

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



GreenProof
Sustainable Food Supply Chain

Supervisore

Prof. Luca Spalazzi

Autori

Loris Bottegoni
Leonardo Cambiotti
Valerio Crocetti
Angelo Kollcaku
Alex Voltattorni

Indice

1	Introduzione	1
1.1	Funzionamento della supply chain	1
1.2	Introduzione ai capitoli successivi	2
2	Valutazione del Rischio	3
2.1	Diagrammi i*	3
2.1.1	SD/SR ruoli supply chain senza sistema	3
2.1.2	SD/SR ruoli supply chain più sistema	4
2.1.3	SD/SR sistema e attaccanti con alberi di attacco	5
2.2	Tabella Dual_Stride	7
2.3	Abuse Case	19
2.4	Misuse Case	36
3	Design Sicuro	39
3.1	Architettura	39
3.2	Design degli asset	40
3.2.1	Sommerville	40
3.2.2	OWASP	41
3.2.3	Saltzer & Schroeder	41
3.3	Scelte tecnologiche	41
3.4	Modellazione mediante Markov chain di una unità	45
3.4.1	Markov Chain della funzione di login	45
3.4.2	Implementazione della funzione di login in PRISM	46
3.4.3	Verifica di una proprietà di Safety	50
3.4.4	Verifica di una proprietà di Response	51
3.4.5	Realizzazione dei monitor di Runtime Enforcement	52
4	Programmazione Sicura	54
4.1	Programmazione off-chain	54
4.2	Programmazione on-chain	55
4.2.1	GreenToken	55
4.2.2	EmissionTracker	56

5 Deployment	60
5.1 Prerequisiti	60
5.2 Installazione e Configurazione	61
5.3 Configurazione dopo l'avvio del sistema	62
5.4 Compatibilità con i Sistemi Operativi	63
5.4.1 Windows	63
5.4.2 Linux	63
5.4.3 macOS	63
5.5 Interfacce	63
5.5.1 Home Interface	64
5.5.2 Registration and Login	66
5.5.3 Manage User Account	69
5.5.4 Manage Company for Administrator Account	71
5.5.5 Interfaces for System Admin	79
5.5.6 Information about Company	80
5.5.7 Information about Product	82

Elenco delle figure

1.1 Sustainable Food Supply Chain	1
2.1 SD/SR ruoli supply chain senza sistema	5
2.2 SD/SR ruoli supply chain più sistema	6
2.3 SD/SR sistema e attaccanti con alberi di attacco	7
3.1 Database Schema	42
3.2 Markov chain relativo alla funzione di login	46
3.3 Simulazione del sistema da parte di un utente buono che vuole accedere al sistema	47
3.4 Simulazione del sistema da parte di un utente buono in cui ha deciso di effettuare il recupero della password	48
3.5 Simulazione del sistema da parte di un utente malevolo che cerca di accedere al sistema	49
3.6 Simulazione del sistema da parte di un utente malevolo che cerca di modificare la password di un utente	49
3.7 Simulazione del sistema da parte di un utente malevolo che conosce le credenziali di un utente	50
3.8 Probabilità relativa alla proprietà di Safety	51
3.9 Probabilità relativa alla proprietà di Response	52
3.10 Monitor di RE relativo alla proprietà di Safety	52
3.11 Monitor di RE relativo alla proprietà di Response	53
4.1 Solidity Analyzers - GreenToken.sol	56
4.2 Solidity Analyzers - EmissionTracker.sol	59
5.1 Docker	61
5.2 MetaMask Network Configuration	62
5.3 Home Interface For Not Login User	64
5.4 Home Interface For a Generic User	65
5.5 Home Interface For Admin	65
5.6 Home Interface For Company Administrator	66
5.7 Register User Interface	66
5.8 Two-Factor Authentication Interface	67
5.9 Verification Code Interface	67
5.10 Login Account Interface	68

5.11 Recover Password Interface	68
5.12 Reset Password Email	69
5.13 Change Password Interface	69
5.14 User Account Interface	70
5.15 Register company	70
5.16 Company Registration Approved Email	71
5.17 Notification Interface	71
5.18 Company Catalog Interface For Administrator	72
5.19 Edit Company Details Interface	72
5.20 Product Management Interface	73
5.21 Processor Product Management Interface	73
5.22 Trasport List Interface	74
5.23 Seller Product Management Interface	74
5.24 Production and Trasportation Planning Interface	75
5.25 Order Request Details Interface	75
5.26 Order Request Details Interface	76
5.27 Notification Confirmation by Supplier and Buyer	76
5.28 Notification of Transport	77
5.29 Employee Management System Interface	77
5.30 Token Balance Interface	78
5.31 Request of Token Interface	78
5.32 Accept Request with MetaMask	79
5.33 User Management System Interface	79
5.34 Company Management System Interface	80
5.35 Admin of System Notification Interface	80
5.36 Company Catalog Interface	81
5.37 Information Company Interface	81
5.38 Greener Companies List Interface	82
5.39 Seller Catalog Interface	82
5.40 Product of a Seller Interface	83
5.41 CO2 History Interface	83

CAPITOLO 1

Introduzione

Il progetto si propone di sviluppare un software dedicato alla rappresentazione e gestione della supply chain alimentare europea, seguendo lo schema rappresentato in Figura 1.1, promuovendo una maggiore sostenibilità per quanto riguarda le emissioni di gas serra (GHG) lungo l'intero ciclo di vita dei prodotti alimentari, dalla produzione al consumo. Un elemento chiave sarà l'integrazione della tecnologia blockchain, che garantirà trasparenza e tracciabilità dei dati sulle emissioni.

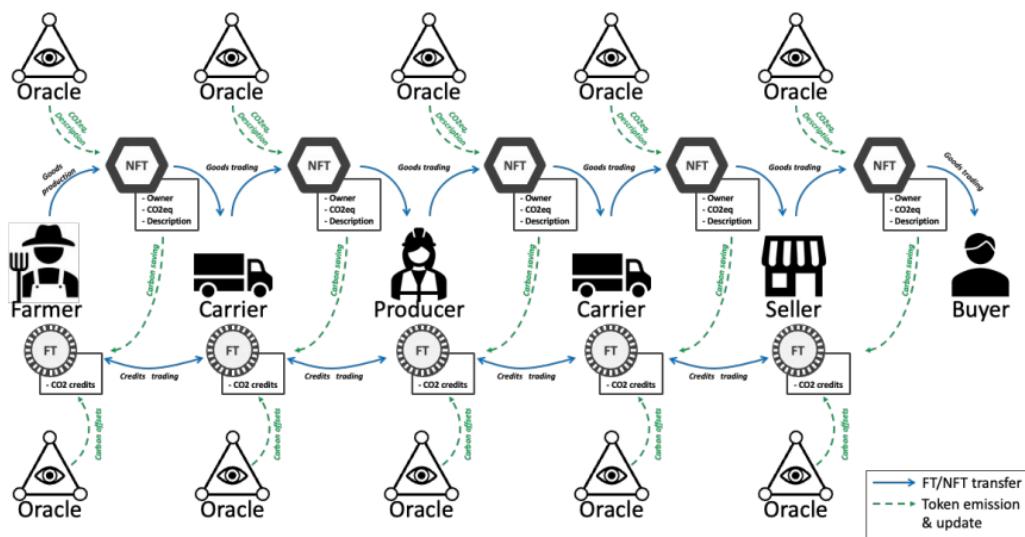


Figura 1.1: Sustainable Food Supply Chain

1.1 Funzionamento della supply chain

Questa infrastruttura blockchain supporterà un sistema di compensazione delle emissioni, consentendo la generazione, lo scambio e il monitoraggio dei *CO2 credits (carbon credits)*. Gli attori della filiera avranno come obiettivo quello di minimizzare la loro impronta ecologica e

migliorare la loro reputazione nel mercato, contribuendo attivamente agli obiettivi climatici globali. La piattaforma integrerà tecnologie off-chain come un database per la gestione dei dati, e strumenti di sviluppo come Python e JavaScript per offrire flessibilità e scalabilità. L'infrastruttura si concentrerà sulla riduzione delle emissioni nei settori agricolo, ittico, logistico, manifatturiero e vendita, promuovendo azioni ecologiche e pratiche sostenibili in tutto il ciclo di vita dei prodotti alimentari. In particolare, è utile definire il concetto di *CO₂ equivalent*, un'unità di misura che consente di quantificare l'impatto sul riscaldamento globale di una certa quantità di gas serra (*GHG*) rispetto alla stessa quantità di anidride carbonica (*CO₂*). Esso è espresso in kg CO₂e o t CO₂e e permette di confrontare e sommare i contributi di diversi gas serra per stimare l'impronta ecologica associata a una determinata attività umana. La contabilità del carbonio (*GHG accounting*), invece, è un insieme di metodi utilizzati per misurare e monitorare le emissioni di gas serra prodotte da un'organizzazione. All'interno di questo quadro, il mercato delle emissioni (*Emission Trading Scheme, ETS*) introduce un sistema di scambio di quote che limita le emissioni, incentivando così le riduzioni. Alla base di questo meccanismo sono presenti due diverse tipologie di token:

- **CO₂ Token:** Vengono emessi quando avviene una riduzione (risparmio) o rimozione (compensazione) di 1 tonnellata di CO₂ equivalent.
- **NFT Token:** Vengono emessi ogni volta che avviene una misurazione per le emissioni. Essi contengono le informazioni sul proprietario, sulla quantità di CO₂ equivalente.

1.2 Introduzione ai capitoli successivi

Nei successivi capitoli verranno affrontate le tematiche legate alla sicurezza, con un focus sulla valutazione dei rischi e sul design e programmazione sicura.

In particolare, il **Capitolo 2** sarà dedicato alla *valutazione del rischio*. Verranno illustrati diversi strumenti e metodologie per l'analisi delle minacce e delle vulnerabilità, tra cui i *diagrammi i**, il modello *Dual_STRIDE* e gli schemi di Jacobson di tipo *abuse* e *misuse* case. Questi strumenti permetteranno di comprendere meglio le potenziali minacce ai sistemi e di sviluppare strategie di mitigazione efficaci.

Nel **Capitolo 3**, invece, si affronterà il tema del *design sicuro*, con un focus sulle scelte architettoniche, tecnologiche e sulla progettazione degli asset. Saranno analizzati i principi fondamentali della sicurezza nel design dei sistemi, evidenziando le best practice e le strategie per integrare la sicurezza fin dalle prime fasi dello sviluppo.

Il **Capitolo 4** sarà dedicato alla *programmazione sicura*, trattando le tecniche e le pratiche per scrivere codice robusto contro le vulnerabilità più comuni.

Infine, il **Capitolo 5** tratterà il *deployment*, il quale svolgerà il ruolo di manuale per l'utilizzo del software.

Questi capitoli forniranno una panoramica completa delle metodologie per la sicurezza informatica, dalla valutazione dei rischi alla progettazione e implementazione di soluzioni sicure ed efficaci.

CAPITOLO 2

Valutazione del Rischio

In questo capitolo verrà trattata la valutazione del rischio, illustrando le metodologie adottate per identificare e mitigare le potenziali minacce. Nelle seguenti sottosezioni verranno analizzati i relativi aspetti:

- **Diagrammi i***: Utilizzati per modellare gli attori e le dipendenze all'interno del sistema;
- **Tabella Dual_Stride**: Un metodo strutturato per classificare e valutare le minacce;
- **Abuse Case**: Scenari che descrivono possibili utilizzi malevoli del sistema, aiutando a individuare e prevenire comportamenti indesiderati;
- **Misuse Case**: Simili agli abuse case, ma focalizzati su come i clumsy actor, utilizzando il sistema, potrebbero generare danni in maniera non intenzionale.

2.1 Diagrammi i*

In questa sezione verranno riportati i Diagrammi i* relativi alla food supply chain. In particolare, verrà riportato nella prima sottosezione il mondo della supply chain, nella seconda verrà integrato l'attore sistema e, infine, nella terza verranno inseriti gli alberi d'attacco ricavati attraverso il modello Dual_Stride riportato nella sezione successiva.

2.1.1 SD/SR ruoli supply chain senza sistema

Questo diagramma i* rappresenta una catena di produzione in cui sono presenti cinque attori principali: Agricoltura e Pesca, Trasporto, Manifattura dei prodotti, Rivendita e Consumatore finale. Ognuno di essi svolge un ruolo cruciale nel processo. Inoltre, per ogni attore vengono riportate le attività, le risorse, gli obiettivi e le loro dipendenze. Il diagramma viene riportato in Figura 2.1.

Gli attori hanno le seguenti caratteristiche:

- **Agricoltura e Pesca**: Questo attore rappresenta l'origine del processo produttivo, responsabile dell'approvvigionamento e della produzione di materie prime. Le sue azioni includono la produzione e l'acquisto di risorse necessarie per quest'ultima, la gestione delle risorse e la misurazione dei dati relativi alle emissioni.

- **Trasporto:** Questo attore svolge un ruolo chiave nella logistica, occupandosi del trasporto di materie prime e prodotti lavorati tra gli altri attori. Le sue azioni comprendono il trasporto e la misurazione delle emissioni.
- **Manifattura dei prodotti:** Questo attore è responsabile della lavorazione e trasformazione delle materie prime in prodotti finiti. Le sue azioni includono la manifattura, la misurazione delle emissioni e la vendita del prodotto trasformato.
- **Rivendita:** Questo attore gestisce il prodotto finito e la sua immissione sul mercato. Le sue azioni comprendono la gestione del magazzino, la vendita, l'acquisto dei prodotti e la selezione dei fornitori. Questo attore si occupa anche della misurazione dei dati relativi alle emissioni.
- **Consumatore finale:** Questo attore rappresenta il destinatario finale del prodotto. Le sue azioni principali sono l'acquisto del prodotto e la possibilità di consultare i dati relativi al prodotto.

Le relazioni tra gli attori sono:

- **Agricoltura e pesca:** Questo attore fornisce materie prime a Trasporto, che a sua volta le trasferisce agli altri attori della filiera.
- **Trasporto:** Questo attore movimenta le materie prime a favore di Manifattura dei prodotti, che le utilizza per la trasformazione in prodotto lavorato. Inoltre, esso collabora anche con Agricoltura e Pesca e con Rivenditore.
- **Manifattura dei prodotti:** Questo attore trasferisce il prodotto lavorato a Trasporto, che lo consegna a Rivenditore.
- **Rivendita:** Questo attore distribuisce il prodotto lavorato al Consumatore finale, che lo acquista.
- **Consumatore finale:** Questo attore dipende da Rivenditore per reperire e acquistare il prodotto lavorato.

2.1.2 SD/SR ruoli supply chain più sistema

Questo diagramma i* introduce, rispetto a quello precedente, due nuovi attori che sono Supply Chain e Sistema. Esso viene riportato in Figura 2.2.

Gli attori hanno le seguenti caratteristiche:

- **Supply Chain:** Questo attore generalizza gli attori Agricoltura e Pesca, Trasporto, Manifattura dei prodotti e Rivendita. Esso rappresenta l'intera catena di fornitura; in particolare, fornisce l'accesso al "Sistema", gestisce gli utenti attraverso attività C.R.U.D. (Create, Read, Update, Delete), riceve crediti di CO₂ tramite acquisizione, vendita e generazione di crediti stessi e interagisce con il "Consumatore finale", fornendo il prodotto finito.
- **Sistema:** Questo attore svolge un ruolo centrale nella gestione dei dati e nell'integrazione delle diverse fasi. Il sistema gestisce gli utenti, acquisisce dati dai sensori, genera e permette lo scambio di crediti CO₂, gestisce e genera token NFT, verifica i crediti di CO₂, permette di visualizzare le transazioni, controlla i dati degli utenti e gestisce le attività C.R.U.D. .

Infine, tutti gli attori sono collegati al Sistema per la gestione dei dati.

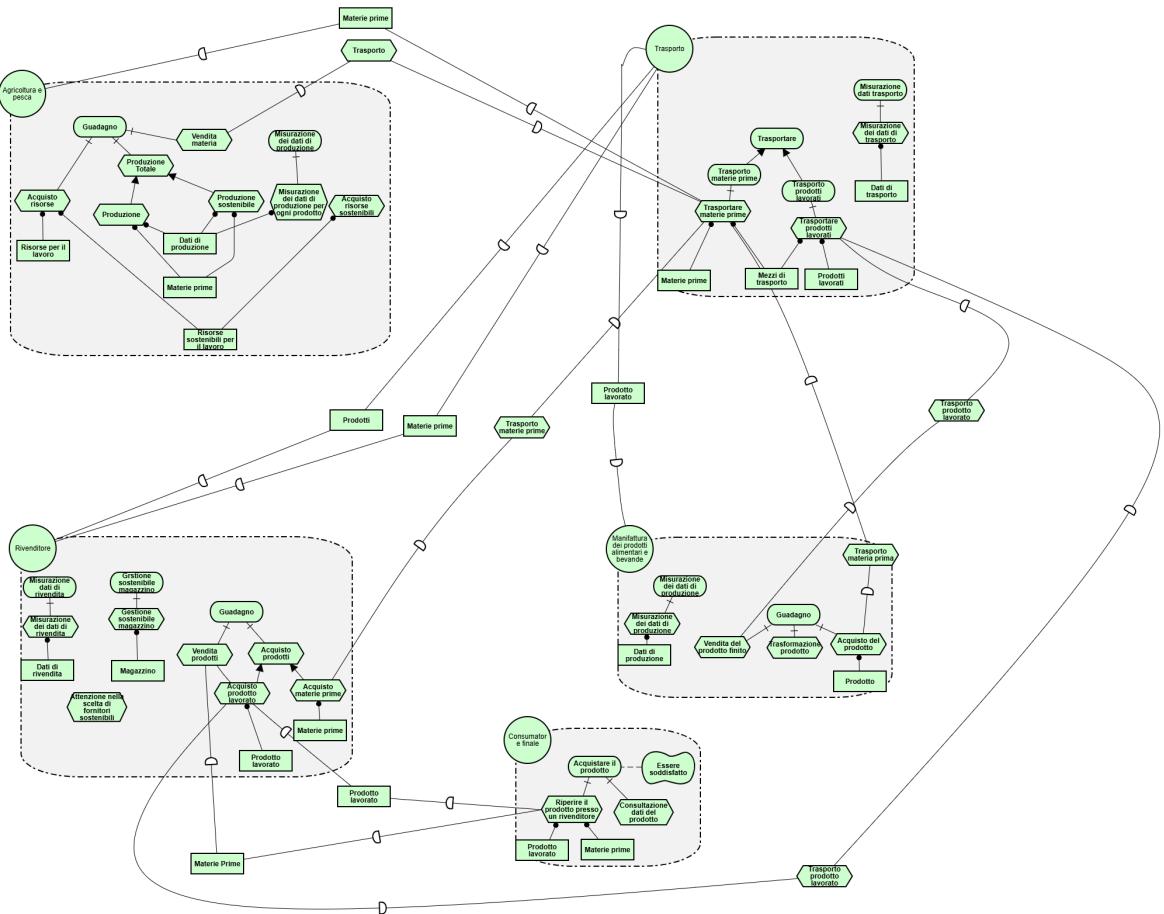


Figura 2.1: SD/SR ruoli supply chain senza sistema

2.1.3 SD/SR sistema e attaccanti con alberi di attacco

La novità principale di questo diagramma i*, rispetto ai precedenti, è l'introduzione di quattro nuovi attori: "Attacker", "Insider Attacker", "Outsider Attacker" e "Clumsy Actor", che rappresentano diverse tipologie di minacce alla sicurezza del sistema. Gli alberi di attacco, come specificato in precedenza, sono stati ricavati dalla Tabella Dual_Stride. Il diagramma viene riportato in Figura 2.3.

I nuovi attori hanno le seguenti caratteristiche:

- **Attacker:** Questo attore si propone di violare aspetti chiave del sistema, come l'integrità, la riservatezza, l'autenticazione, l'autorizzazione, la disponibilità e l'accountability. Tra i suoi obiettivi figurano anche attività di spoofing, manomissione dei dati, interruzione della disponibilità del sistema, intercettazione dei dati, accesso non autorizzato a risorse riservate, mascheramento di attività non autorizzate, alterazione dei dati dei sensori e impedimento della tracciabilità delle modifiche. Per raggiungere questi obiettivi, l'Attacker svolge diverse attività: cancellare i log di accesso, disabilitare il logging delle modifiche, decifrare dati criptati, effettuare attacchi di phishing e forza bruta, alterare record di emissioni, manipolare transazioni, modificare dati, intercettare e manipolare dati, bloccare l'accesso ai database, installare malware, creare account falsi con diritti di accesso, utilizzare credenziali rubate, eseguire privilege escalation e sfruttare vulnerabilità di accesso.
- **Insider Attacker:** Questo attore è una specializzazione di Attacker e si riferisce agli

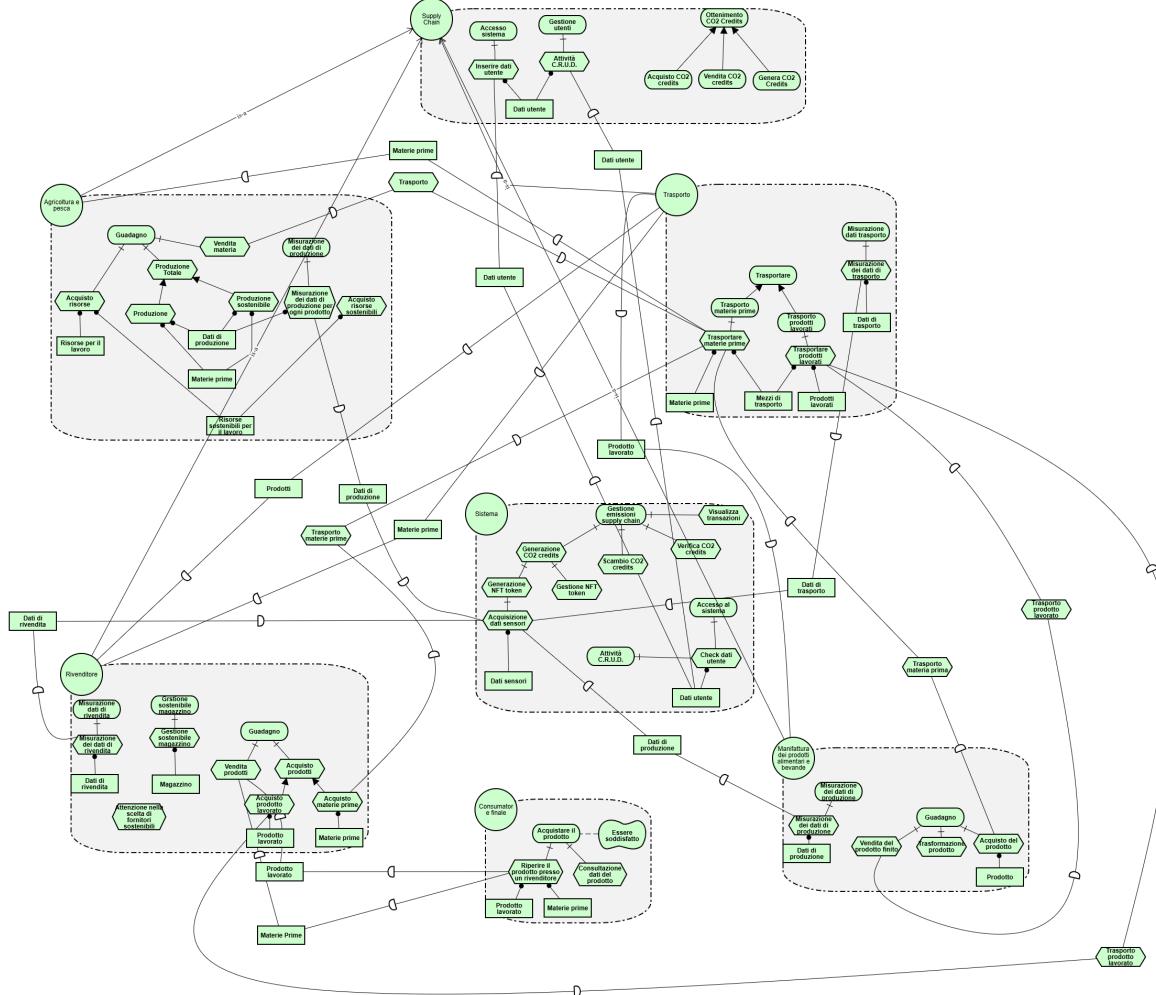


Figura 2.2: SD/SR ruoli supply chain più sistema

attori che agiscono dall'interno del sistema. Inoltre, l'Insider Attacker, rispetto all'attore generico ha ulteriori modi per violare l'autenticazione, la disponibilità, la riservatezza dei dati sensibili e delle comunicazioni interne, con lo scopo di ottenere accesso non autorizzato ai dati, copiare informazioni riservate, rubare credenziali di colleghi, intercettare comunicazioni interne o interrompere i servizi. Le attività intraprese dall'Insider Attacker includono l'accesso diretto al database, la lettura di e-mail interne e messaggi aziendali, l'accesso fraudolento agli account di altri utenti, l'esportazione di report e dati critici, la disattivazione di sistemi essenziali e l'uso di sessioni di altri utenti.

- **Outsider Attacker:** Questo attore è una specializzazione di Attacker e si riferisce agli attori che agiscono dall'esterno del sistema.
- **Clumsy Actor:** Il Clumsy Actor, agendo in modo accidentale, può violare la riservatezza e l'integrità dei dati attraverso operazioni come modifiche, eliminazioni o inserimenti non intenzionali. Può anche copiare dati su dispositivi locali o esterni e inviare informazioni tramite canali non corretti. Le sue attività includono modifiche, eliminazioni, inserimenti, download accidentali e invio di informazioni sul canale sbagliato.

Infine, questi nuovi attori sono connessi al Sistema e agli asset in esso contenuti.

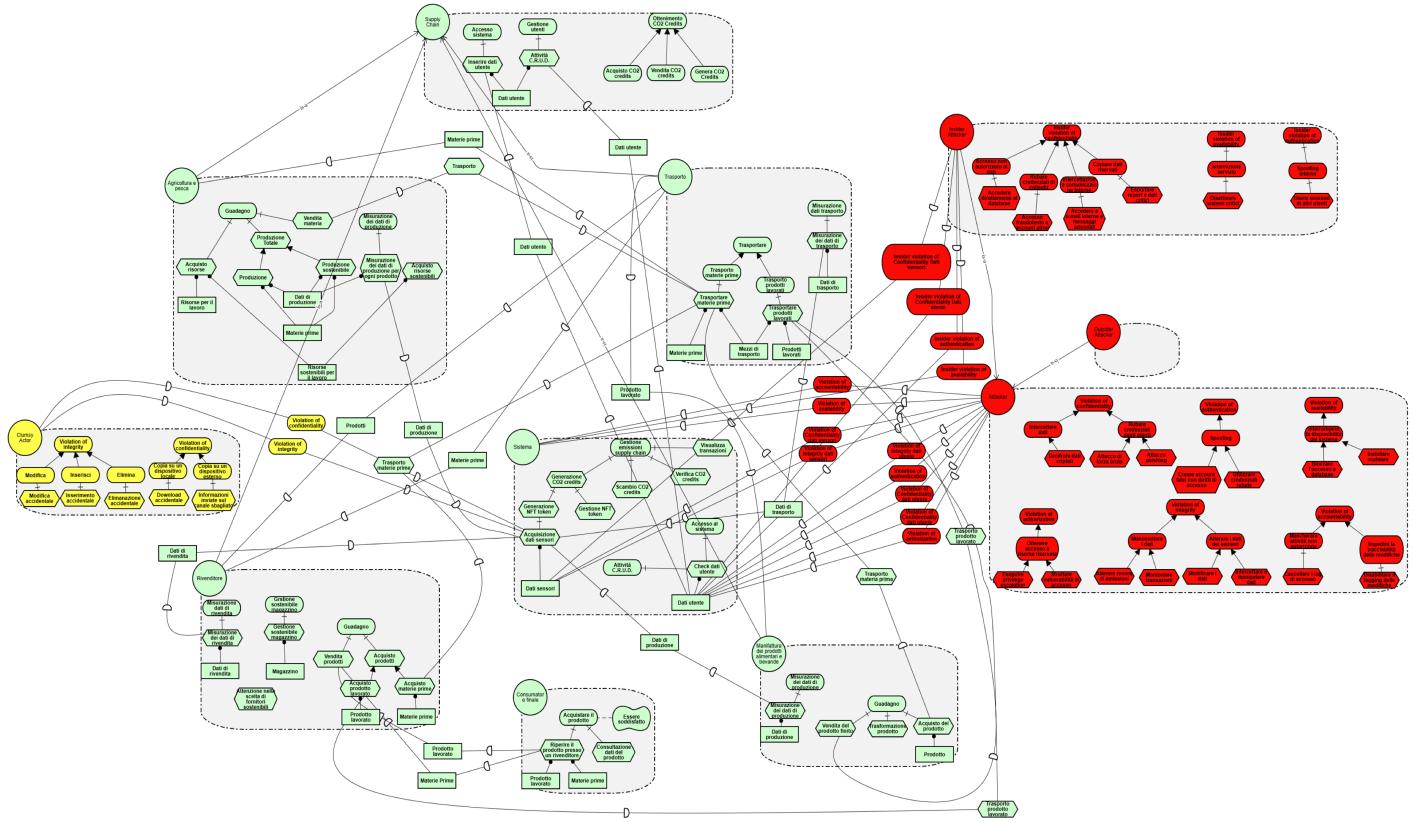


Figura 2.3: SD/SR sistema e attaccanti con alberi di attacco

2.2 Tabella Dual_Stride

In questa sezione, riportiamo la tabella Dual_Stride, utilizzata al fine di valutare le principali minacce per gli asset del nostro sistema ed individuare, tramite la valutazione del R.o.c., le migliori strategie di difesa. In particolare, gli asset individuati per il nostro sistema sono:

- *Dati Utente*: I dati riservati degli utenti che utilizzano il sistema;
- *Dati Sensori*: I dati acquisiti tramiti sensori durante le varie fasi della supply chain rispetto alle emissioni di CO2;
- *CO2 Credits*: I token emessi quando avviene una riduzione (risparmio) o rimozione (compensazione) di 1 tonnellata di CO2 equivalent;
- *NFT Token*: I token emessi ogni volta che avviene una misurazione per le emissioni.

Asset	Value	Spoofing	Tampering	Repudiation	Information disclosure	DOS	Elevation of privilege	Danger	Unreliability	Absence of Resilience	Exposure	Attack	Inherent Probability	Inherent Risk	Control	Cost	Feasibility	Residual Probability	Residual Impact	Residual Risk	R.o.C	Overall Cost
Dati Utente	€250.000 - €500.000		X				X			€25.000 - €50.000	Audit Log Manipulation (CAPEC 268)	60%	€15.000 - €30.000	Implementare un sistema di logging sicuro con controlli di integrità (es. hash) per rilevare modifiche.	€4.600 - €18.400	Fattibile, ma richiede configurazioni avanzate e una gestione continua della sicurezza del logging.	4%	€5.000 - €12.500	€200,00 - €500,00	2,22/0,6	€4.800 - €18.900	
	€250.000 - €500.000					X				€125.000 - €250.000	Privilege Escalation (CAPEC 233)	45%	€56.250 - €112.500	Implementare l'autenticazione a più fattori (MFA) per azioni sensibili	€9.200 - €36.800	Tecnologicamente fattibile, ma potrebbe incontrare resistenze da parte degli utenti.	6%	€50.000 - €100.000	€450,00 - €900,00	5,07/2,03	€9.650 - €37.700	
	€250.000 - €500.000				X	X				€75.000 - €150.000	Exploiting Incorrectly Configured Access Control Security Levels (CAPEC 180)	50%	€37.500 - €75.000	Configurare correttamente il controllo degli accessi	€4.600 - €13.800	Fattibile, ma dipende dalla complessità dell'infrastruttura esistente.	16%	€20.000 - €40.000	€3200,00 - €6400,00	6,46/3,97	€7.800 - €20.200	
	€250.000 - €500.000	X								€25.000 - €50.000	Authentication Abuse (CAPEC 114)	60%	€17.500 - €35.000	Applicare MFA, impostare politiche di password robuste	€4.600 - €13.800	Fattibile, ma necessita di gestione accurata delle credenziali e formazione degli utenti.	6,25%	€6.250 - €17.500	€390,63 - €1093,75	2,72/1,46	€4.990,63 - €14.893,75	
	€250.000 - €500.000				X		X	X		€125.000 - €250.000	Targeted Malware (CAPEC 542)	50%	€62.500 - €125.000	1) Implementare strumenti di rilevamento 2) mantenere aggiornati i sistemi e i software 3) utilizzare la segmentazione di rete per limitare la diffusione del malware.	1)€5.000 - €10.000 2)€4.000 - €6.000 3)€4.800 - €30.000	1)Fattibile, richiede monitoraggio continuo e aggiornamenti frequenti. 2)Fattibile, richiede sforzo costante per mantenere aggiornati i sistemi. 3)Fattibile, ma richiede progettazione attenta e competenze tecniche.	1)15% 2)10% 3)10%	1)€40.000 - €80.000 2)€45.000 - €90.000 3)€25.000 - €50.000	1)€6.000 - €12.000 2)€4.500 - €9.000 3)€2.500 - €5.000	1)10,3/10,3 2)13,5/18,33 3)11,5/3	1) €11.000 - €22.000 2) €8.500 - €15.000 3) €7.300 - €35.000	

	€250.000 - €500.000	X								€25.000 - €50.000	Credential Stuffing (CAPEC 600)	65%	€16.250 - €32.500	Utilizzare l'autenticazione a più fattori per tutti i servizi di autenticazione 2) monitorare i registri di sistema e di dominio per rilevare eventuali accessi anomali alle credenziali.	1)€1.600 - €7.800 2)€3.200 - €5.000	Fattibile, ma può comportare complessità nella gestione dei registri e delle configurazioni MFA. 2)Fattibile, necessita di strumenti appropriati e monitoraggio continuo.	1)5% 2)12%	1)€4.000 - €16.000 2)€5.000 - €20.000	1)€200 - €800 2)€600 - €2.400	1)9,03/3,06 2)3,89/5,02	1) €1.800 - € 8.600 2) €3.800 - €7.400
	€250.000 - €500.000		X							€25.000 - €50.000	Cryptanalysis (CAPEC 97)	80%	€7.500 - €15.000	1)Utilizzare algoritmi di crittografia moderne e forti e ruotare regolarmente le chiavi di crittografia 2)rimanere aggiornati sulle vulnerabilità crittografiche e applicare immediatamente patch quando vengono identificate nuove debolezze.	1)€3.000 - €10.000 2)€1.600 - €8.400	Fattibile, ma richiede una gestione attenta delle chiavi e aggiornamenti periodici. 2) Fattibile, necessita di monitoraggio costante e applicazione rapida delle patch.	1)10% 2)15%	1)€3.500 - €8.000 2)€5.000 - €12.000	1)€350 - €800 2)€750 - €1.800	1)1,38/0,42 2)3,22/0,57	1) €3.350 - €10.800 2) €2.350 - €10.200
	€250.000 - €500.000		X							€25.000 - €50.000	Brute Force (CAPEC 112)	40%	€10.000 - €20.000	1)Usare MFA 2) limitare i tentativi di login.	1)€3.000 - €9.000 2)€1.600 - €4.800	Fattibile, richiede configurazione e sensibilizzazione degli utenti. 2)Fattibile, necessita di policy e configurazione del sistema.	8% 10%	1)€3.000 - €7.000 2)€6.000 - €16.000	1)€240 - €560 2)€600 - €1.600	1) 2,25/1,16 2)4,88/2,83	1) €3.240 - €9.560 2) €2.200 - €6.400
	€250.000 - €500.000		X							€25.000 - €50.000	Phishing (CAPEC 98)	70%	€17.500 - €35.000	Utilizzare filtri per email e monitorare attività email anomale.	€9.200 - €23.000	Fattibile, ma richiede una gestione continua dei filtri e una risposta tempestiva agli eventi anomali.	20%	€5.000 - €12.500	€1000,00 - €2500,00	0,79/0,41	€10.200 - €25.500

	€250.000 - €500.000		X						€25.000 - €50.000	Typo Squatting (CAPEC 630)	60%	€15.000 - €30.000	Registrare le versioni più comuni di errori di battitura del proprio dominio, monitorare le registrazioni di domini per individuare possibili typo-squatting.	€920 - €4.600	Fattibile, ma richiede risorse per il monitoraggio continuo dei domini.	5%	€1.250 - €7.500	€62,50 - €375,00	15,24/5,44	€982,50 - €4.975
	€250.000 - €500.000		X						€75.000 - €150.000	Pull Data From System Resources (CAPEC 544)	55%	€41.250 - €82.500	1) Applicare controlli di accesso rigorosi e logging sulle risorse di sistema sensibili 2) Seguire regolari audit delle autorizzazioni e utilizzare strumenti di prevenzione della perdita di dati (DLP) per rilevare e prevenire l'accesso non autorizzato ai dati.	1)€4.500 - €10.000 2)€4.700 - €13.000	1) Fattibile, richiede configurazione precisa e monitoraggio continuo. 2) Fattibile, ma può avere impatti sulla performance se non configurato correttamente.	1)6% 2)4%	1)€30.000 - €51.000 2)€22.000 - €40.000	1)€1.800 - €3.060 2)€880 - €1.600	1)7,77/6,94 2)7,59/5,22	1) €6.300 - €13.060 2) €5.580 - €14.600
	€250.000 - €500.000		X	X	X				€175.000 - €350.000	Disabling Network Hardware (CAPEC 583)	50%	€87.500 - €175.000	1) Implementare controlli di sicurezza fisici e monitorare i dispositivi di rete per comportamenti insoliti 2) Assicurarsi che i sistemi di backup siano presenti per l'hardware critico.	1)€4.500 - €6.000 2)€4.000 - €14.000	1)Fattibile, ma richiede un investimento in infrastrutture fisiche e monitoraggio continuo. Richiede sorveglianza costante e strumenti adeguati. 2)Fattibile, necessita di pianificazione e test periodici.	1)7% 2)3%	1)€50.000 - €120.000 2)€30.000 - €80.000	1)€3.500 - €8.400 2)€900 - €2.400	1)17,67/26,77 2)20,65/11,33	€4.937,50 - €14.643,75

	€250.000 - €500.000	X								€25.000 - €50.000	Reusing Session Ids (CAPEC 60)	65%	€16.250 - €32.500	1) Usare pratiche di gestione delle sessioni sicure, generare ID di sessione unici 2) Utilizzare autenticazione a più fattori.	1)€2.400 - €3.500 2)€2.200 - €5.700	1)Fattibile, ma potrebbe complicare la gestione delle sessioni per gli utenti. 2)Fattibile, richiede implementazione tecnica e formazione degli utenti.	1)5% 2)2%	1)€9.000 - €18.000 2)€6.000 - €16.000	1)€450 - €900 2)€120 - €320	1) 5,58/8,03 2)6,33/4,65	1) €2.850 - €4.400 2) €2.320 - €6.020
Dati Sensori	€200.000 - €400.000		X			X				€20.000 - €40.000	Audit Log Manipulation (CAPEC 268)	60%	€12.000 - €24.000	Implementare un sistema di logging sicuro con controlli di integrità (es. hash) per rilevare modifiche.	€4.600 - €18.400	Fattibile, ma richiede configurazioni avanzate e una gestione continua della sicurezza del logging.	4%	€7.500 - €15.000	€300,00 - €600,00	1,54/0,27	€4.900 - €19.000
	€200.000 - €400.000				X					€100.000 - €200.000	Privilege Escalation (CAPEC 233)	40%	€40.000 - €80.000	Implementare l'autenticazione a più fattori (MFA) per azioni sensibili	€4.600 - €13.800	Tecnologicamente fattibile, ma potrebbe incontrare resistenze da parte degli utenti.	8%	€4.000 - €8.000	€360,00 - €720,00	7,62/4,74	€4.960 - €14.520
	€200.000 - €400.000			X	X					€60.000 - €120.000	Exploiting Incorrectly Configured Access Control Security Levels (CAPEC 180)	50%	€30.000 - €60.000	Configurare correttamente il controllo degli accessi	€4.600 - €13.800	Fattibile, ma dipende dalla complessità dell'infrastruttura esistente.	16%	€6.250 - €12.500	€1000,00 - €2000,00	5,3/3,2	€5.600 - €15.800
	€200.000 - €400.000			X		X	X	X		€100.000 - €200.000	Targeted Malware (CAPEC 542)	50%	€50.000 - €100.000	1) Implementare strumenti di rilevamento 2) mantenere aggiornati i sistemi e i software 3) utilizzare la segmentazione di rete per limitare la diffusione del malware.	1)€5.000 - €10.000 2)€4.000 - €6.000 3)€4.800 - €30.000	1)Fattibile, richiede monitoraggio continuo e aggiornamenti frequenti. 2)Fattibile, richiede sforzo costante per mantenere aggiornati i sistemi. 3)Fattibile, ma richiede progettazione attenta e competenze tecniche.	1)15% 2)10% 3)10%	1)€40.000 - €80.000 2)€45.000 - €90.000 3)€25.000 - €50.000	1)€6.000 - €12.000 2)€4.500 - €9.000 3)€2.500 - €5.000	1)10,3/10,3 2)13,5/18,33 3)11,5/3	1) €11.000 - €22.000 2) €8.500 - €15.000 3) €7.300 - €35.000

	€200.000 - €400.000	X								€20.000 - €40.000	Credential Stuffing (CAPEC 600)	65%	€13.000 - €26.000	- Utilizzare l'autenticazione a più fattori per tutti i servizi di autenticazione 2) monitorare i registri di sistema e di dominio per rilevare eventuali accessi anomali alle credenziali.	1)€1.600 - €7.800 - €3.200 - €5.000	1) Fattibile, ma può comportare complessità nella gestione dei registri e delle configurazioni MFA. 2)Fattibile, necessita di strumenti appropriati e monitoraggio continuo.	1)5% - 2)12%	1)€4.000 - €16.000 - €5.000 - €20.000	1)€200 - €800 - €600 - €2.400	1)€200 - €800 - €600 - €2.400	1)9,03/3,06 - 2)3,89/5,02	1) € 1.800 - € 8.600 - 2) €3.800 - €7.400
	€200.000 - €400.000		X				X			€60.000 - €120.000	Development Alteration (CAPEC 444)	55%	€33.000 - €66.000	- Applicare un controllo rigoroso sulle modifiche al codice e utilizzare strumenti di gestione del codice sorgente con restrizioni di accesso	€9.200 - €27.600	Fattibile, ma può rallentare i cicli di sviluppo.	6%	€2.000 - €8.000	€120,00 - €480,00	2,57 / 1,37	€9.320 - €28.080	
	€200.000 - €400.000		X				X			€60.000 - €120.000	Input data manipulation (CAPEC 153)	50%	€30.000 - €60.000	- Validare tutti gli input utente, applicare pratiche di codifica sicure	€4.600 - €13.800	Fattibile, richiede una formazione continua per sviluppatori.	7.5%	€4.000 - €8.000	€300,00 - €600,00	5,46 / 3,3	€4.900 - €14.400	
	€200.000 - €400.000			X						€20.000 - €40.000	Cryptanalysis (CAPEC 97)	80%	€6.000 - €12.000	- Utilizzare algoritmi di crittografia moderne e forti e ruotare regolarmente le chiavi di crittografia 2) rimanere aggiornati sulle vulnerabilità crittografiche e applicare immediatamente patch quando vengono identificate nuove debolezze.	1)€3.000 - €10.000 - €1.600 - €8.400	1)Fattibile, ma richiede una gestione attenta delle chiavi e aggiornamenti periodici. 2) Fattibile, necessita di monitoraggio costante e applicazione rapida delle patch.	1)10% - 2)15%	1)€3.500 - €8.000 - €5.000 - €12.000	1)€350 - €800 - €750 - €1.800	1)1,38 / 0,42 - 2)3,22 / 0,57	1) €3.350 - €10.800 - 2) €2.350 - €10.200	

	€200.000 - €400.000	X							€60.000 - €120.000	Pull Data From System Resources (CAPEC 544)	55%	€33.000 - €66.000	1) Applicare controlli di accesso rigorosi e logging sulle risorse del sistema sensibili 2) Seguire regolari audit delle autorizzazioni e utilizzare strumenti di prevenzione della perdita di dati (DLP) per rilevare e prevenire l'accesso non autorizzato ai dati.	1)€4.500 - €10.000 2)€4.700 - €13.000	1) Fattibile, richiede configurazione precisa e monitoraggio continuo. 2) Fattibile, ma può avere impatti sulla performance se non configurato correttamente.	1)6% 2)4%	1)€30.000 - €51.000 2)€22.000 - €40.000	1)€1.800 - €3.060 2)€880 - €1.600	1)7,77/6,94 2)7,59/5,22	1) €6.300 - €13.060 2) €5.580 - €14.600
	€200.000 - €400.000			X	X	X		€140.000 - €280.000	Disabling Network Hardware (CAPEC 583)	50%	€70.000 - €140.000	1) Implementare controlli di sicurezza fisici e monitorare i dispositivi di rete per comportamenti insoliti 2) Assicurarsi che i sistemi di backup siano presenti per l'hardware critico.	1)€4.500 - €6.000 2)€4.000 - €14.000	1)Fattibile, ma richiede un investimento in infrastrutture fisiche e monitoraggio continuo. Richiede sorveglianza costante e strumenti adeguati. 2)Fattibile, necessita di pianificazione e test periodici.	1)7% 2)3%	1)€50.000 - €120.000 2)€30.000 - €80.000	1)€3.500 - €8.400 2)€900 - €2.400	1)17,67/26,77 2)20,65/11,33	€4.937,50 - €14.643,75	
CO2 Credits	€400.000 - €800.000		X					€40.000 - €80.000	Audit Log Manipulation (CAPEC 268)	60%	€24.000 - €48.000	Implementare un sistema di logging sicuro con controlli di integrità (es. hash) per rilevare modifiche.	€4.600 - €18.400	Fattibile, ma richiede configurazioni avanzate e una gestione continua della sicurezza del logging.	4%	€8.750 - €17.500	€350.00 - €700.00	4,14/1,57	€4.950 - €19.100	
	€400.000 - €800.000				X			€200.000 - €400.000	Privilege Escalation (CAPEC 233)	45%	€90.000 - €180.000	Implementare l'autenticazione a più fattori (MFA) per azioni sensibili	€9.200 - €36.800	Tecnologicamente fattibile, ma potrebbe incontrare resistenze da parte degli utenti.	4%	€4.000 - €10.000	€360.00 - €900.00	8,74/3,87	€9.560 - €37.700	
	€400.000 - €800.000			X	X			€120.000 - €240.000	Exploiting Incorrectly Configured Access Control Security Levels (CAPEC 180)	55%	€66.000 - €132.000	Configurare correttamente il controllo degli accessi	€4.600 - €13.800	Fattibile, ma dipende dalla complessità dell'infrastruttura esistente.	16%	€5.000 - €15.000	€800.00 - €2400,00	13,17/8,39	€5.400 - €16.200	

	€400.000 - €800.000	X								€40.000 - €80.000	Authenticatio n Abuse (CAPEC 114)	70%	€28.000 - €56.000	Applicare MFA, imporre politiche di pas- sword robuste	€4.600 - €13.800	Fattibile, ma ne- cessita di gestione accurata delle cre- denziali e formazio- ne degli utenti.	6.25%	€12.000 - €25.000	€750,00 - €1562,50	4,92/2,94	€5.350 - €15.362,50
	€400.000 - €800.000			X		X				€200.000 - €400.000	Targeted Malware (CAPEC 542)	50%	€110.000 - €220.000	1) Imple- mentare strumenti di rilev- amento 2)man- tenere aggiornati i sistemi e i software 3) utilizzare la segmen- tazione di rete per limitare la diffu- sione del malware.	1)€5.000 - €10.000 2)€4.000 - €6.000 3)€4.800 - €30.000	1) Fattibile, richiede monito- raggio continuo e aggior- namen-ti frequen-ti. 2)Fattibile, richiede sforzo co- stante per mantene aggiornati i sistemi. 3)Fatti- bile, ma richiede proget- tazione attenta e com- petenze tecniche.	1)15% 2)10% 3)10%	1)€40.000 - €80.000 2)€45.000 - €90.000 3)€25.000 - €50.000	1)€6.000 - €12.000 2)€4.500 - €9.000 3)€2.500 - €5.000	1)10,3/10,3 2)13,5/18,33 3)11,5/3	1) €11.000 - €22.000 2) €8.500 - €15.000 3) €7.300 - €35.000
	€400.000 - €800.000	X								€40.000 - €80.000	Credential Stuffing (CAPEC 600)	65%	€26.000 - €52.000	1) Utili- izzare l'autenti- cazione a più fattori per tutti i servizi di autentica- zione 2) monitora- re i registri di sistema e di do- minio per rilevare eventuali accessi anomali alle cre- denziali.	1)€1.600 - €7.800 2)€3.200 - €5.000	1) Fatti- bile, ma può com- portare comple- sità nella gestione dei registri e delle configura- zioni MFA. 2)Fattibile, necessita di stru- menti appro- priati e monito- raggio continuo.	1)5% 2)12%	1)€4.000 - €16.000 2)€5.000 - €20.000	1)€200 - €800 2)€600 - €2.400	1)9,03/3,06 2)3,89/5,02	1) €1.800 - € 8.600 2) €3.800 - €7.400
	€400.000 - €800.000		X				X			€120.000 - €240.000	Development Alteration (CAPEC 444)	60%	€72.000 - €144.000	Applicare un control- lo rigoroso sulle mo- difiche al codice, utilizzare strumenti di gestione del codice sorgente con restri- zioni di accesso.	€9.200 - €27.600	Fattibile, ma può rallentare il ciclo di sviluppo.	6%	€7.500 - €17.500	€450,00 - €1050,00	6,78/4,18	€9.650 - €28.650

	€400.000 - €800.000	X					X		€120.000 - €240.000	Transaction or an event tampering via application API manipulation (CAPEC 385)	50%	€60.000 - €120.000	Implementare controlli di sicurezza API gateway e convalidare rigorosamente le richieste API.	€9.200 - €27.600	Tecnologico	Difficile	€5.000 - €12.500	€250,00 - €625,00	5,49/3,33	€9.450 - €28.225
	€400.000 - €800.000			X					€40.000 - €80.000	Pull Data From System Resources (CAPEC 544)	55%	€18.000 - €36.000	1) Applicare controlli di accesso rigorosi e logging sulle risorse di sistema sensibili 2) Seguire regolari audit delle autorizzazioni e utilizzare strumenti di prevenzione della perdita di dati (DLP) per rilevare e prevenire l'accesso non autorizzato ai dati.	1)€4.500 - €10.000 2)€4.700 - €13.000	1) Fattibile, richiede configurazione precisa e monitoraggio continuo. 2) Fattibile, ma può avere impatti sulla performance se non configurato correttamente.	1)6% 2)4%	1)€30.000 - €51.000 2)€22.000 - €40.000	1)€1.800 - €3.060 2)€880 - €1.600	1)7,77/6,94 2)7,59/5,22	1) €6.300 - €13.060 2) €5.580 - €14.600
	€400.000 - €800.000				X		X	X	€280.000 - €560.000	Disabling Network Hardware (CAPEC 583)	50%	€168.000 - €336.000	1) Implementare controlli di sicurezza fisici e monitorare i dispositivi di rete per comportamenti insoliti 2) Assicurarsi che i sistemi di backup siano presenti per l'hardware critico.	1)€4.500 - €6.000 2)€4.000 - €14.000	1)Fattibile, ma richiede un investimento in infrastrutture fisiche e monitoraggio continuo. Richiede sorveglianza costante e strumenti adeguati. 2)Fattibile, necessita di pianificazione e test periodici.	1)7% 2)3%	1)€50.000 - €120.000 2)€30.000 - €80.000	1)€3.500 - €8.400 2)€900 - €2.400	1)17,67/26,77 2)20,65/11,33	€4.937,50 - €14.643,75
	€400.000 - €800.000	X							€40.000 - €80.000	Reusing Session Ids (CAPEC 60)	65%	€26.000 - €52.000	1) Usare pratiche di gestione delle sessioni sicure, generare ID di sessione unici 2) Utilizzare autenticazione a più fattori.	1)€2.400 - €3.500 2)€2.200 - €5.700	1)Fattibile, ma potrebbe complicare la gestione delle sessioni per gli utenti. 2)Fattibile, richiede implementazione tecnica e formazione degli utenti.	1)5% 2)2%	1)€9.000 - €18.000 2)€6.000 - €16.000	1)€450 - €900 2)€120 - €320	1) 5,58/8,03 2)6,33/4,65	1) €2.850 - €4.400 2) €2.320 - €6.020

NFT Token	€300.000 - €600.000		X							€30.000 - €60.000	Audit Log Manipulation (CAPEC 268)	50%	€15.000 - €30.000	Implementare un sistema di logging sicuro con controlli di integrità (es. hash) per rilevare modifiche.	€4.600 - €18.400	Fattibile, ma richiede configurazioni avanzate e una gestione continua della sicurezza del logging.	9%	€2.500 - €5.000	€225,00 - €450,00	2,21/0,61	€4.825 - €18.850
	€300.000 - €600.000				X					€150.000 - €300.000	Privilege Escalation (CAPEC 233)	55%	€82.500 - €165.000	Implementare l'autenticazione a più fattori (MFA) per azioni sensibili	€4.600 - €13.800	Tecnologicamente fattibile, ma potrebbe incontrare resistenze da parte degli utenti.	6%	€6.000 - €12.000	€960,00 - €1920,00	16,73/10,82	€6.960 - €15.720
	€300.000 - €600.000			X	X					€90.000 - €180.000	Exploiting Incorrectly Configured Access Control Security Levels (CAPEC 180)	65%	€58.500 - €117.000	Configurare correttamente il controllo degli accessi	€4.600 - €13.800	Fattibile, ma dipende dalla complessità dell'infrastruttura esistente.	7,5%	€10.000 - €20.000	€750,00 - €1500,00	11,55/7,37	€5.350 - €15.300
	€300.000 - €600.000	X								€30.000 - €60.000	Authentication Abuse (CAPEC 114)	65%	€19.500 - €39.000	Applicare MFA, impostare politiche di password robuste	€4.600 - €13.800	Fattibile, ma necessita di gestione accurata delle credenziali e formazione degli utenti.	2%	€6.000 - €15.000	€120,00 - €300,00	3,21/1,8	€4.720 - €14.100
	€300.000 - €600.000		X		X	X	X			€150.000 - €300.000	Targeted Malware (CAPEC 542)	50%	€82.500 - €165.000	1) Implementare strumenti di rilevamento 2) mantenere aggiornati i sistemi e i software 3) utilizzare la segmentazione di rete per limitare la diffusione del malware.	1)€5.000 - €10.000 2)€4.000 - €6.000 3)€4.800 - €30.000	1)Fattibile, richiede monitoraggio continuo e aggiornamenti frequenti. 2)Fattibile, richiede sforzo costante per mantenere aggiornati i sistemi. 3)Fattibile, ma richiede progettazione attenta e competenze tecniche.	1)15% 2)10% 3)10%	1)€40.000 - €80.000 2)€45.000 - €90.000 3)€25.000 - €50.000	1)€6.000 - €12.000 2)€4.500 - €9.000 3)€2.500 - €5.000	1)10,3/10,3 2)13,5/18,33 3)11,5/3	1) €11.000 - €22.000 2) €8.500 - €15.000 3) €7.300 - €35.000

	€300.000 - €600.000	X								€30.000 - €60.000	Credential Stuffing (CAPEC 600)	65%	€19.500 - €39.000	- Utilizzare l'autenticazione a più fattori per tutti i servizi di autenticazione 2) monitorare i registri di sistema e di dominio per rilevare eventuali accessi anomali alle credenziali.	1)€1.600 - €7.800 2)€3.200 - €5.000	1) Fattibile, ma può comportare complessità nella gestione dei registri e delle configurazioni MFA. 2)Fattibile, necessita di strumenti appropriati e monitoraggio continuo.	1)5% 2)12%	1)€4.000 - €16.000 2)€5.000 - €20.000	1)€200 - €800 2)€600 - €2.400	1)9,03/3,06 2)3,89/5,02	1) €1.800 - € 8.600 2) €3.800 - €7.400
	€300.000 - €600.000	X				X				€90.000 - €180.000	Development Alteration (CAPEC 444)	55%	€49.500 - €99.000	- Applicare un controllo rigoroso sulle modifiche al codice e utilizzare strumenti di gestione del codice sorgente con restrizioni di accesso	€9.200 - €27.600	Fattibile, ma può rallentare il ciclo di sviluppo.	6%	€7.500 - €12.500	€450.00 - €750.00	4,33/2,56	€7.950 - €28.350
	€300.000 - €600.000	X				X				€90.000 - €180.000	Transaction or an event tampering via application API manipulation (CAPEC 385)	50%	€45.000 - €90.000	- Implementare controlli di sicurezza API gateway e convalidare rigorosamente le richieste API.	€9.200 - €27.600	Tecnologicamente fattibile; potrebbe richiedere configurazioni complesse per integrarsi con altre misure di sicurezza.	6%	€5.000 - €10.000	€150.00 - €300.00	3,88/2,25	€9.350 - €27.900
	€300.000 - €600.000			X						€30.000 - €60.000	Pull Data From System Resources (CAPEC 544)	55%	€13.500 - €27.000	- 1) Applicare controlli di accesso rigorosi e logging sulle risorse di sistema sensibili 2) Seguire regolari audit delle autorizzazioni e utilizzare strumenti di prevenzione della perdita di dati (DLP) per rilevare e prevenire l'accesso non autorizzato ai dati.	1)€4.500 - €10.000 2)€4.700 - €13.000	1) Fattibile, richiede configurazione precisa e monitoraggio continuo. 2) Fattibile, ma può avere impatti sulla performance se non configurato correttamente.	1)6% 2)4%	1)€30.000 - €51.000 2)€22.000 - €40.000	1)€1.800 - €3.060 2)€880 - €1.600	1)7,77/6,94 2)7,59/5,22	1) €6.300 - €13.060 2) €5.580 - €14.600

	€300.000 - €600.000	X	X	X	€210.000 - €420.000	Disabling Network Hardware (CAPEC 583)	50%	€126.000 - €252.000	1) Implementare controlli di sicurezza fisici e monitorare i dispositivi di rete per comportamenti insoliti 2) Assicurarsi che i sistemi di backup siano presenti per l'hardware critico.	1)€4.500 - 2)€4.000 - €14.000	1)Fattibile, ma richiede un investimento in infrastrutture fisiche e monitoraggio continuo. Richiede sorveglianza costante e strumenti adeguati. 2)Fattibile, necessita di pianificazione e test periodici.	1)7% 2)3%	1)€50.000 - 2)€30.000 - €80.000	1)€3.500 - 2)€900 - €2.400	1)17,67/26,77 2)20,65/11,33	€4.937,50 - €14.643,75
--	---------------------	---	---	---	---------------------	--	-----	---------------------	---	-------------------------------	---	-----------	---------------------------------	----------------------------	-----------------------------	------------------------

2.3 Abuse Case

In questa sezione, vengono riportati gli schemi di Jacobson relativi agli abuse case. In particolare, si analizzerà ogni tipologia di attacco individuato nella tabella Dual_Stride.

Case Type	Abuse Case	Case ID AT-01
Case Name	Audit Log Manipulation (CAPEC 268)	
Actors	Supply Chain, Sistema, Attacker	
Description	L'attaccante inietta, manipola, elimina o falsifica voci di registro dannose nel file di registro, nel tentativo di fuorviare un audit del file di registro o coprire le tracce di un attacco. A causa di controlli di accesso insufficienti dei file di registro o del meccanismo di registrazione, l'attaccante è in grado di eseguire tali azioni.	
Data	Dati Utente, Dati Sensori, CO2 Credits, NFT Token.	
Stimulus and Pre-conditions	<ul style="list-style-type: none"> • L'host di destinazione registra le azioni e i dati dell'utente. • L'host di destinazione non protegge sufficientemente l'accesso ai log o ai meccanismi di registrazione. • L'attaccante deve comprendere il funzionamento del meccanismo di registrazione. • Facoltativamente, l'aggressore deve conoscere la posizione e il formato delle singole voci dei file di registro. 	
Basic Flow	File Deletion (T1070.004):	L'attaccante elimina i file di registro critici per nascondere le sue tracce. Questo include la cancellazione dei log di sistema o di applicazioni specifiche, utilizzando comandi integrati del sistema operativo, script automatizzati o strumenti di hacking per rimuovere i file senza lasciare tracce evidenti.
Alternative Flow	Timestamp (T1070.006):	L'attaccante modifica i timestamp delle voci di registro per nascondere il momento reale delle attività.
Exception Flow	Clear Windows Event Logs (T1070.001):	L'attaccante svuota i registri degli eventi di Windows per eliminare prove di azioni non autorizzate, impedendo ai revisori di analizzare gli eventi precedenti.
Response and Postconditions	I sistemi log sono disattivati.	
Non Functional Requirements	Utilizzare un file di log immutabile per registrare gli eventi significativi, salvando l'identificativo univoco, il timestamp e il dettaglio dell'azione eseguita.	
Mitigations	Implementare un sistema di logging sicuro con controlli di integrità (es. hash) per rilevare modifiche.	

Comments	Audit log manipulation è particolarmente critico nei sistemi con elevate esigenze di tracciabilità e conformità normativa. Strumenti di monitoraggio attivi e protezioni anti-manomissione sono essenziali.	
Case Type	Abuse Case	Case ID AT-02
Case Name	Privilege Escalation (CAPEC 233)	
Actors	Supply Chain, Sistema, Attacker	
Description	Un attaccante sfrutta una debolezza che gli consente di aumentare i propri privilegi e di compiere un'azione che non dovrebbe essere autorizzato a compiere.	
Data	Dati Utente, Dati Sensori, CO2 Credits, NFT Token.	
Stimulus and Pre-conditions	<ul style="list-style-type: none"> Il sistema contiene un meccanismo di controllo dei privilegi mal configurato o vulnerabile. L'attaccante ha un accesso limitato al sistema. L'attaccante conosce o riesce a dedurre una vulnerabilità sfruttabile nel controllo dei privilegi. 	
Basic Flow	<i>Elevated Execution with Prompt</i> (T1548.004):	L'attaccante tenta di eseguire un programma o un comando privilegiato. In alcuni casi, se il sistema è mal configurato, l'attaccante può riuscire a ottenere privilegi elevati senza dover inserire una password.
Alternative Flow	<i>Bypass User Account Control</i> (T1548.002):	L'attaccante elude il controllo dell'User Account Control (UAC) su Windows per ottenere privilegi elevati senza l'intervento dell'utente. Questa tecnica è utile in scenari in cui l'attaccante ha accesso fisico o remoto al sistema, ma il controllo UAC non è configurato correttamente.
Exception Flow	<i>Temporary Elevated Cloud Access</i> (T1548.005):	L'attaccante ottiene temporaneamente privilegi elevati su un sistema cloud sfruttando configurazioni errate nelle policy di accesso. Questa tecnica è spesso vista in ambienti cloud pubblici, dove le credenziali o i permessi errati possono consentire a un attaccante di ottenere accesso privilegiato per un breve periodo.
Response and Postconditions	I privilegi aumentati vengono utilizzati per eseguire operazioni non autorizzate.	
Non Functional Requirements	Deve essere garantita una gestione dei privilegi sicura, proteggendo i meccanismi di escalation e prevenendo configurazioni errate. Monitoraggio continuo e auditing dei privilegi devono essere implementati per rilevare tentativi di escalation non autorizzati.	
Mitigations	Implementare l'autenticazione a più fattori (MFA) per azioni sensibili.	

Comments	È essenziale combinare MFA, monitoraggio continuo e gestione rigorosa dei privilegi per prevenire exploit di questo tipo.
-----------------	---

Case Type	Abuse Case	Case ID AT-03
Case Name	Exploiting Incorrectly Configured Access Control Security Levels (CAPEC 180)	
Actors	Supply Chain, Sistema, Attacker	
Description	Un aggressore sfrutta una debolezza nella configurazione dei controlli di accesso ed è in grado di aggirare la protezione prevista da queste misure e quindi ottenere un accesso non autorizzato al sistema o alla rete. Le funzionalità sensibili dovrebbero sempre essere protette con i controlli di accesso. Tuttavia, configurare tutti i sistemi di controllo di accesso, tranne quelli più banali, può essere molto complicato e ci sono molte opportunità di errori. Se un aggressore riesce a scoprire impostazioni di sicurezza di accesso configurate in modo errato, potrebbe essere in grado di sfruttarle in un attacco.	
Data	Dati Utente, Dati Sensori, CO2 Credits, NFT Token	
Stimulus and Pre-conditions	Il target deve applicare controlli di accesso, ma configurarli in modo errato. Tuttavia, non tutte le configurazioni errate possono essere sfruttate da un aggressore. Se la configurazione errata applica una sicurezza troppo bassa a qualche funzionalità, allora l'aggressore potrebbe essere in grado di sfruttarla se il controllo di accesso fosse l'unica cosa che impedisce l'accesso di un aggressore.	
Basic Flow	L'aggressore esamina l'applicazione di destinazione, possibilmente come un utente valido e autenticato. Esplora il sito web per trovare tutti i link disponibili. Utilizzare la forza bruta per indovinare tutti i nomi delle funzioni/azioni con privilegi diversi. L'aggressore esamina il controllo di accesso per funzioni e dati identificati nella fase di esplorazione per identificare potenziali debolezze nella configurazione dei controlli di accesso. L'aggressore tenta di ottenere l'accesso autenticato alle funzioni e ai dati presi di mira. L'aggressore tenta di accedere senza autenticazione alle funzioni e ai dati presi di mira. L'aggressore tenta di accedere indirettamente e tramite canali laterali alle funzioni e ai dati presi di mira. Accedere alla funzione o ai dati aggirando il controllo di accesso: l'aggressore esegue la funzione o accede ai dati identificati nella fase di esplorazione aggirando il controllo di accesso.	
Alternative Flow	DLL Search Order Hijacking (T1574.001):	L'attaccante sfrutta l'ordine di ricerca delle DLL nei sistemi Windows. Inserendo una DLL dannosa in una directory preferenziale, il sistema carica questa versione invece di quella legittima. Ciò consente all'attaccante di eseguire codice arbitrario con i privilegi dell'applicazione bersaglio.

Exception Flow	<i>Dylib Hijacking (T1574.004):</i>	L'attaccante sfrutta il meccanismo di caricamento delle librerie dinamiche. Inserendo una dylib malevola in una directory di ricerca prioritaria, l'attaccante può indurre un'applicazione a caricare la libreria modificata, permettendo l'esecuzione di codice dannoso.
Response and Postconditions	L'aggressore, sfruttando le debolezze nella configurazione, ottiene l'accesso al sistema per compiere azioni malevoli.	
Non Functional Requirements	Deve essere garantita un'accurata configurazione dei controlli di accesso, includendo protezioni contro l'accesso non autorizzato e verifiche regolari sulle configurazioni del sistema.	
Mitigations	Configurare correttamente il controllo degli accessi.	
Comments	Gli errori nelle configurazioni di accesso sono comuni ma possono essere mitigati tramite audit regolari e una corretta segmentazione delle directory e dei privilegi.	

Case Type	Abuse Case	Case ID AT-04
Case Name	Authentication Abuse (CAPEC 114)	
Actors	Supply Chain, Sistema, Attacker	
Description	Un aggressore ottiene l'accesso non autorizzato a un'applicazione, un servizio o un dispositivo tramite la conoscenza delle debolezze intrinseche di un meccanismo di autenticazione o sfruttando un difetto nell'implementazione dello schema di autenticazione. In un attacco di questo tipo, un meccanismo di autenticazione funziona, ma una sequenza di eventi attentamente controllata fa sì che il meccanismo conceda l'accesso all'aggressore.	
Data	Dati Utente, CO2 Credits, NFT Token	
Stimulus and Pre-conditions	<ul style="list-style-type: none"> • Un meccanismo o sottosistema di autenticazione che implementa una qualche forma di autenticazione, come password, autenticazione digest, certificati di sicurezza, ecc., che presenta qualche difetto. • Un'applicazione client, un accesso da riga di comando a un binario o un linguaggio di scripting in grado di interagire con il meccanismo di autenticazione. 	
Basic Flow	<i>Bypass User Account Control (T1548.002):</i>	L'attaccante sfrutta la configurazione errata del meccanismo di controllo degli account utente, consentendo l'esecuzione di codice arbitrario con privilegi elevati senza richiedere autorizzazioni.
Alternative Flow	<i>Elevated Execution with Prompt (T1548.004):</i>	L'attaccante induce l'utente a eseguire un'applicazione o uno script dannoso che sfrutta il prompt di elevazione per ottenere privilegi superiori.

Exception Flow	<i>Temporary Elevated Cloud Access (T1548.005):</i>	Utilizzando credenziali esposte o mal gestite, l'attaccante ottiene un accesso temporaneo con privilegi elevati su un servizio cloud.
Response and Postconditions	L'aggressore ottiene l'accesso non autorizzato ed effettua azioni malevoli.	
Non Functional Requirements	Garantire che tutti i meccanismi di autenticazione siano sicuri, includendo protezioni contro l'elevazione dei privilegi non autorizzata. Eseguire audit regolari per rilevare configurazioni errate o credenziali compromesse.	
Mitigations	<ul style="list-style-type: none"> • Applicare MFA • Imporre politiche di password robuste 	
Comments	Gli attacchi all'autenticazione sono una delle cause principali di compromissioni. La combinazione di MFA, auditing continuo e training degli utenti può ridurre significativamente il rischio.	

Case Type	Abuse Case	Case ID AT-05
Case Name	Targeted Malware (CAPEC 542)	
Actors	Supply Chain, Sistema, Attacker	
Description	Un avversario sviluppa malware mirati che sfruttano una vulnerabilità nota in un ambiente informatico aziendale. Il malware creato per questi attacchi si basa specificamente su informazioni raccolte sull'ambiente tecnologico. L'esecuzione corretta del malware consente a un avversario di ottenere un'ampia varietà di impatti tecnici negativi.	
Data	Dati Utente, Dati Sensori, CO2 Credits, NFT Token.	
Stimulus and Pre-conditions	<ul style="list-style-type: none"> • L'aggressore deve raccogliere informazioni sull'ambiente target. • Identificare vulnerabilità e creare malware ad hoc per sfruttarle. 	
Basic Flow	<i>Develop Capabilities(T1587.001):</i>	L'attaccante raccoglie informazioni sull'ambiente tecnologico e sviluppa un malware specifico mirato per sfruttare vulnerabilità conosciute.
Alternative Flow	<i>Binary Padding (T1027.001):</i>	L'attaccante applica padding ai file binari per mascherare la presenza di codice dannoso e impedire il rilevamento tramite analisi statica.
Exception Flow	<i>Software Packing (T1027.003):</i>	L'attaccante utilizza strumenti di packing per comprimere il file binario del malware, rendendo difficile l'analisi del contenuto e mascherando le attività dannose.
Response and Postconditions	L'aggressore riesce ad eseguire malware mirati contro il sistema.	

Non Functional Requirements	Garantire che il sistema effettui un monitoraggio avanzato per rilevare le minacce.
Mitigations	<ul style="list-style-type: none"> • Implementare strumenti di rilevamento. • Mantenere aggiornati i sistemi e i software.
Comments	Gli avversari spesso utilizzano tecniche di offuscamento quando sviluppano malware allo scopo di evitare il rilevamento o impedire al bersaglio di effettuare reverse engineering. Alcune di queste tecniche includono, ma non sono limitate a, binary padding, software packing, stripping di simboli e stringhe da un payload e utilizzo di risoluzione API dinamica.

Case Type	Abuse Case	Case ID AT-06
Case Name	Credential Stuffing (CAPEC 600)	
Actors	Supply Chain, Sistema, Attacker	
Description	Un avversario prova combinazioni di nome utente/password note contro sistemi, applicazioni o servizi diversi per ottenere un accesso autenticato aggiuntivo. Gli attacchi di Credential Stuffing si basano sul fatto che molti utenti sfruttano la stessa combinazione di nome utente/password per più sistemi, applicazioni e servizi.	
Data	Dati Utente, Dati Sensori, CO2 Credits, NFT Token.	
Stimulus and Pre-conditions	<ul style="list-style-type: none"> • Il sistema/l'applicazione utilizza l'autenticazione basata su password a un fattore, SSO e/o autenticazione basata su cloud. • Il sistema/l'applicazione non dispone di una solida politica sulle password da applicare. • Il sistema/l'applicazione non implementa un meccanismo efficace di limitazione delle password. • L'avversario possiede un elenco di account utente noti e delle relative password che potrebbero essere presenti sul bersaglio. • Una macchina con risorse sufficienti per il lavoro (ad esempio CPU, RAM, HD). • Un elenco noto di combinazioni nome utente/password. • Uno script personalizzato che sfrutta l'elenco delle credenziali per lanciare l'attacco. 	

Basic Flow	<p>Un avversario acquista combinazioni di nome utente/password violate o password con hash trapelate dal dark web. Un avversario sfrutta un keylogger o un attacco di phishing per rubare le credenziali dell’utente non appena vengono fornite. Un avversario conduce un attacco sniffing per rubare le credenziali mentre vengono trasmesse. Un avversario ottiene l’accesso a un database e sottrae gli hash delle password. Un avversario esamina i file di configurazione e di proprietà rivolti verso l’esterno per scoprire le credenziali codificate. Un avversario esamina i criteri delle password del sistema/applicazione di destinazione per determinare se le credenziali note rientrano nei criteri specificati. Un avversario esamina la lunghezza minima e massima consentita per le password. Un avversario esamina il formato delle password consentite. Un avversario esamina la politica di blocco dell’account. Prova ogni combinazione nome utente/password finché la destinazione non concede l’accesso. L’aggressore inserisce manualmente o automaticamente ciascuna combinazione nome utente/password tramite l’interfaccia del target. L’aggressore può utilizzare esperimenti o autenticazioni riuscite per impersonare un utente o un sistema autorizzato o per muoversi lateralmente all’interno di un sistema o di un’applicazione. Inoltre, possono essere iniettati nel sistema di destinazione o nel sistema di un utente vittima da un avversario. L’aggressore può anche spacciarsi per un utente legittimo per eseguire attacchi di ingegneria sociale. L’aggressore può ottenere dati sensibili contenuti nel sistema o nell’applicazione.</p>	
Alternative Flow	<i>Password Guessing(T1110.001):</i>	L’aggressore prova combinazioni di password facili o comuni per cercare di accedere al sistema, basandosi su informazioni conosciute sull’utente.
Exception Flow	<i>Password Spraying(T1110.003):</i>	L’attaccante prova una sola password su molteplici account per evitare il blocco degli account a causa di troppi tentativi falliti.
Response and Postconditions	L’aggressore riesce ad ottenere l’accesso al sistema.	
Non Functional Requirements	Garantire il monitoraggio dei registri di sistema e l’implementazione dell’autenticazione a più fattori.	
Mitigations	<ul style="list-style-type: none"> • Utilizzare l’autenticazione a più fattori per tutti i servizi di autenticazione. • Monitorare i registri di sistema e di dominio per rilevare eventuali accessi anomali alle credenziali. 	
Comments	Gli attacchi di Credential Stuffing sono più efficaci quando gli utenti riutilizzano le stesse credenziali su più servizi. L’adozione di MFA può ridurre significativamente l’impatto di questi attacchi.	

Case Type	Abuse Case	Case ID AT-07
Case Name	Cryptanalysis (CAPEC 97)	

Actors	Supply Chain, Sistema, Attacker	
Description	<p>La crittoanalisi è un processo di individuazione di debolezze negli algoritmi crittografici e di utilizzo di tali debolezze per decifrare il testo cifrato senza conoscere la chiave segreta. A volte la debolezza non è nell'algoritmo crittografico in sé, ma piuttosto nel modo in cui viene applicato, il che rende la crittoanalisi un successo. Un aggressore può avere anche altri obiettivi, come: Total Break (trovare la chiave segreta), Global Deduction (trovare un algoritmo funzionalmente equivalente per la crittografia e la decrittografia che non richieda la conoscenza della chiave segreta), Information Deduction (ottenere alcune informazioni sui testi in chiaro o sui testi cifrati che non erano precedentemente note) e Distinguishing Algorithm (l'aggressore ha la capacità di distinguere l'output della crittografia (testo cifrato) da una permutazione casuale di bit).</p>	
Data	Dati Utente, Dati Sensori	
Stimulus and Pre-conditions	<ul style="list-style-type: none"> • Il software di destinazione utilizza una sorta di algoritmo crittografico. • Esiste un punto debole di fondo nell'algoritmo crittografico utilizzato o nel modo in cui è stato applicato a una particolare porzione di testo in chiaro. • L'algoritmo di crittografia è noto all'aggressore. • Un utente malintenzionato ha accesso al testo cifrato. • I requisiti delle risorse informatiche varieranno in base alla complessità di una determinata tecnica di crittoanalisi. È inoltre richiesto l'accesso alle routine di crittografia/decrittografia dell'algoritmo. 	
Basic Flow	<i>Data Encrypted (T1486):</i>	L'attaccante tenta di eseguire un attacco per cifrare o "rendere irrecuperabili" i dati, al fine di applicare un "Total Break" per ottenere la chiave segreta e decifrare il testo cifrato. Questo si riferisce all'uso della crittografia per impedire l'accesso ai dati fino al raggiungimento della chiave segreta.
Alternative Flow	<i>Application Layer Protocol (T1437.001):</i>	L'aggressore cerca di raccogliere informazioni dal testo cifrato per determinare il tipo di algoritmo utilizzato e individuare una possibile debolezza nell'implementazione del sistema.
Exception Flow	<i>DNS (T1071.004):</i>	Se l'attacco crittografico viene rilevato, l'aggressore può tentare di mascherare il traffico o le comunicazioni attraverso il DNS per continuare a estrarre informazioni cifrate senza essere scoperto.

Response and Postconditions	L'aggressore riesce a decifrare il testo cifrato.
Non Functional Requirements	Garantire l'utilizzo di algoritmi di crittografia robusti e sicuri e un aggiornamento regolare delle chiavi.
Mitigations	<ul style="list-style-type: none"> • Utilizzare algoritmi di crittografia moderni • Rimanere aggiornati sulle vulnerabilità crittografiche e applicare immediatamente patch quando vengono identificate nuove debolezze
Comments	La crittoanalisi può sfruttare diversi approcci a seconda delle debolezze del sistema di cifratura. È fondamentale che i sistemi utilizzino algoritmi sicuri e aggiornati, e che vengano applicate le best practice in materia di sicurezza crittografica.

Case Type	Abuse Case	Case ID AT-08
Case Name	Brute Force (CAPEC 112)	
Actors	Supply Chain, Sistema, Attacker	
Description	In questo attacco, un asset (informazioni, funzionalità, identità, ecc.) è protetto da un valore segreto finito. L'attaccante tenta di ottenere l'accesso a questo asset utilizzando tentativi ed errori per esplorare in modo esaustivo tutti i possibili valori segreti nella speranza di trovare il segreto (o un valore funzionalmente equivalente) che sbloccherà l'asset.	
Data	Dati Utente	

Stimulus and Pre-conditions	<ul style="list-style-type: none"> L'attaccante deve essere in grado di determinare quando ha indovinato con successo il segreto. In quanto tali, i one-time pad sono immuni a questo tipo di attacco, poiché non c'è modo di determinare quando un'ipotesi è corretta. Non sono richieste risorse specializzate per eseguire questo tipo di attacco. La velocità con cui un aggressore scopre un segreto è direttamente proporzionale alle risorse computazionali che l'aggressore ha a disposizione. Questo metodo di attacco è costoso in termini di risorse: avere grandi quantità di potenza computazionale non garantisce un successo tempestivo, ma avere solo risorse minime rende il problema intrattabile contro tutte le procedure di selezione dei segreti, tranne le più deboli. L'attacco richiede semplicemente una capacità di scripting di base per automatizzare l'esplorazione dello spazio di ricerca. Gli aggressori più sofisticati potrebbero essere in grado di utilizzare metodi più avanzati per ridurre lo spazio di ricerca e aumentare la velocità con cui viene individuato il segreto.
Basic Flow	<p>L'aggressore analizza le possibilità di parallelizzare l'attacco, sfruttando risorse multiple per dividere lo spazio di ricerca e accelerare il processo di brute force. Tuttavia, un collo di bottiglia, come la necessità di controllare risposte con un'autorità esterna, può compromettere l'efficacia dell'attacco. Inoltre, si concentra sulla riduzione dello spazio di ricerca, identificando modalità per restringere il numero di ipotesi necessarie. Ad esempio, se la password è stata generata algoritmicamente, l'analisi dell'algoritmo potrebbe rivelare schemi che ne riducono la complessità. L'aggressore può ricorrere alla crittoanalisi per scoprire debolezze nei generatori casuali, individuare periodicità o schemi, oppure impiegare tecniche di ingegneria sociale per studiare le abitudini del bersaglio. Informazioni su segreti precedenti possono offrire indizi utili, come sostituzioni di caratteri o preferenze tematiche (date, nomi, testi). Tali informazioni consentono di focalizzare i tentativi iniziali su aree più probabili dello spazio di ricerca. In alcuni casi, l'aggressore può determinare caratteristiche specifiche del segreto, come la lunghezza o il carattere iniziale, eliminando così ampie porzioni dello spazio possibile. Infine, l'aggressore raccoglie informazioni utili per eseguire l'attacco in modo indipendente. Può, ad esempio, catturare un testo crittografato o un dizionario di password, riducendo la necessità di consultare un'autorità esterna. Questo approccio aumenta l'efficacia dell'attacco.</p>

Alternative Flow	<i>Password Guessing (T1110.001):</i>	L'aggressore prova combinazioni di password facili o comuni per cercare di accedere al sistema, basandosi su informazioni conosciute sull'utente.
Exception Flow	<i>Credential Stuffing (T1110.004):</i>	L'aggressore utilizza un elenco di credenziali compromesse per tentare l'accesso a più servizi e applicazioni.
Response and Postconditions	L'attaccante riesce ad ottenere l'accesso all'asset.	
Non Functional Requirements	Garantire l'utilizzo della MFA e un controllo sul numero di tentativi di login.	
Mitigations	<ul style="list-style-type: none"> • Usare MFA. • Limitare i tentativi di login. 	
Comments	Gli attacchi di brute force possono essere ridotti significativamente con misure di sicurezza come la MFA, la limitazione dei tentativi e il monitoraggio continuo delle attività sospette.	

Case Type	Abuse Case	Case ID AT-09
Case Name	Phishing (CAPEC 98)	
Actors	Supply Chain, Sistema, Attacker	
Description	Il phishing è una tecnica di ingegneria sociale in cui un aggressore si maschera da entità legittima con cui la vittima potrebbe fare affari per indurre l'utente a rivelare alcune informazioni riservate (molto spesso credenziali di autenticazione) che possono essere utilizzate in seguito da un aggressore. Il phishing è essenzialmente una forma di raccolta di informazioni o "pesca" di informazioni.	
Data	Dati Utente	
Stimulus and Pre-conditions	Un aggressore deve avere un modo per avviare un contatto con la vittima. In genere ciò avverrà tramite e-mail. Un utente malintenzionato deve indovinare correttamente l'entità con cui la vittima fa affari e impersonificarla. Nella maggior parte dei casi i phisher utilizzano semplicemente le banche/servizi più popolari e inviano i loro "ganci" a molte potenziali vittime. Un utente malintenzionato deve disporre di un invito all'azione sufficientemente convincente da indurre l'utente ad agire. Ad esempio un sito Web replicato che deve apparire estremamente simile al sito Web originale e l'URL utilizzato per accedere a quel sito Web deve assomigliare all'URL reale di detta entità aziendale.	

Basic Flow	L'aggressore acquisisce un nome di dominio che visivamente somiglia al dominio di un sito legittimo. Successivamente, l'aggressore esplora il sito legittimo e ne crea una copia fedele. Questo può avvenire utilizzando software di spidering per scaricare copie delle pagine web, salvando manualmente le pagine o sviluppandone di nuove che riproducano fedelmente il design e le funzionalità dell'originale. Il sito contraffatto presenta spesso un modulo di accesso in cui la vittima è indotta a inserire le proprie credenziali di autenticazione. Sebbene il contenuto possa essere copiato dall'originale, a volte gli aggressori creano pagine con contenuti nuovi, ma con un aspetto e una struttura simili al sito autentico. Una volta ottenute informazioni sensibili, come credenziali di accesso o dati della carta di credito, l'aggressore può sfruttarle per scopi fraudolenti.	
Alternative Flow	<i>Spearphishing</i> (T1566.002):	<i>Link</i> L'aggressore invia un'e-mail con un link che reindirizza la vittima a un sito web di phishing dove le credenziali vengono rubate o altre informazioni riservate vengono raccolte.
Exception Flow	<i>DNS</i> (T1071.004):	Se l'attaccante è ostacolato nell'invio di email di phishing tramite canali tradizionali, può utilizzare il traffico DNS come canale di comunicazione per condurre l'attacco di phishing bypassando le restrizioni sui protocolli di posta elettronica.
Response and Postconditions	L'aggressore riesce ad ottenere le informazioni riservate.	
Non Functional Requirements	Garantire l'implementazione di filtri avanzati e il monitoraggio e l'analisi delle attività anomale.	
Mitigations	Utilizzare filtri per email e monitorare attività email anomale.	
Comments	Gli attacchi di phishing sono tra le tecniche più comuni di ingegneria sociale e richiedono l'uso di misure preventive come filtri di posta elettronica, alert di phishing e autenticazione a più fattori.	

Case Type	Abuse Case	Case ID AT-10
Case Name	Typo Squatting (CAPEC 630)	
Actors	Supply Chain, Sistema, Attacker	
Description	Un avversario registra un nome di dominio con almeno un carattere diverso da un dominio attendibile. Un attacco TypoSquatting sfrutta i casi in cui un utente digita male un URL (ad esempio www.goggle.com) o non verifica visivamente un URL prima di cliccarci sopra (ad esempio attacco di phishing). Di conseguenza, l'utente viene indirizzato a una destinazione controllata dall'avversario. TypoSquatting non richiede un attacco contro il dominio attendibile o un reverse engineering complicato.	
Data	Dati Utente	

Stimulus and Pre-conditions	Un avversario richiede la conoscenza di domini popolari o ad alto traffico, che potrebbero essere utilizzati per ingannare potenziali obiettivi.	
Basic Flow	<p>Masquerade Task or Service (T1036.004): L'avversario identifica inizialmente siti web popolari o ad alto traffico, puntando su quelli considerati affidabili per massimizzare l'efficacia dell'attacco. Successivamente, registra un dominio sfruttando errori tipografici (TypoSquatting) per imitare il sito legittimo, conferendo al dominio fraudolento un'apparenza familiare e credibile.</p> <p>Per attirare le vittime sul sito falso, l'aggressore utilizza strategie come attacchi di phishing. Invia e-mail ingannevoli contenenti collegamenti al dominio TypoSquatted, persuadendo gli utenti a cliccarli. In alternativa, sfrutta errori di digitazione che possono portare inconsapevolmente gli utenti al sito fraudolento. Questi metodi consentono all'avversario di dirottare il traffico verso il proprio dominio malevolo, compromettendo la sicurezza delle vittime.</p>	
Alternative Flow	<i>Match Legitimate Name or Location</i> (T1036.005):	L'aggressore può registrare un dominio che corrisponde al nome legittimo o alla posizione di un'organizzazione per aumentare la probabilità che l'utente lo confonda con il sito legittimo e venga ingannato in un attacco di phishing.
Exception Flow	DNS (T1071.004):	Se l'attaccante è in grado di utilizzare un nome di dominio simile a quello legittimo, ma mascherato attraverso il traffico DNS, potrebbe bypassare alcuni sistemi di protezione e fare in modo che il traffico verso il sito compromesso non venga rilevato facilmente.
Response and Postconditions	L'aggressore riesce a registrare un nome di dominio errato.	
Non Functional Requirements	Garantire il monitoraggio e la protezione dei nomi di dominio.	
Mitigations	<ul style="list-style-type: none"> • Registrare le versioni più comuni di errori di battitura del proprio dominio • Monitorare le registrazioni di domini per individuare possibili typo-squatting 	
Comments	Gli attacchi di typo-squatting sono difficili da prevenire, ma le buone pratiche di educazione degli utenti e di monitoraggio dei domini possono ridurre significativamente il rischio.	

Case Type	Abuse Case	Case ID AT-11
Case Name	Pull Data From System Resources (CAPEC 545)	
Actors	Supply Chain, Sistema, Attacker	

Description	Un avversario autorizzato o in grado di cercare risorse di sistema note, lo fa con l'intenzione di raccogliere informazioni utili. Le risorse di sistema includono file, memoria e altri aspetti del sistema di destinazione. In questo schema di attacco, l'avversario non sa necessariamente cosa troverà quando inizia a estrarre dati.	
Data	Dati Utente, Dati Sensori, CO2 Credits, NFT Token.	
Stimulus and Pre-conditions	L'attaccante deve essere in grado di avere accesso alle risorse di sistema.	
Basic Flow	Data from Local System (T1005): L'attaccante esegue uno script o utilizza uno strumento per scoprire e raccogliere dati dalle risorse di sistema del target, come file, directory, o configurazioni di sistema, senza conoscere preventivamente cosa troverà.	
Alternative Flow	<i>Keychain (T1555.001):</i>	L'aggressore raccoglie le credenziali di sistema da un keychain per ottenere accesso a password o altre informazioni riservate memorizzate nel sistema.
Exception Flow		
Response and Postconditions	L'aggressore riesce ad ottenere le informazioni di interesse.	
Non Functional Requirements	Garantire l'applicazione di rigorosi controlli di accesso alle risorse di sistema sensibili e il monitoraggio in tempo reale degli accessi non autorizzati.	
Mitigations	Applicare controlli di accesso rigorosi e logging sulle risorse di sistema sensibili.	
Comments	L'attacco può avvenire in modo discreto, sfruttando l'accesso legittimo o compromesso alle risorse di sistema, rendendo difficile rilevarlo senza strumenti di monitoraggio avanzati.	

Case Type	Abuse Case	Case ID AT-12
Case Name	Reusing Session Ids (CAPEC 60)	
Actors	Supply Chain, Sistema, Attacker	
Description	Questo attacco mira al riutilizzo di un ID di sessione valido per falsificare il sistema di destinazione al fine di ottenere privilegi. L'attaccante tenta di riutilizzare un ID di sessione rubato utilizzato in precedenza durante una transazione per eseguire spoofing e dirottamento di sessione. Un altro nome per questo tipo di attacco è Session Replay.	
Data	Dati Utente, CO2 Credits	
Stimulus and Pre-conditions	L'host di destinazione utilizza gli ID di sessione per tenere traccia degli utenti. Gli ID di sessione vengono utilizzati per controllare l'accesso alle risorse. Gli ID di sessione utilizzati dall'host di destinazione non sono ben protetti dal furto di sessione.	
Basic Flow	L'aggressore interagisce con l'host di destinazione e scopre che gli ID di sessione vengono utilizzati per autenticare gli utenti. L'aggressore ruba un ID di sessione da un utente valido. Infine l'aggressore tenta di utilizzare l'ID di sessione rubato per ottenere l'accesso al sistema con i privilegi del proprietario originale dell'ID di sessione.	

Alternative Flow	<i>Web Session Cookie</i> (T1550.004):	L'attaccante ottiene un cookie di sessione valido tramite vari metodi (ad esempio, sniffing di rete o XSS) e lo usa per accedere al sistema senza bisogno di ri-autenticarsi.
Exception Flow	<i>Application Layer Protocol</i> (T1071):	Se il sistema implementa un controllo della validità dell'ID di sessione, l'attaccante potrebbe essere bloccato nel tentativo di utilizzare un ID di sessione rubato. L'attaccante tenterà di aggirare questo controllo modificando l'ID di sessione o provando altre tecniche di spoofing.
Response and Postconditions	L'aggressore riesce a riutilizzare un ID di sessione.	
Non Functional Requirements	Garantire una gestione sicura delle sessioni e implementazione di tecniche di protezione avanzate contro il furto di sessione.	
Mitigations	<ul style="list-style-type: none"> • Usare pratiche di gestione delle sessioni sicure, generare ID di sessione unici • Utilizzare autenticazione a più fattori 	
Comments	L'attacco può avere impatti significativi su sistemi che non gestiscono correttamente le sessioni, in particolare su quelli che non implementano un controllo rigoroso degli ID di sessione e della loro validità.	

Case Type	Abuse Case	Case ID AT-13
Case Name	Development Alteration (CAPEC 444)	
Actors	Supply Chain, Sistema, Attacker	
Description	Un avversario modifica una tecnologia, un prodotto o un componente durante il suo sviluppo per ottenere un impatto negativo una volta che il sistema è distribuito. L'obiettivo dell'avversario è modificare il sistema in modo tale che l'impatto negativo possa essere sfruttato quando il sistema viene distribuito in seguito. Gli attacchi di alterazione dello sviluppo possono includere attacchi che inseriscono logica dannosa nel software del sistema, modificano o sostituiscono componenti hardware e altri attacchi che hanno un impatto negativo sul sistema durante lo sviluppo. Questi attacchi richiedono generalmente l'accesso interno per modificare il codice sorgente o manomettere i componenti hardware. Il prodotto viene quindi consegnato all'utente dove l'impatto negativo può essere sfruttato in un secondo momento.	
Data	Dati Sensori, CO2 Credits, NFT Token	
Stimulus and Pre-conditions	Accesso al sistema durante la fase di sviluppo per alterare e/o modificare componenti software e hardware. Questo accesso è spesso ottenuto tramite accesso interno o sfruttando un altro schema di attacco per ottenere permessi che l'avversario normalmente non avrebbe.	

Basic Flow	<i>Compromise Software Dependencies and Development Tools (T1195.001):</i>	L'attaccante compromette le dipendenze software e gli strumenti di sviluppo, alterando le librerie, i pacchetti o gli strumenti utilizzati nel processo di sviluppo per inserire vulnerabilità o comportamenti dannosi nel software che verrà distribuito agli utenti finali.
Alternative Flow	<i>Compromise Software Supply Chain (T1195.002):</i>	L'attaccante compromette la catena di approvvigionamento software, manipolando i pacchetti o i componenti software utilizzati durante lo sviluppo per iniettare codice dannoso o vulnerabilità che si propagheranno nel prodotto finale.
Exception Flow	<i>Compromise Hardware Supply Chain (T1195.003):</i>	L'attaccante compromette la catena di approvvigionamento hardware, modificando o alterando i componenti hardware durante la fase di sviluppo. Questi componenti compromettono il prodotto finale una volta che vengono integrati nel sistema o nel dispositivo.
Response and Postconditions	L'aggressore riesce a modificare una tecnologia, un prodotto o un componente.	
Non Functional Requirements	Garantire l'applicazione di un controllo rigoroso sulle modifiche al codice.	
Mitigations	Applicare un controllo rigoroso sulle modifiche al codice e utilizzare strumenti di gestione del codice sorgente con restrizioni di accesso.	
Comments	Questo tipo di attacco è particolarmente insidioso, in quanto l'impatto negativo non si verifica immediatamente, ma solo quando il prodotto o sistema compromesso viene distribuito e utilizzato dagli utenti finali.	

Case Type	Abuse Case	Case ID AT-14
Case Name	Input data manipulation (CAPEC 153)	
Actors	Supply Chain, Sistema, Attacker	
Description	Un aggressore sfrutta una debolezza nella convalida dell'input controllando il formato, la struttura e la composizione dei dati in un'interfaccia di elaborazione dell'input. Fornendo input in un formato non standard o inaspettato, un aggressore può avere un impatto negativo sulla sicurezza del target.	
Data	Dati Sensori	
Stimulus and Pre-conditions	Accettare i dati dell'utente per l'elaborazione e il modo in cui tali dati vengono elaborati deve dipendere da qualche aspetto del formato o dei flag che l'aggressore può controllare.	
Basic Flow	<i>Web Protocols (T1071.001):</i>	L'aggressore manipola i dati in input tramite protocolli web, come HTTP o HTTPS, fornendo input malformati o intenzionalmente alterati per influenzare l'elaborazione dei dati, sfruttando la mancanza di validazione lato server.

Alternative Flow	<i>File Transfer Protocol (FTP) (T1071.002):</i>	L'attaccante sfrutta la manipolazione di dati in input tramite FTP per inviare file malevoli o alterati al sistema target, sfruttando debolezze nella gestione dei file e nella validazione dei dati.
Exception Flow	<i>File and Directory Permissions Modification (T1222):</i>	Se il sistema di destinazione non ha una protezione adeguata per la gestione dei file o delle directory, l'aggressore potrebbe manipolare la configurazione dei permessi sui file per consentire l'esecuzione di input dannosi o la modifica di configurazioni sensibili che influenzano la sicurezza del sistema.
Response and Postconditions	L'aggressore riesce a manipolare l'input.	
Non Functional Requirements	Garantire la validazione di tutti gli input utente e l'applicazione di pratiche di codifica sicure per prevenire manipolazioni.	
Mitigations	<ul style="list-style-type: none"> • Validare tutti gli input utente • Applicare pratiche di codifica sicure 	
Comments	La manipolazione dell'input è una tecnica comune utilizzata per sfruttare vulnerabilità nei sistemi che non eseguono una corretta validazione o sanificazione dei dati. L'implementazione di misure preventive può ridurre significativamente il rischio.	

Case Type	Abuse Case	Case ID AT-15
Case Name	Transaction or an event tampering via application API manipulation (CAPEC 385)	
Actors	Supply Chain, Sistema, Attacker	
Description	Un aggressore ospita o si unisce a un evento o a una transazione all'interno di un framework applicativo per modificare il contenuto di messaggi o elementi che vengono scambiati. L'esecuzione di questo attacco consente all'aggressore di manipolare il contenuto in modo tale da produrre messaggi o contenuti che sembrano autentici ma possono contenere collegamenti ingannevoli, sostituire un elemento o un altro, falsificare un elemento esistente e condurre uno scambio falso o altrimenti modificare gli importi o l'identità di ciò che viene scambiato. Le tecniche richiedono l'uso di software specializzati che consentono all'aggressore di comunicare in modalità man-in-the-middle tra il browser Web e il sistema remoto per modificare il contenuto di vari elementi dell'applicazione. Spesso, gli elementi scambiati nel gioco possono essere monetizzati tramite vendite di monete, dollari virtuali, ecc. Lo scopo dell'attacco è truffare la vittima intrappolando i pacchetti di dati coinvolti nello scambio e alterando l'integrità del processo di trasferimento.	
Data	CO2 Credits, NFT Token	

Stimulus and Pre-conditions	Il software mirato utilizza le API del framework applicativo. Un programma software che consente l'uso di comunicazioni Adversary-in-the-Middle (CAPEC-94) tra client e server, come un proxy man-in-the-middle.	
Basic Flow	<i>LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001):</i>	L'attaccante sfrutta la vulnerabilità di LLMNR (Link-Local Multicast Name Resolution) e NBT-NS (NetBIOS over TCP/IP) per eseguire un attacco di poisoning della cache di nome, intercettando le richieste di rete e redirigendo la comunicazione API tra client e server al suo sistema.
Alternative Flow	<i>ARP Cache Poisoning (T1557.002):</i>	L'aggressore sfrutta una vulnerabilità nella cache ARP (Address Resolution Protocol), manipolando le risposte ARP tra client e server per indirizzare tutto il traffico API verso il proprio sistema, intercettando e modificando i dati.
Exception Flow	<i>DHCP Spoofing (T1557.003):</i>	L'aggressore impersona un server DHCP (Dynamic Host Configuration Protocol) falso, assegnando indirizzi IP malintenzionati al client per redirigere il traffico API verso il proprio sistema. Questo consente all'aggressore di intercettare e manipolare le comunicazioni.
Response and Postconditions	L'aggressore riesce a modificare il contenuto di messaggi o elementi che vengono scambiati.	
Non Functional Requirements	Garantire l'implementazione di meccanismi di sicurezza nelle comunicazioni API.	
Mitigations	Implementare controlli di sicurezza API gateway e convalidare rigorosamente le richieste API.	
Comments	Il rischio di manipolazione delle transazioni o degli eventi tramite API è elevato quando la protezione delle comunicazioni non è adeguata. La gestione sicura delle API è fondamentale per prevenire attacchi di tipo man-in-the-middle.	

2.4 Misuse Case

In questa sezione, vengono riportati gli schemi di Jacobson relativi agli misuse case.

Case Type	Misuse Case	Case ID MS-01
Case Name	Condivisione non sicura delle credenziali	
Actors	Supply Chain, Sistema, Clumsy Actor	
Description	L'utente condivide accidentalmente le proprie credenziali con un collega o le scrive in un luogo visibile, rendendole accessibili a persone non autorizzate.	
Data	Dati Utente, CO2 Credits	

Stimulus and Pre-conditions	L'utente necessita di accedere frequentemente al sistema e, per comodità, scrive le credenziali o le condivide via e-mail o chat aziendale.
Basic Flow	L'utente scrive o invia le credenziali. Una terza persona non autorizzata ottiene l'accesso al sistema.
Alternative Flow	L'utente conserva le credenziali in un file non sicuro. Un malware o un attaccante accede al file.
Exception Flow	
Response and Postconditions	Possibile accesso non autorizzato al sistema da parte di attori interni o esterni.
Non Functional Requirements	Garantire l'avviso dell'utente se le credenziali vengono utilizzate da dispositivi o luoghi insoliti.
Mitigations	<ul style="list-style-type: none"> • Utilizzo di autenticazione a più fattori (MFA) • Educazione degli utenti sulla gestione sicura delle credenziali
Comments	La mitigazione deve essere supportata da policy aziendali rigorose.

Case Type	Misuse Case	Case ID MS-02
Case Name	Accettazione errata di una transazione	
Actors	Supply Chain, Sistema, Clumsy Actor	
Description	L'utente accetta una transazione di CO2 Credits che non dovrebbe essere approvata a causa di dati mancanti o incongruenti.	
Data	CO2 Credits	
Stimulus and Pre-conditions	Il sistema consente all'utente di accettare manualmente le transazioni. La verifica automatica non segnala incongruenze o l'utente ignora i warning.	
Basic Flow	L'utente visualizza una transazione. L'utente accetta la transazione senza controllare.	
Alternative Flow		
Exception Flow		
Response and Postconditions	Transazione non valida o fraudolenta completata, con conseguenti perdite economiche o violazione delle policy aziendali.	
Non Functional Requirements	Garantire la rilevazione di anomalie nei dati della transazione e bloccare transazioni sospette.	
Mitigations	<ul style="list-style-type: none"> • Doppia conferma per transazioni critiche • Automazione delle verifiche di coerenza dei dati 	
Comments	Include controlli automatici sulle regole di business per le transazioni.	

Case Type	Misuse Case	Case ID MS-03
Case Name	Sessione non disconnessa su dispositivo condiviso	
Actors	Supply Chain, Sistema, Clumsy Actor	
Description	L'utente non disconnette la propria sessione su un dispositivo condiviso, lasciando accesso aperto ai propri dati e funzionalità.	

Data	Dati Utente, CO2 Credits
Stimulus and Pre-conditions	L'utente utilizza un dispositivo condiviso, come un computer aziendale, ma dimentica di effettuare il logout.
Basic Flow	L'utente accede al sistema. Dimentica di disconnettersi. Un'altra persona utilizza il dispositivo e accede ai suoi dati.
Alternative Flow	
Exception Flow	
Response and Postconditions	Possibile violazione della privacy o accesso non autorizzato a dati sensibili.
Non Functional Requirements	Garantire timeout automatici e logout forzati su dispositivi condivisi.
Mitigations	Educazione degli utenti sull'importanza del logout.
Comments	Potrebbe essere utile un sistema di notifica che segnala sessioni aperte su dispositivi condivisi.

CAPITOLO 3

Design Sicuro

Il design costituisce la seconda fase del processo per la realizzazione di un software; essa risulta fondamentale per la creazione di sistemi affidabili e resistenti alle minacce. Occuparsi della sicurezza fin dalle prime fasi di progettazione è cruciale. Infatti, è estremamente complesso e spesso inefficace rendere sicuro un sistema per il quale non è stata originariamente data rilevanza alle tematiche legate alla sicurezza.

In questo capitolo, descriveremo le scelte effettuate nella fase di design per il nostro progetto. Come prima cosa, è bene ricordare che la progettazione sicura influenza profondamente altre caratteristiche del sistema, quali la *performance*, l'*usability* e l'*acceptability*. Infatti, l'implementazione dei controlli di sicurezza aggiuntivi può rallentare il sistema e incidere negativamente sia sui tempi di risposta che sulla facilità di comprensione per l'utente finale.

Nelle successive sezioni, riportiamo le scelte effettuate durante questa fase. Esse riguardano:

- **Architettura:** In questa sezione discuteremo delle scelte architettoniche effettuate per il nostro progetto;
- **Design degli asset:** In questa sezione tratteremo delle strategie utili alla progettazione degli asset;
- **Scelte Tecnologiche:** In questa sezione discuteremo le varie scelte tecnologiche per il nostro progetto.
- **Modellazione mediante Markov chain di una unità:** In questa sezione tratteremo la rappresentazione di un processo tramite catena di Markov e, attraverso essa, verificheremo una proprietà di Safety e una di Response.

3.1 Architettura

In questa fase dobbiamo scegliere l'architettura del sistema che stiamo progettando, considerando, che in generale, essa può essere *Centralizzata/Decentralizzata* e *Distribuita/Non Distribuita*. In particolare, il nostro sistema prevede l'utilizzo di una blockchain. Sarà quindi presente una parte on-chain e una off-chain. Il sistema on-chain possiede un'architettura distribuita, decentralizzata e diversificata. Una blockchain è considerata distribuita perché i dati sono memorizzati in una rete di nodi, sparsi in diverse località geografiche. Ogni

nodo della rete ha una copia del registro completo o parziale della blockchain. Quando una nuova transazione viene aggiunta, viene replicata su tutti i nodi della rete. La blockchain è decentralizzata, ovvero non esiste un'autorità centrale che controlla la rete. In essa, il consenso per l'approvazione delle transazioni viene raggiunto attraverso un meccanismo distribuito che coinvolge più nodi. Una blockchain è considerata diversificata perché i componenti ridondanti del sistema, come i nodi, sono spesso di diverso tipo. Questa diversità aumenta la probabilità che eventuali guasti non si verifichino nello stesso modo su tutti i componenti. Inoltre, la blockchain, oltre ad essere decentralizzata, distribuita e diversificata, implementa delle tecniche di offuscamento, monitoraggio e isolamento, consentendo di raggiungere un buon livello di protezione, tolleranza ai guasti e resilienza. Le blockchain, offuscano le identità degli utenti tramite indirizzi crittografici, non collegati direttamente a informazioni personali. Ogni nodo della rete mantiene una copia completa della blockchain, consentendo il monitoraggio delle transazioni in tempo reale. Inoltre, tutti i blocchi sono verificati e validati da più nodi, aumentando la trasparenza e prevenendo modifiche non autorizzate. La blockchain è isolata in quanto ogni nodo opera indipendentemente e ha una copia separata del registro. Una volta confermate, le transazioni sono immutabili.

Per quanto riguarda l'architettura off-chain, abbiamo scelto un modello centralizzato, in cui tutte le decisioni e la gestione dell'applicativo vengono prese da un unico nodo centrale. Questo nodo è responsabile della gestione delle informazioni non memorizzate sulla blockchain e dell'interazione con quest'ultima. In particolare, per la memorizzazione delle informazioni abbiamo scelto di utilizzare un database in cloud che permetterà di distribuire gli asset su nodi fisici differenti.

3.2 Design degli asset

In questa sezione, riportiamo la fase di design degli asset. Essa consiste nello scegliere alcune linee guida proposte da OWASP, Saltzer & Schroeder e Sommerville, le quali verranno illustrate nelle successive sottosezioni.

3.2.1 Sommerville

Per quanto riguarda le linee guida di Sommerville, proposte nel 2017, abbiamo scelto:

- **Avoid a single point of failure:** Questa linea guida suggerisce di evitare possibili single point of failure, facendo sì che un singolo errore non possa compromettere totalmente il sistema.
- **Use redundancy and diversity to reduce risk:** Questa linea guida consiglia di usare ridondanza e diversità, consentendo di ridurre il rischio. In particolare, ciò sarà garantito dall'utilizzo della blockchain.
- **Specify the format of all system input:** Questa strategia suggerisce di verificare e filtrare tutti gli input del sistema.
- **User log action:** Questa strategia suggerisce di registrare e monitorare le attività degli utenti per garantire sicurezza, conformità e rilevamento delle minacce.
- **Compartmentalize your asset:** Questa linea guida consiglia di distribuire gli asset tra i vari componenti.
- **Design for deployment:** Questa strategia suggerisce di descrivere i vari passaggi per un deployment sicuro.

3.2.2 OWASP

Per quanto riguarda le linee guida fornite da OWASP, proposte nel 2016, abbiamo scelto:

- **Minimize Attack surface Area:** Questa linea guida consiglia di ridurre la superficie di attacco al fine di diminuire il rischio, limitando i modi che un utente malevolo ha per attaccare il sistema.
- **Defense in depth:** Questa linea guida consiglia di implementare diversi meccanismi di difesa per uno stesso asset al fine di ridurre le possibilità che un attacco ha di avere successo. Un possibile esempio è l'implementazione dell'autenticazione a più fattori.
- **Establish Secure Default:** Questa strategia suggerisce di definire delle regole di sicurezza applicate di default dal sistema. Ad esempio si potrebbero adottare automaticamente politiche di password sicure.
- **Don't trust services:** Questo principio consiglia di fidarsi il meno possibile dei servizi esterni, facendo sì che tutte le decisioni vengano prese internamente al sistema.
- **Separation of duties:** Questa linea guida suggerisce di separare i compiti tra i vari ruoli, consentendo ad ogni figura di poter svolgere solamente le attività ad essa collegate.

3.2.3 Saltzer & Schroeder

Per quanto riguarda le linee guida di Saltzer & Schroeder, proposte nel 1975, abbiamo scelto:

- **Least privilege:** Questa strategia consiglia di assegnare ai vari utenti solo i privilegi strettamente necessari a svolgere le proprie attività. In particolare, si forniranno alle varie tipologie di utenti solamente le funzionalità essenziali. Ad esempio, l'amministratore di sistema avrà solamente i privilegi per svolgere le proprie attività senza poter compiere azioni riservate ad altre tipologie di utenti.
- **Open design:** Questo principio consiglia di non basare la sicurezza del programma sulla segretezza del codice.
- **Kiss:** Questa strategia suggerisce di privilegiare i meccanismi di difesa più semplici poiché spesso essi risultano facilmente implementabili e riscontrano una maggiore accettazione da parte degli utenti finali.
- **Psicological acceptability:** Questa strategia consiglia di prendere sempre in considerazione, oltre alla sicurezza, anche l'usabilità per l'utente finale.

3.3 Scelte tecnologiche

In questa sezione riportiamo le varie scelte tecnologiche effettuate. Come detto in precedenza, il sistema si comporrà di due differenti parti, una on-chain e l'altra off-chain. Innanzitutto tratteremo le tecnologie utilizzate per la parte off-chain. Tali tecnologie sono state scelte dopo aver effettuato delle analisi di resistenza, ambiguità e sopravvivenza. Inoltre, la scelta è stata effettuata anche prendendo in considerazione le potenziali debolezze associate alle varie tecnologie e sono state individuate strategie di difesa atte a risolvere eventuali problematiche. Le scelte tecnologiche sono:

- **Linguaggio off-chain**

- **Python:** abbiamo scelto di usare Python poiché è il linguaggio di programmazione più usato al mondo oggigiorno, dispone quindi di grandissima documentazione e inoltre fornisce molte librerie per ogni caso d’uso. Inoltre, Python offre diversi strumenti per garantire la sicurezza nello sviluppo software, grazie a librerie avanzate per la crittografia, la gestione delle autenticazioni e la protezione da vulnerabilità comuni. In particolare, offre anche diverse librerie per interfacciarsi con la blockchain di Ethereum, tra cui *Web3*. Essa permette di inviare transazioni, leggere smart contract e gestire chiavi crittografiche in modo sicuro.
- **JavaScript:** abbiamo scelto di usare JavaScript poiché è uno dei linguaggi di programmazione più diffusi nel mondo dello sviluppo web. Grazie alla sua versatilità, può essere utilizzato sia lato client che lato server, in particolare con *Node.js*. Inoltre, anche esso, offre numerose librerie e framework per interfacciarsi con la blockchain facilitando l’interazione con gli smart contracts.

- **Database**

- **Supabase:** per la gestione del database, è stato scelto *Supabase*, una piattaforma open-source su cloud che offre un backend-as-a-service basato su *PostgreSQL*. Inoltre, grazie ai meccanismi nativi di quest’ultimo, esso permette di ottenere risposte in tempo reale, di avere una gestione avanzata delle transazioni e di consentire una scalabilità orizzontale¹, rendendolo una soluzione solida e affidabile per il nostro sistema. In Figura 3.1 riportiamo lo schema del database che abbiamo pensato per il nostro progetto.

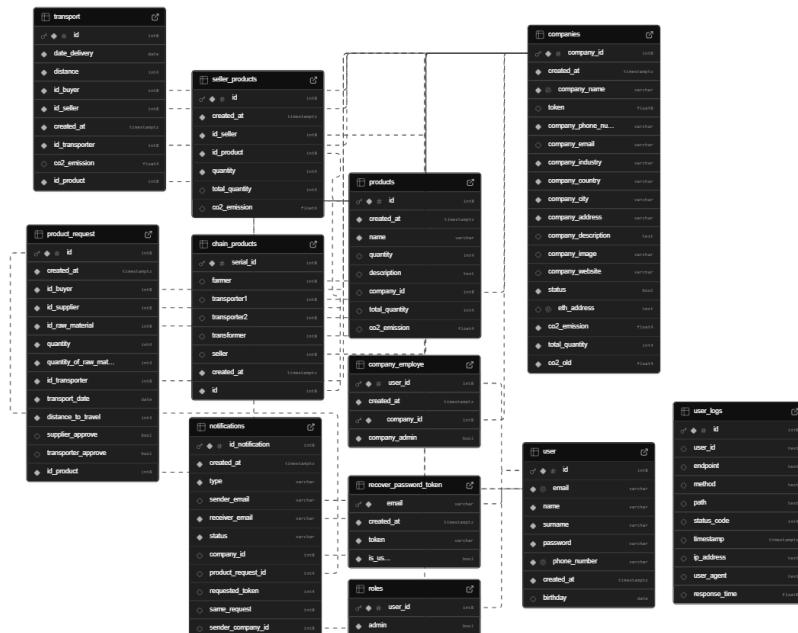


Figura 3.1: Database Schema

- **User Interface**

- **Flask:** abbiamo scelto *Flask* per lo sviluppo della User Interface. Esso è un framework Python leggero e flessibile, ideale per creare applicazioni web. La sua

¹La scalabilità orizzontale si riferisce alla capacità di un sistema di gestire un aumento del carico distribuendo il lavoro su più macchine o istanze, anziché potenziare un singolo server

semplicità e modularità permettono di integrare facilmente componenti personalizzati e librerie esterne. Flask si basa su *Werkzeug*, una libreria WSGI che gestisce le richieste e le risposte HTTP, il routing delle URL e fornisce strumenti avanzati per lo sviluppo web. Werkzeug supporta funzionalità come il debugging, la gestione delle sessioni sicure e la protezione da vulnerabilità comuni, rendendolo un elemento fondamentale per la stabilità e la sicurezza di Flask.

- **HTML:** è il linguaggio base per la costruzione delle pagine web, ed è utilizzato per strutturare i contenuti dell’interfaccia utente. La sua facile integrazione con Flask consente di generare pagine dinamiche e di gestire facilmente l’interazione con il backend, rendendo l’applicazione web interattiva e ben organizzata. In particolare, Flask utilizza *Jinja2*, che permette di incorporare codice dinamico all’interno delle pagine HTML. Grazie a *Jinja2*, è possibile utilizzare variabili, eseguire cicli e condizioni, e includere frammenti di codice riutilizzabili tramite i template, favorendo così una maggiore modularità e manutenibilità del progetto.
- **CSS:** è stato scelto per gestire lo stile e il design visivo dell’interfaccia utente. Grazie a CSS, possiamo definire layout, colori, font e animazioni per migliorare l’aspetto dell’applicazione e offrire agli utenti un’esperienza visiva gradevole e coerente. L’uso di framework come *Bootstrap* può semplificare ulteriormente la creazione di design responsivi e professionali.

- **Containerizzazione**

- **Docker:** abbiamo utilizzato Docker per gestire i nodi validatori della blockchain, sfruttando la sua capacità di creare ambienti isolati e facilmente scalabili. Docker consente di containerizzare i nodi, garantendo che ognuno di essi esegua il suo ambiente in modo indipendente e uniforme su qualsiasi sistema, semplificando la gestione, il deployment e il monitoraggio. Inoltre, grazie alla sua portabilità e alla rapida configurazione, Docker permette di distribuire i nodi validatori in modo efficiente e sicuro, migliorando la resilienza dell’infrastruttura. Per orchestrare e gestire container in modo coordinato, una tecnologia utile è *Docker Compose*, uno strumento che permette di definire e avviare applicazioni multi-container attraverso un file di configurazione YAML. Grazie a Docker Compose, è possibile specificare facilmente le dipendenze tra i vari servizi, automatizzare l’avvio dei nodi validatori e gestire la configurazione dell’intera infrastruttura in modo centralizzato, facilitando il deployment e la scalabilità del sistema.

- **Strategie di difesa** Dall’analisi delle possibili strategie di difesa, avvenuta con la stesura del modello Dual_Stride, sono stati ricavati questi possibili metodi di difesa:

- **MFA:** è stata scelta per rispettare il principio di *defense in depth*, aumentando la sicurezza degli accessi utente. La Multi-Factor Authentication richiede che l’utente fornisca più di un fattore di autenticazione durante il processo di login. Questo approccio riduce notevolmente il rischio di accessi non autorizzati, anche nel caso in cui uno dei fattori venga compromesso.
- **Log user action:** si basa sulla registrazione e il monitoraggio delle azioni degli utenti per garantire sicurezza, tracciabilità e conformità. Prevede la raccolta e l’analisi dei log per rilevare attività sospette, supportare audit e indagini forensi, migliorare la sicurezza e prevenire minacce.
- **Recupero password:** è stato scelto di fornire una procedura di recupero della password che consente all’utente di recuperare l’accesso al proprio account in caso di smarrimento della password. Questo processo, che prevede l’invio di un link di

reset tramite email, rappresenta una concreta applicazione del principio *Avoid a single point of failure*. Garantendo la possibilità di recuperare l'accesso, si riduce il rischio di bloccare completamente l'utente in caso di problemi con le credenziali, aumentando così la resilienza del sistema.

- **Validare tutti gli input al sistema:** è stata selezionata come strategia di difesa contro attacchi come la manipolazione dei dati in input o errori da parte dell'utente. La validazione assicura che tutti i dati immessi nel sistema siano conformi al formato atteso, prevenendo quindi l'inserimento di dati dannosi o malformati. Questa strategia si allinea ai principi di *Specify the format of all system inputs*, garantendo che ogni input venga rigorosamente controllato prima di essere elaborato, riducendo il rischio di vulnerabilità e migliorando la sicurezza complessiva del sistema.
- **Crittografia per dati sensibili:** si è scelto di utilizzare algoritmi di crittografia avanzati per proteggere i dati sensibili sia del sistema che degli utenti. La crittografia assicura che informazioni delicate, come credenziali di accesso, dati personali e transazioni, siano conservate in modo sicuro, rendendo i dati illeggibili per chiunque non possieda le chiavi di decriptazione appropriate. Questa misura protegge la privacy degli utenti e garantisce la conformità alle normative sulla protezione dei dati, come il GDPR.
- **Limitare tentativi di log-in:** è stato scelta una politica che limita il numero di tentativi di accesso consentiti per l'utente in un determinato periodo di tempo. Questa misura è stata adottata per proteggere il sistema da attacchi di Brute Force, dove un malintenzionato tenta ripetutamente di indovinare la password dell'utente. Limitando i tentativi, si riduce significativamente la possibilità di successo di tali attacchi, migliorando la sicurezza complessiva del sistema.
- **Sessioni uniche:** si è deciso di adottare la policy di rendere le sessioni di log-in degli utenti uniche.
- **Politiche di password robuste:** è stata scelta di richiedere password robuste agli utenti, al fine di migliorare la protezione contro i furti di account. Le password devono rispettare criteri di complessità, come l'uso di lettere maiuscole e minuscole, numeri e caratteri speciali, aumentando così la difficoltà per gli attaccanti di indovinare o forzare la password. Questa misura contribuisce a ridurre il rischio di accessi non autorizzati e a rafforzare la sicurezza complessiva del sistema.

Per la parte on-chain abbiamo utilizzato le seguenti tecnologie:

- **Linguaggio**
 - **Solidity:** è stato scelto Solidity in quanto è il linguaggio di programmazione nativo della blockchain di Ethereum, progettato specificamente per scrivere Smart Contract. Inoltre, la robusta documentazione e la community attiva lo rendono particolarmente adatto a progetti blockchain che richiedono un alto livello di sicurezza, di scalabilità e di affidabilità.
- **Libreria per contratti**
 - **OpenZeppelin:** è stata scelta per la creazione dei contratti intelligenti grazie alla sua libreria affidabile e sicura, che offre implementazioni già testate e auditate di standard ben consolidati come ERC20 ed ERC721. La modularità di OpenZeppelin consente di sviluppare contratti personalizzati riutilizzando componenti predefiniti, riducendo così i rischi di vulnerabilità e velocizzando il processo di sviluppo.

3.4 Modellazione mediante Markov chain di una unità

Le catene di Markov sono uno strumento matematico utile a rappresentare, tramite un insieme di stati, i processi del nostro sistema permettendo di determinare la probabilità delle possibili sequenze di stati attraverso una matrice stocastica. Essa definisce la probabilità di transizione da uno stato all'altro senza considerare gli stati precedenti (*memoryless*). Nella successiva sottosezione riporteremo la modellazione, attraverso catena di Markov, della funzione di login del nostro sistema. Successivamente, attraverso il modello abbiamo verificato una proprietà di *Safety* e una di *Response*. Infine, per tali proprietà è stato realizzato un monitor di *Routine Enforcement*.

3.4.1 Markov Chain della funzione di login

Come detto in precedenza, abbiamo deciso di modellare, attraverso una Markov chain, la funzione di login del nostro sistema. Il modello, rappresentato in Figura 3.2, è costituito da 9 stati e tre contatori:

- C_l per tener conto del numero di tentativi di inserimento di email e password;
- C_m per enumerare il numero di inserimenti del codice per l'mfa che sono stati effettuati;
- C_e per tener conto del numero di email provate durante la procedura di recupero password.

Nel momento in cui un utente vuole accedere al sistema, esso partirà dallo stato 0 ovvero quello iniziale. A questo punto, se verranno inseriti email e password, avverrà una transizione verso lo stato 1 e sarà incrementato il contatore C_l . Se le informazioni inserite risultano corrette ovvero che l'email sia valida e sia stata inserita la password corretta ad essa associata, si passerà allo stato 2. Tuttavia, qualora le informazioni inserite risultino errate e se C_l è minore di 3, si torna allo stato 1, mentre se sono già stati effettuati tre tentativi si finisce nello stato 9 che rappresenta lo stato di errore nel quale l'utente rimane bloccato. Una volta raggiunto lo stato 2, per implementare un'autenticazione a più fattori, verrà inviato sull'email inserita precedentemente un codice di verifica. A questo punto, l'utente potrà richiedere un nuovo invio del codice rimanendo quindi nello stato 2 e azzerando il numero di tentativi effettuati. Mentre, se prova ad inserire il codice di verifica, si passerà allo stato 3 e il contatore C_m verrà incrementato. Nel caso in cui l'inserimento risulti corretto, l'utente riuscirà ad accedere al sistema raggiungendo lo stato 4. Mentre, se l'inserimento è avvenuto in modo errato e C_m è minore di 3, tornerà allo stato 2. Infine, qualora siano già stati effettuati tre tentativi, si passerà allo stato di errore (stato 9). Quando si trova nello stato 0 l'utente potrebbe anche avviare la procedura di recupero password, portando il modello allo stato 5. A questo punto, dovrà inserire un'email che servirà per il recupero della password dell'account; ciò porterà a una transizione verso lo stato 6 e il contatore C_e verrà incrementato. Se l'email inserita esiste allora verrà inviato un messaggio tramite posta elettronica con un link che consentirà di modificare la password passando allo stato 7. Tuttavia, se la email non esiste e C_e è minore di 3 si torna allo stato 5. Mentre, se sono stati già effettuati 3 tentativi si passa allo stato di errore. Una volta che ci si trova nello stato 7, l'utente dovrà inserire la nuova password e la sua conferma passando allo stato 8. Qualora, esse non coincidano si torna allo stato 7, altrimenti si passa allo stato 0.

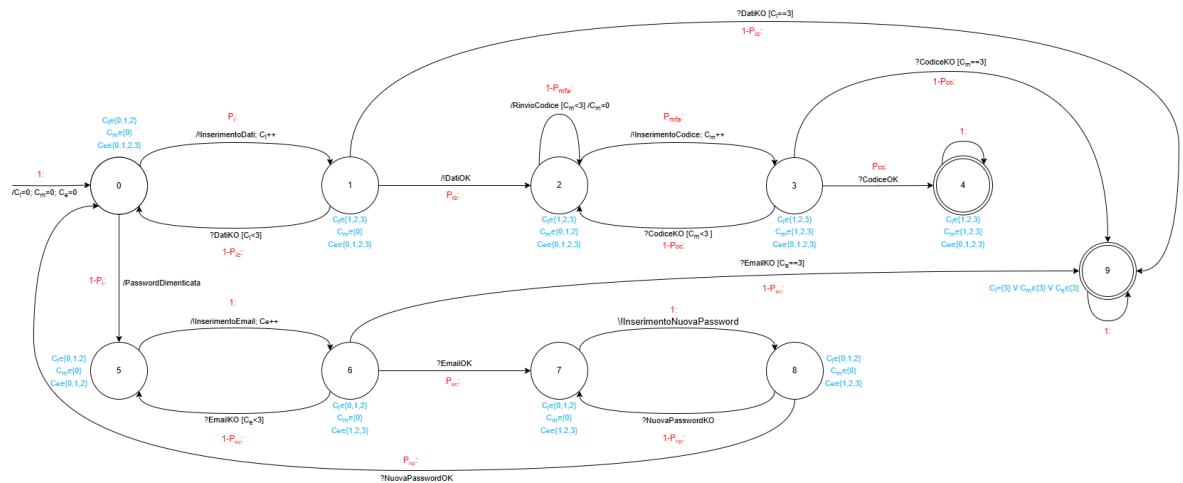


Figura 3.2: Markov chain relativo alla funzione di login

3.4.2 Implementazione della funzione di login in PRISM

Per creare e analizzare la catena di Markov illustrata precedentemente è stato utilizzato il software PRISM. Quest’ultimo, è un software open-source per la modellazione, verifica e analisi di sistemi probabilistici come le catene di Markov. Supporta diversi tipi di modelli, tra cui MDP (Markov Decision Proces) e DTMC (Discrete-Time Markov Chain), permettendo l’analisi di proprietà tramite logiche formali. È ampiamente utilizzato in ambiti come la sicurezza e l’affidabilità dei sistemi. Di seguito viene riportato il codice del modello per la Markov chain associata alla funzione di login del nostro sistema. Da notare come, in questo caso, i valori assegnati alle probabilità si riferiscono a un utente buono che sta cercando di accedere al sistema.

```

1 dtmc
2
3 const double Pi = 0.85;
4 const double Pic = 0.8;
5 const double Pmfa = 0.8;
6 const double Pcc = 0.9;
7 const double Pec = 0.85;
8 const double Pnp = 0.9;
9
10
11
12 module login_function
13
14 s: [0..9] init 0;
15 cl : [0..3] init 0;
16 cm : [0..3] init 0;
17 ce : [0..3] init 0;
18
19 [] (s=0) ->
20   Pi: (s'=1) & (cl' = min(cl + 1, 3)) +
21   (1-Pi): (s'=5);
22
23 [] (s=1) & (cl<3) -> Pic: (s'=2) + (1-Pic): (s'=0);
24 [] (s=1) & (cl=3) -> Pic: (s'=2) + (1-Pic): (s'=9);
25
26 [] (s=2) ->

```

```

27 Pmfa: (s'=3) & (cm' = min(cm + 1, 3))
28 + (1-Pmfa): (s'=2) & (cm' = 0);
29
30 [] (s=3) & (cm<3) -> Pcc: (s'=4) + (1-Pcc): (s'=2);
31 [] (s=3) & (cm=3) -> Pcc: (s'=4) + (1-Pcc): (s'=9);
32
33 [accesso_consentito] (s=4) -> 1: (s'=4);
34
35 [] (s=5) -> 1: (s'=6) & (ce' = min(ce + 1, 3));
36
37 [] (s=6) & (ce<3) -> Pec: (s'=7) + (1-Pec): (s'=5);
38 [] (s=6) & (ce=3) -> Pec: (s'=7) + (1-Pec): (s'=9);
39
40 [] (s=7) -> 1: (s'=8);
41
42 [] (s=8) -> Pnp: (s'=0) + (1-Pnp): (s'=7);
43
44 [accesso_negato] (s=9) -> 1: (s'=9);
45
46 endmodule

```

Listing 3.1: Funzione di login in PRISM applicato a un utente buono

Attraverso la modalità *Simulator* messa a disposizione da PRISM abbiamo effettuato delle simulazioni sul funzionamento del modello precedentemente definito.

Nella Figura 3.3 viene mostrato il caso in cui un utente accede direttamente al suo account.

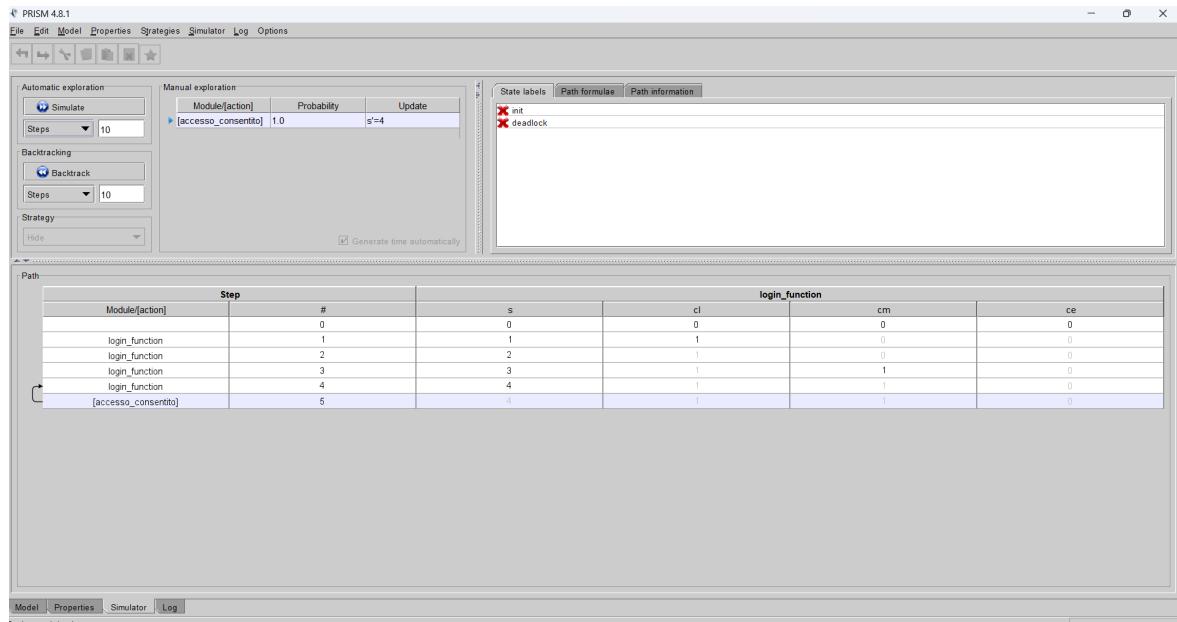


Figura 3.3: Simulazione del sistema da parte di un utente buono che vuole accedere al sistema

Nella Figura 3.4 viene riportato il caso in cui l’utente buono cerca di recuperare la password, e successivamente, di accedere con le nuove credenziali.

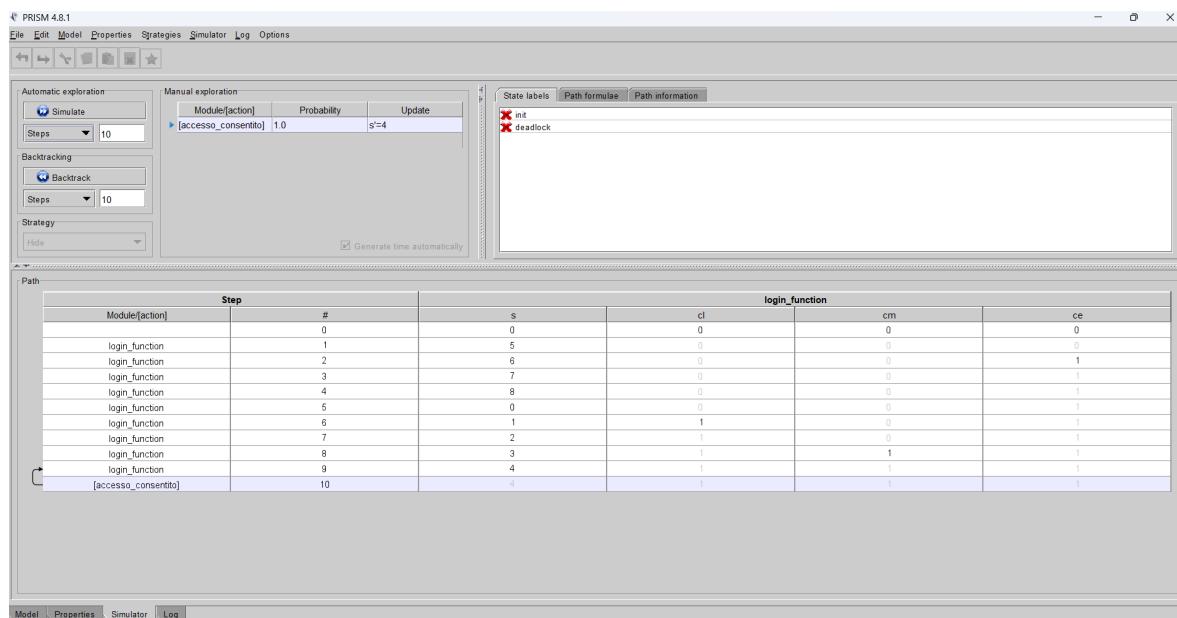


Figura 3.4: Simulazione del sistema da parte di un utente buono in cui ha deciso di effettuare il recupero della password

Di seguito vengono riportati i valori assegnati alle probabilità qualora sia un utente malevolo ad interagire con il sistema.

```

1 const double Pi = 0.9;
2 const double Pic = 0.01;
3 const double Pmfa = 0.85;
4 const double Pcc = 0.01;
5 const double Pec = 0.01;
6 const double Pnp = 0.9;
```

Listing 3.2: Funzione di login in PRISM applicato a un utente malevolo

Di seguito, vengono riportate le simulazioni del comportamento della funzione di login nel caso di interazione con un utente malevolo.

Nella Figura 3.5 viene riportato il caso in cui l’utente malevolo non riesca ad indovinare l’email e la password.

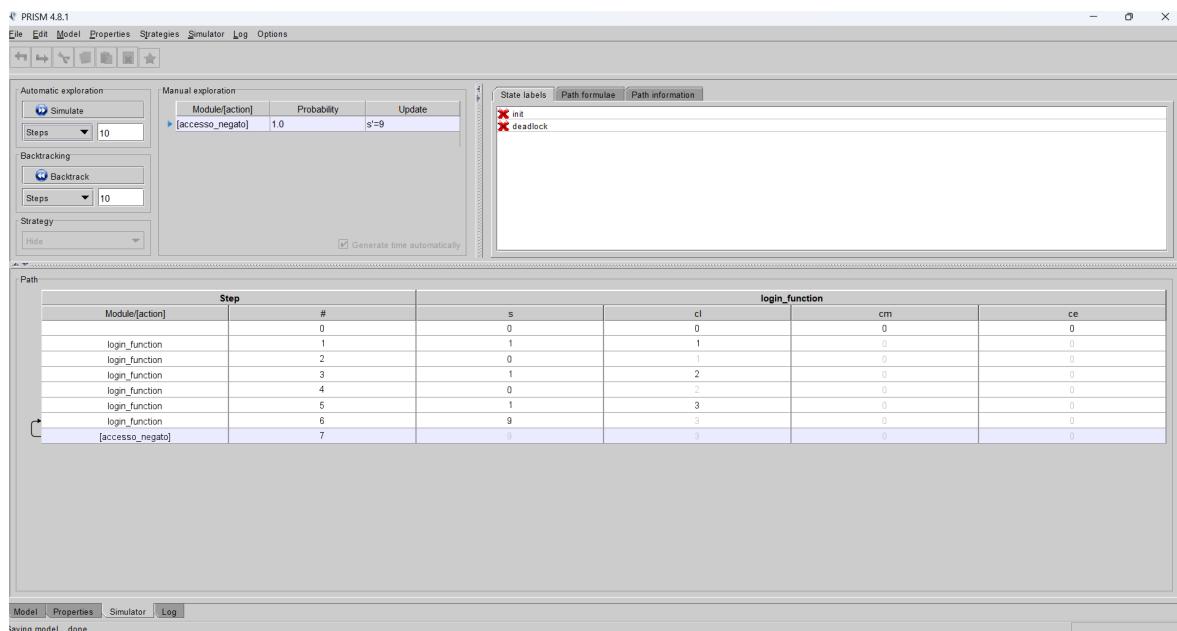


Figura 3.5: Simulazione del sistema da parte di un utente malevolo che cerca di accedere al sistema

Nella Figura 3.6 viene illustrato lo scenario in cui un utente malevolo cerca di sfruttare la procedura di recupero password per poter poi accedere al sistema.

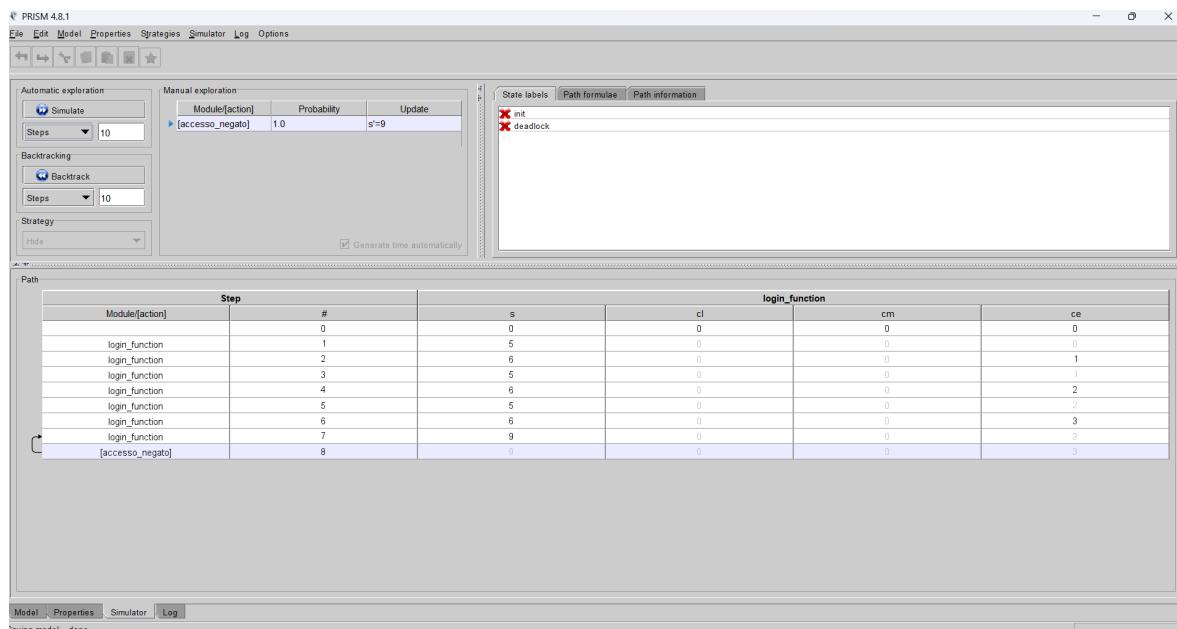


Figura 3.6: Simulazione del sistema da parte di un utente malevolo che cerca di modificare la password di un utente

Nella Figura 3.7 viene riportato il caso in cui l’utente malevolo riesca ad indovinare email e password ma non inserisce il codice di verifica corretto.

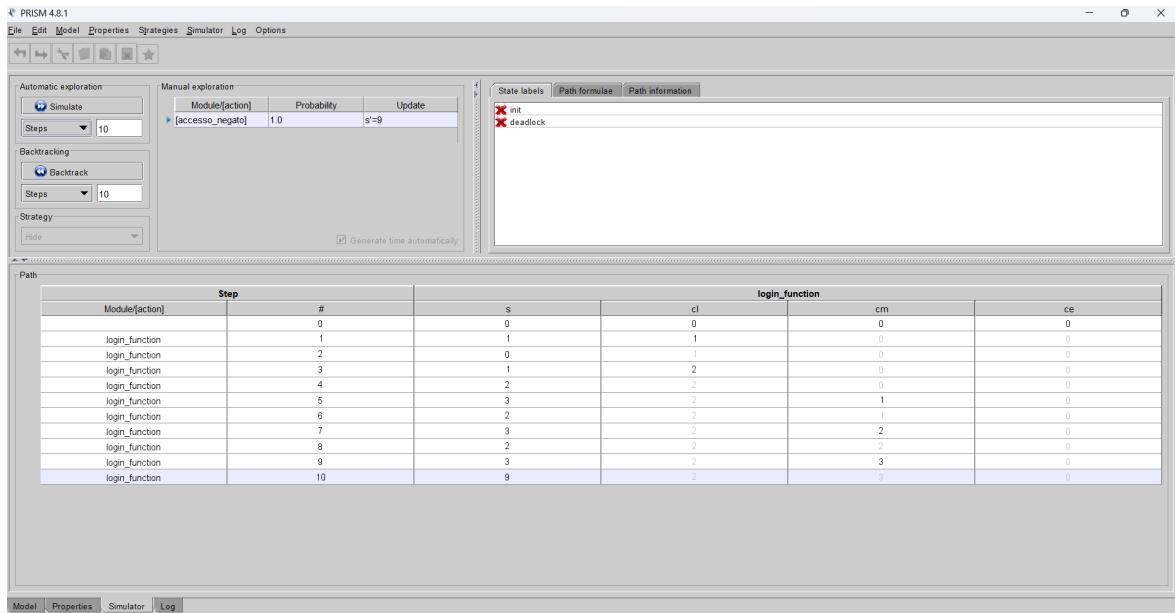


Figura 3.7: Simulazione del sistema da parte di un utente malevolo che conosce le credenziali di un utente

3.4.3 Verifica di una proprietà di Safety

In questa sottosezione abbiamo deciso di verificare la seguente proprietà di Safety:

«*Un utente malevolo non deve mai riuscire ad accedere al sistema.*»

Si può osservare, nel caso in cui un utente malevolo prova ad accedere al sistema, come la proprietà venga rispettata solamente se il modello finisce nello stato 9, ovvero lo stato di errore, dove l'attaccante rimarrà bloccato.

La proprietà precedentemente definita viene rappresentata dal modello riportato in seguito. Esso si compone di due stati. Il modello rimarrà nello stato 0, ovvero quello iniziale, fino a quando il sistema negherà l'accesso all'utente malevolo. Se l'attaccante riuscirà ad ottenere l'accesso, allora si avrà una transizione verso lo stato 1, portando alla violazione della proprietà di Safety. Una volta raggiunto lo stato 1 qualunque cosa accada il sistema rimarrà in questo stato, in quanto, oramai, la proprietà è stata violata in modo irrimediabile.

```

1 module Safety_Property
2
3 q: [0..1] init 0;
4
5 [acesso_negato] (q=0) -> (q'=0);
6 [acesso_consentito] (q=0) -> (q'=1);
7 [] (q=1) -> (q'=1);
8
9 endmodule

```

Listing 3.3: Modellazione della proprietà di Safety in PRISM

La proprietà precedentemente definita, viene successivamente espressa nel linguaggio PRISM in *Properties* nella seguente formula:

$$P = ? [F(s = 9)]$$

Attraverso la funzione *Verify* abbiamo valutato che la proprietà analizzata venga rispetta, ciò viene riportato nella Figura 3.8.

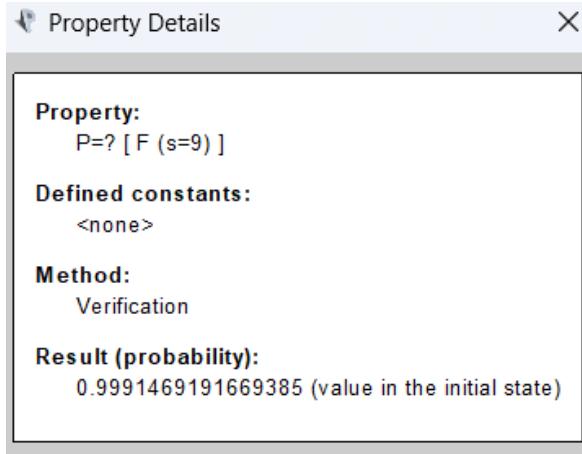


Figura 3.8: Probabilità relativa alla proprietà di Safety

3.4.4 Verifica di una proprietà di Response

In questa sottosezione abbiamo deciso di verificare la seguente proprietà di Response:

«Un utente buono, una volta effettuata la richiesta, deve riuscire ad accedere al sistema infinitamente spesso.»

Si può osservare, nel caso in cui un utente buono prova ad accedere al sistema, come la proprietà venga rispettata solamente se il modello finisce nello stato 4, ovvero lo stato in cui viene fornito l'accesso all'utente.

La proprietà precedentemente definita viene rappresentata dal modello riportato in seguito. Esso si compone di due stati, il modello rimarrà nello stato 0, ovvero quello iniziale, fino a quando l'utente buono non inserisce le informazioni necessarie per accedere al sistema. Una volta inserite le sue credenziali si avrà una transizione verso lo stato 1. Una volta che si arriva allo stato 1 si rimarrà in esso fino a quando il sistema non fornirà l'accesso all'utente; quando ciò avviene si torna allo stato 0. Infine, se ci troviamo nello stato 0 e avviene l'evento accesso consentito si passa ad uno stato 2 di errore poiché l'utente non può ottenere l'accesso se prima non ha inserito le proprie credenziali. Una volta che si è giunti nello stato 2 si rimarrà in esso indipendentemente dagli eventi che avvengono poiché la proprietà risulta violata.

```

1 module Response_Property
2
3 z: [0..1] init 0;
4
5 [] (z=0) -> (z'=0);
6 [] (z=0) -> (z'=1);
7 [accesso_consentito] (z=0) -> (z'=2);
8 [] (z=1) -> (z'=1);
9 [accesso_consentito] (z=1) -> (z'=0);
10
11 endmodule

```

Listing 3.4: Modellazione della proprietà di Response in PRISM

La proprietà precedentemente definita, viene successivamente espressa nel linguaggio PRISM in *Properties* nella seguente formula:

$$P =? [F s = 4]$$

Attraverso la funzione *Verify* abbiamo valutato che la proprietà analizzata venga rispetta, ciò viene riportato nella Figura 3.9.

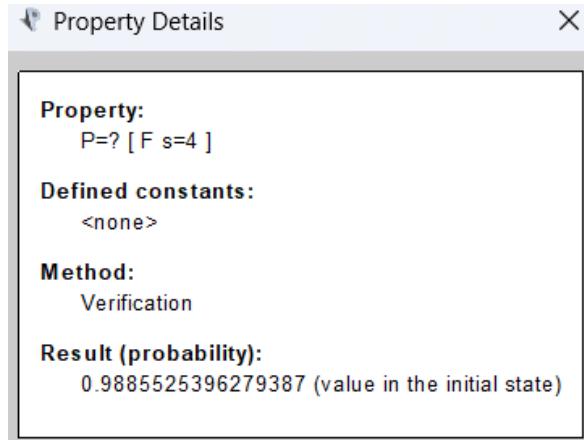


Figura 3.9: Probabilità relativa alla proprietà di Response

3.4.5 Realizzazione dei monitor di Runtime Enforcement

Per le proprietà trattate nelle sottosezioni precedenti sono stati sintetizzati dei monitor di Runtime Enforcement.

Nella Figura 3.10 è riportato il monitor per la proprietà di Safety. Da notare come, sono possibili due eventi:

- *a*: il sistema non fornisce l'accesso all'utente malevolo
- *b*: il sistema fornisce l'accesso all'utente malevolo

La proprietà viene espressa tramite questa espressione regolare $P = a^w$. Analizzando il funzionamento del monitor riportato, si osserva che, fino a quando avviene l'evento *a*, la proprietà è possibilmente rispettata e il monitor compierà l'azione di *dump*. Nel momento in cui avviene l'evento *b* la proprietà è sicuramente non rispettata e quindi da questo punto in poi il monitor compierà sempre l'azione di *halt*.

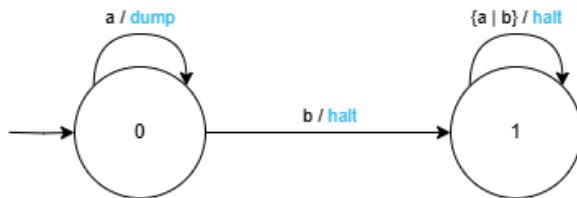


Figura 3.10: Monitor di RE relativo alla proprietà di Safety

Nella Figura 3.11 è riportato il monitor per la proprietà di Response. Si osserva che sono possibili tre eventi:

- *a*: qualunque evento diverso da *b* o *c*
- *b*: l'utente buono inserisce le credenziali per effettuare l'accesso
- *c*: il sistema fornisce l'accesso all'utente buono

La proprietà viene espressa tramite questa espressione regolare $P = ((a^*b^+) \cdot (a + b)^* \cdot c)^\omega$. Analizzando il funzionamento del monitor riportato, si osserva che, fino a quando avvengono gli eventi *a* e *b*, la proprietà possibilmente non viene rispettata e il monitor effettua l'azione di *store*. Se l'evento *c* avviene quando mi trovo nello stato 1 allora la proprietà possibilmente

viene rispettata e viene effettuato un *dump*. Mentre se l'evento *c* avviene quando ci si trova nello stato 0 allora la proprietà viene violata e da qui in poi il monitor effettuerà solamente azioni di *halt*.

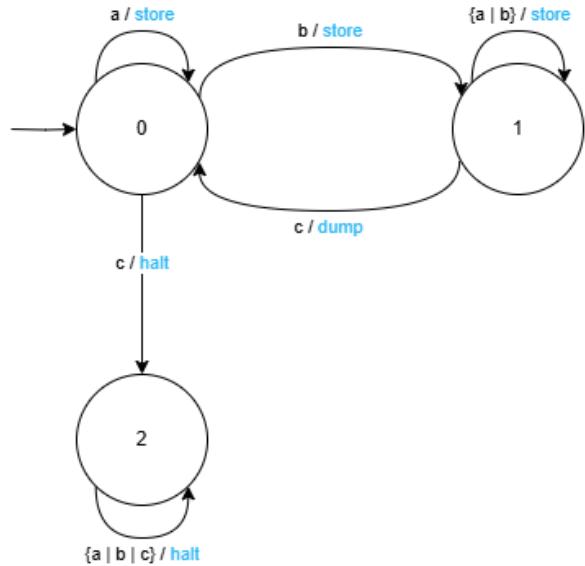


Figura 3.11: Monitor di RE relativo alla proprietà di Response

CAPITOLO 4

Programmazione Sicura

In questo capitolo vengono presentate le linee guida e le strategie adottate per garantire un'implementazione software sicura ed efficiente. La programmazione sicura è essenziale per prevenire vulnerabilità, migliorare la resilienza del sistema e garantire l'affidabilità del software. L'obiettivo di questo capitolo è fornire un quadro chiaro delle pratiche di sicurezza seguite nello sviluppo dell'applicazione, con un focus sia sugli aspetti off-chain che on-chain.

Nelle successive sezioni, riportiamo gli aspetti principali di questa fase. Esse riguardano:

- **Programmazione off-chain**: In questa sezione vengono illustrate le principali linee guida per lo sviluppo sicuro del software off-chain, con particolare attenzione alla gestione della visibilità delle informazioni, alla validazione degli input, alla gestione delle eccezioni e alla riduzione dell'uso di costrutti soggetti a errori. Inoltre, vengono illustrati gli strumenti software utilizzati per verificare la qualità del software.
- **Programmazione on-chain**: In questa sezione, verranno riportati gli smart contracts realizzati in Solidity e i test su essi effettuati utilizzando *Remix IDE*.

4.1 Programmazione off-chain

Per quanto riguarda la programmazione della parte off-chain è stato seguito quanto precedentemente dichiarato in fase di progettazione. Inoltre, per garantire la qualità del codice, abbiamo condotto un'analisi approfondita utilizzando l'analizzatore statico *SonarQube*. Questo strumento si è rivelato particolarmente utile per esaminare il codice sorgente e identificare eventuali vulnerabilità, code smell e problemi di sicurezza. In particolare, l'analisi ha permesso di individuare aree del codice potenzialmente migliorabili in termini di leggibilità, manutenibilità ed efficienza, consentendoci di intervenire tempestivamente per ottimizzarne la struttura e ridurre il rischio di errori.

In particolare, per effettuare una buona progettazione sicura abbiamo deciso di seguire delle linee guida che sono state adottate nell'implementazione del software. Esse sono:

- ***Limit the visibility of information in a program***: abbiamo limitato la visibilità delle informazioni dall'esterno del sistema. In particolare, l'utente potrà accedere ai dati solo attraverso le interfacce messe a disposizione.

- **Check all inputs for validity:** abbiamo validato tutti gli input del sistema per evitare che ci siano degli input errati. In particolare, sono stati effettuati dei controlli sull'inserimento di caratteri particolari, sulla dimensione (come l'immagine), sulla sensatezza e sull'appartenenza al range.
- **Provide a handler for all exceptions:** abbiamo gestito le eccezioni tramite parti di codice (*try/except*), assicurandoci che eventuali errori imprevisti non causino il crash del sistema. Inoltre, abbiamo implementato meccanismi di logging per tracciare gli errori e facilitarne il debug.
- **Minimize the use of error-prone constructs:** abbiamo evitato l'uso di costrutti che possono portare a errori e l'uso di variabili globali. Inoltre, sono state seguite le best practice per la scrittura di codice sicuro e manutenibile.
- **Check array bounds:** abbiamo evitato accessi fuori dai limiti degli array utilizzando controlli esplicativi prima di accedere agli elementi. Abbiamo anche impiegato strutture dati sicure che forniscono verifiche automatiche dei limiti, riducendo il rischio di buffer overflow.

4.2 Programmazione on-chain

Gli smart contract sono programmi che vengono eseguiti direttamente sulla blockchain, garantendo trasparenza, immutabilità e sicurezza delle transazioni. L'uso di librerie consolidate, come OpenZeppelin, consente di implementare contratti sicuri e robusti, riducendo il rischio di vulnerabilità grazie a moduli standardizzati e ben testati.

4.2.1 GreenToken

```

1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.20;
3
4 import {ERC20} from "@openzeppelin/contracts/token/ERC20/ERC20.sol";
5 import {Ownable} from "@openzeppelin/contracts/access/Ownable.sol";
6
7 contract GreenToken is ERC20, Ownable {
8     address public gasSponsorship;
9     mapping(address => bool) public minters;
10
11    constructor(address initialOwner)
12        ERC20("GreenToken", "GTK")
13        Ownable()
14    {
15        _transferOwnership(initialOwner);
16        gasSponsorship = initialOwner;
17        minters[initialOwner] = true;
18        _mint(initialOwner, 1_000_000 * 10 ** decimals());
19    }
20
21    function setMinter(address minter, bool status) public onlyOwner {
22        require(minter != address(0), "Invalid minter address");
23        minters[minter] = status;
24    }
25
26    function setGasSponsor(address newSponsor) public onlyOwner {

```

```

27     require(newSponsor != address(0), "Invalid sponsor address");
28     gasSponsorship = newSponsor;
29 }
30
31 function sponsoredTransfer(address from, address to, uint256 amount)
32 public {
33     require(msg.sender == gasSponsorship, "Only sponsor can execute")
34     ;
35     require(from != address(0), "Transfer from zero address");
36     require(to != address(0), "Transfer to zero address");
37     _transfer(from, to, amount);
38 }
39
40 function mint(address to, uint256 amount) public {
41     require(minters[msg.sender], "Only authorized minters can mint");
42     _mint(to, amount);
43 }
44
45 function burn(uint256 amount) public {
46     _burn(msg.sender, amount);
47 }
48
49 interface IGreenToken {
50     function mint(address to, uint256 amount) external;
51 }
```

GreenToken è un token ERC20 che sfrutta la libreria OpenZeppelin per la gestione standardizzata del token e dei permessi di accesso. L'uso di Ownable garantisce che solo il proprietario possa modificare le autorizzazioni dei minter e del gas sponsor, migliorando la sicurezza del contratto. Inoltre, la funzione di trasferimento sponsorizzato consente un'ottimizzazione dei costi del gas per transazioni specifiche.

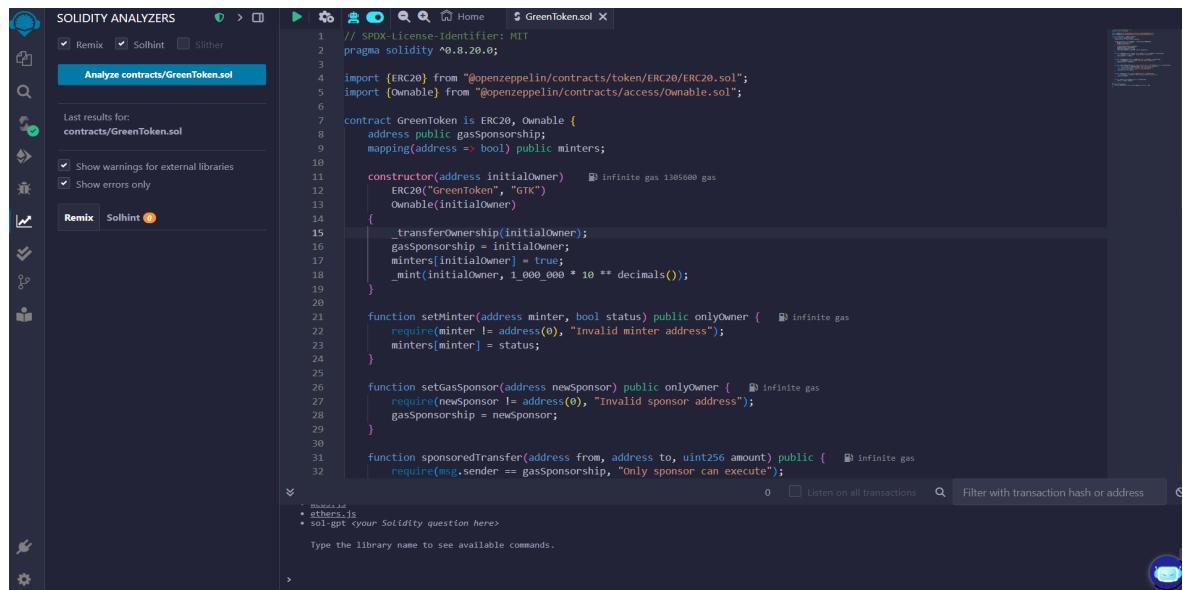


Figura 4.1: Solidity Analyzers - GreenToken.sol

4.2.2 EmissionTracker

```
1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.20;
3
4 import {Ownable} from "@openzeppelin/contracts/access/Ownable.sol";
5 import {GreenToken} from "./GreenToken.sol";
6
7 contract EmissionTracker is Ownable {
8     GreenToken public greenToken;
9     address public gasSponsorship;
10
11     struct CompanyStats {
12         bool is_processor;
13         bool is_manufacturer;
14         bool is_seller;
15         bool is_transporter;
16         uint256 currentPeriodProducts;
17         uint256 currentPeriodEmissions;
18         uint256 previousPeriodProducts;
19         uint256 previousPeriodEmissions;
20         uint256 tokenBalance;
21     }
22
23     uint256 public processorEmissionThreshold = 115;
24     uint256 public manufacturerEmissionThreshold = 11;
25     uint256 public sellerEmissionThreshold = 3;
26     uint256 public transporterEmissionThresholdPerKm = 111;
27
28     uint256 public baseTokenReward = 50 * 10**18;
29     uint256 public volumeBonusThreshold = 100;
30     uint256 public volumeBonusAmount = 20 * 10**18;
31     uint256 public efficiencyBonusPercent = 10;
32
33     mapping(address => CompanyStats) public companyStats;
34     address[] private registeredCompanies;
35     mapping(address => bool) private isRegistered;
36
37     event CompanyEmissionsUpdated(address company, uint256 newEmissions);
38     event CompanyRoleUpdated(address company, string role, bool status);
39     event TokensRewarded(address company, uint256 amount, string reason);
40     event PeriodicDistribution(uint256 timestamp, uint256
41                             totalTokensDistributed);
42
43     constructor(address _greenTokenAddress, address initialOwner)
44         Ownable()
45     {
46         greenToken = GreenToken(_greenTokenAddress);
47         _transferOwnership(initialOwner);
48         gasSponsorship = initialOwner;
49     }
50
51     function setGasSponsor(address newSponsor) public onlyOwner {
52         require(newSponsor != address(0), "Invalid sponsor address");
53         gasSponsorship = newSponsor;
54     }
55
56     function sponsoredBatchUpdateCompany(
57         address company,
```

```
57     bool isProcessor,
58     bool isManufacturer,
59     bool isSeller,
60     bool isTransporter,
61     uint256 averageEmissions,
62     uint256 totalQuantity
63 ) external {
64     require(msg.sender == gasSponsorship, "Only sponsor can execute")
65     ;
66     if (!isRegistered[company]) {
67         registeredCompanies.push(company);
68         isRegistered[company] = true;
69     }
70
71     CompanyStats storage stats = companyStats[company];
72     stats.previousPeriodProducts = stats.currentPeriodProducts;
73     stats.previousPeriodEmissions = stats.currentPeriodEmissions;
74     stats.currentPeriodProducts = totalQuantity;
75     stats.currentPeriodEmissions = averageEmissions;
76     stats.is_processor = isProcessor;
77     stats.is_manufacturer = isManufacturer;
78     stats.is_seller = isSeller;
79     stats.is_transporter = isTransporter;
80
81     emit CompanyEmissionsUpdated(company, averageEmissions);
82 }
```

EmissionTracker utilizza OpenZeppelin per la gestione sicura del controllo degli accessi con *Ownable*, garantendo che solo il proprietario possa modificare parametri critici. Il contratto consente di registrare le emissioni di CO₂ delle aziende e premiare quelle che operano in modo efficiente con token GreenToken. Il meccanismo di distribuzione basato su soglie e bonus incentiva le aziende a ridurre le emissioni nel tempo. Inoltre, l'uso di eventi permette un monitoraggio trasparente delle emissioni e dei premi distribuiti.

Grazie a OpenZeppelin, entrambi i contratti sono implementati in modo sicuro, seguendo best practices consolidate per la protezione da vulnerabilità comuni come overflow, autorizzazioni improprie e gestione dei ruoli.

The screenshot shows the Solidity Analyzers interface with the following details:

- Left Sidebar:** Includes tabs for Remix, Solhint, Slither, and a "Last results for contracts/EmissionTracker.sol" section with checkboxes for "Show warnings for external libraries" and "Show errors only".
- Central Area:** Displays the Solidity code for `EmissionTracker.sol`. The code defines a `Ownable` contract with a `greenToken` and `gassponsorship` address. It includes a `CompanyStats` struct with metrics for current and previous periods, and role-specific emission thresholds for processor, manufacturer, seller, and transporter. A base token reward is also defined.
- Bottom Navigation:** Shows recent files (`msg.sender.sol`, `ether.js`, `sol-gpt`), a command input field ("Type the library name to see available commands."), and transaction monitoring tools like "Listen on all transactions" and "Filter with transaction hash or address".

Figura 4.2: Solidity Analyzers - EmissionTracker.sol

CAPITOLO 5

Deployment

In questo capitolo verrà illustrato il processo di deployment per il nostro progetto *GreenProof*. In particolare, verrà fornita una guida dettagliata su come installare, configurare e avviare l'applicazione. *GreenProof* è una piattaforma basata su blockchain progettata per garantire trasparenza e sicurezza delle transazioni. L'obiettivo di questa sezione è quello di riportare tutte le istruzioni che l'utente deve seguire per poter configurare correttamente l'ambiente di sviluppo e testare il sistema in un ambiente controllato. Verranno descritti i prerequisiti, i passaggi per l'installazione e la configurazione dell'ambiente. Infine, verranno presentate alcune interfacce chiave dell'applicazione. Sono presenti le seguenti sezioni:

- **Prerequisiti:** In questa sezione tratteremo dei prerequisiti da avere per poter installare correttamente l'applicazione;
- **Installazione e Configurazione:** In questa sezione discuteremo l'installazione e la configurazione dell'applicazione;
- **Compatibilità con i Sistemi Operativi:** In questa sezione vengono riportate le compatibilità con i vari sistemi operativi;
- **Interfaccie:** In questa sezione illustreremo le interfacce chiave dell'applicazione.

5.1 Prerequisiti

Prima di installare GreenProof, bisogna assicurarsi di avere installati sul proprio sistema tutti i seguenti strumenti:

- **Python 3.10+ :** esso è necessario per i servizi backend. Da notare come sia necessario possedere una versione di questo linguaggio pari o successiva alla 3.10;
- **Node.js 21+ e npm:** queste tecnologie solo utilizzate per lo sviluppo di smart contract. Si noti, che per Node.js è necessario installare una versione pari o successiva alla 21;
- **Docker e Docker Compose:** queste tecnologie sono utilizzate per la containerizzazione dell'applicazione (Figura 5.1);
- **Truffle:** esso è il framework di sviluppo per Ethereum;

- **MetaMask:** questa tecnologia è il Wallet Ethereum per i test sulla blockchain;
- **Account Supabase:** esso è utilizzato per gestire il database backend.

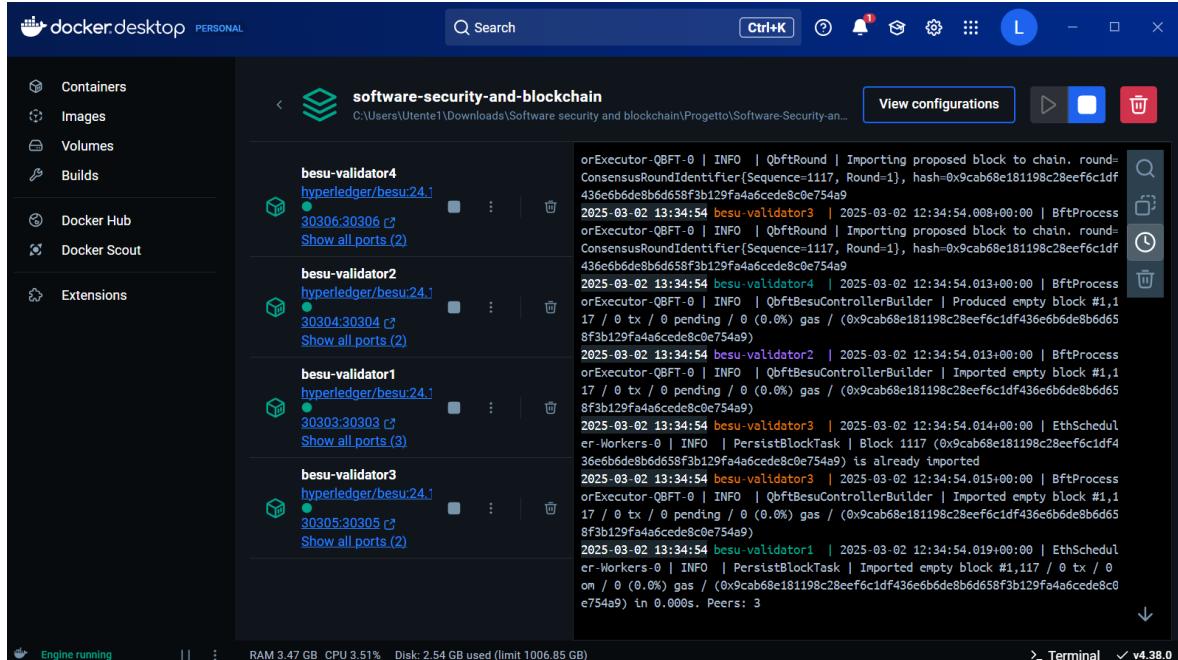


Figura 5.1: Docker

5.2 Installazione e Configurazione

Per iniziare, è necessario clonare il repository dal seguente link e direzionarci all'interno della cartella:

```
1 git clone https://github.com/yourusername/Software-Security-and-Blockchain.git
2 cd Software-Security-and-Blockchain
```

In seguito, bisogna installare le dipendenze *Python* necessarie per il backend utilizzando il comando:

```
1 pip install -r requirements.txt
```

A questo punto, si deve passare alla directory dei contratti intelligenti e installare le dipendenze necessarie utilizzando i seguenti comandi:

```
1 cd app/token
2 npm install
```

Successivamente, bisogna installare globalmente *Truffle* per gestire i contratti su *Ethereum*:

```
1 npm install -g truffle
```

Infine, è necessario avviare i servizi *Docker* in background con il seguente comando:

```
1 docker-compose up -d
```

5.3 Configurazione dopo l'avvio del sistema

Per interagire con la parte on-chain, è necessario configurare correttamente MetaMask aggiungendo la rete GreenProof con le seguenti caratteristiche:

- **Nome rete:** GreenProof
- **Default RPC URL:** `http://localhost:8545`
- **Chain ID:** 1338
- **Simbolo della moneta:** ETH

Le seguenti configurazioni sono visibili in Figura 5.2.

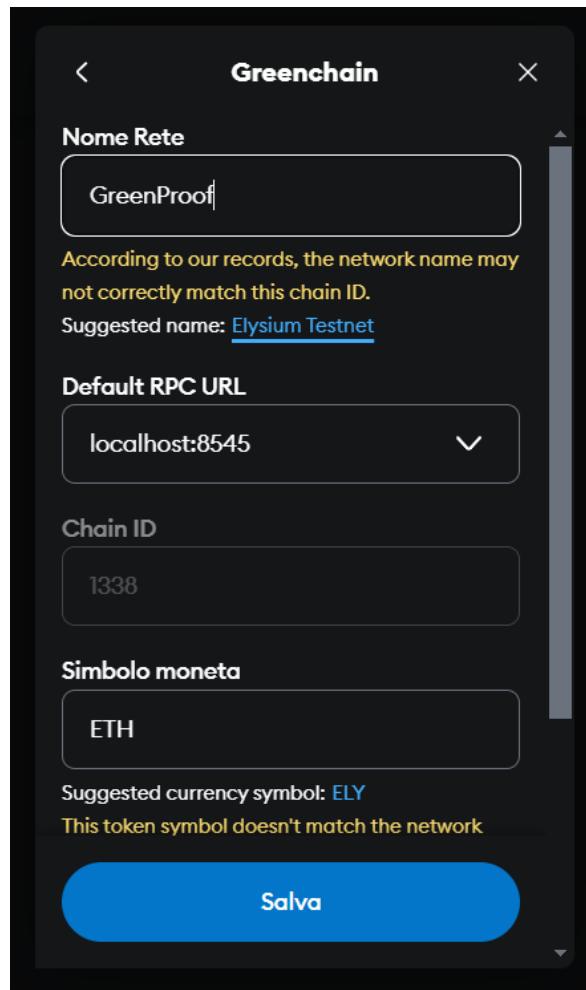


Figura 5.2: MetaMask Network Configuration

Successivamente, per poter effettuare transazioni sul sistema, è necessario importare in MetaMask uno o più account appartenenti alle aziende che desiderano operare, utilizzando la relativa chiave privata. Si possono utilizzare gli account a partire dal quarto in poi, con le rispettive chiavi private disponibili nel file `app/QBFT-Network/genesis.json`. Dopo l'importazione, è necessario approvare la connessione dell'indirizzo a MetaMask. Per visualizzare in MetaMask il numero di GreenToken associato a uno specifico account, segui questi passaggi:

- Accedi alla sezione Tokens.

- Clicca sui tre puntini in alto a destra.
- Seleziona Importa token.
- Inserisci l'indirizzo dello smart contract *GreenToken.sol*, che si trova nel file *app/token/contract_addresses.json*.

In questo modo, il saldo di GreenToken sarà visibile direttamente nel wallet MetaMask.

5.4 Compatibilità con i Sistemi Operativi

GreenProof è stato sviluppato e testato con diversi livelli di compatibilità a seconda del sistema operativo.

5.4.1 Windows

GreenProof è pienamente supportato e testato su Windows 11, dove tutte le funzionalità sono disponibili. Windows 11 è la piattaforma consigliata per l'uso in produzione e tutti i passaggi di installazione descritti in questa documentazione sono stati verificati su questo sistema operativo.

5.4.2 Linux

Su Linux è disponibile un supporto di base, sebbene i test siano stati limitati. In alcuni ambienti potrebbe essere necessaria una configurazione aggiuntiva. Sono note alcune limitazioni, tra cui la possibilità della variazione delle prestazioni a seconda della distribuzione utilizzata.

5.4.3 macOS

L'applicazione non è ufficialmente supportata su macOS e non è stata progettata né testata per l'esecuzione su questo sistema operativo. Gli utenti che tentano di eseguire GreenProof su macOS potrebbero riscontrare problemi imprevisti, e non è disponibile alcun supporto ufficiale per la risoluzione di problematiche specifiche.

Per la migliore esperienza e stabilità, si consiglia di eseguire GreenProof su Windows 11.

5.5 Interfacce

In questa sezione vengono riportate le interfacce principali del nostro software divise nelle seguenti sottosezioni:

- **Home Interface**
- **Registration and Login**
- **Manage User Account**
- **Manage Company for Administrator Account**
- **Interfaces for System Admin**
- **Information about Company**

- Information about Product

5.5.1 Home Interface

In questa sottosezione presentiamo le interfacce relative alla schermata *home* (Figura 5.3).

In essa, sia gli utenti loggati che quelli non loggati possono visualizzare le compagnie e i prodotti disponibili.

In particolare, per un utente loggato, si possono verificare tre scenari distinti:

- **Utente senza compagnia associata:** l'utente ha la possibilità di registrare una nuova compagnia, che dovrà essere approvata dall'amministratore di sistema prima di essere operativa (Figura 5.4).
- **Interfaccia dell'amministratore di sistema:** consente all'amministratore di gestire tutte le compagnie e gli utenti presenti nel sistema (Figura 5.5).
- **Utente con ruolo di amministratore di compagnia:** l'utente oltre a gestire le proprie aziende, può amministrare i suoi impiegati, i suoi prodotti e i token (Figura 5.6).

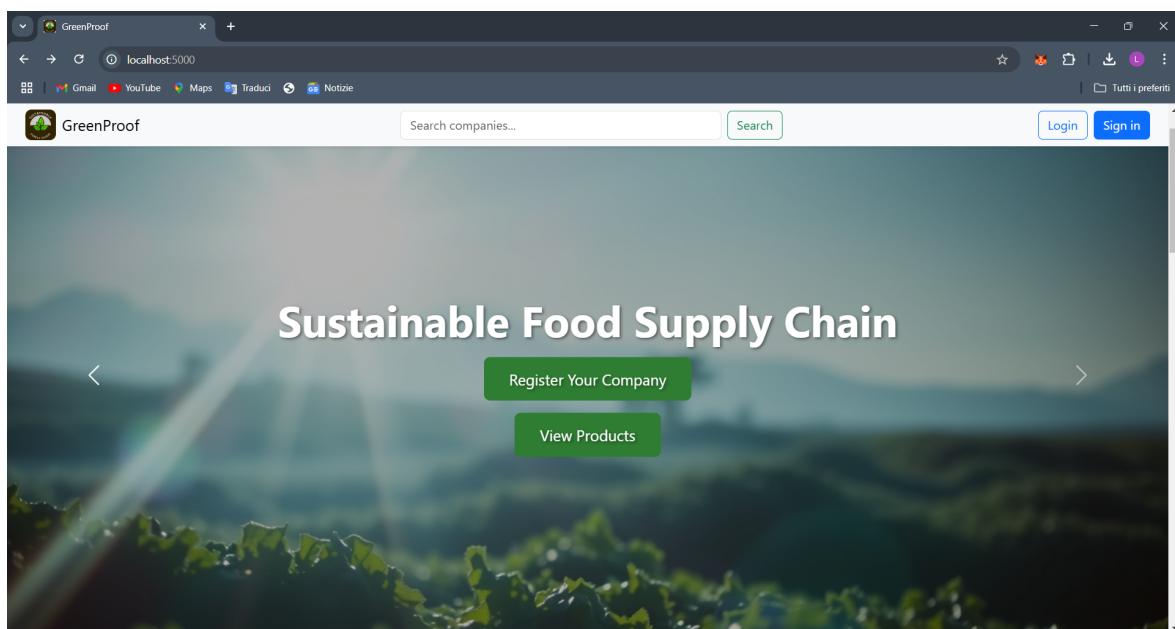


Figura 5.3: Home Interface For Not Login User

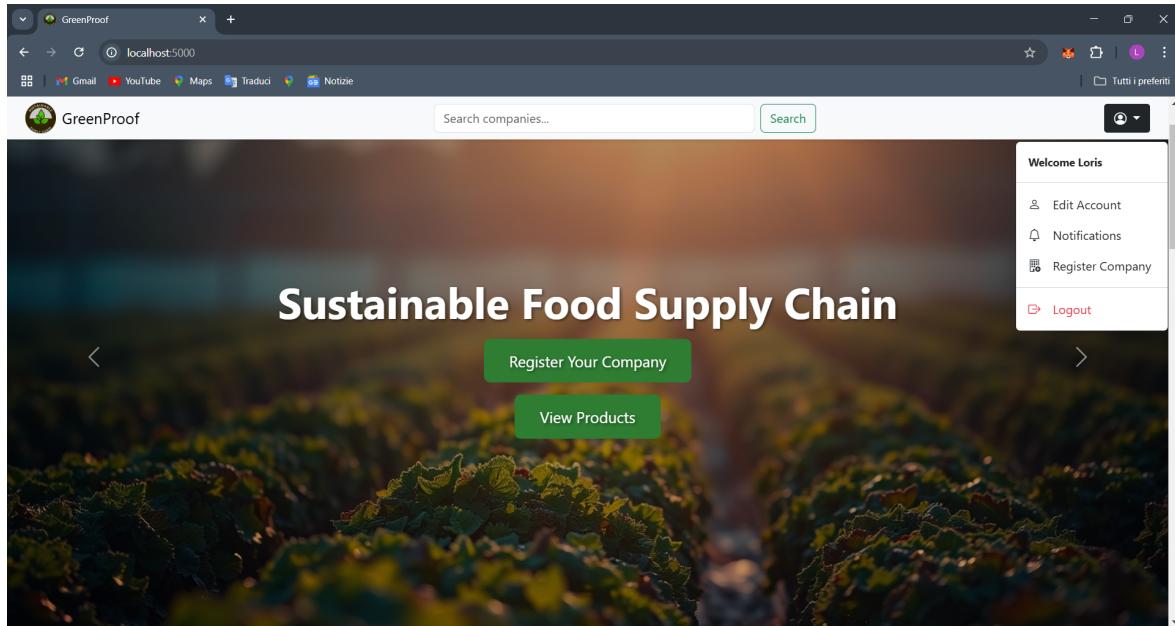


Figura 5.4: Home Interface For a Generic User

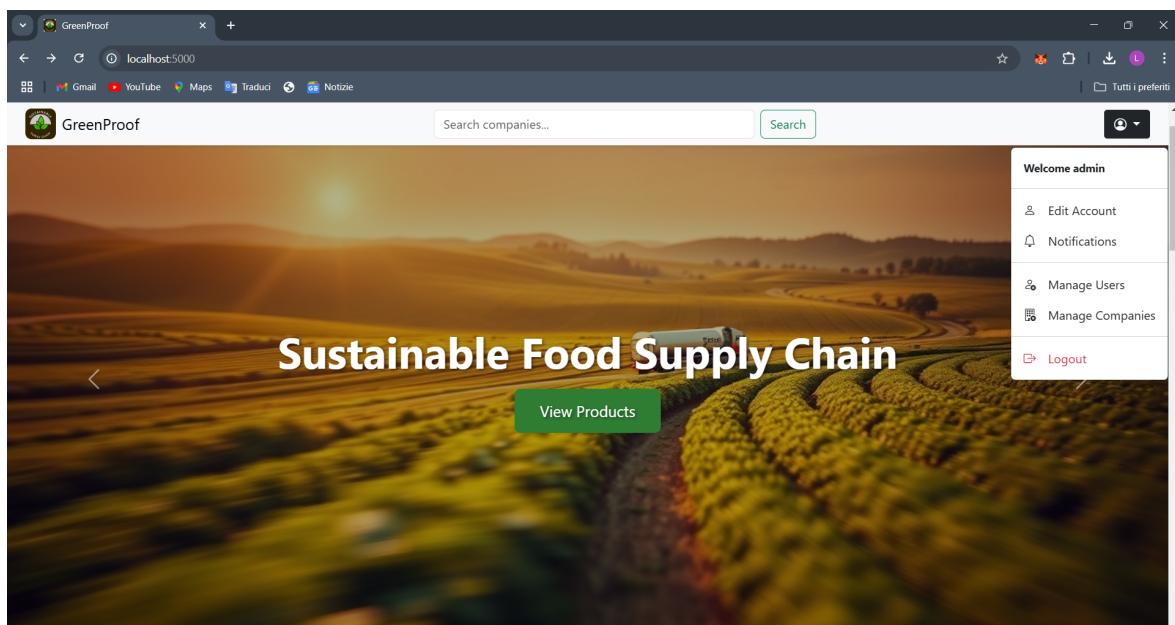


Figura 5.5: Home Interface For Admin

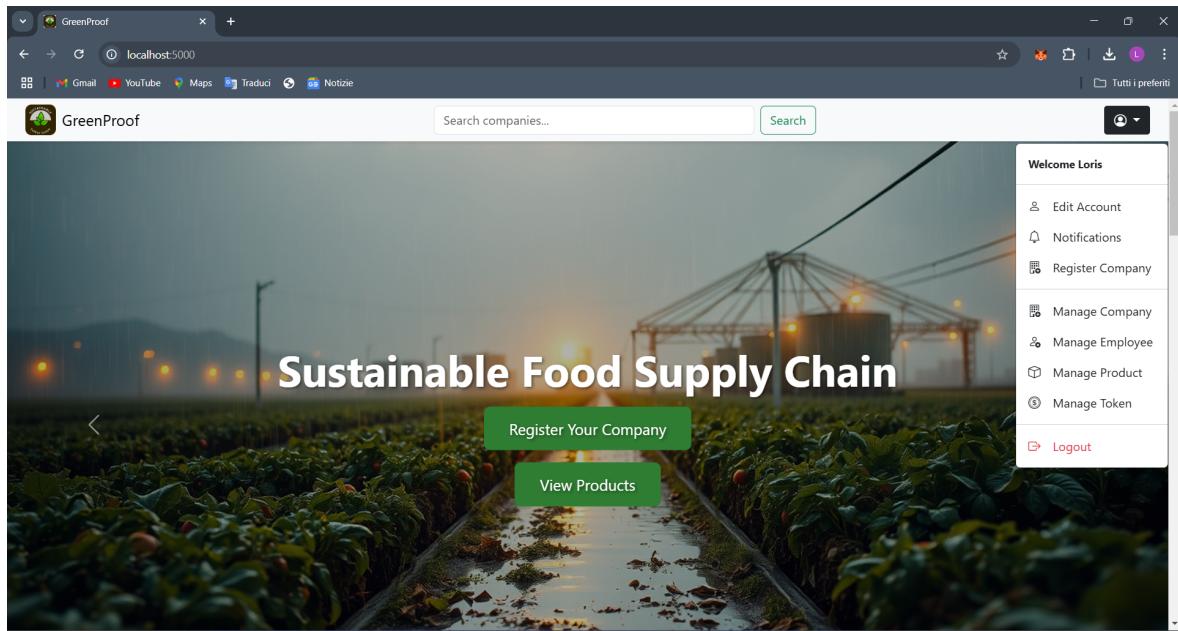


Figura 5.6: Home Interface For Company Administrator

5.5.2 Registration and Login

In questa sottosezione presentiamo le schermate di registrazione e login per l'accesso al sistema da parte di un utente. L'utente, per registrarsi, deve compilare correttamente i seguenti campi: email, nome, cognome, password, numero di telefono e data di nascita. Inoltre, dovrà accettare i termini e le condizioni d'uso, nonché l'informativa sulla privacy (Figura 5.7).

Figura 5.7: Register User Interface

Una volta effettuata la registrazione, verrà reindirizzato alla schermata di autenticazione a più fattori "MFA" (Figura 5.8), dove dovrà inserire il codice ricevuto via email(Figura 5.9).

Se il tempo a disposizione non fosse sufficiente, potrà richiedere l'invio di un nuovo codice di verifica.

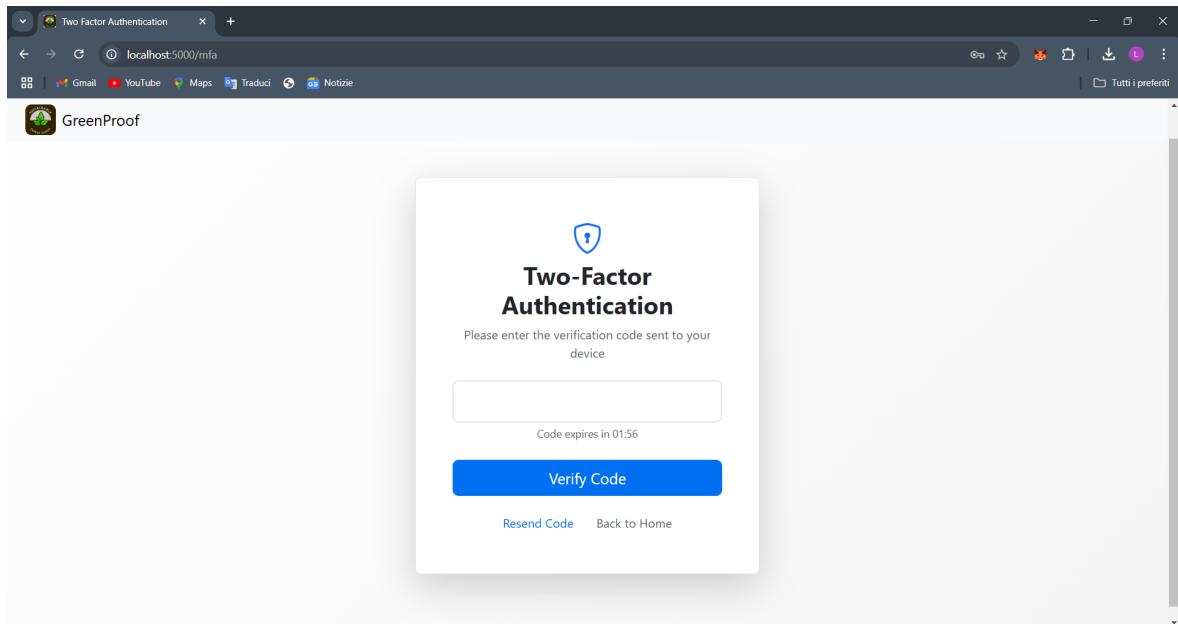


Figura 5.8: Two-Factor Authentication Interface

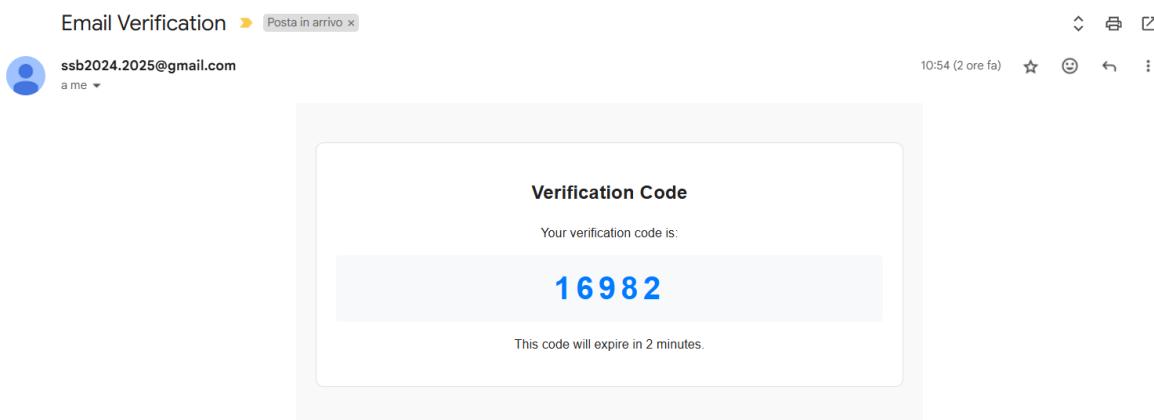


Figura 5.9: Verification Code Interface

Una volta completata con successo questa fase, l'utente avrà accesso al sistema. Quest'ultimo può avvenire anche tramite la schermata di login (Figura 5.10), dove, dopo aver inserito correttamente email e password, l'utente verrà nuovamente indirizzato alla schermata di autenticazione MFA.

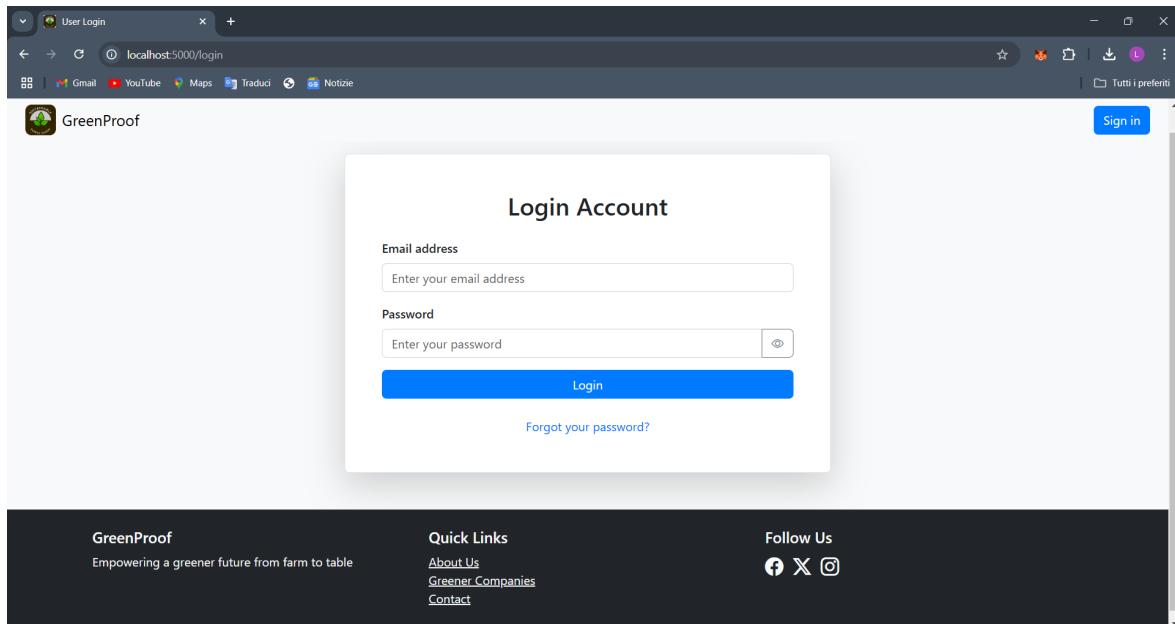


Figura 5.10: Login Account Interface

Nel caso in cui l'utente abbia dimenticato la password, potrà selezionare l'opzione *Forgot password* (Figura 5.11), inserire la propria email e ricevere un messaggio con le istruzioni per il recupero della password (Figura 5.12).

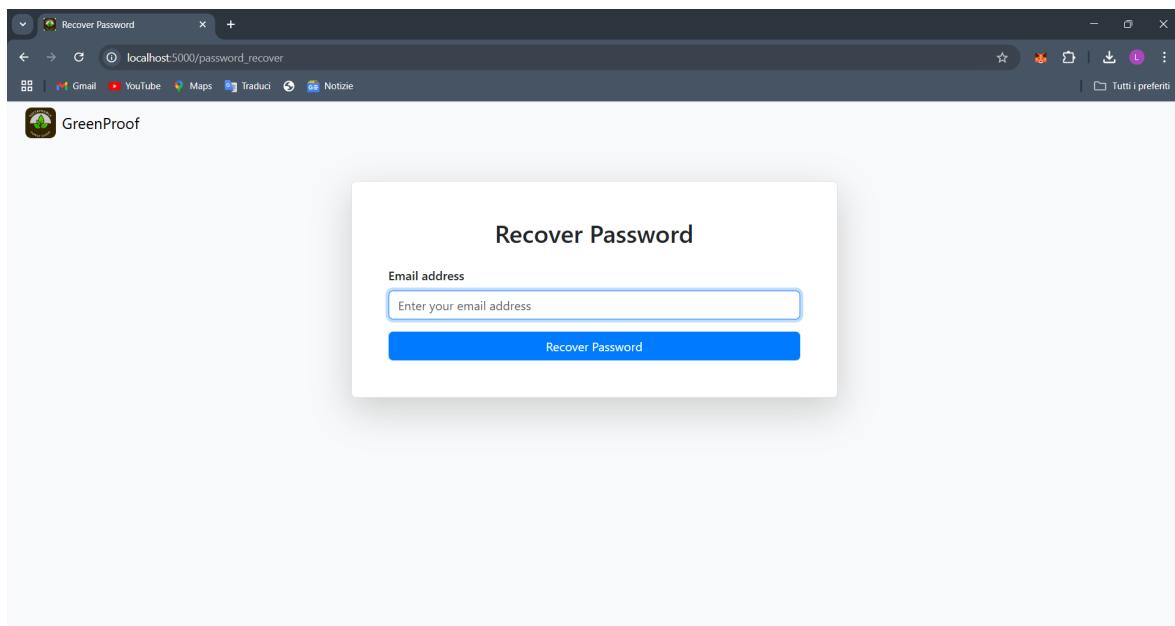


Figura 5.11: Recover Password Interface

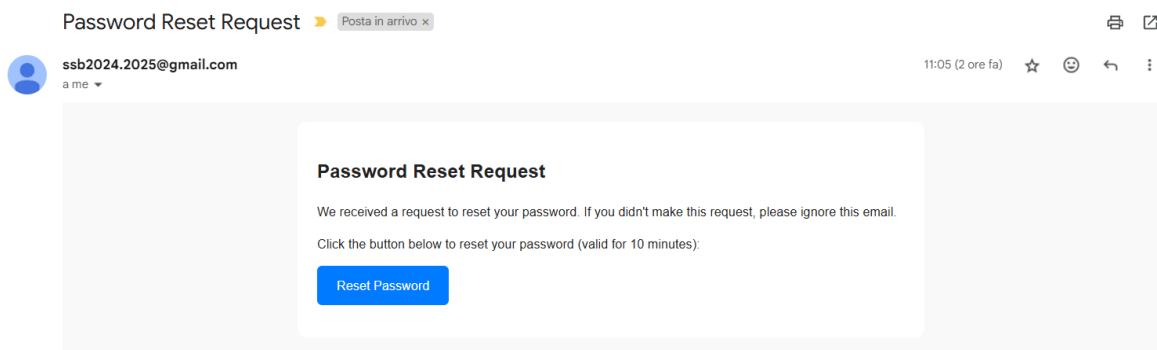


Figura 5.12: Reset Password Email

Una volta ricevuta l'email, si potrà accedere alla schermata per cambiare password (Figura 5.13).

A screenshot of a web browser window titled "Change Password". The URL bar shows "localhost:5000/password_recover_2/e3bca66f-78d1-4ce7-97aa-e96dc6ae0cf5". The page content is a "Change Password" form with the following fields:

- New Password: A text input field with placeholder text "Enter your new password".
- Confirm Password: A text input field with placeholder text "Confirm your password".
- Instructions: "Password must contain at least:
 - 8 characters
 - One uppercase letter
 - One lowercase letter
 - One number
 - One special character (@#\$%^&@)
- Buttons: "Update Password" (blue) and "Cancel" (grey).

Figura 5.13: Change Password Interface

5.5.3 Manage User Account

Una volta effettuato l'accesso al sistema, l'utente potrà gestire il proprio account e modificare alcune delle sue informazioni (Figura 5.14).

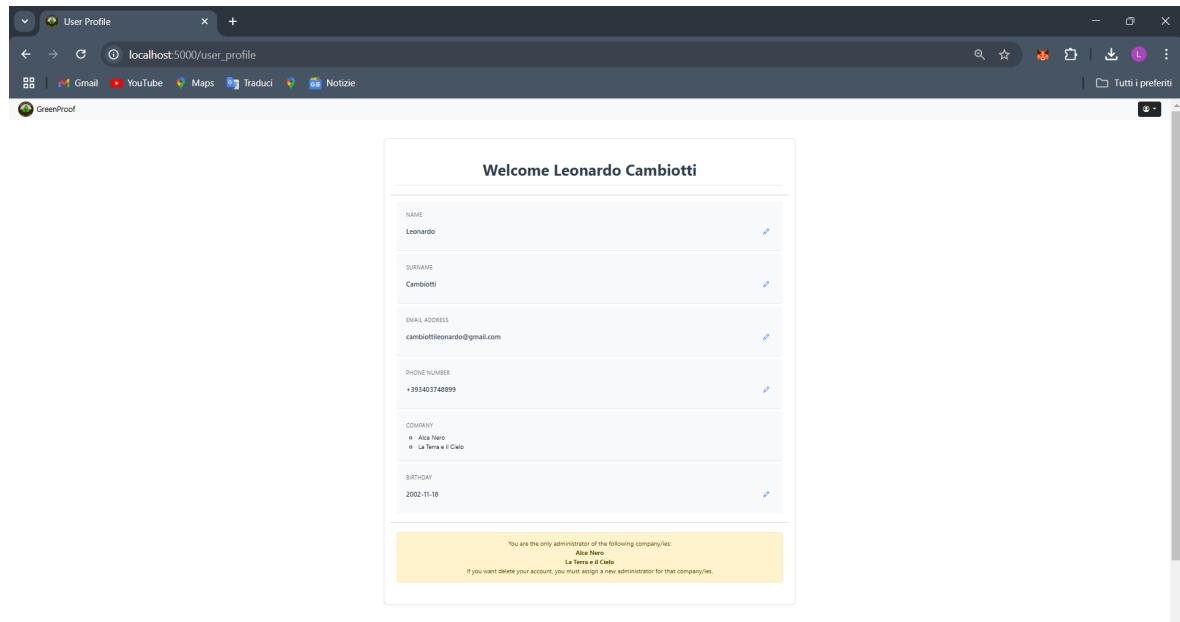


Figura 5.14: User Account Interface

Avrà inoltre la possibilità di registrare una nuova compagnia (Figura 5.15), la cui attivazione sarà soggetta all'approvazione dell'amministratore di sistema.

The screenshot shows a web browser window titled 'Company Registration' at 'localhost:5000/company_register'. The form includes fields for Company Name*, Phone Number*, Email Address*, Industry*, Country*, City*, Address*, Company Description*, Website, and Company Logo. A checkbox for accepting terms and conditions is present, along with a 'Register Company' button.

Figura 5.15: Register company

Una volta che ciò è avvenuto verrà notificata attraverso un'email (Figura 5.16).

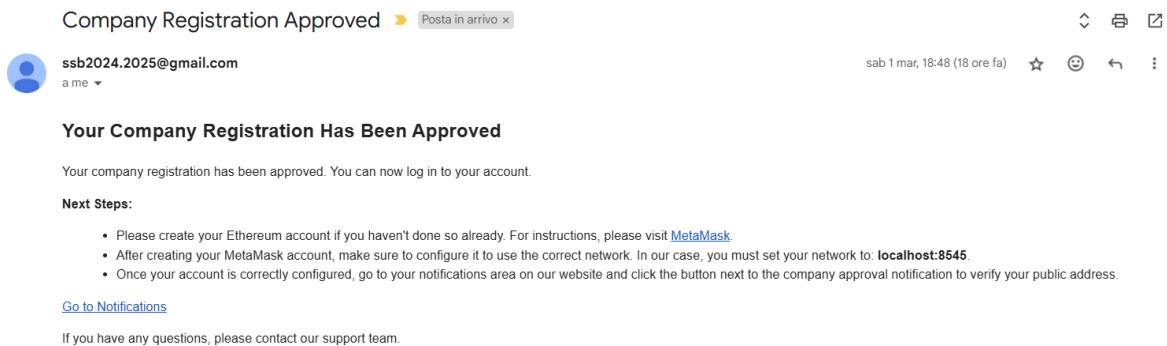


Figura 5.16: Company Registration Approved Email

Infine, l'utente potrà visualizzare eventuali messaggi ricevuti da altri utenti all'interno del sistema (Figura 5.17).

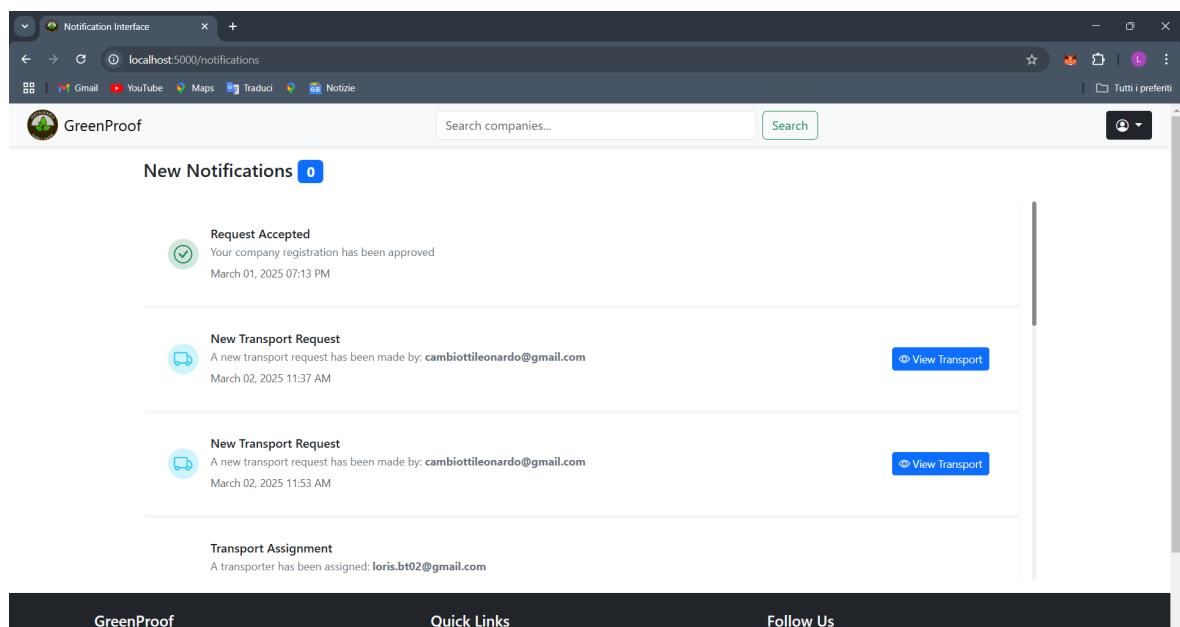


Figura 5.17: Notification Interface

5.5.4 Manage Company for Administrator Account

Quando un amministratore di un'azienda accede al sistema, può gestire le proprie compagnie (Figura 5.18).

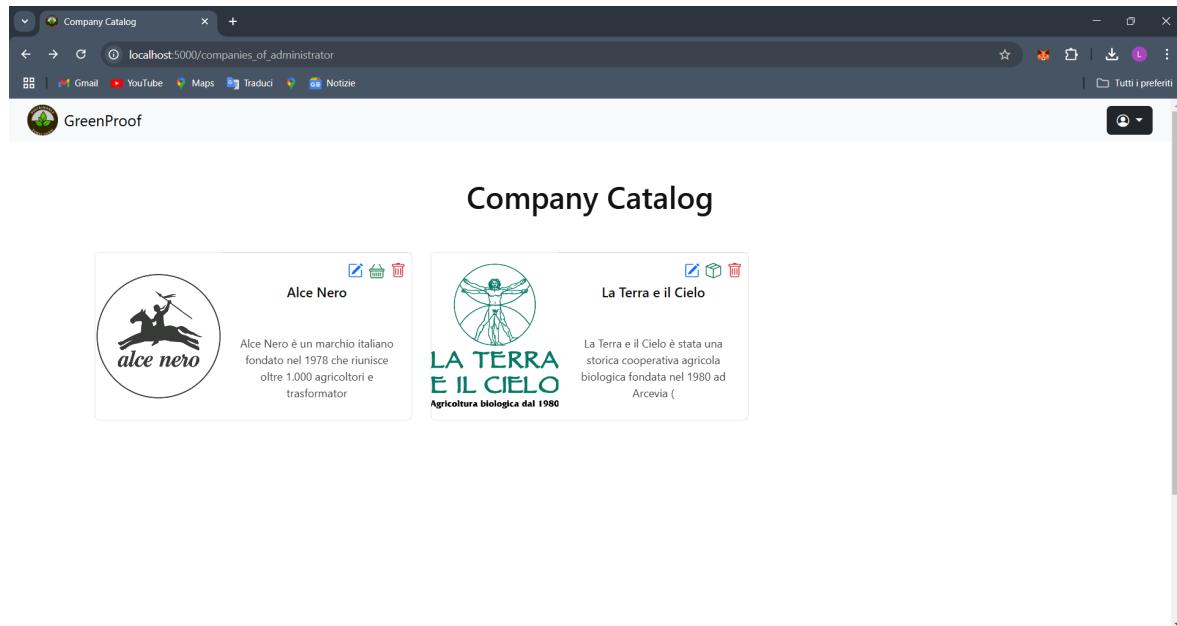


Figura 5.18: Company Catalog Interface For Administrator

Inoltre, ha la possibilità di modificare alcuni dati di un'azienda (Figura 5.19) o eliminarla, previa approvazione dell'amministratore di sistema.

The screenshot shows a web browser window titled 'Company Details Edit' at the URL 'localhost:5000/modify_company/293646233'. It displays the 'Edit Company Details' form for 'Alce Nero':

- Logo:** Current logo of Alce Nero.
- Company Name:** Alce Nero
- Phone Number:** +390516540211
- Email Address:** info@alcenero.it
- Industry:** manufacturer
- Website:** https://www.alcenero.com
- ETH Public Address:** 0xf17f52151EbEF6C7334FAD080c5704D77216b732
- Company Description:** A detailed description of Alce Nero's mission and history.
- Buttons:** 'Cancel' and 'Save Changes'.

Figura 5.19: Edit Company Details Interface

Inoltre, può gestire i prodotti della propria organizzazione attraverso un pulsante specifico, il cui aspetto varia in base al settore industriale. Questo pulsante reindirizza all'interfaccia di gestione dei prodotti "Manage Product", rappresentata da:

- **Figura 5.20** per i produttori (*Manufacturer*);



The screenshot shows a web browser window titled "Product Management Interface" with the URL "localhost:5000/manage_product/293646233". The page has a header "Product Management" and a "Add New Product" button. Below is a table with columns: Product Name, Description, Quantity, and Actions. The table contains three rows of data:

Product Name	Description	Quantity	Actions
legumi e cereali	Fagioli, lenticchie, ceci e cereali come farro e orzo, provenienti da coltivazioni biologiche italiane.	60	
miele	Mieli monoflora e millefiori prodotti da apicoltori italiani.	10	
olio extravergine di oliva	Ottenuto da olive italiane, spremuto a freddo per preservarne le qualità organolettiche.	55	

At the bottom of the page is a footer with the GreenProof logo, a mission statement "Empowering a greener future from farm to table", quick links to "About Us", "Greener Companies", and "Contact", and social media links for Facebook, X, and Instagram.

Figura 5.20: Product Management Interface

- **Figura 5.21** per i trasformatori (*Processor*);



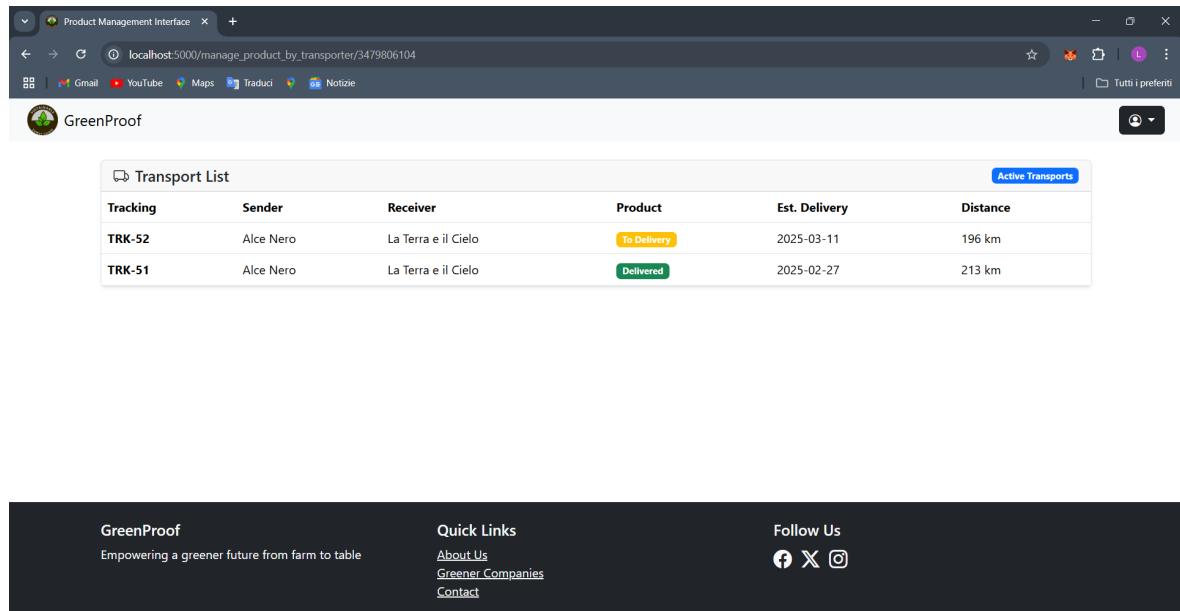
The screenshot shows a web browser window titled "Processor Product Management" with the URL "localhost:5000/manage_product_by_processor/2012445105". The page has a header "Processor Product Management" and a "Add New Product" button. Below is a table with columns: Product Name, Description, Quantity, and Actions. The table contains two rows of data:

Product Name	Description	Quantity	Actions
hummus	L'hummus è una crema spalmabile preparata principalmente con ceci cotti, tahina (pasta di sesamo), limone e aglio. È un piatto tradizionale mediorientale e un'ottima fonte di proteine vegetali.	15	
burger vegetali	I burger vegetali sono un tipo di hamburger a base di ingredienti completamente vegetali, utilizzati come alternativa ai tradizionali burger di carne. Questi burger sono molto apprezzati da chi segue una dieta vegetariana, vegana o semplicemente chi desidera ridurre il consumo di	12	

At the bottom of the page is a footer with the GreenProof logo, a mission statement "Empowering a greener future from farm to table", quick links to "About Us", "Greener Companies", and "Contact", and social media links for Facebook, X, and Instagram.

Figura 5.21: Processor Product Management Interface

- **Figura 5.22** per i trasportatori (*Transporter*);



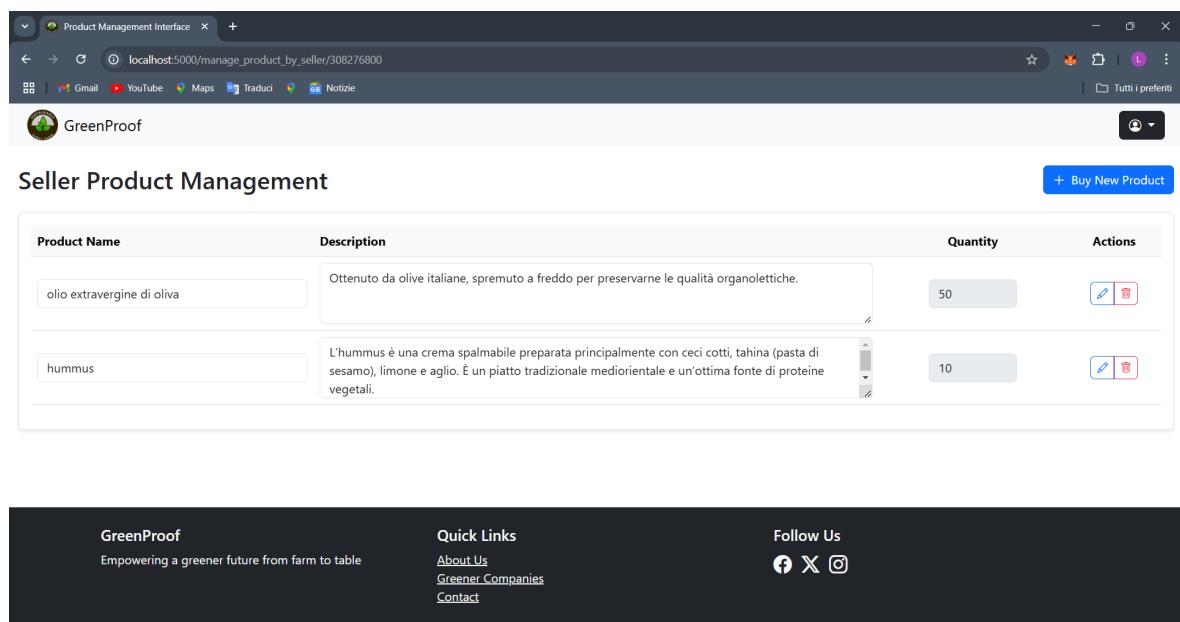
The screenshot shows a web browser window titled "Product Management Interface" with the URL "localhost:5000/manage_product_by_transporter/3479806104". The page header includes the GreenProof logo and a "Transport List" section. Below the header is a table with the following data:

Tracking	Sender	Receiver	Product	Est. Delivery	Distance
TRK-52	Alce Nero	La Terra e il Cielo	To Delivery	2025-03-11	196 km
TRK-51	Alce Nero	La Terra e il Cielo	Delivered	2025-02-27	213 km

At the bottom of the page is a footer with the GreenProof logo, a "Quick Links" menu with links to "About Us", "Greener Companies", and "Contact", and social media icons for Facebook, X, and Instagram.

Figura 5.22: Trasport List Interface

- **Figura 5.23** per i venditori (*Seller*).



The screenshot shows a web browser window titled "Product Management Interface" with the URL "localhost:5000/manage_product_by_seller/308276800". The page header includes the GreenProof logo and a "Seller Product Management" section. Below the header is a table with the following data:

Product Name	Description	Quantity	Actions
olio extravergine di oliva	Ottenuto da olive italiane, spremuto a freddo per preservarne le qualità organolettiche.	50	Edit Delete
hummus	L'hummus è una crema spalmabile preparata principalmente con ceci cotti, tahina (pasta di sesamo), limone e aglio. È un piatto tradizionale mediorientale e un'ottima fonte di proteine vegetali.	10	Edit Delete

At the bottom of the page is a footer with the GreenProof logo, a "Quick Links" menu with links to "About Us", "Greener Companies", and "Contact", and social media icons for Facebook, X, and Instagram.

Figura 5.23: Seller Product Management Interface

Se l'amministratore della compagnia è un *Processor* e desidera produrre un nuovo prodotto, dovrà prima richiedere le materie prime ai *Manufacturer* che si occupano della loro produzione (Figura 5.24).

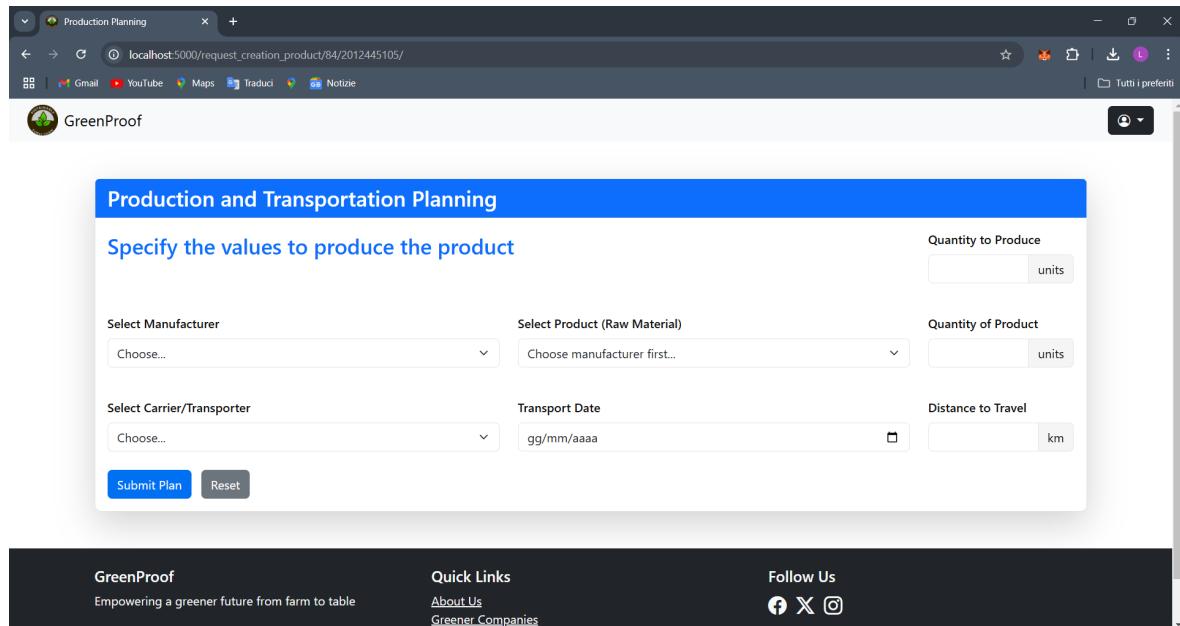


Figura 5.24: Production and Transportation Planning Interface

Inoltre, dovrà selezionare un *Trasporter* per effettuare la consegna entro una data prestabilita e per un numero specifico di chilometri. A questo punto, una volta inviata la richiesta, le aziende coinvolte potranno accettarla (Figura 5.25) o rifiutarla (Figura 5.26).

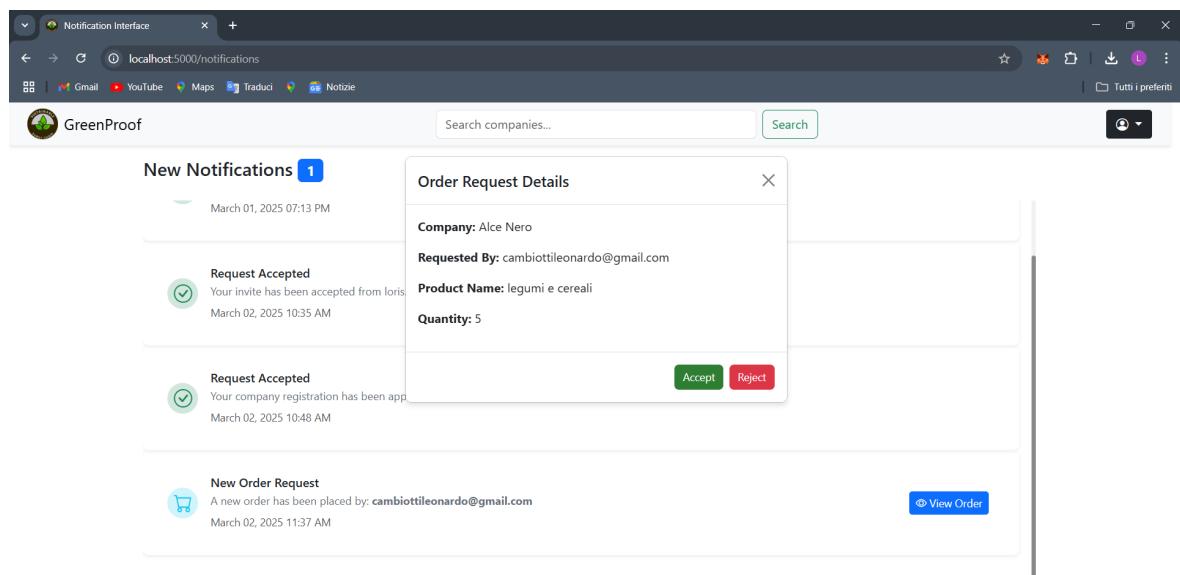


Figura 5.25: Order Request Details Interface

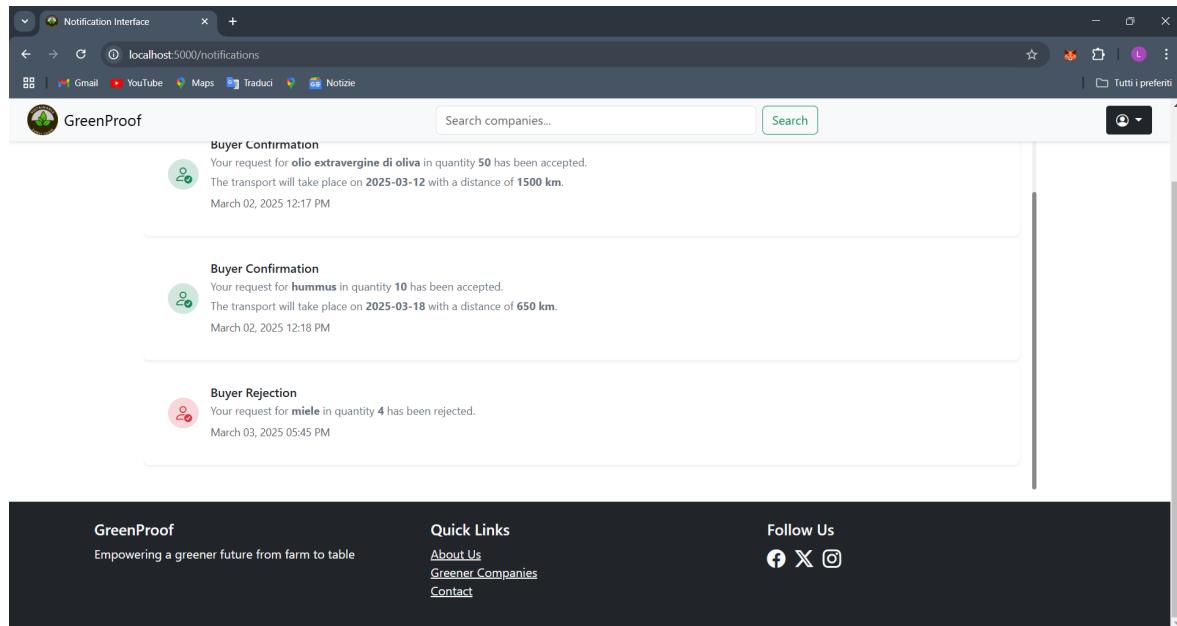


Figura 5.26: Order Request Details Interface

Si noti come, un’interfaccia simile è prevista anche qualora l’amministratore della compagnia sia un *Seller*. In particolare, esso può acquistare prodotti sia dai Manufacturer che dai Processor. Nel caso in cui tutte le aziende coinvolte accettano la richiesta, l’ordine viene confermato e le parti riceveranno una notifica di conferma (Figure 5.27 e 5.28).

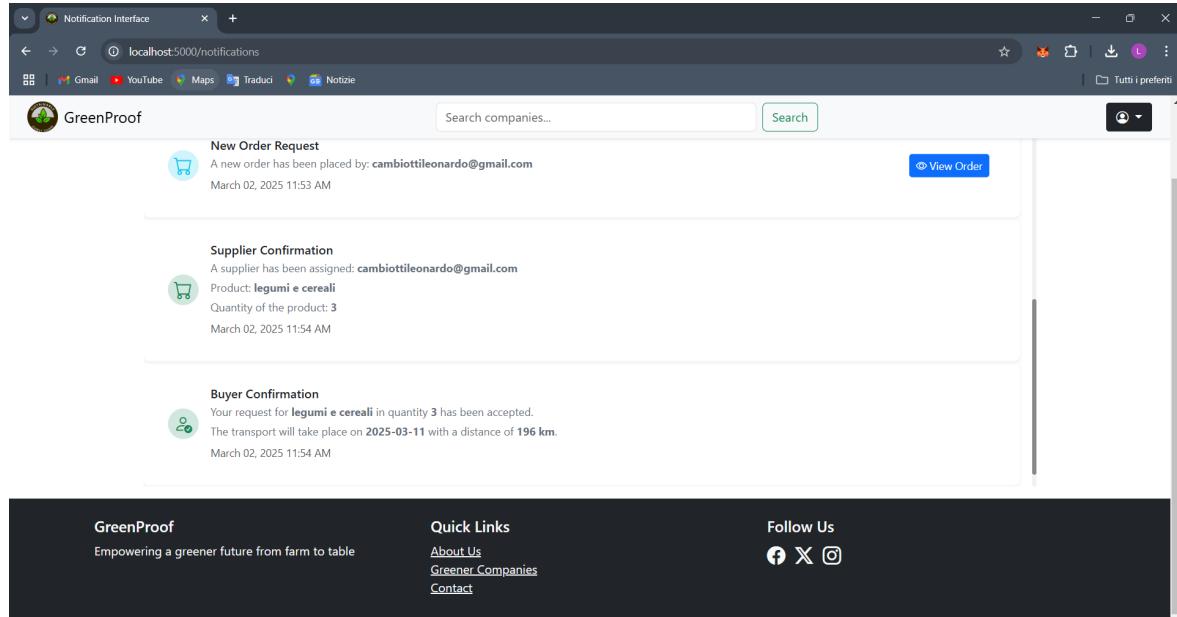


Figura 5.27: Notification Confirmation by Supplier and Buyer

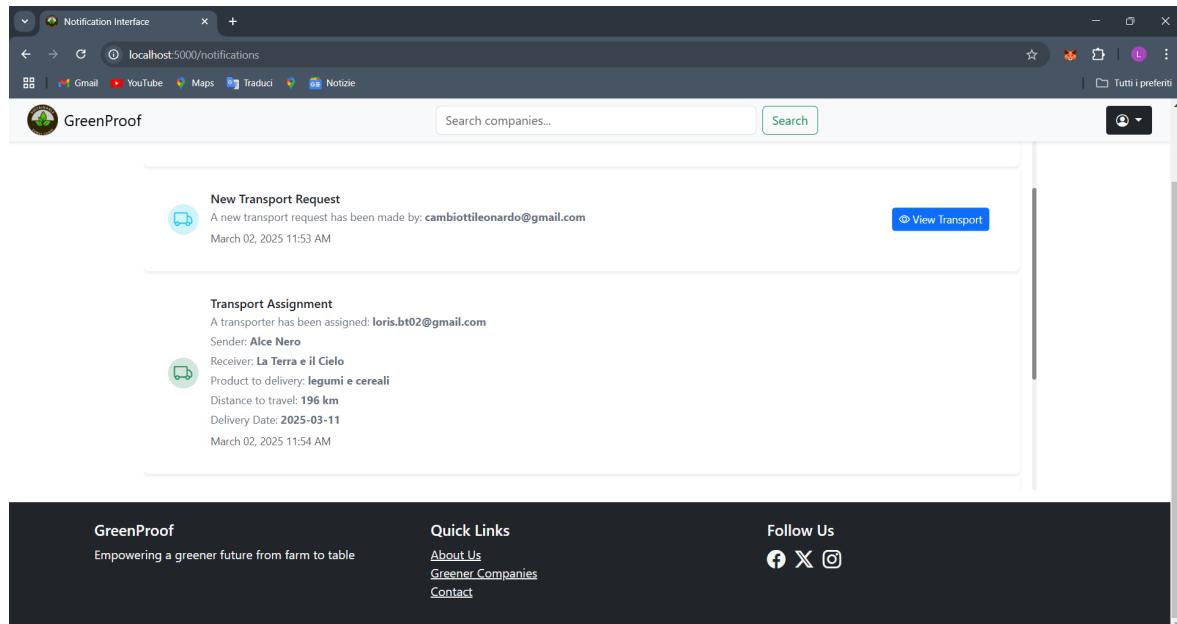


Figura 5.28: Notification of Transport

L'amministratore della compagnia potrà anche gestire i propri dipendenti tramite l'interfaccia mostrata in Figura 5.29. In particolare, avrà la possibilità di visualizzare i lavoratori associati alle proprie compagnie e invitare altri utenti già presenti nel sistema (con un'email valida) a diventare dipendenti di una sua specifica compagnia.

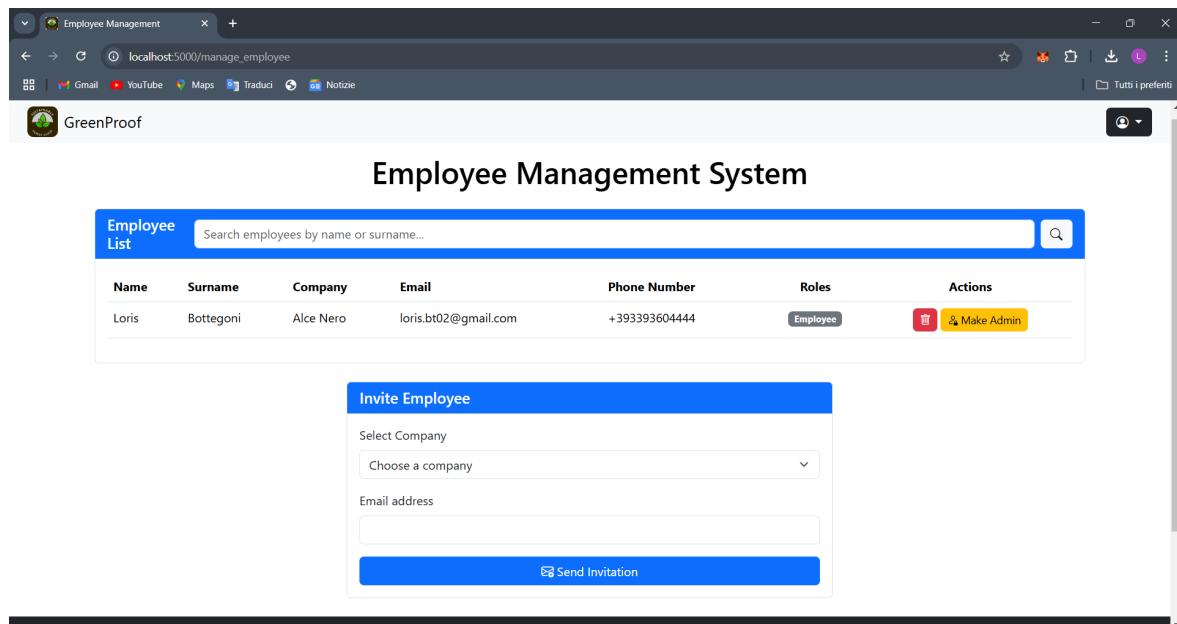


Figura 5.29: Employee Management System Interface

Inoltre, l'amministratore della compagnia potrà gestire i token, per una specifica azienda, tramite un interfaccia dedicata (Figura 5.30). Si osservi come, dopo un intervallo di tempo predefinito, verranno valutate le emissioni medie in rapporto alla quantità di prodotti realizzati e alla quantità di CO₂ generata nel periodo precedente. In base a queste valutazioni, eventualmente verrà assegnata una determinata quantità di CO₂ Token (*GreenToken*).

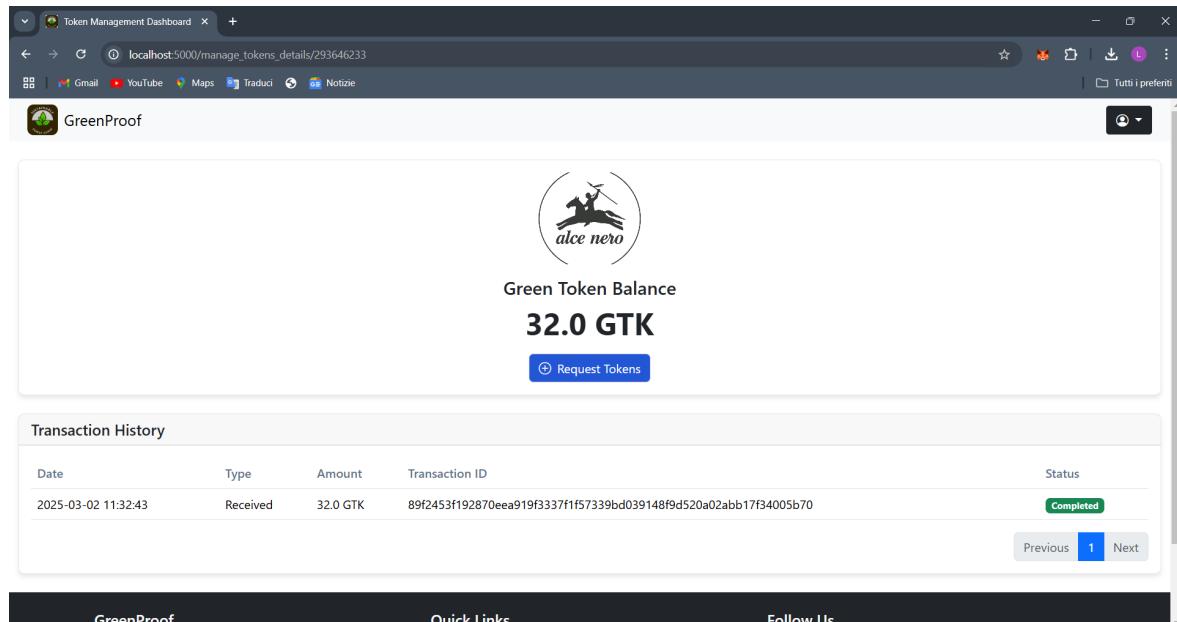


Figura 5.30: Token Balance Interface

Qualora un’azienda necessita di ulteriori token, l’utente potrà specificare la quantità di cui necessita e selezionare, tramite un menù a tendina, una delle aziende che dispone di un numero sufficiente di token (Figura 5.31).

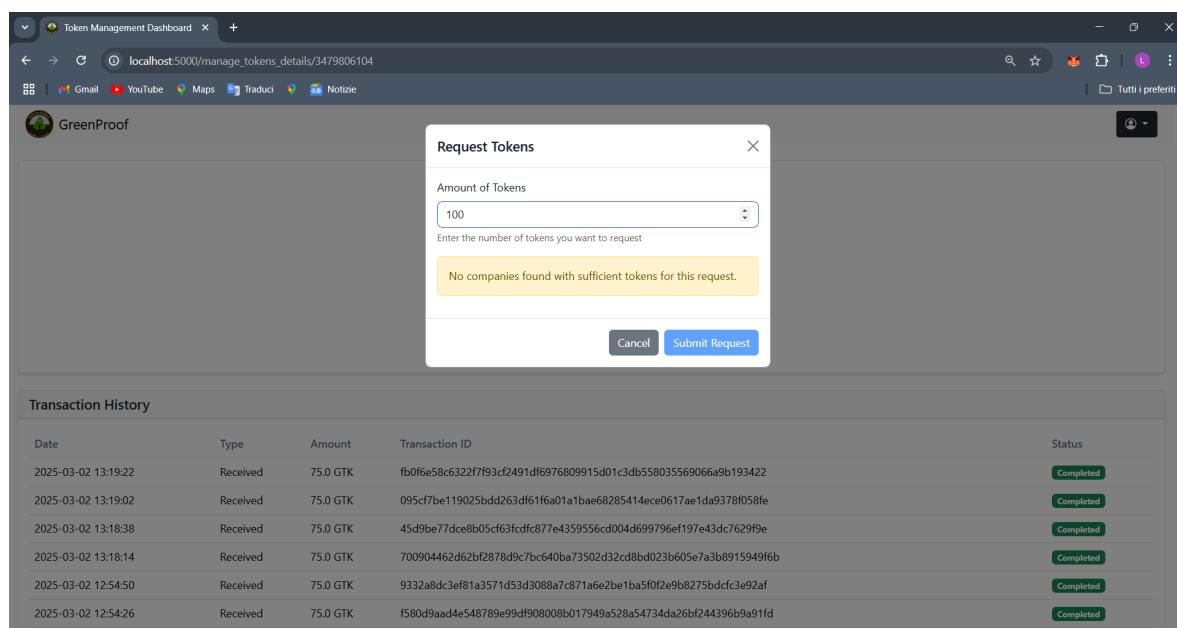


Figura 5.31: Request of Token Interface

L’utente potrà quindi inviare una notifica, che dovrà essere accettata dall’azienda che ha ricevuto la richiesta attraverso MetaMask (Figura 5.32). Infine, sarà possibile visualizzare lo storico delle transazioni effettuate.

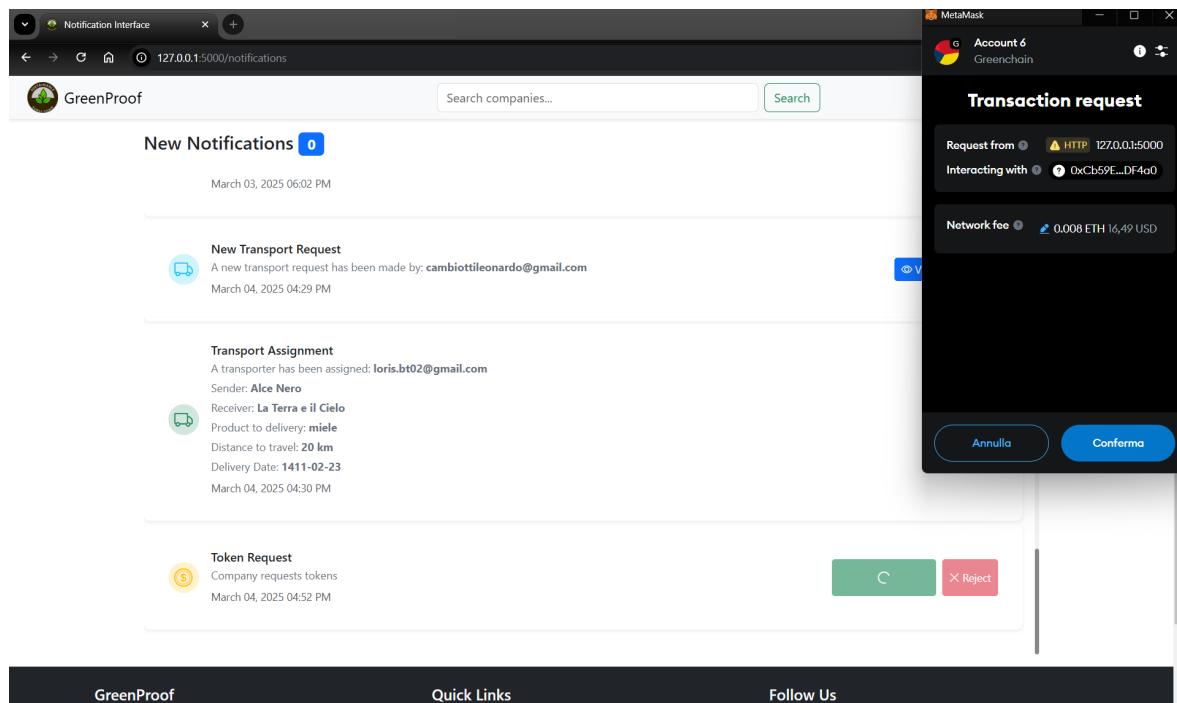


Figura 5.32: Accept Request with MetaMask

5.5.5 Interfaces for System Admin

L'amministratore di sistema ha la possibilità di gestire gli utenti, con la possibilità di eliminarli, a patto che non siano gli unici amministratori di una compagnia (Figura 5.33).

The screenshot shows a web browser window titled 'User Management' at the URL 'localhost:5000/admin/admin_manage_user'. The title bar also shows 'Gmail YouTube Maps Traduci Notizie' and a 'GreenProof' icon.

The main content is titled 'User Management System' and features a 'User List' table. The table has the following data:

Name	Surname	Birthday	Email	Phone Number	Actions
Loris	Bottegoni	2002-08-26	loris.bt02@gmail.com	+393393604444	Admin
Valerio	Crocetti	2002-11-28	valerio.crocetti@gmail.com	+3912345675	Admin
Leonardo	Cambotti	2002-11-18	cambiotileonardo@gmail.com	+393403748899	Admin

Figura 5.33: User Management System Interface

Inoltre, può gestire le compagnie, modificandone i dati o procedendo alla loro eliminazione (Figura 5.34).

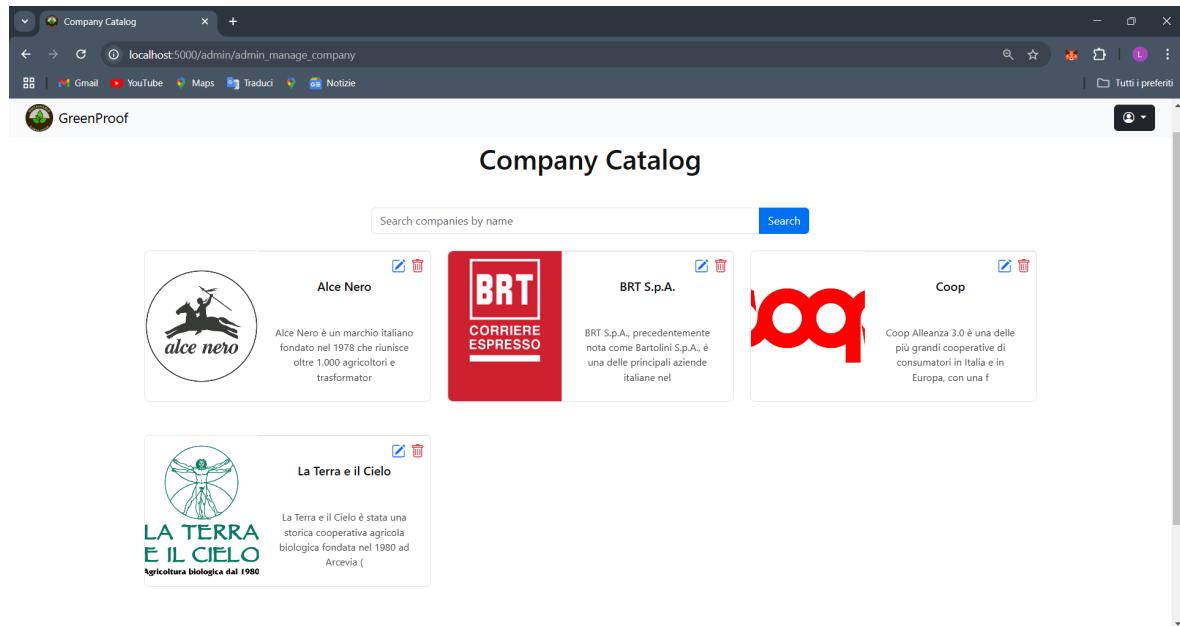


Figura 5.34: Company Management System Interface

Infine, l'amministratore svolge un ruolo fondamentale nell'approvazione delle richieste di registrazione degli utenti alle aziende, nonché nell'autorizzazione di eventuali cancellazioni. (Figura 5.35).

The screenshot shows a web browser window titled 'Notification Interface' at the URL 'localhost:5000/notifications'. The page has a search bar at the top right. A message box at the top left says 'New Notifications 1'. The main content area displays a single notification:

New Company Registration Request
New company registration for GustaBio has been requested from: loris.bt02@gmail.com
March 03, 2025 08:27 PM

With two buttons at the bottom right: a green 'Approve' button and a red 'Reject' button.

At the bottom of the screen, there is a footer navigation bar with links for 'GreenProof', 'Quick Links' (About Us, Greener Companies, Contact), and 'Follow Us' (Facebook, X, Instagram icons).

Figura 5.35: Admin of System Notification Interface

5.5.6 Information about Company

Un qualsiasi utente che desidera informarsi sulle compagnie presenti nel sistema può utilizzare il pulsante *Search* all'interno della schermata iniziale per visualizzare l'elenco di tutte le aziende (Figura 5.36).

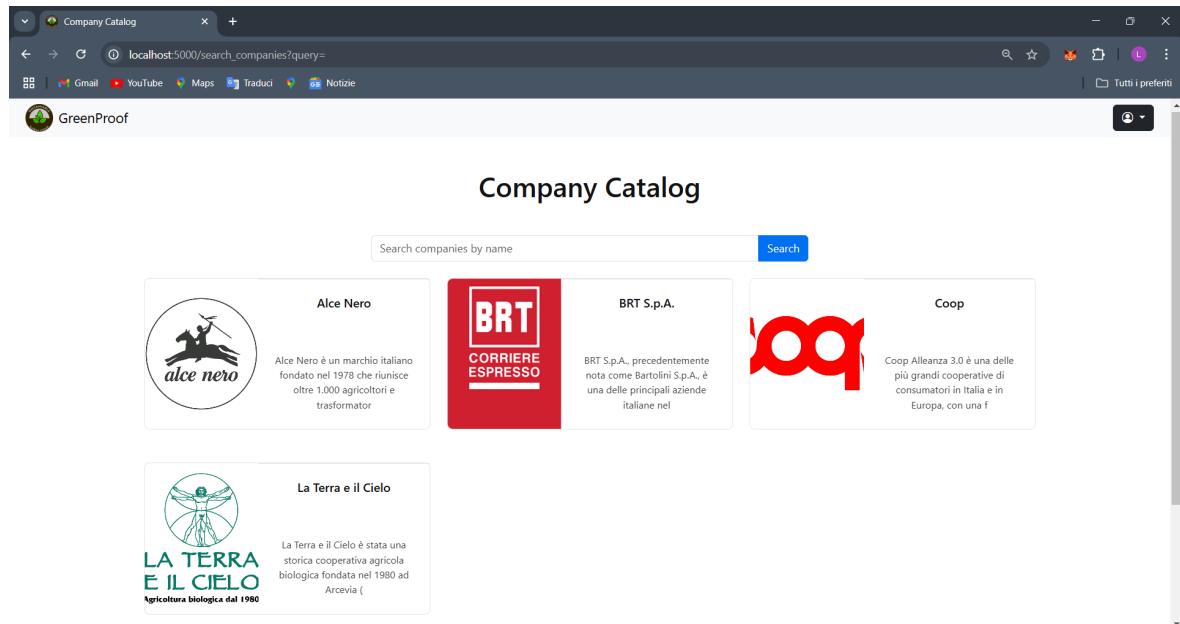


Figura 5.36: Company Catalog Interface

Si noti come sia possibile anche cercare una specifica compagnia digitandone il nome o soltanto un parte di esso. Inoltre, per ottenere maggiori dettagli, l’utente, cliccando sulla card associata alla compagnia, può accedere a informazioni più dettagliate (Figura 5.37).

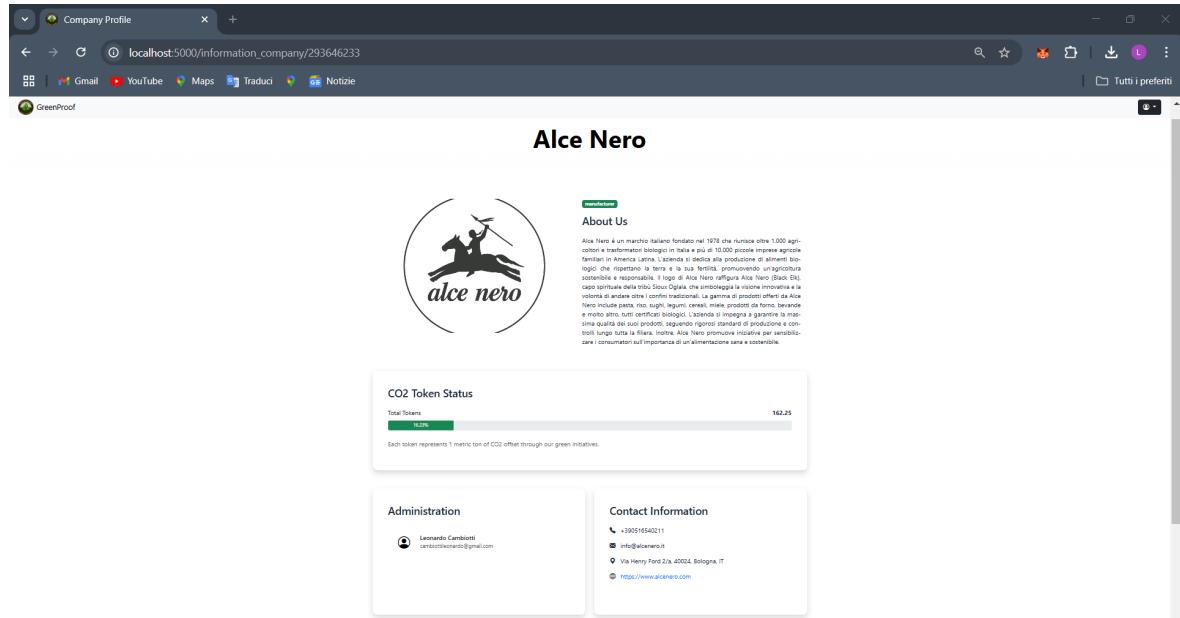


Figura 5.37: Information Company Interface

Infine, nella schermata iniziale verranno evidenziate le aziende con il maggior numero di *GreenToken*, sottolineando il loro impegno verso la sostenibilità e la riduzione dell’inquinamento (Figura 5.38).

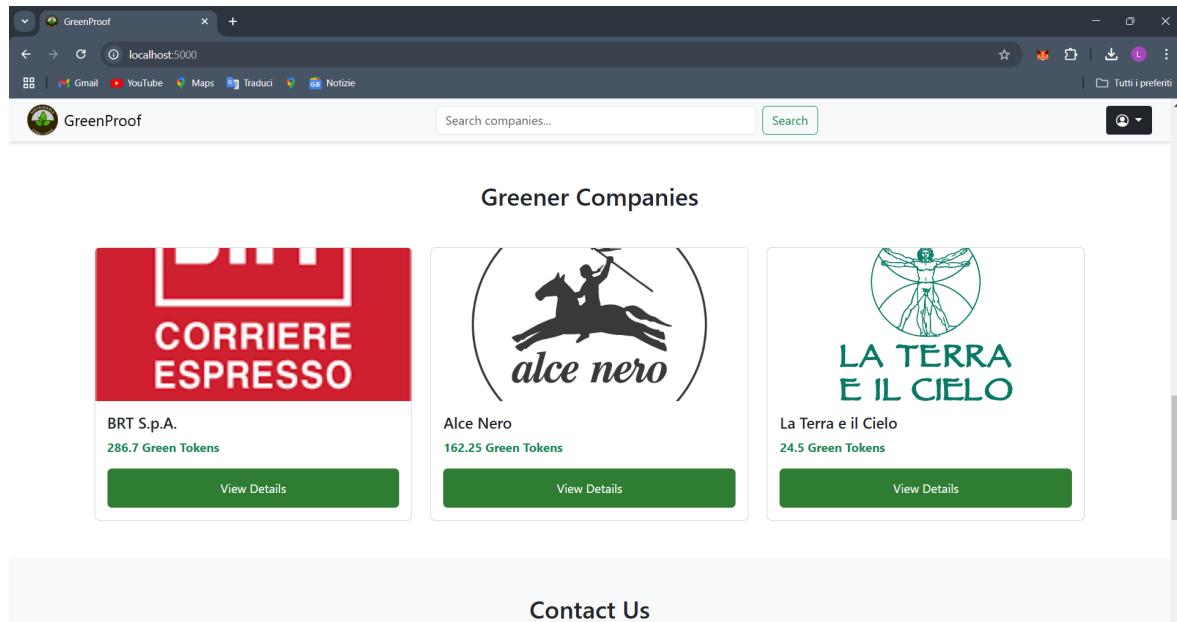


Figura 5.38: Greener Companies List Interface

5.5.7 Information about Product

Un qualsiasi utente che desidera ottenere informazioni sui prodotti può accedere tramite il pulsante *View Product*, presente nell’interfaccia principale. Una volta selezionato, verrà reindirizzato a un’interfaccia in cui sono visibili esclusivamente le compagnie che svolgono la professione di *Seller* e hanno dei prodotti ad esse associati (Figura 5.39).

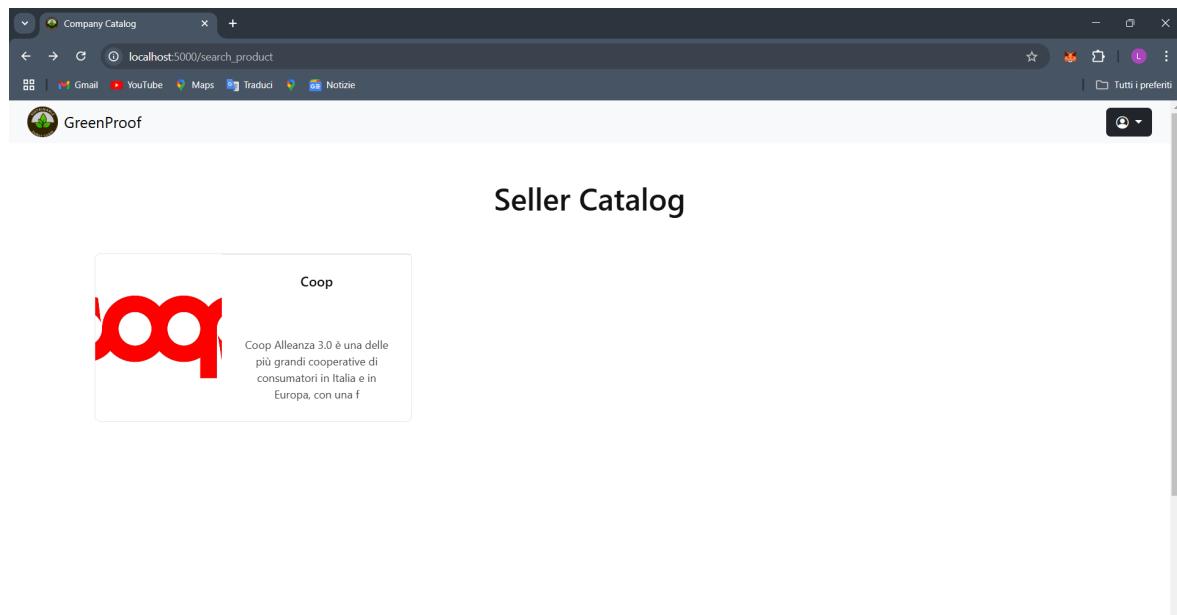


Figura 5.39: Seller Catalog Interface

Cliccando sulla card di una compagnia, sarà possibile visualizzare l’elenco dei prodotti disponibili per quello specifico *Seller* (Figura 5.40).

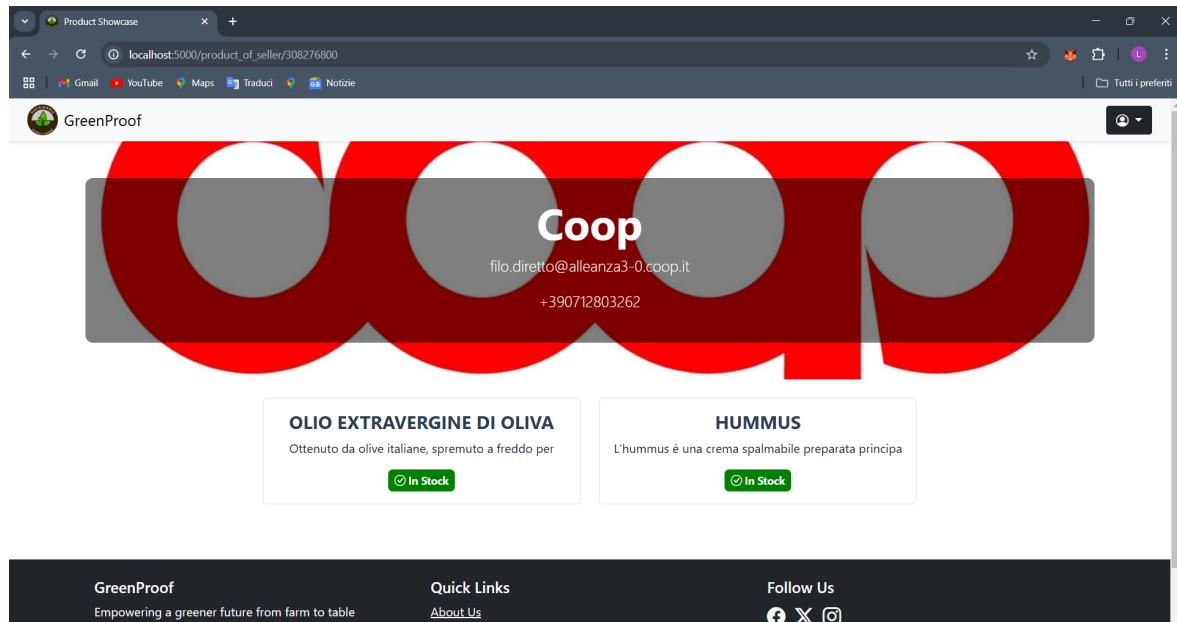


Figura 5.40: Product of a Seller Interface

Per avere ulteriori dettagli relativi a un prodotto, l’utente potrà accedere a informazioni aggiuntive, tra cui le compagnie coinvolte nella sua produzione e la quantità di CO₂ emessa durante il processo (Figura 5.41).

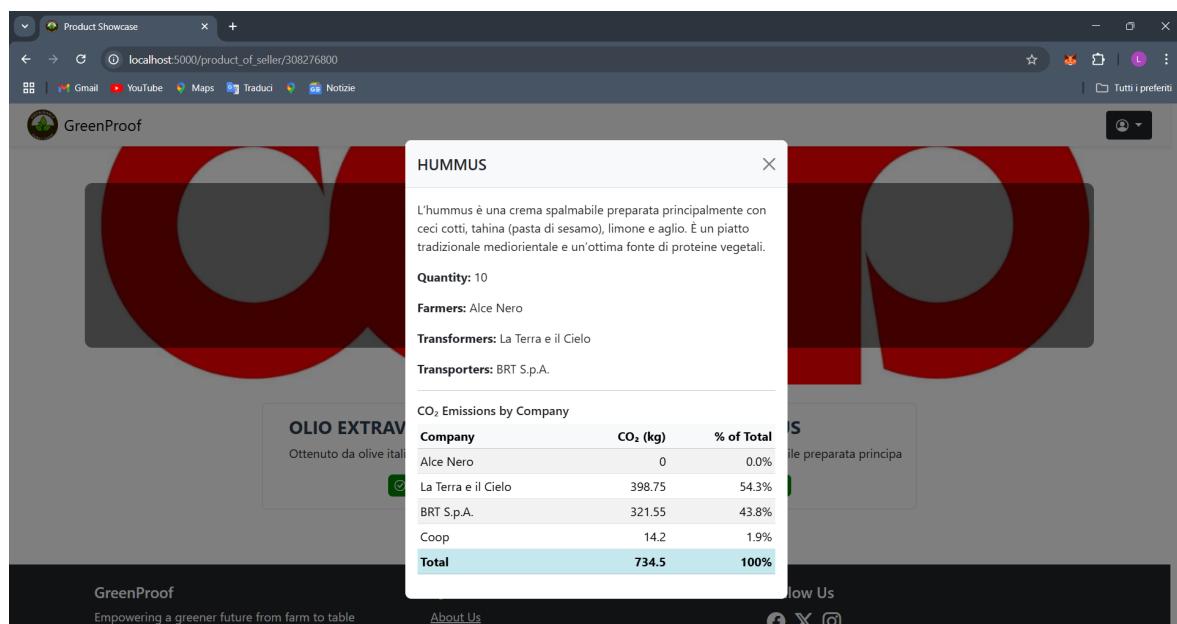


Figura 5.41: CO₂ History Interface