmitted via Bluetooth to the mobile app or gateway. The gateway represents a potential future solution: a centralized household device that aggregates health-related information from multiple IoMT devices before sharing it with healthcare authorities.

Scenario S3: Direct Cloud Integration The third scenario involves wearable devices sending data directly to commercial cloud services (e.g., Apple Health, Garmin Connect, or Fitbit) or to dedicated data collection services established by healthcare authorities. The data is subsequently uploaded to the health journal or other designated storage systems, while the data provenance layer receives metadata from the uploaded data. This scenario poses the highest integration complexity, as it requires cooperation from proprietary vendors such as Apple, Garmin, and Fitbit. Additionally, healthcare authorities must establish regulatory frameworks to monitor and audit the data before it is shared with third parties, including private healthcare companies conducting research.

3.2 Data Provenance Challenges

Low-cost IoT and IoMT devices are often designed with limited security considerations, rendering them vulnerable to cyber-attacks that compromise both the device and connected systems. Numerous studies and documented incidents, particularly in healthcare, demonstrate risks associated with device exploitation and data manipulation [19]. Findings from previous research studies on IoMT cybersecurity [17–19], confirm the inherent untrustworthiness of consumer-grade IoMT devices. To address these limitations, our work shifts the focus of device and data provenance away from unregulated and non-standardized devices, instead adopting a zero-trust approach that establishes verifiable and secure associations among mobile applications, IoMT devices, and end-users.

Requirements for Secure IoMT Systems: Designing a secure IoMT environment requires meeting several essential requirements. First, device security must ensure that both hardware and software components are protected from tampering or exploitation. This includes safeguarding against unauthorized modifications that could compromise device functionality or data integrity. Second, data security and privacy are fundamental to protecting patient information against unauthorized access while maintaining user confidentiality. Given the sensitive nature of health data, systems must implement robust protection mechanisms that prevent data breaches and unauthorized disclosures throughout the data lifecycle. Third, end-to-end security is necessary to ensure that communication and data handling remain secure from the point of generation to final storage or use. This encompasses secure data transmission protocols, encrypted storage solutions, and protected processing environments that maintain data integrity across all stages of the data flow. Finally, data provenance capabilities must capture and maintain reliable metadata that verifies the origin, integrity, and history of IoMT-generated data. This requirement is particularly critical in healthcare settings where data authenticity and traceability are essential for clinical decision-making, regulatory compliance, and research validity. These requirements highlight key practical challenges for implementing secure IoMT ecosystems: resource constraints, lack of standardization, limited trusted hardware, and market-driven trade-offs. These collectively hinder the realization of consistent data provenance guarantees.

Key challenges in IoMT: Meeting these requirements in real-world IoMT systems is difficult due to several fundamental challenges. Resource constraints pose a significant obstacle, as most IoMT devices have limited power and processing capabilities. These limitations make it difficult to implement strong cryptographic mechanisms or complex security protocols without significantly impacting battery life and device performance. The lack of standardization across the IoMT ecosystem further complicates security efforts. Security levels vary widely across devices, with different manufacturers implementing inconsistent protection measures. For example, a Fitbit may not meet the same security standards as an Apple Watch, resulting in a fragmented security landscape where some devices are significantly more vulnerable than others. This inconsistency makes it challenging to establish uniform security policies across diverse device ecosys-

tems. Many consumer IoMT devices also suffer from the absence of trusted hardware components. Unlike enterprise-grade systems, most wearable devices lack built-in hardware security features such as secure enclaves or Trusted Platform Modules (TPMs). Without these foundational security elements, devices cannot establish strong roots of trust or securely store cryptographic keys, leaving them vulnerable to sophisticated attacks. Finally, manufacturers often face security trade-offs driven by market pressures. To remain competitive, companies frequently prioritize cost reduction and performance optimization over robust security implementations. This results in compromised protection mechanisms, as security features that increase manufacturing costs or reduce battery efficiency are often deprioritized or omitted entirely.

In addition to the security challenges outlined above, IoMT-based healthcare data sharing presents further obstacles to establishing reliable data provenance:

- **Authentication and Access Control:** Ensuring that data originates from legitimate users and devices while maintaining patient privacy is difficult. Balancing identity verification, consent management, and anonymity in health data sharing remains an unresolved challenge.
- **Scalable and Immutable Storage:** IoMT environments generate vast amounts of data that must be collected, stored, and traced without modification. Achieving both immutability and scalability simultaneously requires efficient distributed systems capable of handling high data throughput.
- **Data Verifiability and Integrity:** Ensuring that health data has not been altered or tampered with during collection, transmission, or aggregation is a persistent problem. Provenance systems must provide cryptographic assurance that the data analyzed or shared reflects the true, original values generated by IoMT devices.

4 Data Provenance Architecture

Building on the design principles introduced in Section 3, the proposed solution follows a two-layer architecture that separates trust establishment from data provenance management. The first layer, referred to as the mobile trust layer, anchors data authenticity and user verification at the mobile application level. The second layer, the blockchain provenance layer, ensures immutable recording, access control, and auditability using Hyperledger Fabric. To help readers understand our proposed solution, this section first introduces the terminology and components that make up the data provenance architecture. We then present the architecture itself and explain the reasoning behind our design decisions.

4.1 Terminology and Architectural Components

The proposed data provenance architecture comprises several key entities that collectively enable secure and traceable health data management within the IoMT ecosystem. This subsection defines the core terminology used throughout our architectural description of the three data sharing scenarios. Figure 2 illustrates these components and interaction with data provenance layer.

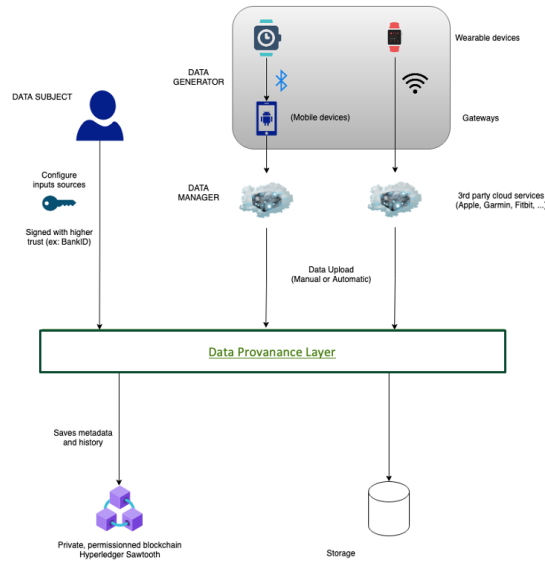


Fig. 2: IoMT data sharing scenarios and architecture components

Data Subject: The data subject refers to the individual—typically a patient or research participant—who generates and voluntarily shares personal health data for healthcare delivery or research purposes. The data subject maintains sovereignty over their health information and grants consent for its collection and use.

Data Generator: The data generator encompasses wearable devices and IoMT sensors (e.g., Fitbit, Apple Watch, or Oura Ring) that continuously collect physiological measurements and health-related data. These devices serve as the primary source of health information in our scenarios and operate at the edge of the data flow architecture.

Gateway: The gateway functions as an intermediary data transfer node, typically instantiated as a mobile phone equipped with a dedicated application. The gateway facilitates the transmission of health data from wearable devices to networked systems. Data uploads through the gateway may occur through two modes: manual (user-initiated) or automatic (based on pre-configured, consent-based periodic uploads).

Mobile Application (App): The mobile application—represented as "Mobile Device" in Figure 2 and "Phone + App" in Figure 4—constitutes a critical component of the data provenance layer. This application may function as a standalone software solution or as an integrated module within established healthcare platforms such as Helsenorge¹, Norway’s national digital health service portal. The application establishes secure Bluetooth Low Energy (BLE) communica-

¹ Helsenorge is the official website for information about and access to health services for residents of Norway- <https://www.helsenorge.no/en/about-helsenorge/>

tion with wearable devices to collect health data and subsequently forwards this information to downstream components for provenance tracking and validation.

Data Manager: The data manager operates within the blockchain layer and functions as a trusted intermediary entity responsible for collecting, validating, and distributing health data to authorized healthcare providers or research institutions. Within the Norwegian healthcare context, this role may be fulfilled by governmental health authorities or designated platforms such as Helsenorge, which serve as official data custodians within the national healthcare infrastructure. The data manager ensures compliance with regulatory requirements and maintains audit trails through blockchain-based provenance mechanisms.

4.2 Design Rationale: Mobile-Device Based Provenance Initiation

Given the constraints and challenges outlined in the previous section, our proposed system operates under the assumption that IoMT devices should be treated as potentially compromised and not inherently trustworthy. Deploying custom provenance mechanisms directly on such devices is impractical without extensive collaboration from regulatory authorities and IoT manufacturers, particularly given their closed-source nature and limited accessibility for security modifications. Furthermore, data exchange between wearable devices and external systems typically occurs through short-range communication interfaces—such as Bluetooth—which limit the ability to implement provenance tracking at the device level. To address these limitations, our architecture establishes the mobile device and its associated application (Mobile Device + App) as the initial point for data provenance tracking, rather than the IoMT device itself. This design decision is justified by several factors. First, mobile devices offer significantly greater computational resources and security capabilities compared to resource-constrained wearables. Second, mobile platforms provide established frameworks for user authentication and authorization, enabling reliable identity verification before data enters the provenance chain. Third, the mobile application serves as a controllable intermediary that can implement standardized security protocols regardless of the diversity and security inconsistencies among IoMT devices. By initiating data provenance at the mobile device layer with proper user authentication and authorization, the system creates a trusted boundary where data can be validated, annotated with provenance metadata, and securely forwarded to subsequent components. This approach effectively decouples the security and trustworthiness of the provenance system from the inherent vulnerabilities of consumer-grade IoMT devices, while still capturing essential information about data origin and collection context.

4.3 Data Provenance Architecture

Figure 3 illustrates the proposed blockchain-based provenance architecture that ensures trust, integrity, and accountability for personal health data generated by IoMT devices. The architecture adopts a zero-trust approach, recognizing that IoMT devices may be vulnerable or compromised and are therefore unsuitable as

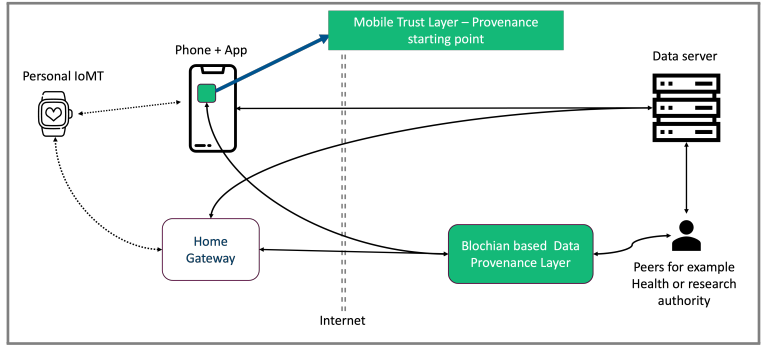


Fig. 3: Overview of the proposed two-layer data provenance architecture, consisting of the mobile trust layer and the blockchain provenance layer.

starting points for provenance tracking. Instead, the provenance process begins at the mobile device and application layer, which establishes the first verifiable point of trust between the user and the healthcare ecosystem.

Mobile Device + App: It serves as a secure gateway responsible for authentication, authorization, and privacy policy enforcement. Each data subject—whether a patient or research participant—must authenticate using secure credentials before any data is transferred or recorded. Upon successful authentication, the application initializes a provenance record that associates the collected data with verified user credentials and essential metadata, including timestamps, device identifiers, and consent information. This authentication-first approach ensures that all data entering the provenance chain is linked to a verified identity.

Data Collection and Transmission: Data generated by wearable IoMT devices is transmitted to the mobile application over secure short-range communication channels like Bluetooth. Users can upload this data either manually through direct interaction or automatically based on previously granted consent. The mobile application then forwards these authenticated data packets to the Home Gateway for further processing.

Home Gateway: The Home Gateway aggregates data from multiple devices within the same household or user domain. It performs intermediate validation, encryption, and routing functions to prepare the data for secure transmission to the Data Provenance Layer. This aggregation point provides flexibility for users with multiple IoMT devices while maintaining a consistent security posture across all data streams. The Home Gateway component is optional and primarily serves multi-device households or aggregation scenarios.

Blockchain-based Data Provenance Layer: The Data Provenance Layer, implemented using Hyperledger Fabric, serves as the immutable ledger for all provenance information. Each event - whether a data upload, update, or deletion - is recorded as a blockchain transaction, ensuring integrity, traceability, and non-repudiation. Smart contracts within the Fabric network enforce data access rules and consent policies, while provenance metadata enables comprehensive audit-

ing and verification of data authenticity across multiple stakeholders, including healthcare providers, researchers, and regulatory bodies.

5 Implementation and Evaluation

To validate the proposed data provenance architecture, we developed a working prototype using *Hyperledger Fabric v2.5.6* deployed within Docker containers. The implementation demonstrates the feasibility and effectiveness of our design approach in a realistic healthcare data sharing scenario.

Network Configuration and Components: The blockchain network consists of two peer organizations—one representing a patient-side application provider and the other representing a healthcare provider—along with a single orderer node responsible for maintaining transaction consensus and ordering. The chaincode implements essential dataset lifecycle operations, including registration, update, deletion, query, and history retrieval. To facilitate interaction and demonstration, we connected the blockchain network to a lightweight gateway application that exposes RESTful HTTP endpoints, enabling external systems to invoke provenance functions through standard web protocols. Figure 4 illustrates the implementation setup. Data from personal IoMT devices is transmitted to a mobile interface implemented as an HTTP module rather than a native mobile app. In this prototype, the mobile layer was implemented as an HTTP module emulating mobile application functions for proof-of-concept evaluation. This module handles data registration and securely forwards it to the Hyperledger Fabric network over the internet. Within the Fabric network, healthcare participants such as hospitals and general practitioners (Fastlege) maintain their own ledger databases, each holding immutable provenance records for the datasets they receive.

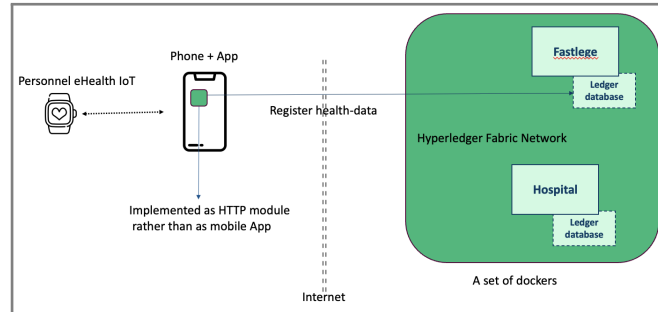


Fig. 4: Prototype Implementation Architecture

Permissioned Blockchain Architecture: In our implementation (Figure 4), the permissioned blockchain architecture is implemented using Hyperledger Fabric to meet provenance and privacy requirements. The network includes two organizations—representing healthcare entities such as hospitals and general prac-

titioners—each operating as peers within Docker-based containers. The Membership Service Provider (MSP) enforces PKI-backed identities, ensuring that only authenticated participants can transact, thereby addressing the authentication and authorization needs of healthcare data management.

Channels isolate transaction traffic between organizations, protecting sensitive health data and enforcing confidentiality. Private Data Collections (PDCs) store actual patient information off-chain while recording only cryptographic hashes on-chain, ensuring both immutability and verifiable integrity. Fabric’s support for zero-knowledge protocols (Idemix, ZKAT) further enables anonymous yet auditable transactions, maintaining accountability without exposing patient identities. This setup operationalizes the permissioned blockchain model, providing a secure, privacy-preserving foundation for IoMT data provenance. Additionally, OAuth 2.0-based authentication is implemented through integration with the Norwegian BankID² service, enabling secure IoMT user access within the national health platform *HelseNorge*.

Evaluation Results: Our evaluation confirms functional correctness, data immutability, and verifiable provenance integrity across multi-organizational peers. The prototype successfully registers datasets immutably, with each upload creating a permanent blockchain record. Subsequent updates or deletions generate cryptographically verifiable provenance records maintaining a complete audit trail. Typical transaction times for dataset registration were observed under 300 ms in a two-peer setup, consistent with prior Fabric evaluations. Query operations correctly retrieve both current dataset states and complete historical lineage, including all modifications and actor identities. This capability to reconstruct full data lifecycles is essential for regulatory compliance and forensic analysis in healthcare. These results confirm that the architecture delivers secure, transparent, and privacy-preserving data provenance for IoMT-enabled healthcare environments.

6 Limitations and Future Work

The proposed architecture anchors trust at the mobile application layer, mitigating IoMT device vulnerabilities while leveraging Hyperledger Fabric’s privacy features to ensure regulatory compliance and auditability. However, several limitations require attention. The prototype lacks evaluation for critical performance metrics including latency, throughput, and scalability under large-scale healthcare workloads. Future work will include comprehensive stress testing with higher transaction volumes and multi-organizational peer networks to assess operational viability. The system assumes mobile devices and gateways are trusted provenance initiators, introducing security risks if compromised. Integrating trusted execution environments (TEEs) or remote attestation mechanisms could further strengthen this trust model. Practical challenges persist in integrating with proprietary IoMT cloud platforms (e.g., Apple Health, Fitbit), managing network

² In Norway, BankID is a personal electronic identification method designed for secure online authentication and digital signing. <https://bankid.no/en/about-us>

membership and channels at scale, and improving consent workflow usability for patients and healthcare professionals.

While Fabric’s privacy mechanisms provide foundational confidentiality controls, effective cross-domain data sharing requires interoperability standards and compatible identity federation models. Although OAuth 2.0–based authentication via Norwegian BankID is implemented, broader integration with international identity providers is necessary for cross-border healthcare data exchange. Future work will explore system resilience against emerging threats, comparative analysis of zero-knowledge and access-control methods, and integration with international identity providers to support cross-border data exchange. These evaluations aim to provide deeper understanding of the architecture’s robustness, scalability, and feasibility for real-world healthcare deployment.

7 Conclusion

This paper presents a two-layer blockchain-based data provenance architecture that addresses the fundamental challenge of establishing trust in IoMT-generated health data where the devices themselves cannot be trusted. The architecture comprises a mobile trust layer and a blockchain provenance layer that decouples data trust from device trust. By initiating provenance at the mobile device layer rather than at potentially compromised IoMT devices, the architecture anchors data trustworthiness in a verifiable, blockchain-backed infrastructure that provides auditable and privacy-preserving data sharing. The prototype demonstrates that our approach offers a practical foundation for secure health data sharing, enabling healthcare providers to leverage patient-generated data while giving patients transparent control over their information. This work unlocks the clinical and research value of personal health monitoring technologies while upholding trust, accountability, and privacy in healthcare systems.

Acknowledgments. This research was partly co-funded by the European Union under the Horizon Europe programme through the *NEMECYS* project (Grant Agreement No. 101119747) and by the Research Council of Norway through the *Health Democratization* and *NORCICS* projects(RCN no. 310105).

References

1. El-Deep, A., Alloghani, M., Hussain, A., et al.: A comprehensive survey on the impact of the Internet of Medical Things on healthcare. *Artificial Intelligence Review* (2024). <https://doi.org/10.1007/s10462-024-11063-z>
2. Yang, Y., Zhang, X., Huang, Y., et al.: Internet of Medical Things: A systematic review. *Neurocomputing* **564**, 126–140 (2023). <https://doi.org/10.1016/j.neucom.2023.07.086>
3. Lee, Y.H., Kim, D.H., Lee, J.H., et al.: Portable ECG-based Internet of Medical Things system for abnormal signal detection: Results from a 2,000-participant study. *Bioengineering* **11**(8), 836 (2024). <https://doi.org/10.3390/bioengineering11080836>

4. Al-Marzooq, A., Liyanage, M., Braeken, A., et al.: Clinical benefits and risks of remote patient monitoring: An umbrella review of systematic reviews. *BMC Health Services Research* **25**, 72 (2025). <https://doi.org/10.1186/s12913-025-12292-w>
5. Bhattacharya, S., Zhang, Y., Xu, W., et al.: Healthcare and the Internet of Medical Things: Applications, trends, and future challenges. *Informatics* **11**(3), 47 (2024). <https://doi.org/10.3390/informatics11030047>
6. Phuyal, S., Elvas, L.B., Ferreira, J.C., Bista, R. (2025). Blockchain Technology in Healthcare: Unifying Patient Medical Records - A Survey. *Bio-Inspired Computing. IBICA 2023. Lecture Notes in Networks and Systems*, vol 1231. Springer, Cham.
7. Mejía-Granda, C.M., Fernández-Alemán, J.L., Carrillo-de-Gea, J.M. et al. Security vulnerabilities in healthcare: an analysis of medical devices and software. *Med Biol Eng Computing*, 257–273 (2024). <https://doi.org/10.1007/s11517-023-02912-0>
8. L. Dzamesi and N. Elsayed, "A Review on the Security Vulnerabilities of the IoMT Against Malware Attacks and DDoS," 2025 IEEE 4th International Conference on Computing and Machine Intelligence (ICMI), MI, USA, 2025, pp. 01-08.
9. W3C Provenance Incubator Group , "Provenance XG Final Report," 2010, <https://www.w3.org/2005/Incubator/prov/XGR-prov-20101214/>
10. Sudha Ram and Jun Liu. 2009. A new perspective on semantics of data provenance. In *Proceedings of the First International Conference on Semantic Web in Provenance Management - Volume 526 (SWPM'09)*. CEUR-WS.org, Aachen, DEU, 35–40.
11. Fariha Tasmin Jaigirdar, Carsten Rudolph, and Chris Bain. 2019. Can I Trust the Data I See? A Physician's Concern on Medical Data in IoT Health Architectures. *ACSW '19*, NY, USA, Article 27, 1–10. <https://doi.org/10.1145/3290688.3290731>
12. Sigwart, M., Garcia-Castro, R., Gómez-Pérez, A.: Blockchain-based data provenance for the Internet of Things. In *Proceedings of the IEEE International Conference on Internet of Things (iThings)*, pp. 161–168. IEEE (2022).
13. Abdullah, M., Dongfang, Z.: Blockchain-based data provenance for distributed systems. In: 2021 IEEE International Conference on Big Data (Big Data), pp. 4563–4571. IEEE (2021). <https://doi.org/10.1109/BigData52589.2021.9671893>
14. Aravind, K., Nair, M., George, S.: A blockchain-based platform for secure data provenance in IoT. *Journal of Network and Computer Applications* **202**, 103390 (2022). <https://doi.org/10.1016/j.jnca.2022.103390>
15. National Institute of Standards and Technology (NIST): Blockchain Technology Overview. NISTIR 8202 (2018). <https://doi.org/10.6028/NIST.IR.8202>
16. Androulaki, E., Barger, A., Bortnikov, V., et al.: Hyperledger Fabric: A distributed operating system for permissioned blockchains. *Eurosys'18*, pp. 1–15. ACM (2018).
17. Bour, G et al (2023). Security Analysis of the Internet of Medical Things (IoMT): Case Study of the Pacemaker Ecosystem. In: Roque, A.C.A., et al. *Biomedical Engineering Systems and Technologies. BIOSTEC 2022. Communications in Computer and Information Science*, vol 1814. Springer, Cham.
18. Y. Sun et al, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," in *IEEE Access*, vol. 7, pp. 183339-183355, 2019, doi: 10.1109/ACCESS.2019.2960617.
19. A. J. Burns, M. Eric Johnson, and Peter Honeyman. 2016. A brief chronology of medical device security. *Commun. ACM* 59, 10 (October 2016), 66–72. <https://doi.org/10.1145/2890488>