Blockchain-based electronic health record system with patient-centred data access control

Devendhu MD
S7 CSE
KTE20CS024

Guide: Prof.Anu Bonia Francis
Department Of Computer Science and Engineering
Rajiv Gandhi Institute of Technology, Kottayam

October 8, 2023

Table of Contents

Blockchain-based electronic health record system with patient-centred data access control

2023 IEEE/ACM 6th International Workshop on Emerging Trends in Software Engineering for Blockchain

Authors: Stavros Koumpounis, Mark Perry

Published: 14 May 2023

Introduction

- The study focuses on the increasing prevalence of mental health issues among young adults in the UK.
- Only 25 percentage of young adults in the UK receive professional help for mental health issues due to barriers like limited awareness, service availability, and fear of stigma.
- The NHS is undertaking a decade-long digital transformation, emphasizing interoperability, patient data control, and patient-centered care, while simultaneously reengineering legacy systems for security and GDPR compliance.
- The seminar proposes a decentralized, zero-trust model for transparent patient-centered data access control, meeting stringent security standards and GDPR regulations to address these challenges.

Literature Study

Challenges of Public Blockchains in Healthcare:

- Public blockchains, like Ethereum, have nodes distributed globally.
- Concerns arise regarding data privacy and compliance with data transfer agreements, as personal data may be sent outside the EEA .
- Patient data erasure requests can complicate solutions based on public blockchains..

Ancile: A Permissioned Blockchain Solution (Addressing Attacks):

- Ancile proposes the use of a permissioned blockchain to address security concerns.
- This approach sacrifices some transparency in access control.
- It relies on trust in the platform managing the system.

Literature Study

FHIRChain: Permissionless Blockchain for Record Sharing

- FHIRChain focuses on interoperability and follows FHIR standards for record sharing..
- It stores data pointers on the blockchain using a token-based permission model with public key cryptography..
- This approach mitigates some limitations of permissionless blockchains.

MedBloc: A Patient-Centered Permissioned Blockchain Solution

- MedBloc addresses limitations of FHIRChain.
- It incorporates a patient-centered design with symmetric cryptography and stores all data on-chain using a permissioned blockchain.
- MedBloc introduces features like revoking consent and uses an authentication server for added security.

What is Blockchain ?

- Blockchain is a decentralized and distributed digital ledger technology that records transactions across multiple computers in a way that ensures the security, transparency, and immutability of the data

Methodology

ABCDE Modified Scrum Methodology

- This methodology appears to be a modified version of the Scrum framework, customized for blockchain development.
- Incorporating Test-Driven Development (TDD) and Behavior-Driven Development (BDD) into the testing process of a blockchain component ensure both security and comprehensive test coverage.
- Separate development activities into two distinct flows, one for smart contract development and the other for dApp front-end development.
- A detailed description of the tasks required to plan, create, test, and integrate the dApp system with smart contracts.
- Focused on documentation of the smart contracts using UML diagrams and the BDD test suite, to aid development, security assessment, and visualisation.
- Focused activities related to security auditing.

ABCDE Modified Scrum Methodology

- **Security and performance assessment**
  - Use (OWASP) "top ten" list of proactive controls for application security.
  - For enhancing security implemented ConsenSys' guidelines for smart contract security.
  - Lists of security practices and patterns are being utilized throughout the entire development process.
  - Use Slither framework for automated vulnerability analysis.

ABCDE Modified Scrum Methodology

- **Gas optimization**
  - Gas describes the cost of deploying and running smart contracts on the Ethereum blockchain.
  - By optimization, improve the performance of our solution and reduce the cost of deploying and running the smart contracts.
  - Enhance security by preventing DoS attacks and avoiding unwanted smart contract reverts/failures due to running out of gas.
  - Simplifying Smart Contracts and Limited Functionality helps in gas optimization and reducing complexity .

Designs

Actors and Goals

- **Goals**
  - To operate a smart contract access control list that is managed by patients/users.
  - To securely store encrypted data pointers for personal mood monitoring.
  - To allow patients/users to share their mood monitoring data with therapists if needed.
- **Actors**
  - **Patient:** Creates medical data from mood monitoring questionnaires on the app system. Manages control and flow of data.
  - **Therapist:** Treats patient and wants to access reports to support treatment.

Security requirements and practices

Based on OWASP and ConsenSys guidelines and security checklists paper identified relevant security practices and design patterns.

- **Design patterns for smart contract development**
  - **C1:** Define security Requirements
  - **C2:** Leverage Security Frameworks and Libraries
  - **C5:** Validate All Inputs
  - **C6:** Implement Digital Identity
  - **C7:** Enforce Access Controls
  - **C8:** Protect Data Everywhere
  - **C10:** Handle All Errors and Exceptions

Security requirements and practices

- **Design patterns for Security**
  - **Authorization**: Restrict the execution of critical methods to specific users. Design choice is Embedded addresses to grant permissions pattern
  - **Privacy**: Ensure data integrity, confidentiality and adhere to the GDPR.Design choice is Encrypt on-chain metadata pattern .
- **Design patterns for Gas optimization:**
  - **Storage patterns**: Limit Storage.save the intermediate results in memory or stack and update the storage only at the end of all computations.
  - **Saving space**: Mapping Vs Array:recommended to use mappings to manage lists of data, unless there is a need to iterate, or it is possible to pack data types.
  - **Miscellaneous**:Optimizer .turn on the Solidity Optimizer

Architecture

- AWS was chosen to host the database needed for offchain data, along with the authorization and encryption features.
- WS's Key Management Service (KMS) is a recommended for data protection, aligning with OWASP's security model 'C8.
- DynamoDB with NoSQL matched the pointer system for a simple key-value type of database.
- React.js and ethers.js are widely used frameworks in the web3 space.

Architecture

- **MVC DESIGN pattern**
  - **Model:**
    - AWS cloud DynamoDB NoSQL database. • Ethereum blockchain component holding metadata.
  - **view:**
    - React.js with ethers.js for the front-end client.
  - **Controllers:**
    - AWS Lambda-based serverless APIs for record data retrieval and digital identity authorization using AWS Cognito and STS.
    - Metamask wallet acting as a bridge between the client and the blockchain component.
  - **Controller-invoked blockchain data connector service:**
    - Controls the essential encrypted metadata, including the pointers for the database.
    - Verifies the integrity of the data stored off-chain by the use of cryptographic hashes.
    - Restricts permissions through transparent access control.

Diagrams

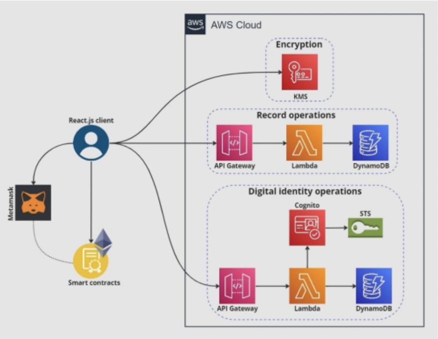

Figure: Architecture overview diagram

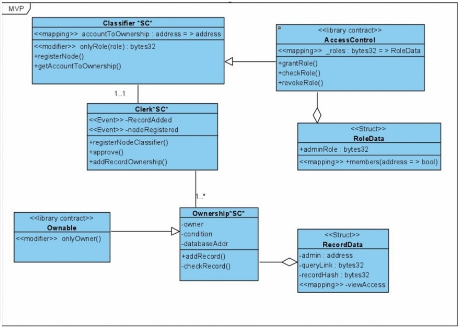

Figure: Blockchain component's class diagram

Encryption

- Use of symmetric key (256-bit AES-GCM) server-side encryption of the metadata that will be stored on-chain.
- Unique keys are created for each patient and limit access to them.
- PKI for sign-then-encrypt for secure data sharing
- Keccak256 for record hashing to be stored on-chain.
- Encryption to happen server-side
- se UUID for a unique and secure id of records, UUIDv4 due to security operation-related context .

UML Diagrams

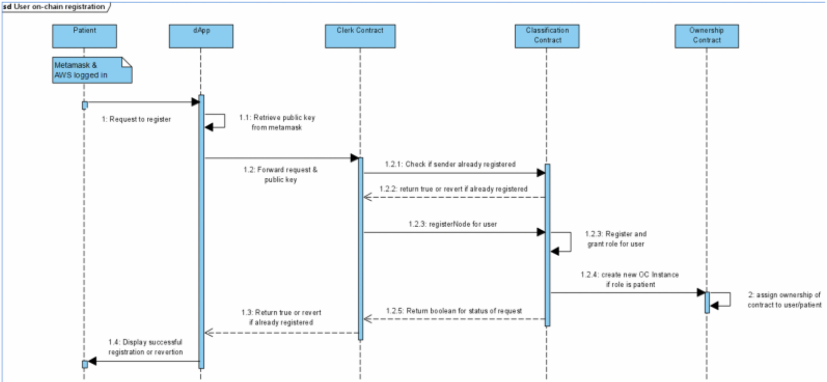

Figure: User on-chain registration sequence diagram

UML Diagrams

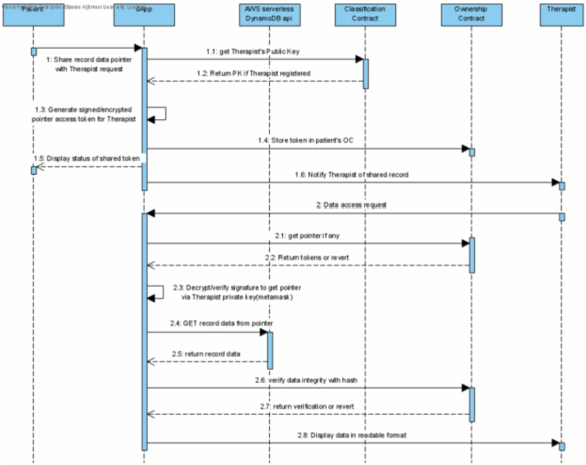

Figure: Record data token-based pointer sharing sequence diagram

Results

- Study demonstrate the development process followed the agile methodology correctly and was able to adapt the design and implementation as needed to better align with the goals of the project.
- Data followed the encryption plan, which enabled securely encrypted pointers with symmetric and asymmetric encryption and integrity verification through hash comparison on-chain
- Implementation of refactoring based design patterns for gas optimization led to a significant decrease in gas consumption.
- The record addition function resulted in a 15.3% decrease, and registration and deployment showed the most substantial reductions at 46.1% and 48.7%, respectively.
- Utilization of TDD and BDD, along with the functionality and reporting provided by Hardhat, resulted 100% test coverage

Limitation and Future Works

- The inclusion of a separate temporary "box" or database for holding only records that are meant to be shared could increase security.
- Use of Polygon is a Level 2 Ethereum-based chain that increases transaction speed and reduces cost substantially.
- By adopting the OpenEHR standard for data format specification, this,could improve its ability to interoperate with other systems.
- The use of the data contract pattern is indeed an effective strategy for gas optimization and efficient data management in blockchain applications.

Conclusion

- The project emphasized the importance of handling sensitive healthcare data and adopted a patient-centered approach in data management.
- Recognized security design patterns and practices, including cryptographic techniques, were employed to protect data integrity and confidentiality.
- The dApp followed security guidelines from OWASP and ConsenSys, ensuring robust security measures were in place. Additionally, GDPR-related issues were addressed for data privacy compliance.
- Smart contracts had 100% test coverage, and gas consumption was reduced by 15-45%, enhancing cost-efficiency.

Reference

1. Agaku, I.T., Adisa, A.O., Ayo-Yusuf, O.A., Connolly, G.N.: Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. Journal of the American Medical Informatics Association 21(2), 374–378 (2014)
2. Anton, K., Manico, J., Bird, J.: Owasp proactive controls for developers. Open Web Application Security Project (OWASP) (2018)
3. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable cities and society 39, 283–297 (2018)
4.L. Wang and J. W. Lu, "A memetic algorithm with competition for the capacitated green vehicle routing problem," *IEEE/CAA J. Autom. Sinica, vol.6, no.2, pp.516–526, Mar. 2019.*

Thank You

Questions ?