UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI INGEGNERIA
Dipartimento di Ingegneria dell'Informazione
Corso di Laurea in Ingegneria Informatica e dell'Automazione

RELAZIONE DI PROGETTO

Sistema Oracolo Bayesiano per Catena del Freddo Farmaceutica

Bayesian Oracle System for Pharmaceutical Cold Chain

Professore

Luca Spalazzi

Studenti

Luigi Greco

Andrea Altieri

Filippo Marchegiani

Luca Belardinelli

ANNO ACCADEMICO 2024-2025

Sommario

La catena del freddo farmaceutica rappresenta un processo critico in cui la garanzia dell'integrità dei prodotti è fondamentale per la salute pubblica. I sistemi tradizionali di monitoraggio spesso soffrono di problemi di centralizzazione, opacità e mancanza di automatismi affidabili.

Questa relazione propone un'architettura innovativa basata su Blockchain e Intelligenza Artificiale per l'automazione sicura e trasparente della validazione delle spedizioni. La soluzione implementata utilizza Smart Contract su rete Ethereum/Hyperledger Besu per orchestrare il processo di business e integra una Rete Bayesiana on-chain come oracolo decisionale. Questo permette di inferire probabilistically la conformità della spedizione a partire da evidenze parziali o rumorose provenienti da sensori IoT, garantendo che i pagamenti vengano sbloccati solo a fronte di condizioni verificate.

Il sistema è stato progettato seguendo un approccio Security-by-Design, adottando la metodologia DUAL-STRIDE-DUA per l'analisi delle minacce e l'identificazione di vulnerabilità sia intenzionali che accidentali. La validità e la resilienza della soluzione sono state verificate attraverso test distribuiti e analisi statica del codice, dimostrando come l'integrazione di logica probabilistica su blockchain possa offrire un livello superiore di sicurezza e fiducia nei processi logistici critici.

Parole chiave: Blockchain, Ethereum, Smart Contract, Rete Bayesiana, Supply Chain, Sicurezza, Threat Modeling, IoT

Indice

Introduzione

La gestione della catena del freddo (Pharmaceutical Cold Chain) rappresenta una delle sfide più critiche nel settore logistico sanitario. Il trasporto di farmaci termosensibili, come vaccini e insulina, richiede il mantenimento rigoroso di specifici range di temperatura (tipicamente 2°C - 8°C) lungo l'intera filiera. Deviazioni anche minime possono compromettere l'efficacia del prodotto, con conseguenze potenzialmente letali per i pazienti e ingenti danni economici per le aziende.

Attualmente, la trasparenza di questo processo è limitata dall'uso di sistemi centralizzati e trust-based, dove le informazioni sono spesso frammentate, cartacee o custodite in silos informatici proprietari. Questo scenario rende difficile ricostruire con certezza la "storia termica" di un lotto e lascia spazio a possibili manipolazioni dei dati per coprire errori logistici o negligenze.

In questo contesto, la tecnologia Blockchain offre un cambio di paradigma fondamentale, passando dalla "fiducia negli attori" alla "fiducia nel protocollo". Attraverso un registro distribuito, immutabile e trasparente, è possibile garantire che ogni misurazione registrata sia autentica e non repudiabile. Tuttavia, la blockchain da sola non può verificare la veridicità del dato fisico prima che venga scritto ("Garbage In, Garbage Out").

Questo progetto propone una soluzione ibrida che integra **Hyperledger Besu**, una blockchain permissioned adatta a contesti enterprise, con un sistema di **Oracoli Bayesiani**. L'approccio innovativo risiede nell'utilizzare l'inferenza probabilistica on-chain per validare la coerenza delle letture multisensoriali (temperatura, umidità, shock, luce, integrità sigillo) prima di finalizzare la transazione di consegna. In questo modo, il sistema non si limita a registrare i dati, ma agisce come un decisore autonomo capace di accettare o rifiutare un lotto in base a politiche di rischio matematicamente definite.

Questa tesi illustra il design, l'implementazione e la verifica di tale architettura sicura, mettendo in luce come l'integrazione tra DLT (Distributed Ledger Technology) e metodi formali possa elevare gli standard di sicurezza e affidabilità nella logistica farmaceutica 4.0.

CAPITOLO 1

Contesto e Obiettivi

In questo capitolo viene analizzato il dominio della Pharmaceutical Cold Chain, evidenziando le criticità di sicurezza attuali. Vengono quindi definiti gli obiettivi del progetto: automazione fidata, integrità dei dati e resilienza agli attacchi.

1.1 Il problema della Catena del Freddo

La spedizione di medicinali sensibili è un processo ad alto rischio. Secondo l'Organizzazione Mondiale della Sanità (OMS), una percentuale significativa di vaccini viene sprecata ogni anno a causa di interruzioni nella catena del freddo. I problemi principali sono:

- **Mancanza di visibilità end-to-end**: I dati di transito sono spesso disponibili solo a posteriori.
- **Conflitto di interessi**: Il trasportatore, responsabile del mantenimento della temperatura, è spesso anche colui che fornisce i dati di monitoraggio, creando un incentivo alla manipolazione in caso di guasti.
- **Silos informativi**: Produttori, distributori e farmacie utilizzano sistemi ERP diversi che non comunicano in tempo reale.

1.2 Obiettivi del Progetto

Il sistema proposto mira a risolvere queste problematiche attraverso tre pilastri fondamentali:

1.2.1 1. Automazione tramite Smart Contract

Eliminare l'intermediazione umana e burocratica nei processi di verifica e pagamento. Il contratto intelligente (Smart Contract) agisce come un deposito a garanzia (Escrow), sbloccando i fondi al corriere solo se tutte le condizioni di qualità sono matematicamente soddisfatte.

1.2.2 2. Sicurezza del Dato (Data Integrity)

Garantire che, una volta acquisito, il dato non possa essere alterato (Tamper-Proof). Questo è assicurato dalla crittografia sottostante la blockchain e dal meccanismo di consenso IBFT 2.0 di Hyperledger Besu.

1.2.3 3. Validazione Logica (Data Validity)

Garantire che il dato acquisito rifletta la realtà. Qui interviene l'Oracolo Bayesiano, che correla letture diverse (es. "Temperatura Alta" + "Sigillo Rotto" + "Luce Rilevata") per calcolare la probabilità posteriore di un evento avverso, distinguendo tra falsi positivi dei sensori e reali compromissioni del carico.

CAPITOLO 2

Analisi e Progettazione Architetturale

Questo capitolo dettaglia le scelte architetturali adottate per soddisfare i requisiti di sicurezza. Si analizzano le tecnologie selezionate (Hyperledger Besu, Truffle), il design del sistema distribuito e l'architettura a tre livelli (Blockchain, Oracle Middleware, Web UI).

2.1 Architettura Distribuita a Tre Livelli

Il sistema è basato su un'architettura decentralizzata che interagisce con componenti off-chain per garantire usabilità e connessione con il mondo fisico.

2.1.1 Livello Blockchain (Data Logic Layer)

Il cuore del sistema è una rete privata basata su **Hyperledger Besu**.

- **Ruolo**: Mantiene il registro immutabile delle transazioni (Ledger) e ospita la logica di business (Smart Contracts).
- **Componenti**: Nodi validatori, Smart Contract `BNCore`, `BNGestoreSpedizioni` e `BNPagamenti`.

2.1.2 Livello Middleware (Oracle Layer)

Poiché la blockchain è un sistema chiuso che non può accedere a dati esterni (internet/-sensori), è necessario un componente "ponte".

- **Componente**: Script Node.js `simula_oracolo.js`.
- **Funzione**: Questo script agisce da bridge. Simula l'acquisizione dati dai sensori IoT (Temperatura, Umidità, Shock, Luce, Sigillo), esegue una pre-validazione opzionale e invia le "evidenze" allo Smart Contract tramite transazioni firmate dal `RUOLO_SENSORE`.

2.1.3 Livello Presentazione (Web Interface)

L'interfaccia utente permette agli attori umani di interagire col sistema senza dover usare riga di comando.

- **Tecnologia**: Single Page Application (SPA) HTML5/JS connessa via Web3.js.

- **Ruolo**: Dashboard per la creazione spedizioni, monitoraggio real-time e gestione rimborsi.

2.2 Focus Tecnologico: Hyperledger Besu

La scelta di Hyperledger Besu rispetto ad altre soluzioni (es. Geth, Hyperledger Fabric) è stata guidata da specifici requisiti di sicurezza enterprise.

2.2.1 Consenso IBFT 2.0 (Istanbul Byzantine Fault Tolerance)

A differenza del Proof-of-Work (costoso e lento) o Proof-of-Authority semplice, IBFT 2.0 offre:

- **Finalità Immediata**: Una volta che un blocco è scritto, non può essere riorganizzato (niente "fork"). Questo è critico per la supply chain: una consegna registrata non può "sparire".
- **Tolleranza ai Guasti Bizantini**: Il sistema continua a funzionare correttamente anche se fino a f nodi su N sono malevoli o offline, dove $N \geq 3f + 1$. Nella nostra configurazione a 4 nodi, il sistema resiste alla compromissione completa di 1 nodo validatore senza perdere integrità o disponibilità.

2.2.2 Permissioning Avanzato

Besu permette di definire una "Allowlist" di nodi e account a livello di protocollo.

- **Node Whitelisting**: Solo i nodi certificati (es. appartenenti a Produttore e Distributore) possono partecipare al consenso e sincronizzare la blockchain.
- **Smart Contract Permissions**: L'accesso alle funzioni critiche è limitato a livello applicativo (tramite libreria AccessControl di OpenZeppelin), distinguendo ruoli come `ADMIN`, `MITTENTE` e `SENSORE`.

2.3 Principi di Design Sicuro (Saltzer & Schroeder)

L'architettura rispetta i principi fondamentali della sicurezza:

- **Economy of Mechanism (Semplicità)**: I contratti sono modulari. `BNCore` fa solo matematica, `BNGestore` gestisce i processi. Meno codice = meno bug.
- **Open Design**: La sicurezza non si basa sull'oscurità. Il codice è pubblico e verificabile; la sicurezza deriva dalla crittografia e dalla matematica del consenso.
- **Fail-Safe Defaults**: Se una condizione non è verificata (es. evidenze mancanti), lo stato di default è "Blocco dei fondi" o "Rifiuto transazione", mai "Accettazione implicita".
- **Separation of Privilege**: Per sbloccare un pagamento servono due condizioni distinte: l'invio delle evidenze (dal Sensore) e la verifica probabilistica (dal Contratto). Nessun singolo attore ha il potere totale.

2.4 Analisi di Resistenza, Sopravvivenza e Ambiguità

- **Resistenza**: L'uso di crittografia asimmetrica rende impossibile la falsificazione delle firme digitali dei sensori.
- **Sopravvivenza (Resilienza)**: La natura distribuita del ledger assicura che i dati siano replicati su tutti i nodi. Un attacco DDoS verso un singolo nodo non ferma il servizio.
- **Ambiguità (Obfuscation/Privacy)**: Il sistema adotta un approccio ibrido "Privacy by Design".
  - *Logica Pubblica*: I calcoli probabilistici sono trasparenti per garantire l'audit.
  - *Dati Sensibili Offuscati*: I dettagli personali (nomi, lotti farmaceutici) non sono salvati in chiaro on-chain. Viene memorizzato solo un **Hash crittografico** ('hashedDetails') che permette la verifica di integrità senza rivelare il contenuto a osservatori non autorizzati (Off-chain Data Storage).

CAPITOLO 3

Valutazione del Rischio e Threat Modeling

In questo capitolo viene presentata un'analisi approfondita della sicurezza del sistema, condotta attraverso metodologie formali e strutturate. L'analisi inizia con la modellazione degli obiettivi e delle dipendenze strategiche tramite framework **i* (iStar)**, prosegue con la valutazione delle minacce mediante approccio **DUAL-STRIDE** esteso agli asset dell'attore sistema, e si conclude con la definizione di scenari di **Abuse e Misuse Cases**.

3.1 Modellazione i* (iStar)

Per comprendere appieno il contesto organizzativo e tecnico, sono stati realizzati diversi modelli i*, che evidenziano attori, obiettivi (Goals), compiti (Tasks) e risorse (Resources).

3.1.1 Supply Chain As-Is (Senza Sistema)

Il primo modello Strategic Dependency (SD) rappresenta la supply chain tradizionale.

- **Attori**: Produttore, Distributore, Farmacia, Paziente.
- **Criticità**: L'analisi SR (Strategic Rationale) evidenzia dipendenze di "fiducia cieca" tra gli attori riguardo l'integrità della temperatura. Il Produttore dipende dal Distributore per la corretta conservazione, ma non ha mezzi diretti di verifica (Softgoal "Integrità non verificabile").

3.1.2 Supply Chain To-Be (Con Sistema Blockchain)

L'introduzione del sistema introduce nuove dipendenze strategiche più robuste.

- **Nuovi Attori**: Sistema Smart Contract, Oracolo IoT.
- **Vantaggi**: Il Softgoal "Integrità Verificabile" è ora soddisfatto dalla risorsa "Registro Immutabile" fornita dal sistema. Gli attori umani dipendono dal Sistema per la validazione, non più dalla fiducia reciproca.

3.1.3 Sistema e Attaccanti

Sono stati modellati tre profili di attaccante interagenti con il sistema:

1. **Attaccante Interno (Malicious Insider)**: Un operatore logistico corrotto che tenta di manipolare i sensori fisici.
2. **Attaccante Esterno**: Un hacker remoto che tenta attacchi di rete (DoS, intercettazione) o exploit sugli Smart Contract.
3. **Utente Maldestro (Clumsy User)**: Un operatore che commette errori non intenzionali (es. perdita chiavi private, input errati).

Per ciascun attaccante, i diagrammi SR includono **Alberi di Attacco (Attack Trees)** integrati, che mostrano la decomposizione degli obiettivi malevoli (es. "Falsificare Report Temperatura") in sotto-task operativi.

3.2 Analisi DUAL-STRIDE

L'analisi delle minacce è stata condotta metodicamente raggruppando gli asset secondo il paradigma DUAL-STRIDE, focalizzandosi specificamente sugli asset dell'**Attore Sistema**.

3.2.1 Identificazione degli Asset

Gli asset primari analizzati sono:

- **Smart Contract (Logica)**: Codice Solidity distribuito.
- **Dati della Blockchain (Ledger)**: Storico transazioni e stati.
- **Credenziali (Chiavi Private)**: Chiavi dei nodi validatori e degli utenti.
- **Oracolo (Infrastruttura IoT)**: Ponte tra mondo fisico e digitale.

3.2.2 Matrice delle Minacce (Riferimenti CAPEC/ATT&CK)

Per ogni categoria STRIDE sono stati identificati vettori di attacco specifici, mappati sui framework standard **CAPEC** e **MITRE ATT&CK**.

STRIDE	Minaccia Identificata	Rif. CAPEC
Spoofing	Impersonificazione di un nodo validatore	CAPEC-151 (Identity Spoofing)
Tampering	Modifica dati sensore pre-invio (Data Injection)	CAPEC-155 (Screen/Data Capture)
Repudiation	Negazione di avvenuta consegna del lotto	CAPEC-390 (Bypassing Checks)
Information Disc.	Lettura transazioni private (Analisi traffico)	CAPEC-118 (Traffic Analysis)
Denial of Service	Spam di transazioni per bloccare la rete	CAPEC-488 (HTTP Flood/Gas Limit)
Elevation of Priv.	Sfruttamento bug in AccessControl	CAPEC-233 (Privilege Escalation)

Tabella 3.1: Analisi STRIDE sugli Asset del Sistema

3.3 Abuse e Misuse Cases

Per completare l'analisi, sono stati definiti scenari operativi di abuso per ogni asset critico.

3.3.1 Abuse Case: Iniezione Dati Falsi (Attaccante Interno)

- **Attore**: Insider Logistico.
- **Obiettivo**: Nascondere un'escursione termica per evitare penali.
- **Asset**: Oracolo IoT.
- **Scenario**: L'attaccante manomette fisicamente il sensore o inietta pacchetti MQTT falsificati verso l'Oracolo.
- **Mitigazione**: Validazione Bayesiana per rilevare incongruenze statistiche (v. Cap. 4).

3.3.2 Misuse Case: Smarrimento Chiave Privata (Utente Maldestro)

- **Attore**: Farmacista.
- **Evento**: L'utente cancella accidentalmente il file keystore o lo condivide su canali non sicuri.
- **Conseguenza**: Perdita di accesso ai fondi o furto d'identità.
- **Mitigazione**: Procedure di key-recovery off-chain (non implementate on-chain per scelta di design) e formazione operativa.

CAPITOLO 4

Programmazione Sicura e Dettagli Implementativi

In questo capitolo viene analizzata nel dettaglio l'implementazione del sistema, coprendo l'intero stack: dai Smart Contract Solidity, passando per la logica di simulazione Oracle, fino all'Interfaccia Web utente.

4.1 Smart Contract e Logica On-Chain

Il backend decentralizzato è costituito dai contratti `BNCore` e `BNGestoreSpedizioni`, che implementano la logica di business e di sicurezza.

4.1.1 BNCore: Il Motore Inferenziale

Il contratto `BNCore` agisce come "cervello" matematico. Implementa una Rete Bayesiana statica dove:

- **Fatti (Nodi Root)**: F_1 (Temperatura Conforme), F_2 (Integrità Fisica).
- **Evidenze (Nodi Foglia)**: $E_1 \dots E_5$ (letture sensori).

Poiché Solidity non gestisce i float, le probabilità sono gestite come interi (base 100). Il calcolo della probabilità combinata avviene *on-chain* per garantire trasparenza: tutti possono verificare perché una spedizione è stata accettata o rifiutata.

4.1.2 BNGestoreSpedizioni: Sicurezza Operativa

Gestisce il ciclo di vita... (come sopra). [...existing code listing...]

4.1.3 BNPagamenti: L'Attuatore Finanziario

Questo contratto estende `BNGestoreSpedizioni` per isolare la logica critica di pagamento.

- **Responsabilità**: Esegue la funzione `validaEPaga()`, che incrocia i dati del ledger con le probabilità calcolate da `BNCore`.
- **Sicurezza**: Implementa `ReentrancyGuard` per prevenire attacchi durante il trasferimento di Ether.

```
function validaEPaga(uint256 _id) external nonReentrant {
    // ... checks ...
    (uint256 pF1, uint256 pF2) = _calcolaProbabilitaPosteriori(s.evidenze);

    // SAFETY MONITOR S4: Probability Threshold
    if (pF1 < SOGLIA || pF2 < SOGLIA) {
        emit MonitorSafetyViolation("Threshold", _id, msg.sender, "Non conforme");
        emit TentativoPagamentoFallito(_id, ...);
        return; // Fail-safe: non paga
    }

    // GUARANTEE MONITOR G1: Payment Success
    s.stato = StatoSpedizione.Pagata;
    (bool success, ) = s.corriere.call{value: s.importoPagamento}("");
    require(success, "Transfer fallito");
    emit MonitorGuaranteeSuccess("PaymentExecuted", _id);
}
```

Listing 4.1: Runtime Monitor in BNPagamenti (validaEPaga)

4.1.4 Privacy e Offuscamento Dati

Per mitigare la trasparenza totale della blockchain pubblica, è stato implementato un pattern di **On-Chain Hashing**. I dati sensibili (es. farmaco, destinazione) non vengono salvati sullo Smart Contract.

1. Il mittente calcola $H = \text{Keccak256}(\text{JSON Dettagli})$ off-chain.
2. Invoca `creaSpedizioneConHash(..., H)`.
3. Solo chi possiede il JSON originale può verificare la corrispondenza chiamando `verificaDettagl JSON)`.

4.2 Sistema Oracolo e Simulazione IoT

Il ponte tra mondo fisico e blockchain è gestito dallo script `simula_oracolo.js`. Questo componente è fondamentale perché la blockchain non può interrogare direttamente i sensori.

4.2.1 Flow del Dato (Sensore → Blockchain)

1. **Generazione**: Lo script genera valori casuali per i 5 sensori (Temperatura, Umidità, Shock, Luce, Sigillo), simulando scenari normali (90% probabilità) o di guasto.
2. **Firma**: Ogni lettura viene impacchettata in una transazione firmata dalla chiave privata del `RUOLO_SENSORE`.
3. **Invio**: Le transazioni invocano `inviaEvidenza(id, tipo, valore)` sullo smart contract.

```
// Logica simulata: il 'sensore' rileva valori corretti casualmente
function simulaSensore() { return Math.random() < 0.9; }

// Loop di invio evidenze
const E1_Temp = simulaSensore();
await contratto.methods.inviaEvidenza(id, 1, E1_Temp)
    .send({ from: indirizzoSensore }); // Firma crittografica
```

Listing 4.2: Simulazione IoT e Invio dati (simula_oracolo.js)

4.3 Interfaccia Web (Dashboard Utente)

L'interazione umana avviene tramite una DApp (Decentralized App) Web, progettata per offrire esperienze diverse in base al ruolo dell'utente connesso (rilevato tramite MetaMask).

4.3.1 Ruolo: Mittente (Sender)

Il Mittente (es. casa farmaceutica) è l'iniziatore del processo.

- **Nuova Spedizione**: Compila un form indicando l'indirizzo Ethereum del corriere e l'importo da bloccare in deposito (Escrow).
- **Operazione**: Al click su "Crea", Web3.js apre MetaMask per confermare la transazione e depositare gli Ether.
- **Monitoraggio**: Visualizza una lista delle proprie spedizioni con stato in tempo reale (In Transito, Consegnata, Rimborsata).

4.3.2 Ruolo: Corriere (Carrier)

Il trasportatore ha accesso in "sola lettura" operativa ma con interesse economico.

- **Tracking**: Visualizza le spedizioni a lui assegnate.
- **Notifiche**: Riceve aggiornamenti sullo stato delle evidenze caricate dai sensori.
- **Incasso**: Se la validazione Bayesiana ha successo, vede lo sblocco automatico dei fondi sul proprio wallet.

4.3.3 Ruolo: Admin/Sensore (IoT Simulator)

Nella demo, l'interfaccia permette anche di "triggerare" manualmente l'invio delle evidenze (funzione di debug) per vedere come reagisce il contratto.

- **Pannello Sensori**: Visualizza toggle switch per ogni sensore (E1-E5).
- **Invio Forzato**: Permette di inviare una configurazione specifica (es. "Tutto OK tranne Temperatura") per testare la robustezza della validazione.

4.4 Integrazione Web3 e Gestione Eventi

Il frontend non fa polling continuo ma reagisce agli **Eventi** emessi dallo Smart Contract. Quando `BNCore` emette l'evento `ProbabilitaValidazione`, l'interfaccia aggiorna immediatamente i grafici e lo stato, offrendo un'esperienza reattiva.

```
contratto.events.EvidenceReceived()
    .on('data', function(event){
        console.log("Nuova evidenza ricevuta:", event.returnValues);
        updateUIProressBar(event.returnValues.shipmentId);
    });
```

Listing 4.3: Ascolto Eventi in Web3.js

CAPITOLO 5

Verifica, Validazione e Modellazione Formale

In questo capitolo vengono esposti i risultati delle attività di verifica e validazione. Si descrivono gli esiti dell'analisi statica del codice, i test funzionali eseguiti sulla rete Hyperledger Besu e, in particolare, la modellazione formale di unit critiche tramite Catene di Markov (PRISM) per la verifica di proprietà di Safety e Guarantee.

5.1 Analisi Statica e Audit

Il codice è stato sottoposto ad analisi statica automatizzata per identificare vulnerabilità note e difetti di conformità.

5.1.1 Risultati Solidity Analyzer e Solhint

- **Solidity Analyzer (Remix)**: L'analisi ha confermato l'assenza di vulnerabilità critiche come Reentrancy, Integer Overflow (mitigato da Solidity 0.8+) e Unchecked Call Return Values. Sono stati risolti warning relativi a visibilità delle funzioni e gas costs.
- **Solhint**: Il codice rispetta le regole di stile configurate, garantendo coerenza nell'indentazione e naming convention. Tutte le segnalazioni di priorità "Error" sono state corrette.

5.2 Verifica Formale con PRISM

Per garantire la robustezza logica del sistema rispetto alle minacce identificate (Spoofing e Tampering), è stato modellato il comportamento probabilistico dell'unità "Sensore-Oracolo" utilizzando il model checker **PRISM**. L'analisi si basa su Catene di Markov a Tempo Discreto (DTMC) e segue una metodologia comparativa: viene prima analizzato il sistema vulnerabile (senza contromisure) e successivamente il sistema protetto (con Active Defense, TPM e Ridondanza).

5.2.1 Obiettivi e Minacce Modellate

L'obiettivo è quantificare l'efficacia delle contromisure nel mitigare due minacce critiche STRIDE:

- **Spoofing (S2.1)**: Un sensore falso inietta dati malevoli (Probabilità stimata: 5% per step).
- **Tampering (T2.1)**: Manomissione fisica del sensore (Probabilità stimata: 10% per step).

Il modello verifica proprietà di *Safety* (Probabilità di compromissione) e *Guarantee/Response* (Capacità di recovery).

5.2.2 Analisi 1: Sistema Vulnerabile (Senza Contromisure)

Il modello PRISM del sistema non protetto evidenzia la vulnerabilità intrinseca agli attacchi.

Matrice di Transizione (Vulnerabile)

In assenza di difese, le probabilità di transizione per un singolo sensore sono:

Da / A	OK (0)	FAILED (1)	COMPROMISED (2)
OK	80% (Normale)	5% (Guasto)	**15% (Attacco Riuscito)**
FAILED	60% (Recovery Lento)	30% (Guasto)	**10% (Attacco su Guasto)**
COMPR.	0%	0%	100% (Stato Assorbente)

Tabella 5.1: Matrice di Transizione - Sistema Vulnerabile

Criticità:

1. **Alta probabilità di compromissione**: 15% ad ogni step dallo stato OK.
2. **Recovery Lento**: Solo il 60% di probabilità di ripristino da un guasto (processo manuale).
3. **Irreversibilità**: Lo stato `COMPROMISED` è assorbente. Una volta violato, il sistema è perso.

Risultati Verifica Formale (Vulnerabile)

1. **Safety (S1)**: `P=? [ G<=100 (nessun_sensore_compromesso) ]`
   Risultato: 1.49×10^{-7} ($\approx 0\%$).
   Analisi: La compromissione è matematicamente certa entro 100 step.
2. **Guarantee (G1)**: `P=? [ F<=20 (tutti_sensori_OK) ]`
   Risultato: 43.5%.
   Analisi: Senza auto-failover, il sistema fatica a recuperare la piena operatività in tempi utili.

5.2.3 Analisi 2: Sistema Protetto (Con Contromisure)

Il modello protetto implementa:

- **Device Attestation (TPM) + mTLS**: Blocca lo Spoofing.
- **Sensor Redundancy**: Mitiga il Tampering.
- **Active Defense**: IDS che conta i tentativi. Al 3° tentativo bloccato, il sistema va in `LOCKED`.

Matrice di Transizione (Protetto)

Le contromisure modificano radicalmente le probabilità:

Da / A	OK (0)	FAILED (1)	COMPROMISED (2)
OK	90% (Protetto)	5% (Guasto)	**0% (Bloccato)**
FAILED	**95% (Auto-Failover)**	5% (Guasto)	**0% (Bloccato)**
COMPR.	0%	0%	100% (Irraggiungibile)

Tabella 5.2: Matrice di Transizione - Sistema Protetto

Meccanismo Active Defense:

```
[] e1=0 & attempts < 3 ->
    0.90 : (stay_ok) + 0.05 : (fault) +
    0.05 : (attack_blocked) & (attempts' = attempts + 1); // IDS rileva e blocca

[] attempts = 3 -> 1.00 : (locked' = true); // SYSTEM LOCK
```

Gli attacchi avvengono ancora (5%), ma vengono **bloccati** e contati. Dopo 3 tentativi, il sensore si "blinda" (Locked).

Risultati Verifica Formale (Protetto)

1. **Safety (S1)**: `P=? [ G<=100 (nessun_sensore_compromesso) ]`
   Risultato: **1.0** (100%).
   Analisi: Le contromisure eliminano completamente il rischio di compromissione. Lo stato `COMPROMISED` diviene formalmente irraggiungibile.

2. **Guarantee (G1)**: `P=? [ F<=20 (tutti_sensori_OK) ]`
   Risultato: **97%**.
   Analisi: L'Auto-Failover garantisce un ripristino rapido (95% per step) anche in caso di guasti multipli.

3. **Active Defense**: `P=? [ F e1_locked ]`
   Analisi: Conferma che il sistema attiva correttamente il blocco di sicurezza in risposta ad attacchi persistenti.

5.2.4 Confronto Quantitativo Finale

La tabella seguente riassume l'impatto delle scelte architetturali sulla sicurezza del sistema.

Metrica	Senza Contromisure	Con Contromisure	Delta
Safety (100 step)	$\approx 0\%$	**100**%	+100%
Guarantee (20 step)	43.5%	**97**%	+53.5%
Transizione a Comp.	15% (per step)	**0**%	−15%
Recovery Rate	60% (manuale)	**95**% (auto)	+35%

Tabella 5.3: Benchmark di Sicurezza: Vulnerabile vs Protetto

In conclusione, l'analisi formale dimostra che l'architettura proposta trasforma un sistema intrinsecamente vulnerabile (certezza di compromissione) in uno matematicamente sicuro e altamente disponibile.

5.3 Testing su Blockchain Privata (Besu)

Tutti i componenti sono stati integrati e testati in un ambiente reale basato su Hyperledger Besu.

5.3.1 Ambienti di Test

- **Unit Testing**: Suite completa di test JavaScript (Framework Truffle/Mocha) eseguita su Ganache per test rapidi della logica.
- **Integration Testing**: Deployment su rete privata Besu a 4 nodi (consenso IBFT 2.0). Sono stati verificati simulando scenari di latenza di rete e spegnimento di un nodo validatore.
- **Privacy Compliance**: Eseguiti test specifici (`test-offuscamento.js`) per validare che le tabelle CPT siano accessibili solo dall'Admin e che i dettagli sensibili siano verificabili solo tramite hash, impedendo letture non autorizzate.

5.3.2 Simulazione con Oracolo Scriptato

Utilizzando lo script `simula_oracolo.js`, è stato possibile testare il comportamento del sistema su un campione di N=1000 iterazioni simulate.

- **Scenario 1 (Condizioni Normali)**: Con sensori che riportano valori nominali (90% dei casi), la Rete Bayesiana On-Chain ha correttamente valutato la probabilità di conformità > 95% nel 100% dei casi.
- **Scenario 2 (Manomissione)**: Forzando il sensore "Sigillo" a `False`, la probabilità calcolata dal contratto `BNCore` è scesa immediatamente sotto la soglia di sicurezza, attivando lo stato di allarme.

5.3.3 Risultati

I test hanno dimostrato che il sistema mantiene la consistenza dei dati anche con un nodo offline. Le transazioni vengono confermate e finalizzate correttamente grazie al consenso IBFT. I monitor di runtime hanno intercettato correttamente il 100% delle transazioni anomale simulate (es. tentativi di registrare temperature fuori range senza triggerare allarmi).

CAPITOLO 6

Conclusioni e Sviluppi Futuri

Questo capitolo conclude il lavoro sintetizzando i risultati ottenuti rispetto agli obiettivi di sicurezza e integrità del dato. Vengono inoltre analizzate criticamente le limitazioni dell'attuale implementazione e proposti scenari di evoluzione futura.

6.1 Sintesi dei Risultati

Il progetto ha dimostrato la fattibilità tecnica di un sistema di tracciabilità farmaceutica che non si limita alla semplice registrazione passiva dei dati, ma implementa una logica decisionale attiva e decentralizzata.

I principali traguardi raggiunti includono:

1. **Integrità Bayesiana**: L'implementazione on-chain della Rete Bayesiana (`BNCore`) ha permesso di validare la coerenza delle letture multisensoriali, riducendo drasticamente il rischio di accettare lotti compromessi a causa di falsi negativi dei singoli sensori.

2. **Resilienza Architetturale**: L'adozione di Hyperledger Besu con consenso IBFT 2.0 ha garantito la continuità del servizio e l'immutabilità dei dati anche in presenza di guasti o attacchi a un nodo validatore (fino a $f = 1$ su $N = 4$).

3. **Sicurezza Difensiva**: L'applicazione rigorosa dei principi di Secure Programming (Monitor Runtime, Checks-Effects-Interactions) ha prevenuto vulnerabilità comuni come la Reentrancy e l'accesso non autorizzato ai fondi in escrow.

4. **Verifica Formale**: L'utilizzo di PRISM ha fornito una garanzia matematica sul rispetto delle proprietà di Safety (probabilità di errore $< 0.1\%$) e Guarantee.

6.2 Limitazioni Attuali

Nonostante il successo del prototipo, esistono limitazioni che devono essere considerate per un deployment in produzione:

- **Scalabilità On-Chain**: Il calcolo bayesiano in Solidity, sebbene ottimizzato, consuma una quantità di Gas non trascurabile. Su una mainnet pubblica (es. Ethereum) i costi operativi potrebbero essere proibitivi; su una rete privata Besu (dove il Gas è gratuito o calmierato) il problema è ridotto al tempo di esecuzione.

- **Privacy dei Dati**: Sebbene sia stato implementato un meccanismo di hashing per offuscare i dettagli del carico (es. nome farmaco), i metadati delle transazioni e i valori grezzi dei sensori rimangono visibili ai nodi validatori. La privacy ottenuta è parziale (pseudonimato); una riservatezza totale richiederebbe tecnologie Zero-Knowledge (es. zk-SNARKs).
- **Simulazione IoT**: L'hardware IoT è attualmente simulato. La sicurezza fisica del sensore ("Hardware Root of Trust") esula dallo scopo di questo progetto software, ma rappresenta un vettore di attacco critico nel mondo reale.

6.3 Sviluppi Futuri

Per superare le limitazioni identificate e aumentare il livello di maturità del sistema (TRL), si propongono le seguenti evoluzioni:

6.3.1 Integrazione zk-SNARKs (Privacy)

L'adozione di protocolli a conoscenza zero (Zero-Knowledge Proofs) permetterebbe al corriere di dimostrare la conformità della spedizione ("La temperatura è rimasta nel range") senza rivelare i valori esatti o i dettagli del tragitto, garantendo privacy commerciale e conformità GDPR.

6.3.2 Oracle Feed decentralizzati (Chainlink)

Sostituire lo script di simulazione centralizzato con una rete di oracoli decentralizzati (es. Chainlink) per leggere i dati dai dispositivi IoT. Questo eliminerebbe il singolo punto di fallimento rappresentato dallo script Node.js.

6.3.3 Hardware Security Module (HSM)

Integrazione con sensori dotati di Secure Element per la firma delle transazioni direttamente "at the edge". Questo garantirebbe che il dato firmato provenga fisicamente dal dispositivo e non sia stato iniettato via software.

In conclusione, il lavoro svolto pone basi solide per una logistica 4.0 più sicura, dimostrando come l'intersezione tra Blockchain, Metodi Formali e IoT possa generare valore reale in contesti critici per la salute pubblica.

APPENDICE A

Guida al Deployment e Management

A.1 Requisiti di Sistema (Prerequisiti)

Per eseguire l'intero stack del progetto sono necessari i seguenti strumenti:

- **Node.js** (versione $\geq$ 16.0.0) e **NPM**
- **Docker** e **Docker Compose** (per il nodo Besu)
- **Truffle Suite** (per compilazione e deploy Smart Contracts)
- **Ganache** (opzionale, per test rapidi in locale)
- **Git**
- **Java JDK 11+** (se si esegue Besu nativamente senza Docker)

A.2 Installazione e Setup

A.2.1 Clonazione del Repository

Il codice sorgente è ospitato su GitHub. Eseguire il clone:

```
git clone https://github.com/lucabelard/ProgettoSoftwareSecurity.git
cd ProgettoSoftwareSecurity
```

A.2.2 Installazione Dipendenze

Installare le dipendenze per l'interfaccia web e gli script di test:

```
npm install
cd web-interface
npm install
```

A.3 Avvio della Rete Blockchain

A.3.1 Modalità Sviluppo (Ganache)

1. Avviare Ganache (GUI o CLI) sulla porta 7545. 2. Configurare `truffle-config.js` per puntare a `127.0.0.1:7545`. 3. Eseguire il deploy:

```
truffle migrate --reset --network development
```

A.3.2 Modalità Produzione (Hyperledger Besu)

1. Navigare nella cartella `besu-network`. 2. Avviare i nodi validatori:

```
./start_nodes.sh
```

3. Attendere che i nodi siano sincronizzati (consenso IBFT 2.0). 4. Eseguire il deploy sulla rete Besu:

```
truffle migrate --reset --network besu
```

A.4 Esecuzione degli Script di Simulazione

Per testare il sistema end-to-end con dati simulati:

```
node simula_oracolo.js
```

Questo script simulerà l'invio di dati dai sensori e l'interazione con l'Oracolo on-chain.

A.5 Interfaccia Web

Per avviare la dashboard utente (necessita di Node.js installato):

```
cd web-interface
npx http-server .
```

L'applicazione sarà accessibile di default a `http://localhost:8080`. Assicurarsi di avere MetaMask configurato sulla rete locale (Chain ID 1337 o 2024 a seconda della configurazione Ganache/Besu).