PharmaSys: Towards Preventing Prescription Misuse Using A HIPAA-Compliant Blockchain Protocol

Information and Communication Technology (ICICT), 2024

Aaron Nguyen  Luke Durham  Alex Lewtschuk  Peyton Lundquist  Gaby Dagher

February 21-22, 2024
# Table of Contents

1. Introduction
2. Related Work
3. Background
4. Solution
5. Experimental Evaluation
6. Conclusion
INTRODUCTION
Motivation

- Over the last two decades, drug abuse in the United States has posed a major societal issue that has grown at an alarming rate.
- In 2021, the United States suffered over 100,000 fatalities due to drug overdoses. [6]
- According to a report issued by the U.S. Department of Health and Human Services, illicit drug use imposes an economic burden of $193 billion every year. [7]
Challenges

- Defining an “accurate” prescription
- HIPAA Compliance
- Implementation into BlueChain
The Problem We Address

The healthcare system needs a platform that:

- Empowers individuals through patient-owned data
- Keeps an immutable record of prescription data
- Works towards preventing mis-prescription by doctors
Contributions

- The PharmaSys system
- A HIPPA-Compliant prescription tracking blockchain
- Proof of SHaring (PoSH)
- Implementation and experimental tests on scalability and robustness
RELATED WORK
Medical Blockchain Solutions

- Ancile [5]
  - Handle EHRs maintaining HIPPA-compliance
- ACCORD [3]
  - consensus mechanism utilizing a group of leaders to distribute responsibilities
- SecureRx [1]
  - Drug provenance, recall management system, and cloud storage
Prescription Tracking Blockchain Solutions

- VigilRx [8]
  - Patient-centric solution with focus on interoperability between parties
- Optrak [9]
  - DApp enhances opioid tracking distribution
- FHIRChain [10]
  - Architecture of prescription tracking network
- MedRec [2]
  - Introduce SC deployment for 3 stakeholders
  - Record system for medical records
BACKGROUND
HIPAA

Security & Privacy

- Federal regulations for Private Health Information (PHI)
- Covered entities are health plans, healthcare clearinghouses, and healthcare providers who electronically manage any health information [4]
Quorum-based Consensus

• Select nodes participate in block validation
• Can be chosen based on a variety of factors
• Can tolerate up to 33% faulty nodes in the network
BlueChain

- Research framework developed in Java at Boise State University by Peyton Lundquist
- Utilizes quorum consensus and can facilitate faster development times
- Utilized as the code base for PharmaSys
SOLUTION
Overview

- HIPAA Design Principles
- 3 Node System
- Proof Of SHarding (PoSH)
HIPAA Design Principles

<table>
<thead>
<tr>
<th>HDP#</th>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDP1</td>
<td>Privacy (Right of Access)</td>
<td>An individual has a right of access to inspect and obtain a copy of protected health information about the individual</td>
</tr>
<tr>
<td>HDP2</td>
<td>Privacy (Right of Access, Timely Action)</td>
<td>The covered entity must act on a request for access no later than 30 days after receipt of the request.</td>
</tr>
<tr>
<td>HDP3</td>
<td>Privacy (Right of Access, Manner of Access)</td>
<td>If an individual’s request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual.</td>
</tr>
<tr>
<td>HDP4</td>
<td>Privacy (Effect of Prior Authorizations)</td>
<td>A covered entity may use or disclose protected health information pursuant to an authorization or other express legal permission obtained from an individual</td>
</tr>
<tr>
<td>HDP5</td>
<td>Privacy (De-identification Of Protected Health Information)</td>
<td>Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.</td>
</tr>
<tr>
<td>HDP6</td>
<td>Security (Access Authorization)</td>
<td>Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.</td>
</tr>
<tr>
<td>HDP7</td>
<td>Security (Access Control)</td>
<td>Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those that have been granted access rights.</td>
</tr>
<tr>
<td>HDP8</td>
<td>Security (Audit Control)</td>
<td>Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.</td>
</tr>
<tr>
<td>HDP9</td>
<td>Security (Integrity Controls)</td>
<td>Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.</td>
</tr>
<tr>
<td>HDP10</td>
<td>Security (Encryption And Decryption)</td>
<td>Implement a mechanism to encrypt and decrypt electronic protected health information.</td>
</tr>
<tr>
<td>HDP11</td>
<td>Security (Transmission)</td>
<td>Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.</td>
</tr>
<tr>
<td>HDP12</td>
<td>Security (Protection From Malicious Software)</td>
<td>Procedures for guarding against, detecting, and reporting malicious software.</td>
</tr>
<tr>
<td>HDP13</td>
<td>Security (Unique User Identification)</td>
<td>Assign a unique name and/or number for identifying and tracking user identity.</td>
</tr>
<tr>
<td>HDP14</td>
<td>Security (Data Backup Plan)</td>
<td>Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.</td>
</tr>
</tbody>
</table>
System Overview

- Authorized parties push algorithms on chain
- Authorized parties push transactions to chain
- Quorum is formed and shards work to patients
- Patients return required data and quorum makes decision
System Overview

**Figure:** Three node types in PharmaSys and their responsibilities.
Figure: Prescribers and Pharmacists are randomly selected from their respective pools using the hash of the last block and join the quorum.
Proof of SHarding (PoSH)

Figure: Visualization of an individual quorum member’s algorithm being sharded
Proof of SHarding (PoSH)

**Figure:** Demonstration of instance where two worker nodes have disagreement
EXPERIMENTAL EVALUATION
Setup & Testing Environment

• Setup
  • Executed on a local network within a Virtual Machine
  • MIN_CONNECTIONS = 4 and MAX_CONNECTIONS = 7

• Testing Environment
  • 3.4 GHz Intel I7-6700CPU, NVIDIA Quadro M400 GPU, 32GB of 2133 MHz DDR4 RAM, 512GB PCIe SSD running Windows 10
  • Ubuntu 22.04 LTS (24GB of RAM, 25GB VHDD, 5 cores of CPU utilization that ran Maven V3.9.3 and Java 20 SDK dependency
We experimented on various stages of our transaction process which consisted of quorum formation, quorum decision, block construction, and network communication.

We set up the network with 7 quorum members and incrementally increased the network size from 100 to 500 nodes in steps of 100 for each data recording iteration.

Each iteration we executed 50 transactions and calculated the average duration.

We also measured the client’s response time alongside the in-network processing time.
Scalability Result 1

<table>
<thead>
<tr>
<th>Network Size</th>
<th>Quorum Formation</th>
<th>Quorum Decision</th>
<th>Block Construction</th>
<th>Total Network Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>0.00011329</td>
<td>4.03305100</td>
<td>0.00026780</td>
<td>4.03382640</td>
</tr>
<tr>
<td>200</td>
<td>0.00016470</td>
<td>4.08861959</td>
<td>0.00031734</td>
<td>4.08942926</td>
</tr>
<tr>
<td>300</td>
<td>0.00012304</td>
<td>3.91122543</td>
<td>0.00025875</td>
<td>3.91177063</td>
</tr>
<tr>
<td>400</td>
<td>0.00016594</td>
<td>3.87454129</td>
<td>0.00027795</td>
<td>3.87889664</td>
</tr>
<tr>
<td>500</td>
<td>0.00012681</td>
<td>3.86846344</td>
<td>0.00029122</td>
<td>3.87029214</td>
</tr>
</tbody>
</table>

**Figure:** In-network time of various processes
Scalability Result 2

Figure: Graph of Run Time in relation to Network Size of various processes
Robustness

- A non-accurate transaction occurs when majority of the sub-quorum of patients is malicious
- Malicious Activity in Scientific Research
  - *Ran experiments from 10% to 50% malicious patient nodes in the system*
  - increased by 10% each iteration
- Measured the occurrences of a malicious sub-quorum
Robustness Result 1

Figure: Accuracy of quorum member decision with n percent of malicious patients in network.
CONCLUSION
Summary

- We propose PoSH a novel quorum consensus protocol for prescription validation to flag malicious actors and work towards prevention of prescription misuse
- We propose a HIPPA-compliant design enabling security for patient data
- We implemented a full system of our use-case
- Experimentation proves our system’s scalability and robustness
Future Work

• Future work in this area could allow researchers to develop new methods of predicting surges in drug misuse or the flagging of prescribers acting maliciously through machine learning applications.

• Increase ease of access for parties involved to integrate them into the network. We need to try and make Web3.0 technology as close to Web2.0 ease of use as possible.
Questions?


