



Esame di Sicurezza dei Dati

Requirement Analysis Document

Versione	1.0
Data	Anno accademico 2024/2025
Destinatario	Prof. Alfredo De Santis, Prof. Christiancarmine Esposito
Presentato da	Jacopo de Dominicis, Martina Giugliano

ANNO ACCADEMICO 2024/2025

Indice

1	Introduzione	4
1.1	Contesto e Dominio	4
1.2	Obiettivi del Progetto	4
2	Sistema Corrente e Sistema Proposto	6
2.1	Sistema Corrente	6
2.1.1	Limiti dei Sistemi Esistenti	6
2.2	Sistema Proposto	6
2.3	Differenze tra i Sistemi	7
3	Attori e Stakeholder	8
4	Descrizione del Sistema	9
4.1	Requisiti Funzionali	9
4.2	Requisiti Non Funzionali	9
5	Architettura del Sistema	10
5.1	Livelli Architetturali	10
5.1.1	Livello di Presentazione	10
5.1.2	Livello Applicativo	10
5.1.3	Livello Dati	10
5.2	Componenti Principali	11
5.2.1	Frontend Web Application	11
5.2.2	Smart Contract su Fabric	11
5.2.3	Storage Decentralizzato (IPFS)	11
5.2.4	Backend API	11
5.3	Componenti Principali	11
5.4	Flusso di Dati	11
6	Modellazione del Sistema	12
6.1	Scenari di Utilizzo	12
7	Use Cases	13
7.1	UC1 - Creazione Ricetta	13

7.2	UC2 - Visualizzazione Ricette	13
7.3	UC3 - Verifica QR Code	13
7.4	UC4 - Invalidazione Ricetta	13
8	Piano di Sviluppo	15
8.1	Roadmap del Progetto	15
8.2	Strumenti di Sviluppo e Test	16

Capitolo 1

Introduzione

1.1 Contesto e Dominio

Il progetto **MediChain** è finalizzato allo sviluppo di una piattaforma decentralizzata per la gestione, la verifica e l'archiviazione delle ricette mediche, sfruttando la tecnologia blockchain di **Hyperledger Fabric** e il sistema di archiviazione distribuito **IPFS**. L'obiettivo è garantire un sistema **sicuro, trasparente ed efficiente**, eliminando il rischio di frodi, contraffazioni e alterazioni delle prescrizioni mediche.

L'adozione della blockchain assicura **immutabilità e tracciabilità** dei dati, impedendo modifiche non autorizzate alle ricette e garantendo una verifica immediata da parte dei farmacisti. Questo approccio consente a medici, pazienti e farmacisti di interagire in un ambiente affidabile, senza la necessità di intermediari centralizzati e con la sicurezza di una gestione conforme alle normative di protezione dei dati.

La soluzione proposta è particolarmente vantaggiosa per il settore sanitario, dove la **certezza e la sicurezza delle prescrizioni** rappresentano elementi fondamentali per prevenire errori, ridurre i tempi di verifica e migliorare la qualità dell'assistenza. Inoltre, la possibilità di archiviazione decentralizzata su **IPFS** garantisce la disponibilità continua delle ricette senza il rischio di perdita o alterazione dei documenti.

Questo sistema è progettato in particolare per le **piccole ASL locali**, che spesso dispongono di risorse limitate per implementare soluzioni avanzate di gestione digitale delle prescrizioni. MediChain consente loro di adottare una tecnologia innovativa senza la necessità di infrastrutture complesse, offrendo un **processo automatizzato, scalabile e facilmente integrabile** nei sistemi sanitari esistenti.

1.2 Obiettivi del Progetto

L'obiettivo principale del progetto **MediChain** è la creazione di una piattaforma decentralizzata che consenta alle **piccole ASL locali** di gestire, verificare e archiviare digitalmente le ricette mediche sulla **blockchain di Hyperledger Fabric**, garantendo **autenticità, immutabilità e verificabilità**

in un ambiente sicuro e trasparente.

Le ricette mediche saranno archiviate in formato JSON su **IPFS (InterPlanetary File System)**, mentre sulla blockchain verranno registrati solo i dati essenziali, come il **CID IPFS**, l'**ID del paziente** e lo **stato di validità della ricetta**. Questo approccio assicura che le informazioni siano sempre disponibili senza rischio di **manomissione, perdita o falsificazione**.

La piattaforma è progettata per essere **intuitiva e accessibile**, offrendo strumenti semplici per la **creazione, verifica e gestione** delle prescrizioni digitali. Grazie alla sua scalabilità e facilità di adozione, può essere **integrata rapidamente nei sistemi sanitari esistenti**, consentendo a medici, pazienti e farmacisti di interagire in modo sicuro e immediato, riducendo il rischio di errori e migliorando l'efficienza operativa.

Capitolo 2

Sistema Corrente e Sistema Proposto

2.1 Sistema Corrente

Attualmente, la gestione delle prescrizioni mediche è supportata da diversi sistemi digitali adottati a livello nazionale e internazionale. Questi sistemi consentono ai medici di emettere prescrizioni elettroniche che possono essere recuperate dai pazienti presso le farmacie senza la necessità di documenti cartacei. In alcuni casi, sono anche integrati con piattaforme sanitarie nazionali per garantire la tracciabilità delle cure.

Tuttavia, tutti questi sistemi condividono una caratteristica comune: **sono centralizzati**. Le prescrizioni vengono archiviate in database gestiti da enti governativi o provider privati, i quali fungono da intermediari per l'accesso e la verifica dei dati.

2.1.1 Limiti dei Sistemi Esistenti

Nonostante la digitalizzazione abbia migliorato il processo di prescrizione e distribuzione dei farmaci, i modelli centralizzati presentano sfide strutturali che ne limitano l'efficacia. La necessità di intermediari per l'accesso ai dati può rallentare le operazioni, aumentare i costi di gestione e rendere il sistema meno resiliente in caso di guasti o attacchi informatici.

2.2 Sistema Proposto

MediChain introduce un sistema innovativo per la gestione digitale delle prescrizioni mediche, basato su una **blockchain Hyperledger Fabric** e **archiviazione distribuita su IPFS**. Questa infrastruttura **decentralizzata** supera i limiti delle soluzioni centralizzate, offrendo maggiore sicurezza, trasparenza e disponibilità dei dati, senza bisogno di un'autorità centrale.

A differenza dei modelli tradizionali, MediChain registra sulla blockchain le informazioni essenziali delle prescrizioni, come **ID transazione, riferimento IPFS, ID paziente e stato della ricetta**,

rendendole immutabili e verificabili.

Per garantire scalabilità e privacy, il contenuto completo delle ricette non viene memorizzato direttamente sulla blockchain, ma su **IPFS**. Questo sistema di storage distribuito assicura **integrità e disponibilità**, evitando problemi di accessibilità dovuti a guasti dei server. Ogni prescrizione è identificata da un codice univoco (**CID IPFS**), registrato sulla blockchain per garantirne il recupero sicuro in qualsiasi momento.

Il sistema coinvolge tre attori principali: **medico, paziente e farmacista**. Il medico, dopo autenticazione sicura, seleziona il paziente e genera una prescrizione, che viene immediatamente salvata su **IPFS**, mentre le informazioni chiave vengono registrate sulla blockchain. Il paziente può visualizzare le proprie prescrizioni attraverso un'interfaccia dedicata e generare un **QR code** per ogni ricetta. Il farmacista, scannerizzando il codice, recupera i dati dal sistema e verifica la corrispondenza tra le informazioni del paziente e quelle archiviate su IPFS. Dopo la verifica, la blockchain aggiorna lo stato della prescrizione, invalidandola per impedire riutilizzi.

Questa architettura fornisce un **modello decentralizzato, scalabile e sicuro**, che garantisce trasparenza e integrità dei dati, riduce il rischio di frodi e semplifica il processo di prescrizione e verifica. MediChain è ideale per le **piccole ASL locali**, che possono implementare una soluzione digitale avanzata senza investire in infrastrutture complesse, migliorando efficienza e qualità del servizio sanitario.

2.3 Differenze tra i Sistemi

I sistemi attuali per la gestione delle prescrizioni mediche si basano su **infrastrutture centralizzate** gestite da enti governativi o provider privati. Sebbene abbiano portato miglioramenti nella digitalizzazione del processo, presentano ancora criticità legate alla sicurezza, alla trasparenza e all'interoperabilità. MediChain, invece, introduce un **approccio decentralizzato** basato su blockchain e IPFS, eliminando la necessità di un'autorità centrale e garantendo un sistema più sicuro, scalabile e affidabile.

Capitolo 3

Attori e Stakeholder

- **Medico (Org1):** Registra la ricetta e la salva su IPFS. In blockchain vengono salvati il CID IPFS, l'ID del paziente e un flag di validità.
- **Paziente (Org2):** Recupera le proprie ricette e genera un **QR code** per la verifica.
- **Farmacista (Org3):** Scannerizza il QR code, verifica la ricetta con il CID su IPFS e valida la transazione.

Capitolo 4

Descrizione del Sistema

4.1 Requisiti Funzionali

- **RF1 - Creazione ricetta:** Il medico registra una ricetta su IPFS e salva i dati essenziali in blockchain.
- **RF2 - Recupero ricette:** Il paziente può visualizzare le proprie ricette attive.
- **RF3 - Verifica ricetta:** Il farmacista confronta i dati presentati dal paziente con quelli recuperati tramite IPFS.
- **RF4 - Invalida ricetta:** Una volta utilizzata, la ricetta viene invalidata in blockchain.

4.2 Requisiti Non Funzionali

- **Sicurezza:** L'accesso avviene tramite autenticazione **Fabric-CA**.
- **Immutabilità:** Le transazioni registrate non possono essere modificate.
- **Usabilità:** Il sistema deve essere accessibile via interfaccia web e mobile.

Capitolo 5

Architettura del Sistema

Il sistema MediChain è strutturato su tre livelli principali, garantendo una separazione chiara tra l'interfaccia utente, la logica applicativa e la gestione dei dati.

5.1 Livelli Architetturali

5.1.1 Livello di Presentazione

Il livello di presentazione include le interfacce utente attraverso le quali medici, pazienti e farmacisti interagiscono con il sistema:

- **Sito Web per il Medico:** Un'interfaccia web sviluppata in HTML e CSS per la generazione e gestione delle ricette mediche.
- **Applicazione Android per Pazienti e Farmacisti:** Un'app mobile che permette ai pazienti di consultare le proprie ricette e ai farmacisti di verificare le prescrizioni.

5.1.2 Livello Applicativo

Questo livello gestisce la logica del sistema e l'elaborazione dei dati:

- **Smart Contract su Hyperledger Fabric:** Sviluppati in Go, i contratti intelligenti regolano la creazione, verifica e invalidazione delle ricette.
- **Backend API:** Un backend basato su Node.js e Express per gestire operazioni non critiche come notifiche, analisi, reportistica e manipolazione dei dati.

5.1.3 Livello Dati

Il livello dati si occupa dell'archiviazione e della gestione delle prescrizioni mediche:

- **IPFS (InterPlanetary File System):** Le ricette e i relativi metadati vengono memorizzati in modo decentralizzato, garantendo accessibilità e sicurezza.
- **Blockchain Hyperledger Fabric:** I riferimenti ai dati salvati su IPFS vengono registrati nei contratti intelligenti per garantire immutabilità e accessibilità.

5.2 Componenti Principali

5.2.1 Frontend Web Application

La piattaforma web, sviluppata con HTML e CSS, fornisce un'interfaccia intuitiva per la gestione delle prescrizioni da parte del medico.

5.2.2 Smart Contract su Fabric

Gli smart contract, implementati in Go, consentono la gestione decentralizzata delle ricette e comprendono le seguenti funzionalità:

- Emissione delle ricette per i pazienti da parte del medico;
- Controllo delle ricette disponibili per i pazienti;
- Invalidazione delle ricette dopo l'utilizzo in farmacia.

5.2.3 Storage Decentralizzato (IPFS)

Le ricette e i loro metadati vengono archiviati su IPFS, garantendo accesso distribuito e affidabile. L'hash generato viene memorizzato sulla blockchain per garantirne l'integrità.

5.2.4 Backend API

Un backend basato su Node.js e Express viene utilizzato per la gestione di operazioni non critiche, tra cui:

- Notifiche e aggiornamenti agli utenti;
- Analisi e reportistica sulle prescrizioni;
- Manipolazione dei dati per migliorare l'esperienza utente.

5.3 Componenti Principali

- **Smart contract su Fabric:** Gestione delle transazioni di prescrizione.
- **IPFS:** Archiviazione delle ricette in formato JSON.
- **Client Web:** Accesso per medico, paziente e farmacista.

5.4 Flusso di Dati

1. Il medico salva la ricetta su **IPFS** e registra la transazione su blockchain.
2. Il paziente visualizza e condivide la ricetta tramite **QR code**.
3. Il farmacista verifica la ricetta e aggiorna la blockchain.

Capitolo 6

Modellazione del Sistema

6.1 Scenari di Utilizzo

- **Scenario 1:** Un medico prescrive un farmaco e il paziente lo riceve digitalmente. Il farmacista verifica e convalida la transazione.
- **Scenario 2:** Un paziente vuole visualizzare e stampare una ricetta valida.
- **Scenario 3:** Un farmacista verifica un codice QR e segnala una discrepanza.

Capitolo 7

Use Cases

7.1 UC1 - Creazione Ricetta

Nome	Creazione Ricetta
Attori	Medico
Descrizione	Il medico accede al sistema, seleziona il paziente e compila la prescrizione medica, che viene salvata su IPFS e registrata in blockchain.
Precondizioni	Il medico deve essere autenticato nel sistema.
Postcondizioni	La ricetta viene creata e registrata nel sistema.
Flusso Principale	<ol style="list-style-type: none">1. Il medico accede al sistema.2. Seleziona un paziente.3. Compila la prescrizione.4. La ricetta viene salvata su IPFS e registrata in blockchain.

Tabella 7.1: UC1 - Creazione Ricetta

7.2 UC2 - Visualizzazione Ricette

7.3 UC3 - Verifica QR Code

7.4 UC4 - Invalidazione Ricetta

Nome	Visualizzazione Ricette
Attori	Paziente
Descrizione	Il paziente accede al sistema e visualizza le proprie ricette attive.
Precondizioni	Il paziente deve essere autenticato nel sistema.
Postcondizioni	Le ricette attive vengono mostrate all'utente.
Flusso Principale	<ol style="list-style-type: none"> 1. Il paziente accede al sistema. 2. Consulta la lista delle ricette disponibili. 3. Seleziona una ricetta per visualizzarne i dettagli.

Tabella 7.2: UC2 - Visualizzazione Ricette

Nome	Verifica QR Code
Attori	Farmacista
Descrizione	Il farmacista scansiona il QR Code presentato dal paziente e verifica la validità della ricetta confrontando i dati con quelli registrati su IPFS.
Precondizioni	Il paziente deve avere una ricetta attiva e generare un QR Code.
Postcondizioni	La ricetta viene verificata e il farmacista può procedere alla dispensazione del farmaco.
Flusso Principale	<ol style="list-style-type: none"> 1. Il paziente mostra il QR Code. 2. Il farmacista scansiona il codice. 3. Il sistema recupera i dati da IPFS e li confronta con quelli del paziente. 4. Il farmacista conferma la validità della ricetta.

Tabella 7.3: UC3 - Verifica QR Code

Nome	Invalidazione Ricetta
Attori	Farmacista, Sistema Blockchain
Descrizione	Dopo la verifica e l'utilizzo della ricetta, il sistema aggiorna il suo stato su blockchain, invalidandola per evitare riutilizzi.
Precondizioni	La ricetta deve essere stata verificata e utilizzata.
Postcondizioni	La ricetta viene marcata come non più valida.
Flusso Principale	<ol style="list-style-type: none"> 1. Il farmacista conferma l'erogazione del farmaco. 2. Il sistema aggiorna lo stato della ricetta su blockchain. 3. La ricetta non è più disponibile per un nuovo utilizzo.

Tabella 7.4: UC4 - Invalidatione Ricetta

Capitolo 8

Piano di Sviluppo

8.1 Roadmap del Progetto

Fase	Descrizione
Analisi e Pianificazione	Raccolta dei requisiti, definizione degli obiettivi e delle specifiche tecniche del sistema. Identificazione delle tecnologie e dei framework da utilizzare.
Progettazione dell'Architettura	Creazione del modello architetturale del sistema, inclusi i livelli di presentazione, applicazione e dati. Definizione delle interazioni tra i componenti.
Sviluppo Smart Contract	Implementazione degli smart contract in Go su Hyperledger Fabric per la gestione delle prescrizioni mediche. Test iniziali su ambiente di sviluppo.
Sviluppo Frontend e Mobile	Creazione della piattaforma web per i medici e dell'app mobile per pazienti e farmacisti. Implementazione delle funzionalità di interfaccia e accesso ai dati.
Integrazione con IPFS e Blockchain	Configurazione dell'archiviazione decentralizzata su IPFS e registrazione dei riferimenti sulla blockchain per garantire immutabilità e accessibilità.
Testing e Validazione	Verifica del funzionamento complessivo del sistema, simulazione di casi d'uso e correzione di bug. Test di sicurezza e prestazioni.
Deploy e Manutenzione	Rilascio della piattaforma in ambiente di produzione, monitoraggio delle prestazioni e aggiornamenti futuri per migliorare la scalabilità e la sicurezza.

Tabella 8.1: Roadmap del Progetto

8.2 Strumenti di Sviluppo e Test

Strumento	Descrizione
Go & Hyperledger Fabric	Sviluppo degli smart contract per la gestione decentralizzata delle prescrizioni mediche.
IPFS	Archiviazione decentralizzata per conservare in modo sicuro le prescrizioni evitando dipendenze da server centralizzati.
HTML, CSS e JavaScript	Tecnologie per lo sviluppo dell'interfaccia web, rendendola intuitiva e accessibile per medici, pazienti e farmacisti.
Node.js & Express	Backend API per la gestione delle richieste, notifiche e interazione con smart contract e blockchain.
Docker	Containerizzazione dell'ambiente di sviluppo e test per semplificare la gestione delle dipendenze e la distribuzione del sistema.

Tabella 8.2: Strumenti di Sviluppo e Test