SIMDES: Secure and Interoperable Medical Data Exchange System using Blockchain and HL7 FHIR standards

Mpyana Mwamba Merlec
Department of Computer Science and Engineering
Korea University
Seoul, South Korea
mlecjm@korea.ac.kr

Ait Hamouda Yahia Gaya
Department of Computer and Science and Engineering for Healthcare
EPISEN
Créteil, France
yahia.ait-hamouda@etu.u-pec.fr

Hoh Peter In
Department of Computer Science and Engineering
Korea University
Seoul, South Korea
hoh_in@korea.ac.kr

***Abstract*— The healthcare industry faces significant challenges in managing patient data, including security, privacy, interoperability, and patient control. This paper proposes a decentralized healthcare data management system leveraging blockchain technology to address these issues. By integrating FHIR standards for data exchange and employing smart contracts for access control, insurance claims, and data sharing, the proposed system aims to create a secure, transparent, and patient-centric healthcare ecosystem. The blockchain's immutability and transparency ensure data integrity, while advanced cryptographic techniques safeguard patient privacy. This research explores the potential of blockchain to revolutionize healthcare by enhancing data management, facilitating research, and improving patient outcomes.**

Ajouter conclusion sur l'implémentation

***Index Terms*— Blockchain, healthcare, data management, FHIR, smart contracts, privacy, security, interoperability.**

I. Introduction

The healthcare industry is currently grappling with significant challenges related to the management of patient data. These challenges include ensuring data security, maintaining patient privacy, achieving interoperability among disparate systems, and granting patients control over their own data. As the volume of healthcare data continues to grow, traditional centralized systems have become increasingly inadequate in addressing these issues [1]. Blockchain technology, with its decentralized and immutable nature, presents a promising solution to these challenges by enhancing the security, transparency, and efficiency of healthcare data management [1-7].

The primary purpose of this paper is to propose a decentralized healthcare data management system, SIMDES (Secure, Interoperable, and Managed Data Exchange System), that leverages blockchain technology. By integrating the FHIR (Fast Healthcare Interoperability Resources) standards for data exchange and employing smart contracts for access control, insurance claims, and data sharing, SIMDES aims to create a secure, transparent, and patient-centric healthcare ecosystem. This system is designed to improve data integrity, safeguard patient privacy, and ensure compliance with regulatory requirements, while also facilitating research and enhancing patient outcomes.

This paper is structured as follows: Section II provides an overview of related work, including existing solutions and how SIMDES differentiates itself. Section III discusses the design and architecture of SIMDES, detailing the system's key components and their integration with blockchain technology. Section IV outlines the implementation details, including the modular architecture, off-chain storage, and smart contract development. Section V presents the evaluation and results, covering performance analysis, security assessment, and interoperability testing. Section VI discusses the benefits and challenges associated with SIMDES, and Section VII concludes with a summary of findings and suggestions for future work.

II. Background and Related work

Medical data exchange systems (comment sont-ils conçus, quelles limites ?)

Comment les résoudre ? (FHIR, Blockchain/Smart Contracts etc.)

FHIR and Blockchain-based medical information systems

1) Overview of existing solutions

Various blockchain-based healthcare data management systems have been proposed in recent years to address the challenges of data security, privacy, and interoperability. For example, the system developed by Bae et al. [3] leverages blockchain technology to create a health information exchange platform that uses HL7 FHIR standards for data exchange. Similarly, Do Hoang et al. [4] introduced a blockchain-based system that focuses on the secure and privacy-preserved exchange of personal healthcare records. These solutions highlight the potential of blockchain to enhance healthcare data management, but they often face limitations in terms of scalability, interoperability, and real-world applicability.

The usability of the blockchain-based health information exchange platform using HL7 FHIR standards was evaluated positively in several areas, though some challenges were noted. The platform received a relatively high score in perceived ease of use, with a mean of 3.82 out of 5, indicating that participants generally found the platform easy to understand and interact

with. Similarly, the mean score for perceived usefulness was 3.79 out of 5, reflecting that users found the platform beneficial, particularly in providing useful information and functions for managing their health data. Overall satisfaction with the health information exchange service was notably high, scoring 4.67 out of 5, which underscores a strong positive reception from users.

However, the evaluation also revealed some concerns. Despite blockchain technology's ability to enhance data security and ensure data integrity, there were lingering worries about data privacy, which could impact users' willingness to fully engage with the platform. Additionally, challenges related to interoperability were identified, even with the implementation of HL7 FHIR standards, suggesting that seamless data exchange across different health information systems might still face obstacles. Finally, the potential costs associated with deploying the platform, particularly on a public blockchain, such as transaction fees, were highlighted as possible barriers to adoption, especially for smaller healthcare providers [3].

While existing solutions have made significant strides in utilizing blockchain for healthcare data management, SIMDES offers several unique contributions that set it apart. Unlike other systems that primarily focus on data exchange, SIMDES integrates smart contracts to facilitate not only the secure sharing of health records but also the management of insurance claims, medical prescriptions as well as the governance of data access. These smart contracts ensure automated compliance with regulatory constraints, enabling a more streamlined and transparent process for all stakeholders involved. Additionally, SIMDES enhances patient privacy and data security through advanced cryptographic techniques, including zero-knowledge proofs, which allow for the verification of data without revealing sensitive information. Furthermore, SIMDES supports the advancement of medical research by facilitating the use of anonymized data, enabling researchers to access valuable datasets without compromising patient confidentiality.

SIMDES also differentiates itself by offering a more holistic approach to healthcare data management. By integrating FHIR standards with blockchain technology, SIMDES ensures interoperability with existing healthcare systems while maintaining data integrity and security. Moreover, our solution is designed to be patient-centric, providing patients with greater control over their data and facilitating secure data sharing for research and clinical purposes.

Tableau de caractéristiques

III. Design and Architecture

A. System overview

Fig. 1. System architecture

The SIMDES system is designed as a decentralized platform that utilizes blockchain technology to manage healthcare data securely.

Its core architecture and operational workflow are as follows: at the heart of SIMDES are three key components: smart contracts, FHIR standards, and off-chain storage. Smart contracts automate and enforce rules for data interactions among various stakeholders, ensuring transparency, security, and efficiency. The FHIR standards facilitate the standardized exchange of medical information, ensuring interoperability across different healthcare systems. Meanwhile, off-chain storage is employed to manage large volumes of data, such as medical records and prescriptions, allowing for scalability without compromising the integrity ensured by the blockchain.

SIMDES connects multiple stakeholders, including doctors, nurses, patients, pharmacists, insurance companies, researchers, and system administrators, each playing a crucial role in the ecosystem. Doctors and nurses use the platform to securely access and update medical records and issue prescriptions. Pharmacists retrieve and validate these prescriptions through the DApp, ensuring accuracy and patient safety by cross-referencing relevant medical records. Patients benefit from easy access to their medical data and prescriptions, and the system potentially streamlines the insurance claim process by automatically filling in the necessary details based on their medical records.

Insurance companies interact with SIMDES by receiving and validating claims, leveraging the system's secure data to streamline the claim approval process. Researchers can access anonymized medical data, enabling them to conduct studies while maintaining patient privacy. Administrators maintain the system, deploying updates, verifying accounts, and ensuring the overall security and functionality of the DApp.

B. Data mapping process

1) Mapping real-life medical records to FHIR resources

SIMDES employs a FHIR Data Mapper to convert real-life medical records into standardized FHIR resources. This process involves mapping various elements of patient data, such as demographics, medical history, and lab results, to the corresponding FHIR resources.

2) Data structure and storage

Patient data in SIMDES is structured according to FHIR standards and stored off-chain to reduce the blockchain's load. Each patient's data is encrypted and stored in a decentralized storage system, while a hash of the data is recorded on the blockchain to ensure immutability and integrity.

C. Blockchain Integration

Blockchain plays a critical role in SIMDES by providing a decentralized, transparent, and immutable ledger for all transactions related to patient data management. The blockchain ensures that all data access and sharing activities are recorded, preventing unauthorized modifications and ensuring traceability.

D. Off-chain storage

To address the challenges of storing large volumes of healthcare data on the blockchain, SIMDES employs an off-chain storage strategy. This approach involves a decentralized data storage mechanism that securely stores extensive patient records and other sensitive medical information off the blockchain. By leveraging decentralized storage solutions, such as IPFS or a similar distributed file system, SIMDES ensures data redundancy, scalability, and resistance to data tampering.

To maintain the integrity and traceability of off-chain data, SIMDES utilizes blockchain pointers. These pointers are cryptographic references stored on the blockchain that link to the corresponding off-chain data. This mechanism allows for secure and efficient access to large datasets while preserving the benefits of blockchain’s immutability and transparency. The combination of off-chain storage with blockchain pointers ensures that patient data remains secure, accessible only to authorized users, and compliant with regulatory requirements.

E. Smart contracts for governance

1) Permission management

Smart contracts in SIMDES are used to manage permissions for data access and sharing. Patients can grant or revoke access to their data through a user-friendly interface, with the smart contract enforcing these permissions automatically.

2) Data access tracing

Every time a healthcare provider or researcher accesses patient data, the access is recorded on the blockchain, ensuring full traceability. This feature enhances accountability and helps prevent unauthorized access to sensitive information.

3) Compliance with regulatory constraints

Our solution is designed to comply with regulatory requirements such as HIPAA and GPDR. Smart contracts enforce these regulations by controlling data access, anonymizing patient data where necessary, and maintaining audit trails.

F. Security Features

SIMDES shall use public-key cryptography to secure patient data. Each patient and healthcare provider is issued a pair of cryptographic keys, which are used to encrypt and decrypt data.

Additionally, Token-based authentication will be implemented to control access to the SIMDES system. Each user is issued a unique token that must be presented to access the system, ensuring that only authorized users can interact with the blockchain.

Finally, Zero-knowledge proofs will be used in SIMDES to allow for the verification of data transactions without revealing the underlying data. This technique enhances privacy by ensuring that sensitive patient information is not exposed during verification processes.

IV. Implementation and Evaluation

Comment a-t-on adressé les points évoqués dans III ?

A. Modular architecture

1) Detailed description of each module

- *FHIR Data Mapper:* This module translates real-life medical records into FHIR resources, enabling interoperability with other healthcare systems. It ensures that patient data is stored and accessed in a standardized format.
- *Blockchain Network:* Leveraging Hyperledger Besu, the blockchain network acts as a decentralized ledger, recording hashed patient data and transaction records. This ensures that all interactions are immutably logged, providing a transparent and tamper-proof history of patient data management.
- *Smart Contracts:* Deployed on the blockchain, smart contracts manage access control, data sharing, insurance claims, and research facilitation through anonymized data. These contracts automate processes, reducing the need for manual intervention and increasing the system's efficiency.
- *Cryptographic Module:* Advanced cryptographic techniques, such as zero-knowledge proofs, are employed to ensure data confidentiality and privacy. This module secures sensitive patient information, ensuring that only authorized parties can access or modify the data.

2) Interaction Between Modules:

The interaction between these modules is governed by the blockchain, where smart contracts ensure that data flows securely and efficiently between them. For example, when a patient record is updated, the FHIR Data Mapper standardizes the data, the Blockchain Network logs the transaction, and the Cryptographic Module ensures that only authorized users can view or alter the information.

B. Smart contract development

1) Development and deployment of smart contracts

The SIMDES system's smart contracts, written in Solidity, manage various aspects of healthcare data management. The contracts were developed to handle user registration, encounters, conditions, medication requests, and insurance claims. Deployment shall be carried out on the Besu Hyperledger blockchain as we found it to be the most suitable in terms of privacy, performance, scalability, flexibility and compliance with HIPAA and GDPR.

2) Use cases and scenarios

The use cases are as follows:

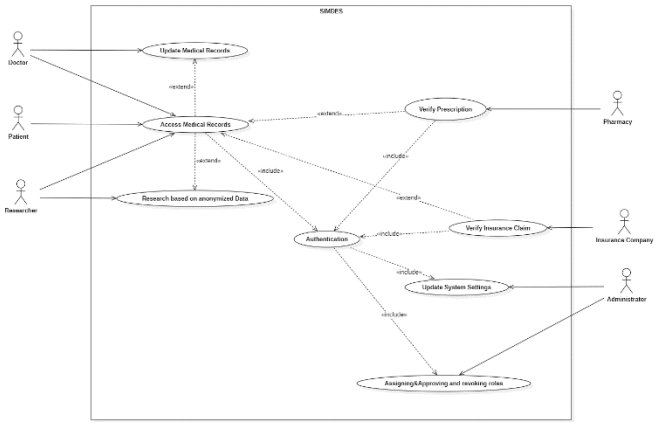

Fig. 2. Overview of the DApp

Data exchange management is handled by the system following this diagram:

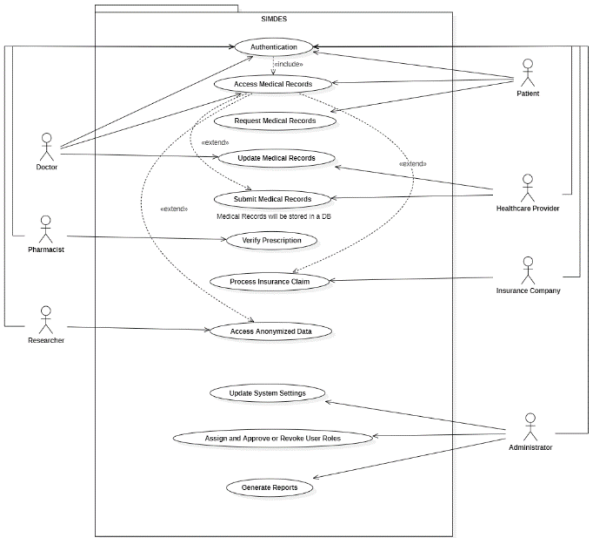

Fig. 3. Data Exchange management

Every user has to authenticate with their personal authentication token and can only manipulate the data they are allowed to, thanks to appropriate the appropriate modifiers and ZKP.

C. Performance analysis

1) System performance metrics

Performance metrics will be evaluated based on transaction throughput, latency, and resource utilization.

2) Scalability tests

Scalability shall be tested by simulating large-scale usage scenarios, including high numbers of simultaneous transactions.

D. Security Assessment

1) Decentralized data storage mechanism

SIMDES will employ a decentralized storage mechanism to handle large healthcare data volumes. Off-chain storage solutions, such as IPFS, will be used to store medical records, while the blockchain will retain cryptographic pointers to this data, ensuring secure and efficient access.

2) Blockchain pointers for secure access

The system will use blockchain pointers to link on-chain records with off-chain data securely. These pointers ensure that data can be accessed only by authorized users, with the blockchain providing an immutable record of all access attempts.

E. Interoperability testing

1) Interoperability with existing healthcare systems

SIMDES presents a need for interoperability with existing healthcare systems, focusing on the seamless integration of FHIR-compliant data with legacy systems. The system has yet to be tested for interaction with other platforms, in order to

demonstrate its ability to operate within diverse healthcare environments.

2) Case studies and examples

In addition to Fig. 2, we introduce the Prescription Verification Process and the Insurance Claim refund use cases:

Fig. 4. Prescription Verification Process

The steps to validate a prescription through our SIMDES system are as follows: a prescription is issued by the Doctor and can be submitted manually by the patient or automatically (implies a default address for the pharmacy, which is why the patient can choose to submit it themselves) by SIMDES according to patient preferences. The pharmacist then proceeds with standard procedure and checks the blockchain for the prescription status in order to prevent double claims and issues of the sort.

Fig. 5. Insurance Claim and Refund

Insurance claims are in fact automatically created whenever an Encounter (any form of meeting between a patient and healthcare professional that would result in costs for the patient) takes place between a patient and a provider. The insurance company then receives both the claim and the medical record once all relevant information has been disclosed and proceeds with their usual procedure. The claim is resolved on the blockchain to prevent double claims and other issues of the sort.

V. Benefits and Challenges

Limites (brèches pour que des personnes intéressées puissent connaitre les axes d'amélioration, de manière globale)

A. Enhanced Data Security

- *Security improvements over existing solutions*

B. Improved Interoperability

- *How SIMDES enhances interoperability*

C. Scalability Considerations

- *Scalability aspects and future-proofing*

D. Initial Setup Costs

- *Cost analysis and considerations*

E. Compatibility with Legacy Systems

- *Strategies for integrating with existing systems*

VI. Conclusion and Future Work

Challenges prioritaires pour nous

1) Summary of findings

2) Future work and potential improvements

Acknowledgment

References

[1] Reegu FA, Abas H, Gulzar Y, Xin Q, Alwan AA, Jabbari A, Sonkamble RG, Dziyauddin RA. Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. *Sustainability*. 2023

[2] Suzanna Schmeelk, Megha Kanabar, Kevin Peterson, Jyotishman Pathak, Electronic health records and blockchain interoperability requirements: a scoping review, *JAMIA Open*, Volume 5, Issue 3, October 2022

[3] Y. S. Bae *et al*., "Development of Blockchain-Based Health Information Exchange Platform Using HL7 FHIR Standards: Usability Test," in *IEEE Access*, vol. 10, pp. 79264-79271, 2022

[4] Do Hoang, Hien, et al. "A blockchain-based secured and privacy-preserved personal healthcare record exchange system." *2021 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT)*. IEEE, 2021.

[5] Carter G, Chevellereau B, Shahriar H, Sneha S. OpenPharma Blockchain on FHIR: An Interoperable Solution for Read-Only Health Records Exchange through Blockchain and Biometrics. Blockchain Healthc Today. 2020 Jun 12;3. doi: 10.30953/bhty.v3.120. PMID: 36777058; PMCID: PMC9907413.

[6] Peng Zhang, Jules White, Douglas C. Schmidt, Gunther Lenz, S. Trent Rosenbloom, FHIRChain: Applying Blockchain to Securely and Scalably

Share Clinical Data, Computational and Structural Biotechnology Journal, Volume 16, 2018, Pages 267-278, ISSN 2001-0370.

[7] Wu, Huiqun, et al. "A patient-centric interoperable framework for health information exchange via blockchain." *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*. 2019.