Demo - MedTech Chain

Decentralised, Secure and Privacy-preserving Platform for Medical Device Data Research*

Petru-Rosu, Alin; Tataru, Tamara; Zelenjak, Jegor; Kromes, Roland; Erkin, Zekeriya

DOI
10.1109/WIFS61860.2024.10810716

Publication date
2024

Document Version
Final published version

Published in
Proceedings - 16th IEEE International Workshop on Information Forensics and Security, WIFS 2024

2024 IEEE International Workshop on Information Forensics and Security (WIFS) | 979-8-3503-6442-2/24/$31.00 ©2024 IEEE | DOI: 10.1109/WIFS61860.2024.10810716

Demo - MedTech Chain: Decentralised, Secure and Privacy-preserving Platform for Medical Device Data Research*

Alin Petru-Rosu, Tamara Tataru, Jegor Zelenjak, Roland Kromes, and Zekeriya Erkin
Delft University of Technology Department of Intelligent Systems
Delft, The Netherlands
a.rou@student.tudelft.nl, t.tataru@student.tudelft.nl, j.zelenjak@student.tudelft.nl,
r.g.kromes@tudelft.nl, z.erkin@tudelft.nl

***Abstract*—Employing blockchain and privacy-enhancing technologies, MedTech Chain promises an authenticated, decentralised, secure, and privacy-preserving environment for the real-time research and monitoring of medical device data. Through its querying functionalities, the platform can provide valuable insights for threat intelligence, medical research and hospital management. To our knowledge, the approach is among the first to employ ϵ-differential privacy in the context of medical device data. The current work details the framework's functionality and demonstrates a negligible time overhead induced by ϵ-differential privacy to data analysis.**

***Index Terms*—blockchain, healthcare, security, privacy, IoT, networked medical devices, ϵ-differential privacy, Hyperledger Fabric**

I. Introduction

Recent technological advancements have revolutionised the healthcare sector. However, they have also introduced significant security and privacy challenges. While offering innovative solutions, networked medical devices have expanded the threat landscape, making the healthcare infrastructure increasingly vulnerable to cyberattacks [1], [2]. In this context, developing methods for protecting medical devices is needed to ensure the security of both patients and healthcare facilities.

Nonetheless, addressing cybersecurity threats relating to networked medical devices is particularly difficult [1], [3]. One major challenge is the absence of effective methods for gathering comprehensive data on medical infrastructure, which is essential for cyber threat intelligence [4]. Even more, the various kinds of medical devices prevent consistent security measures over the entire healthcare network [5]. Consequently, there is a need for advanced solutions enabling the research of networked medical devices with a focus on improving the security of medical infrastructure.

Current solutions fail to address the challenges of monitoring and securing medical device infrastructures. They primarily rely on manual data collection and monitoring, inefficient for the large-scale and diverse nature of modern medical environments [1]. Centralised data repositories have been attempted to manage medical device data. Still, these systems are vulnerable to single points of failure, cyberattacks, and regulatory compliance and privacy issues, making managing and securing sensitive information difficult [4]. Despite these efforts, the lack of decentralised and privacy-preserving solutions has limited the effectiveness of research and monitoring of networked medical devices.

To improve the security of networked medical devices, MedTech Chain focuses on medical device data analysing tools. Device data provides insights into device behaviour, aiming to identify and mitigate cyber threats more effectively [6]. By leveraging blockchain and privacy-enhancing technologies, MedTech Chain provides a decentralised, secure, and privacy-preserving platform for real-time research and monitoring of medical device data. The platform is built using Hyperledger Fabric, an open-source permissioned blockchain framework for enterprise-grade applications. Its modular architecture allows the customisation of various components, making it suitable for healthcare environments. Additionally, the platform employs ϵ-differential privacy [7], which adds controlled noise to data queries to protect sensitive information while allowing aggregate data analysis. These technologies collectively enable MedTech Chain to enhance threat intelligence, medical research and hospital management by providing authenticated access to aggregated medical device data.

The platform's vision is supported and aligns with initiatives like the SEPTON project, which aims to develop a secure data-sharing platform for cyber threat intelligence and statistical analysis on medical devices. Integrating MedTech Chain with SEPTON to securely manage medical device data will support the latter's efforts to enhance cybersecurity and privacy in healthcare. This collaboration ensures that both projects can achieve their shared objective of safeguarding healthcare infrastructure by enabling an efficient research environment of networked medical devices.

II. The MedTech Chain System

A. Architecture

The MedTech Chain architecture involves healthcare facilities/hospitals and a semi-trusted organisation, the MedTech

* This work is supported by the European Union's Horizon Europe research and innovation programme under grant agreement No. 101094901 (SEPTON).

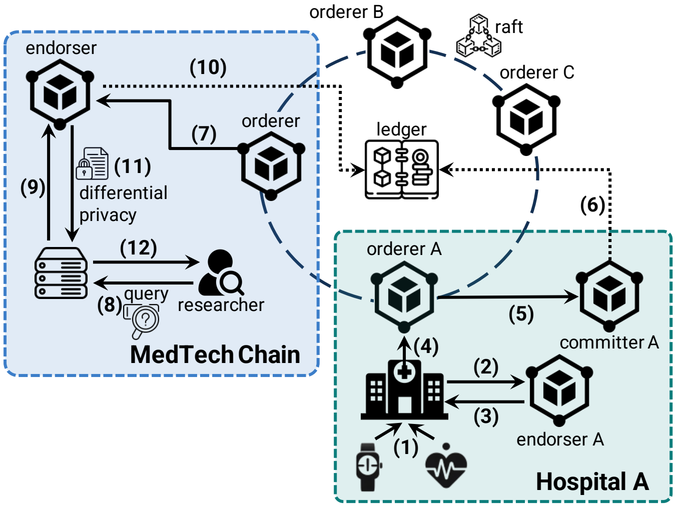


Fig. 1. MedTech Chain architecture based Hyperledger Fabric, comprising three kinds of nodes: endorser peers, committer peers and orderers. The endorsers verify the submitted transaction's validity. The orderers place the valid transactions to a new block in order. The committer peer verifies block validity and commits the transaction on the ledger within a block.

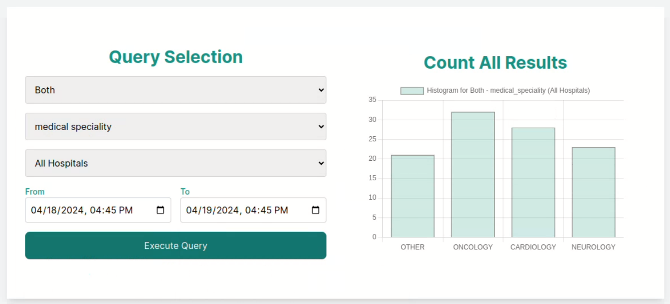
Chain Organisation. Hospitals provide device data, while the MedTech Chain Organisation enables researchers to query it.

1) Hospital Organisations: The current use case considers two types of medical devices—portable and wearable—whose data is stored on the ledger. Each hospital deploys *collectors* to bridge devices and the blockchain, as shown in Figure 1. Collectors gather and process device data (step 1), then regularly submit blockchain transactions with new/updated data. The transaction flow follows: an endorser validates the transaction (steps 2 and 3). If valid, it is submitted to the ordering layer (step 4). Ordered transactions are then submitted within a block to the committer, appending it to the blockchain (steps 5 and 6). The ledger state modification becomes visible to the entire MedTech Chain network (step 7).

2) MedTech Chain Organisation: The MedTech Chain Organisation, highlighted in the blue frame in Figure 1, is a semi-trusted entity facilitating medical device research. Researchers submit queries through the *user application* (step 8). The application translates the query into a transaction evaluated by an endorser (step 9). This read-only transaction does not need to be submitted to the ordering layer. During evaluation, the invoked smart contract reads the ledger's state (step 10), runs the query, applies ϵ-differential privacy, and returns the result to the application (step 11). The result is then returned to the researcher (step 12).

B. Queries

By interacting with the user application, researchers can currently perform three types of privacy-preserving queries on wearable and portable devices data. Firstly, they can retrieve counts of devices filtered by hospitals, period, and other dynamic filters such as operating system versions. Secondly, they can count devices grouped by specified properties, such as medical speciality, with filters like hospital or time frame applied. The result is visualised as a histogram (see Figure 2), yet the design allows for easy extension to other plot types. Lastly, similar to counting, researchers can calculate the average of specific properties of devices with various filters applied. Nevertheless, the system's modular design allows for the easy addition and extension of queries.


Query Selection

Both

medical speciality

All Hospitals

From: 04/18/2024, 04:45 PM

To: 04/19/2024, 04:45 PM

Fig. 2. Graphical Interface for the *Count All* Query

C. Implementation

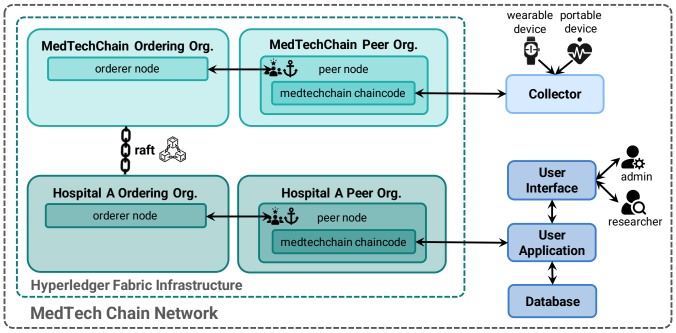


Fig. 3. System Implementation

MedTech Chain operates on a permissioned blockchain network built using Hyperledger Fabric. The network's permissioned nature is reinforced by Membership Service Providers (MSPs), which manage identities and authenticate members. Hyperledger Fabric's channel architecture enables transactions and communications among participants within isolated channels. Though the current implementation of MedTech Chain uses a single channel, such features allow the development of more complex use cases.

The implementation of MedTech Chain is illustrated in Figure 3. The prototype involves hospitals and the MedTech Chain Organisation, each with one orderer and a peer node that acts as an endorser and committer. Each hospital and the MedTech Chain Organisation separates their peers and orderers into distinct Hyperledger organisations. Peers can run two transactions (bundled as ”medtechchain chaincode”): creating device data assets and querying aggregated device data. These contracts include checks to ensure that only authorised submitters can query (i.e., MedTech Chain Organisation) or create assets (i.e., hospitals). The network configurations are set to default, and the network is configured to use TLS during communication.

The platform ensures hospital privacy by using ϵ-differentially private queries. All implemented queries are anonymised with the Laplace mechanism, applying noise directly to the query results within the smart contracts. For grouped counting, a different noise value is added to each count individually. Also, the ϵ value for the noise is configurable, allowing for adjustable privacy levels.

The user application is a semi-trusted service accessible only to registered users like researchers and administrators. For researchers, it provides an interface for efficient interaction with blockchain-stored data through queries. Administrators can manage user accounts through an interface that allows researcher account creation, modification, and revocation.

Implementation-wise, both the user application and collectors are built with Java Spring Boot, which handles processing requests from users (admins or researchers) or devices, respectively, and submitting the corresponding blockchain transactions. The user application also provides basic user management, with a PostgreSQL database storing user account data. The user interface is a React application that communicates with the backend of the user application using HTTPS and maintains user sessions using JSON Web Tokens.

III. Demonstration

The current experiment computed the overhead induced by ϵ-differential privacy on MedTech Chain's queries. The demonstration infrastructure comprised the MedTech Chain Organisation and three hospitals. To facilitate deployment, all prototype services were containerised using Docker. For this experiment, the entire infrastructure was deployed on an AMD EPYC 9334 32-core server with 128 CPUs operating at a minimum 1.5 GHz frequency, with 32 cores per socket.

Additional tooling was used to visualise the blockchain. Blockchain Explorer[2] is a user-friendly web application that allows to view/query blocks, transactions and associated data, network information, transactions, and any other relevant information stored in the ledger. This helped with observing the state of the blockchain.

Initially, the blockchain had to be populated with device data. For demonstration, the collectors of each hospital were mocked to submit device data asset creation transactions to the blockchain regularly. The collectors were left to run until they created approximately 10,000 device data assets.

Next, the blockchain was issued with query transactions. The contracts were configured to both enable or disable differential privacy. In each case, 1000 test queries were evaluated, and their computational time was recorded. Query time is measured as the average time of each test query sent in each case. Table I shows the time to process a query with and without applying differential privacy.

When differential privacy is applied, the query processing recorded a time overhead of 0.172 ms. While the overhead is negligible, differential privacy greatly improves data privacy.

TABLE I
Query execution time

	Query Response Time
DP not applied	243.103 ms
DP applied	243.275 ms

IV. Impact on the information forensics and security community

MedTech Chain balances data utility and privacy, ensuring compliance with privacy regulations while fostering a trustworthy collaborative research environment that is valuable for various users. Furthermore, the monitoring of device data across the healthcare network, such as framework version of medical devices, allows to aid risk management and provide a clearer vision over the cyber threat intelligence landscape. Its design and implementation significantly advance the secure and private analysis of medical device data, aiming to improve healthcare security.

V. Conclusion

This paper presented MedTech Chain, a blockchain-based platform for secure and privacy-preserving research on networked medical device data. The platform uses blockchain technology to ensure data integrity and transparency while leveraging ϵ-differential privacy to protect data during analysis.

MedTech Chain supports functionalities like counting, averaging, and grouped counting with multiple filters over device data. These functionalities are embedded in smart contracts, applying differential privacy with a negligible overhead of approximately 0.2 ms, ensuring privacy without compromising individual data entries. The source code is available here[3].

References

[1] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, 2018. [Online]. Available: https://doi.org/10.1016/j.maturitas.2018.04.008

[2] Check Point Research, "Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most," *Check Point Blog*, Apr 2023, visited on May 17, 2024. [Online]. Available: https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/

[3] S. M. Karunarathne, N. Saxena, and M. K. Khan, "Security and Privacy in IoT Smart Healthcare," *IEEE Internet Computing*, vol. 25, no. 4, pp. 37–48, 2021. [Online]. Available: https://doi.org/10.1109/MIC.2021.3051675

[4] I. Lee *et al.*, "Challenges and Research Directions in Medical Cyber-Physical Systems," *Proc. IEEE*, vol. 100, no. 1, pp. 75–90, 2012. [Online]. Available: https://doi.org/10.1109/JPROC.2011.2165270

[5] P. A. H. Williams and V. McCauley, "Always connected: The security challenges of the healthcare Internet of Things," in *3rd IEEE World Forum on Internet of Things, WF-IoT 2016, Reston, VA, USA, December 12-14, 2016*. IEEE Computer Society, 2016, pp. 30–35. [Online]. Available: https://doi.org/10.1109/WF-IoT.2016.7845455

[6] B. Hodges *et al.*, "Attack Modeling and Mitigation Strategies for Risk-Based Analysis of Networked Medical Devices," in *53rd Hawaii International Conference on System Sciences, HICSS 2020, Maui, Hawaii, USA, January 7-10, 2020*. ScholarSpace, 2020, pp. 1–10. [Online]. Available: https://hdl.handle.net/10125/64538

[7] J. Ficek *et al.*, "Differential privacy in health research: A scoping review," pp. 2269–2276, 2021. [Online]. Available: https://doi.org/10.1093/jamia/ocab135

[2] https://blockchain-explorer.readthedocs.io/en/main/introduction.html

[3] https://github.com/orgs/MedTechChain