OPEN WebIM

Università Politecnica delle Marche

Dipartimento di Ingegneria dell'informazione

Laurea Magistrale in Ingegneria Informatica e dell'Automazione

Corso di Software Cybersecurity

Gruppo 3:

Cattani Lorenzo S1096992

Marzetti Daniele S1096966

Matè Felipe S1093746

Osimani Nico S1092544

Professori:

Luca Spalazzi

Spegni Francesco

INDICE

Introduzione

Per rendere gli appalti più sicuri, cioè per far in modo che ci siano meno illeciti, si è deciso di utilizzare la tecnologia blockchain come piattaforma su cui salvare il giornale dei lavori, il libretto delle misure e lo stato di avanzamento dei lavori. Questo progetto si chiama Open WebIM, in questo documento sarà illustrato tutto il processo che ha portato alla realizzazione di una parte di Open WebIM, cioè quella che ha a che fare con il salvataggio di immagini e misure nella blockchain, in modo tale da non poter più modificare tali informazioni una volta inserite nella catena.

Da un'analisi preliminare, sono emersi i seguenti requisiti di sicurezza:

- L'autenticità delle immagini: si deve poter sapere dove e quando sono state acquisite.
- L'autenticità delle misure: dove e quando sono state calcolate dal servizio di fotogrammetria, e a quali immagini fanno riferimento.
- L'integrità delle immagini: una volta ricevute le immagini dal drone, supponendo che le immagini ricevute non siano state alterate, non devono poter essere modificate.
- L'integrità delle misure: una volta calcolate le misure non devono poter essere alterate.
- Non ripudio di chi ha prodotto immagini e misure

La blockchain è una tecnologia che di per sé già risponde a tali requisiti, per questo si è scelto di adottarla.

In particolare, usando la blockchain, la potenza di calcolo necessaria alla validazione delle transazioni, aumenta all'aumentare dei dati salvati al suo interno, inoltre, hanno una quantità limitata di memoria disponibile per blocco, quindi è estremamente sconveniente utilizzarla direttamente come strumento di salvataggio di immagini e misure.

Ogni blocco conterrà quindi, l'hash della misura e delle immagini associate in modo tale da poter sempre verificare l'integrità dei dati, inoltre conterrà anche i metadati di tali immagini e misure.

Verrà utilizzato un DBMS come strumento di salvataggio dei metadati delle immagini e delle misure, oltre che per gestire l'accesso alla piattaforma web.

N.B. si consiglia di visualizzare i diagrammi e le tabelle direttamente scaricandole dal repository nelle relative cartelle, per ottenere una visualizzazione ottimale.

Early requirement analisys

La fase preliminare di analisi dei requisiti è stata effettuata servendosi del linguaggio di modellazione *i**, tale scelta è avvenuta considerando la capacità di tale linguaggio di astrarre le specifiche del progetto al livello più appropriato per ogni tipo di analisi, inoltre grazie alla sua facilità di uso è in grado di rappresentare in maniera semplice e diretta ogni elemento del sistema e le sue relazioni.

Le immagini vengono acquisite tramite dei droni per poter effettuare controlli e per poter calcolare le misure tramite un servizio di fotogrammetria.

Le immagini saranno registrate nel giornale dei lavori.

Le misure dovrebbero essere salvate nel libretto delle misure, per semplicità saranno salvate solo nel giornale dei lavori.

Considerate le specifiche del progetto, sono state identificate tre componenti fondamentali che devono interagire tra loro: il *direttore dei lavori*, il *drone* e il *servizio di fotogrammetria*, dato che queste entità devono effettuare operazioni più o meno complesse, su risorse disponibili o da acquisire si è deciso di modellarle come attori in modo da delimitare al meglio le loro componenti e gli obbiettivi di ognuno.

Il direttore dei lavori può consultare il giornale dei lavori, ed inserirvi nuovi lavori ovvero misure con relative immagini.

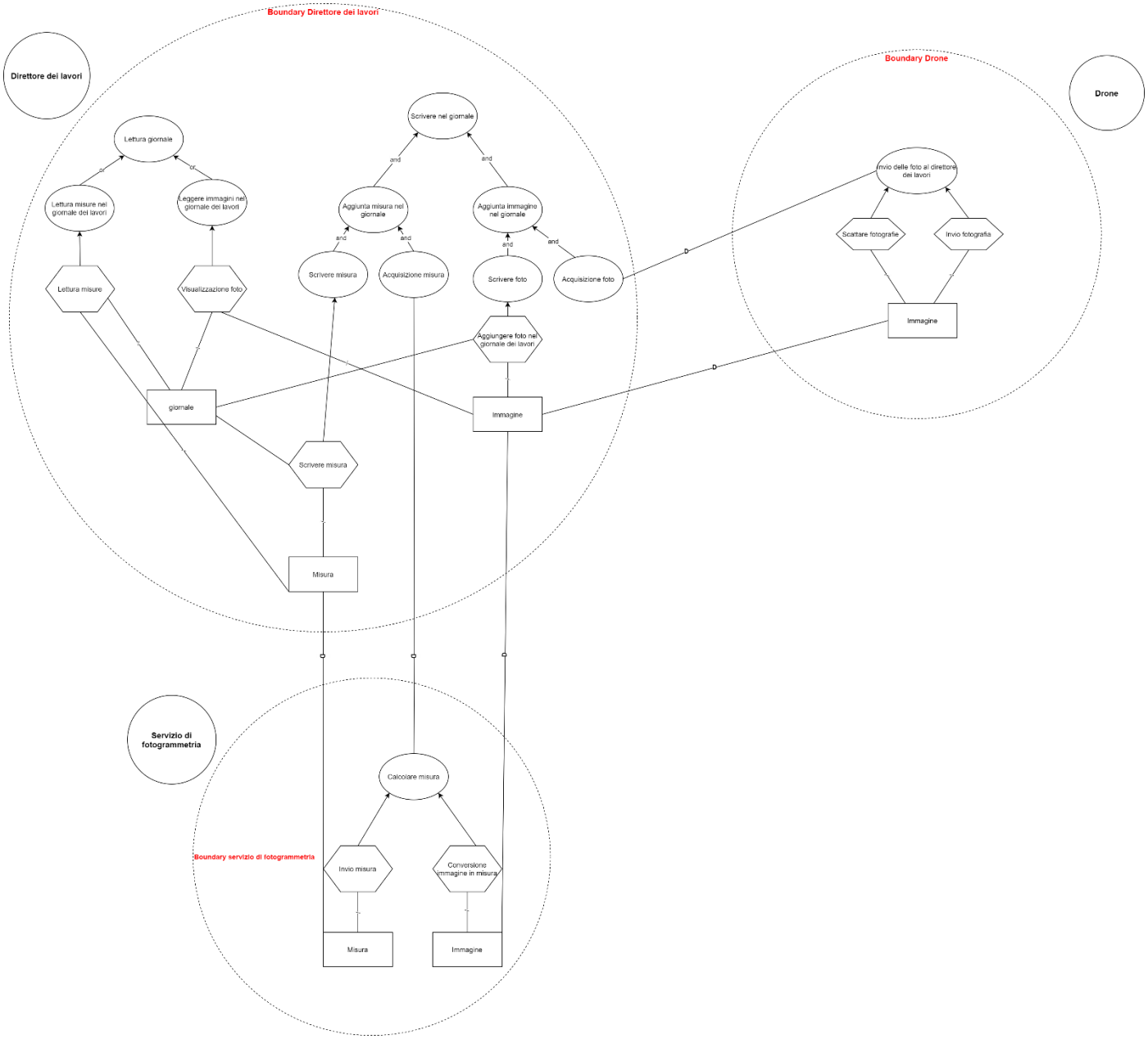
Il servizio di fotogrammetria ha il compito di calcolare una misura a partire da delle immagini.

Il drone ha il compito di scattare fotografie dal cantiere ed inviarle al direttore dei lavori.

Di seguito è riportato il flusso di lavoro per inserire i lavori nel giornale dei lavori:

Il *drone* acquisisce e invio delle immagini al *direttore dei lavori* il quale sarà il responsabile del loro invio al *servizio di fotogrammetria*.

A questo punto il *servizio di fotogrammetria* calcolerà la misura restituendola al *direttore dei lavori*, che avrà il compito di inserirle nel giornale dei lavori in modo da poterle visualizzare e verificare in futuro.


Boundary Direttore dei lavori
Direttore dei lavori
Lettura giornale
Scrivere nel giornale
Lettura misure nel giornale dei lavori
Leggere immagini nel giornale dei lavori
Aggiunta misura nel giornale
Aggiunta immagine nel giornale
Lettura misure
Visualizzazione foto
Scrivere misura
Acquisizione misura
Scrivere foto
Acquisizione foto
Aggiungere foto nel giornale dei lavori
giornale
Immagine
Scrivere misura
Misura
Boundary Drone
Drone
Invio delle foto al direttore dei lavori
Scattare fotografie
Invio fotografia
Immagine
Servizio di fotogrammetria
Calcolare misura
Boundary servizio di fotogrammetria
Invio misura
Conversione immagine in misura
Misura
Immagine

Late requirement analysis - Strategic Dependency Model

Una volta stilato l'early requirement analysis, abbiamo pensato a come far interagire il sistema con gli attori individuati e a come poter dividere in moduli il sistema.

Abbiamo individuato 3 moduli per il sistema, uno per ogni attore***: modulo direttore dei lavori, modulo ricezione foto, servizio di fotogrammetria.***

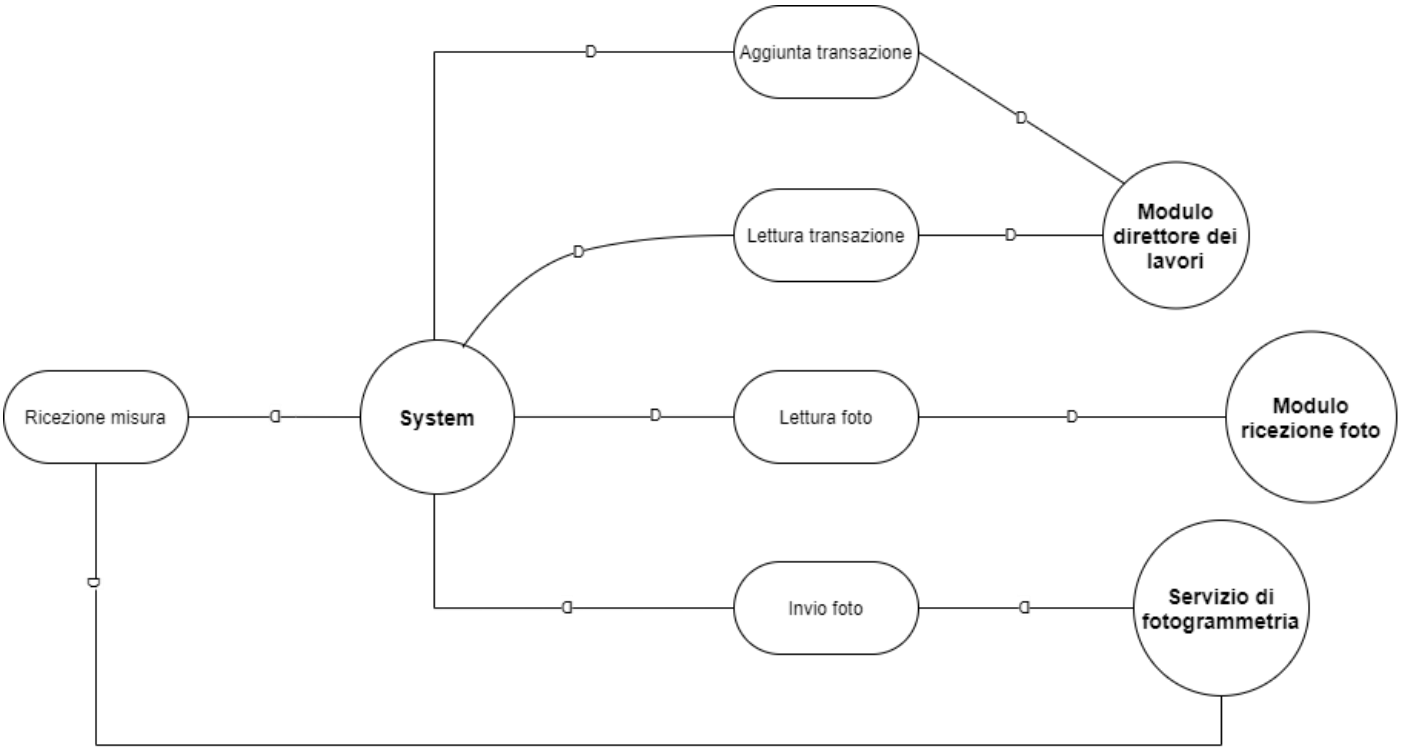
Il primo modulo è realizzato per interagire con il direttore dei lavori e soddisfarne gli obiettivi, quindi leggere e scrivere transazione nella blockchain, ovvero lavori nel giornale dei lavori.

Il modulo ricezione foto si interfaccerà con il drone, appunto per ricevere le foto scattate.

Il modulo servizio di fotogrammetria si interfaccerà con un modulo di fotogrammetria esterno, che ricevendo delle foto in input produrrà le misure di tali fotografie.

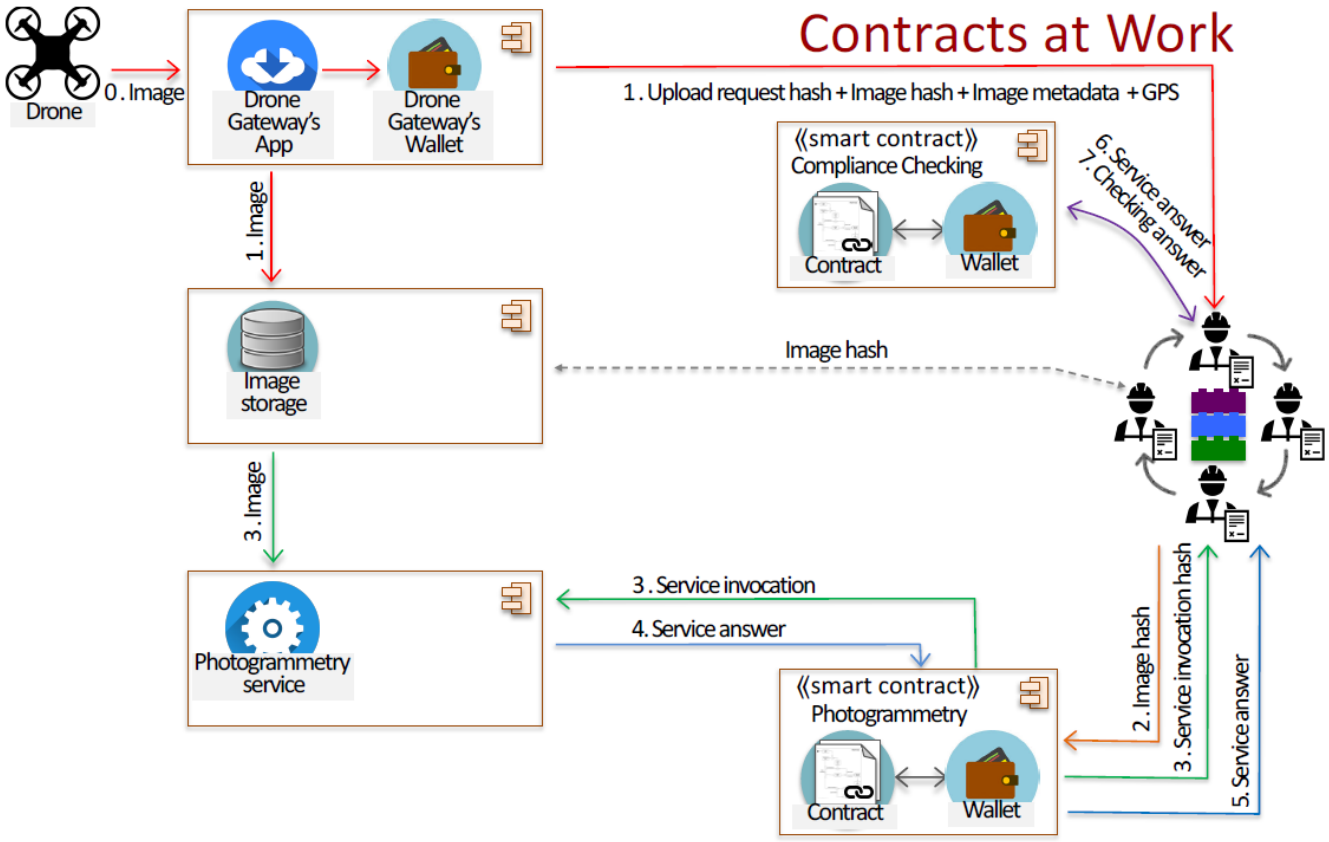
Nel seguente ***strategic dependency model*** sono quindi riportate le dipendenze tra gli obbiettivi e gli attori individuati.

Il sistema, cioè il software prodotto, per funzionare correttamente necessita che tutti gli attori raggiungano pienamente i propri obbiettivi.



Late requirement analysis - Strategic Rationale Model

In questa fase viene stabilito cosa un attore può o non può fare ed è definito il proprio ambito di competenza. Ogni obbiettivo è decomposto nelle sue componenti facendo riferimento alle analisi effettuate nei due capitoli precedenti.



Il *modulo direttore dei lavori,* per poter effettuare una scrittura nel giornale, necessita sia di immagini che di una misura calcolata su di esse, deve quindi interagire con gli altri due moduli.

In particolare, il *modulo ricezione foto* ha il compito di fornire al sistema le immagini acquisite.

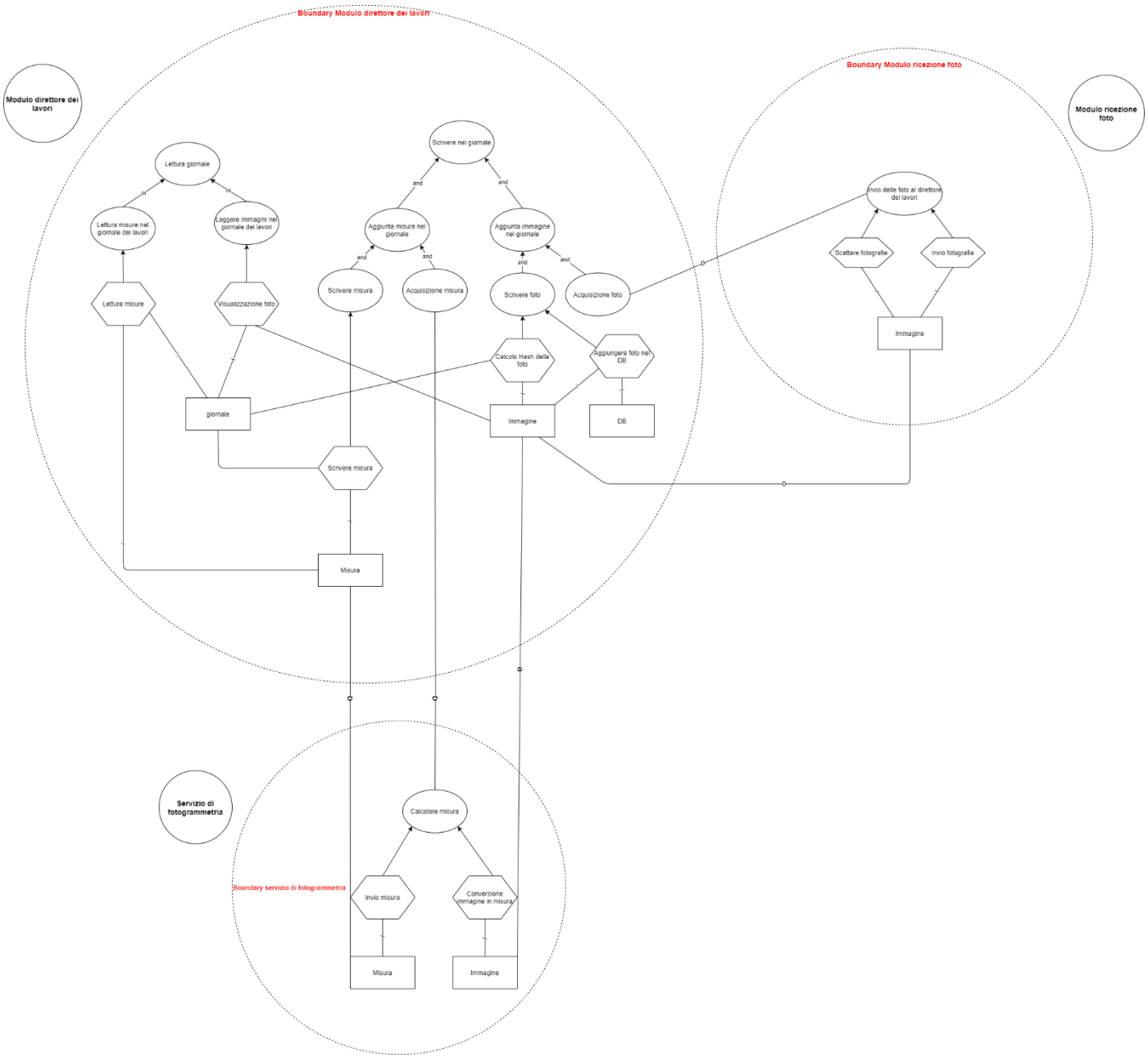
Quando il sistema possiederà un numero sufficiente di foto, che intanto saranno salvate nel server host, il *modulo direttore dei lavori* invocherà il modulo *servizio di fotogrammetria* che, ottenendo delle immagini, restituirà la misura corrispondente.

Appena il sistema otterrà tale misura sarà possibile scrivere nel giornale dei lavori, in particolare essendo sconveniente salvare immagini e misure nella blockchain saranno estratti i metadati dalle immagini e dalle misure, saranno calcolati gli hash di tali dati ed il tutto verrà aggiunto nella blockchain.

Quindi le immagini e le misure saranno salvate nel server host, i metadati nel database e la blockchain servirà per accedere a tali dati e verificare che siano corretti, confrontando i metadati e gli hash salvati nella blockchain con quelli nel sistema.

Tutte le scritture effettuate nel giornale possono essere consultate, inoltre possono essere visualizzate anche le immagini in possesso al direttore dei lavori sulle quali ancora non è stata calcolata alcuna misura.

Dato che alcune immagini ricevute dal drone potrebbero essere non necessarie o scorrette il direttore avrà la possibilità di visualizzare ed eventualmente eliminare quelle che non soddisfano i requisiti prima che vengano calcolate le misure e salvate nel giornale dei lavori.



Use cases

Il software risulterà quasi interamente automatizzato, l'utente in grado di accedervi e di utilizzarlo sarà il *direttore dei lavori* che avrà la possibilità di inserire e visualizzare i dati relativi al giornale dei lavori.

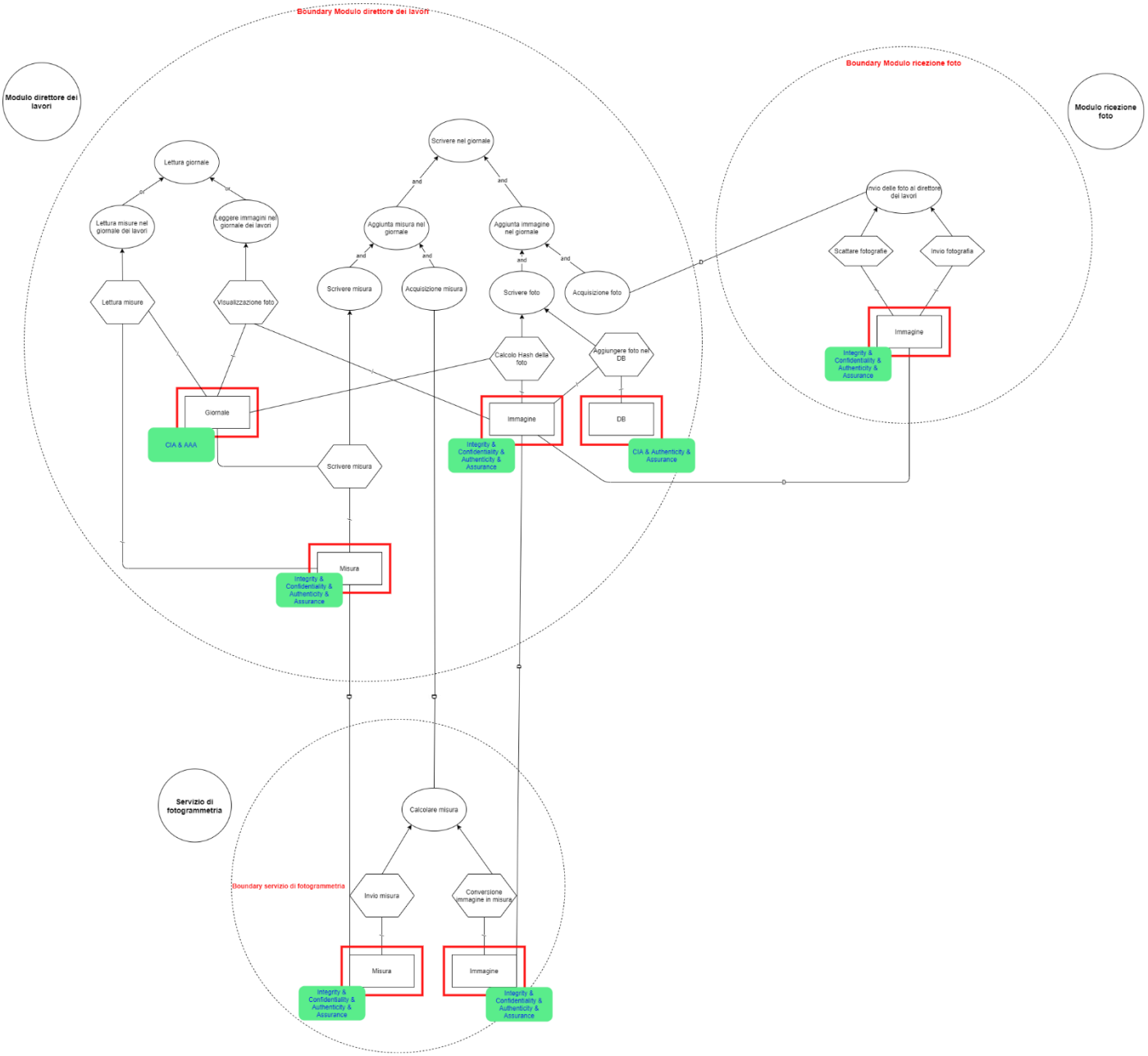
Use case ID: UC-01 Use case Name: Inserimento dati nel giornale dei lavori	
Actors	Modulo direttore dei lavori, Servizio di Fotogrammetria, Modulo ricezione foto.
Description	Il direttore dei lavori vuole scrivere nel giornale dei lavori.
Data	L'immagine è ottenuta dal modulo ricezione foto e le misure vengono calcolate dal servizio di fotogrammetria esterno.
Stimulus and Preconditions	La foto è scattata da un drone ed i calcoli per ricavare le misure vengono eseguiti da un servizio di fotogrammetria esterno, supponiamo che non ci siano errori o modifiche su questi dati e che arrivino integri.
Basic Flow	1. Il modulo di ricezione foto invia la foto al Modulo direttore dei lavori. 2. Il Modulo direttore dei lavori invia la foto al servizio di fotogrammetria esterno, calcola l'hash della foto e ne estrae i metadati salvando la foto in un database. 3. Il Modulo direttore dei lavori riceve le misure dal servizio di fotogrammetria esterno ne estrae i metadati, calcola l'hash e aggiunge tali informazioni, insieme a quelle delle relative immagini, sulla blockchain che è il giornale dei lavori.
Alternative Flow	Il direttore dei lavori può eliminare qualche fotografia ricevuta dal drone se non soddisfa i requisiti, prima di inviarla al servizio di fotogrammetria.
Exception Flow	1. Il modulo di ricezione foto invia la foto al Modulo direttore dei lavori. 2. Il Modulo direttore dei lavori invia la foto al servizio di fotogrammetria esterno, calcola l'hash della foto e ne estrae i metadati salvando la foto in un database. 3. Il Modulo direttore dei lavori non riceve lemisure dal servizio di fotogrammetria. Non è momentaneamente possibile l'aggiunta della transazione nella blockchain
Response and Postconditions	Conferma che i dati sono stati ricevuti ed aggiunti al giornale correttamente.
Non Functional Requirements	Confidenzialità, Integrità ed autenticità delle immagini e delle misure, non ripudio dell'autore delle foto e delle misure, disponibilità ed affidabilità del giornale dei lavori e del database
Comments	I dati non devono essere corrotti o errati.

Use case ID: UC-02 Use case Name: Consultazione giornale dei lavori	
Actors	Modulo direttore dei lavori.
Description	Il direttore dei lavori vuole consultare il giornale dei lavori.
Data	Immagini nel database e misure salvate nel giornale dei lavori.
Stimulus and Preconditions	La foto è scattata da un drone ed i calcoli per ricavare le misure vengono eseguiti da un servizio di fotogrammetria esterno, supponiamo che non ci siano errori o modifiche su questi dati ma che arrivino integri.
Basic Flow	1. Il direttore dei lavori accede al Modulo direttore dei lavori 2. Il Modulo direttore dei lavori permette la visualizzazione del giornale dei lavori 3. Il direttore dei lavori consulta il giornale dei lavori 4. Visualizza le immagini e le relative misure salvate nel giornale dei lavori
Alternative Flow	
Exception Flow	1. Il direttore dei lavori accede al Modulo direttore dei lavori 2. Il Modulo direttore dei lavori permette la visualizzazione del giornale dei lavori 3. Il giornale dei lavori non è raggiungibile 4. Il direttore dei lavori non può momentaneamente consultare il giornale dei lavori
Response and Postconditions	Conferma che i dati sono stati ricevuti ed aggiunti al giornale correttamente.
Non Functional Requirements	Confidenzialità, Integrità ed autenticità delle immagini e delle misure, non ripudio dell'autore delle foto e delle misure, disponibilità ed affidabilità del giornale dei lavori e del database
Comments	I dati non devono essere corrotti o errati.

Identificazione asset

In questa fase sono identificate le minacce e le vulnerabilità delle risorse utilizzate. Sono stati identificati quattro assets: *Immagine*, *Misure*, *Database* e *Giornale*. Nel seguente diagramma si può vedere l'interazione tra i diversi asset tramite il flusso di lavoro dei diversi moduli e servizi del progetto.

Per ogni asset sono stati individuati degli obiettivi di sicurezza e dependability che devono soddisfare rappresentati come soft goal in i star.



Valutazione degli asset e degli impatti

Di seguito sono valutati gli asset ed i relativi impatti in una scala Likert tra 1 e 7, dove 1 corrisponde al valore minimo e 7 al valore massimo. Dato che le misure vengono calcolate a partire dalle immagini, possono essere ricavate da esse anche in caso di eliminazione o di modifica, per questo le immagini hanno un valore ed un impatto più alto rispetto alle misure.

Il giornale dei lavori è l'asset che ha più valore e più impatto essendo il fulcro del progetto, ad esempio se non fosse disponibile sarebbe inutile accedere all'applicativo web.

Asset	Value	Exposure (Impact)
Giornale	7. Necessario a monitorare lo stato dei lavori. Potenzialmente critico.	7. Perdità di integità. Invalidazione di tutti i lavori. Perdita di disponibilità.Necessario dover salvare di nuovo immagini e misure nel giornale
Misure	5. Necessario per consultazione giornale.	5. Perdità di integrità. Necessario ricalcolo delle misure. Dati corrotti nel giornale.
Immagine	6. Necessario per calcolare le misure. Necessario per consultazione giornale. Potenzialmente critico.	6. Perdita di integrità. Non poter calcolare correttamente le misure. Dati corrotti nel giornale. Nuova immagine necessaria.
Database	6. Necessario per salvare le immagini. Potenzialmente critico.	6. Perdita di affidabilità. Non poter controllare l'integrità dei dati dentro il giornale.

Identificazione delle minacce

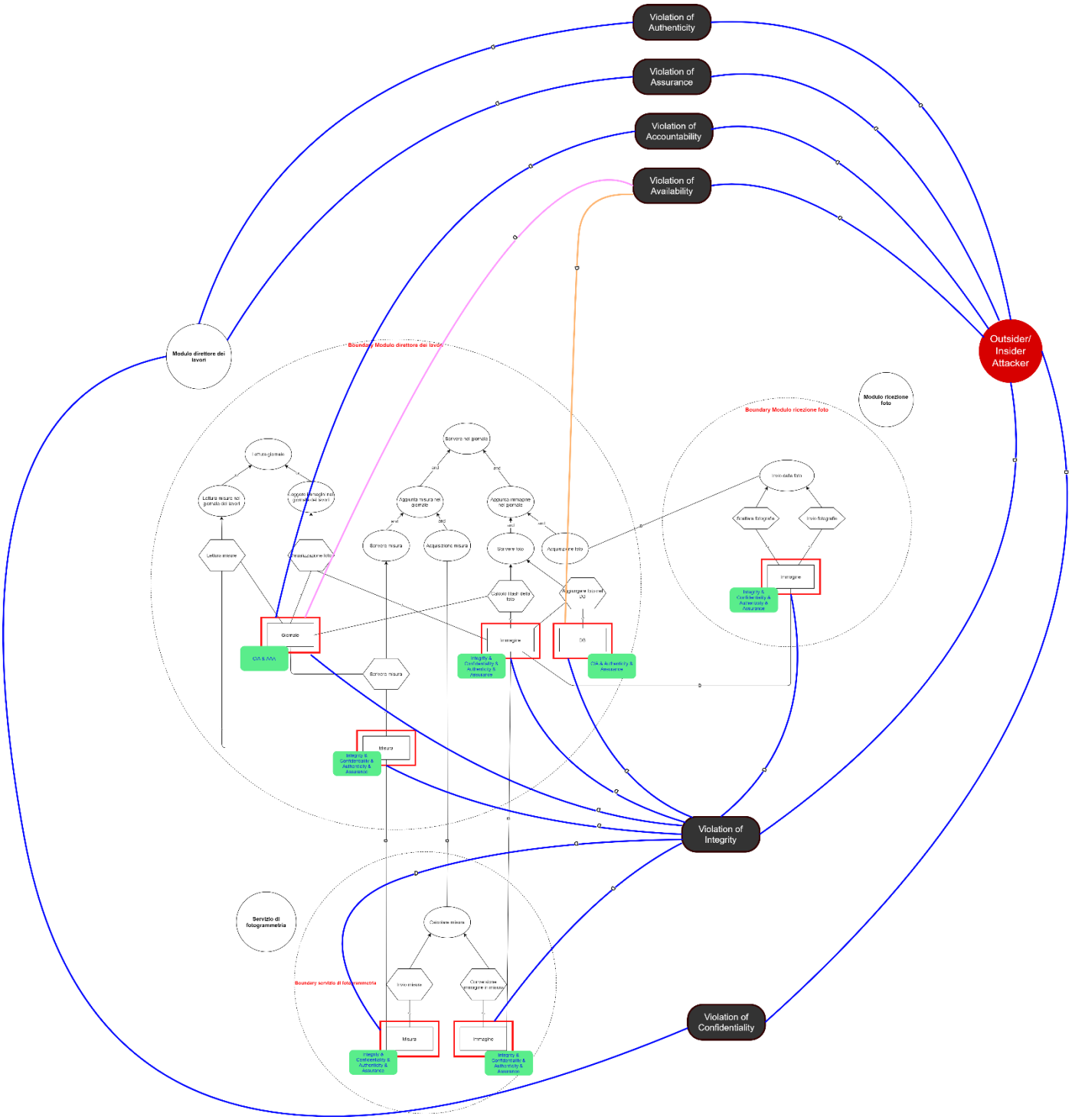
Nella seguente tabella, vengono identificati i tipi di minacce possibili per ognuno degli asset.

L'asset misure è l'unico ad avere una possibile minaccia Danger, perché alterare le misure potrebbe portare anche ad avere costruzioni non a norma e quindi a rischio per gli inquilini.

Asset	Spoofing	Tampering	Repudation	Information Disclusure	Dos	Elevation of privilege	Danger	Unreliability	Absence of Resilience
Giornale	X	X	X	X	X	X		X	X
Misure	X	X	X	X			X	X	
Immagine	X	X	X	X				X	
Database	X	X		X	X			X	X

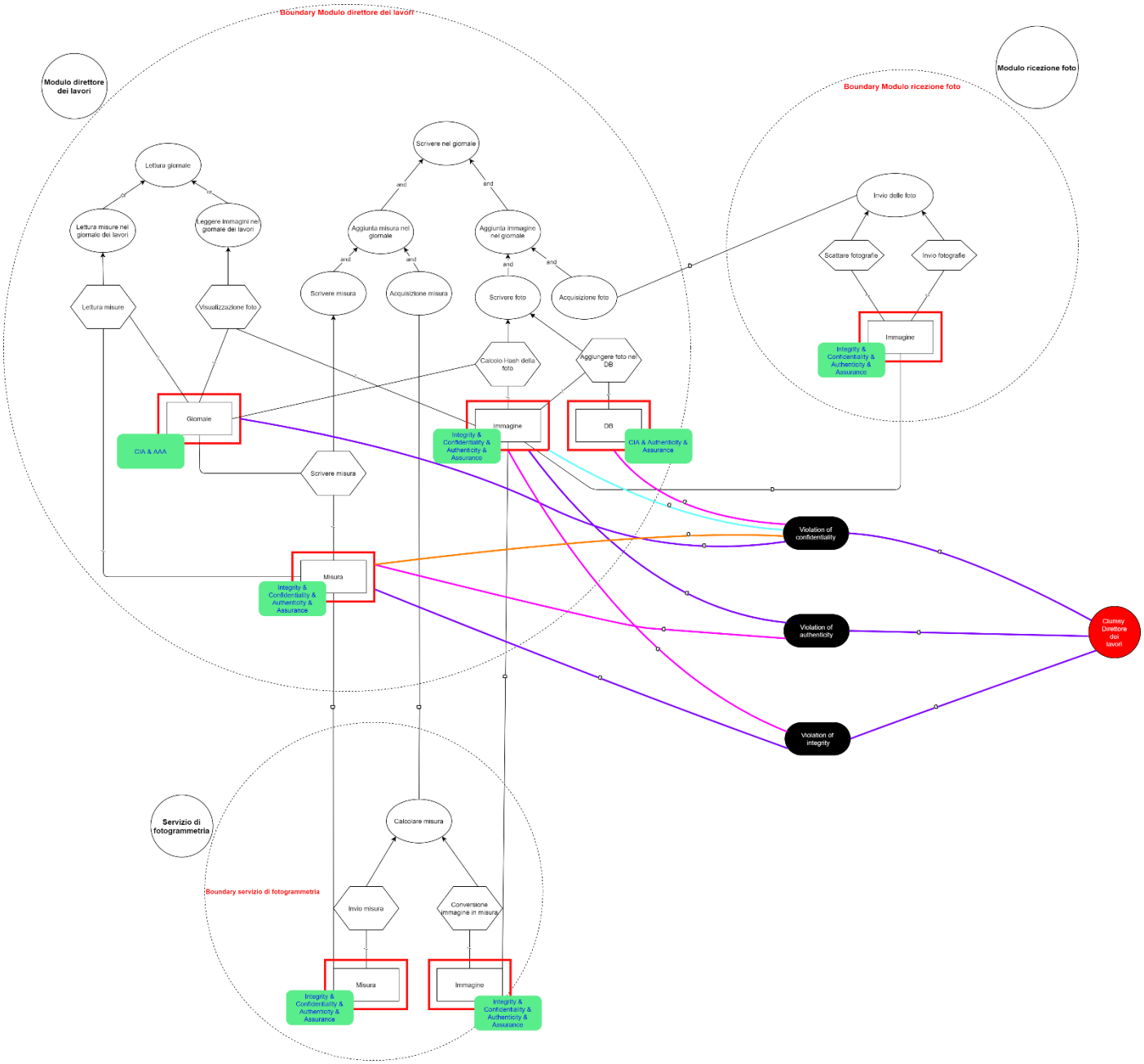
Abuse cases

In questa fase sono state analizzate le possibili violazioni di sicurezza che un attaccante esterno, ma anche interno, può effettuare nel sistema in particolare relativi agli asset individuati in precedenza.



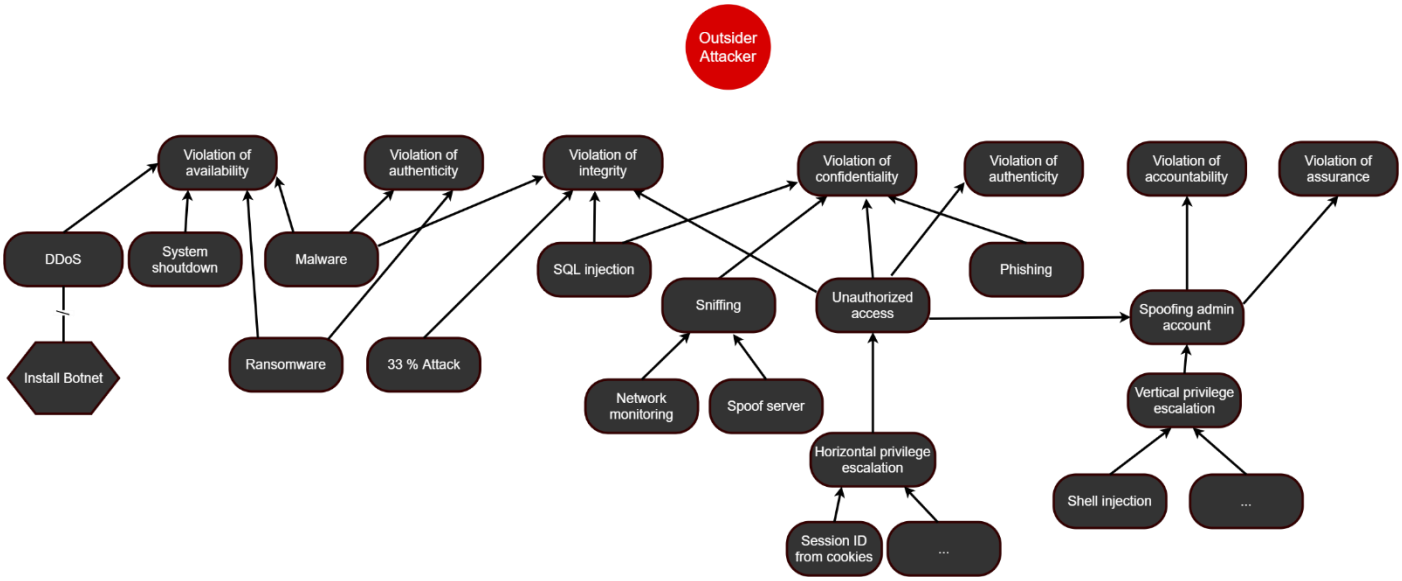
Misuse cases

In questa fase sono state analizzate le possibili violazioni di sicurezza che un direttore dei lavori inesperto o sbadato può recare al sistema, in particolare agli asset identificati.



Outsider attack tree

Viene qui rappresentato l'attack tree riferito all'outsider attacker.



Abuse case specification - Outsider attacker

Nelle seguenti tabelle sono descritti i possibili attacchi riferiti all' outsider attacker e le mitigazioni decise seguendo l'analisi del rischio riportata successivamente.

Use case ID: AT-01-01 Use case Name: System shutdown	
Actors	Modulo direttore dei lavori, Outsider Attacker.
Description	L'attaccante esterno può fare lo shutdown del sistema.
Data (asset)	Giornale dei lavori, DB.
Stimulus and Preconditions	C'è una falla nel sistema che permette all'attaccante esterno di fare injection di comandi rendendo il sistema non disponibile.
Attack 1 Flow	L'attaccante trova una vulnerabilità critica nel sistema, e la sfrutta per eseguire i comandi che rendono offline il sistema.
Attack 2 Flow	
Response and Postconditions	
Mitigations	I sistemi devono essere aggiornati per rendere il sistema meno vulnerabile.
Non Functional Requirements	I sistemi devono essere aggiornati per rendere il sistema meno vulnerabile.

Use case ID: AT-01-02 Use case Name: Sniffing	
Actors	Modulo direttore dei lavori, Outsider Attacker.
Description	L'attaccante esterno intercetta i dati in una transazione e li copia.
Data (asset)	Giornale dei lavori, misure, immagini, DB.
Stimulus and Preconditions	Le immagini sono inviate al servizio di fotogrammetria, la connessione non è cifrata.
Attack 1 Flow	L'invio delle immagini non è criptato, quindi sniffando il traffico di rete è possibile intercettare i dati.
Attack 2 Flow	Si installa un server spoof tra il servizio di fotogrammetria e il direttore dei lavori, fingendo essere il reale,intercettando immagini e misure.
Attack 3 Flow	La connessione con i nodi della blockchain non è criptata, viene intercettato il giornale dei lavori
Response and Postconditions	
Mitigations	Encryption.
Non Functional Requirements	Tutte le comunicazioni tra il servizio di fotogrammetria e il direttore dei lavori deve usare il servizio di SSL. I protocolli di https devono usare certificati di autenticazione ed encryption.

Use case ID: AT-01-03 Use case Name: Unauthorized access	
Actors	Modulo direttore dei lavori, Outsider Attacker.
Description	L'attaccante esterno riesce ad accedere al sistema e svolge delle azioni non autorizzate.
Data (asset)	Giornale dei lavori, misure, immagini, DB.
Stimulus and Preconditions	L'attaccante prende le credenziali di un utente sfruttando i cookie della sessione.
Attack 1 Flow	L'attaccante entra come un utente e modifica i dati sul DB.
Attack 2 Flow	L'account di un utente viene usato dall'attaccante per vedere informazioni interne.
Attack 3 Flow	L'attaccante immette false immagini e misure nel giornale dei lavori
Response and Postconditions	
Mitigations	2FA.
Non Functional Requirements	2FA.

Use case ID: AT-01-04 Use case Name: Spoofing admin account	
Actors	Modulo direttore dei lavori, Outsider Attacker.
Description	L'attaccante esterno ruba i dati di accesso dell'amministratore.
Data (asset)	Giornale dei lavori, DB.
Stimulus and Preconditions	L'amministratore è stato ingannato da uno spoof server ed ha ceduto i propri dati di accesso.
Attack 1 Flow	Come amministratore l'attaccante realizza decisioni che alterano il DB in maniera impropria
Attack 2 Flow	Come amministratore l'attaccante realizza decisioni che alterano il giornale dei lavori in maniera impropria, ad esempio aggiungendo transazioni false.
Response and Postconditions	
Mitigations	2FA, ACL
Non Functional Requirements	2FA, ACL implementata in base ai ruoli.

Use case ID: AT-01-05 Use case Name: DDos	
Actors	Modulo direttore dei lavori, Outsider Attacker.
Description	Un attaccante esterno vuole rendere irraggiungibile il giornale dei lavori.
Data (asset)	Giornale dei lavori.
Stimulus and Preconditions	Non è possibile attaccare direttamente la blockchain.
Attack 1 Flow	Un attaccante esterno crea una botnet con la quale effettua un attacco DDoS sul server host del giornale dei lavori.
Attack 2 Flow	
Response and Postconditions	
Mitigations	Captcha.
Non Functional Requirements	Sovrastimare le risorse hardware, captcha, distribuzione, diversità

Use case ID: AT-01-06 Use case Name: 33% Attack	
Actors	Modulo direttore dei lavori, Outsider Attacker.
Description	Un outsider attacker è in grado di apportare modifiche alla blockchain prendendo il possesso di più del 33% dei nodi calcolatori.
Data (asset)	Giornale dei lavori.
Stimulus and Preconditions	Uso di Quorum.
Attack 1 Flow	L'outsider attacker sfruttando vulnerabilità nei nodi calcolatori ne prende il possesso e può modificare la blockchain.
Attack 2 Flow	
Response and Postconditions	
Mitigations	Controllo sulla concessione dei validatori.
Non Functional Requirements	High-availability designs.

Use case ID: AT-01-07 Use case Name: Malware	
Actors	Modulo direttore dei lavori, Outsider Attacker.
Description	I dispositivi del direttore dei lavori sono infettati da malware.
Data (asset)	Giornale dei lavori, misure, immagini, DB.
Stimulus and Preconditions	Dispositivi non adeguatamente protetti.
Attack 1 Flow	Il malware è in grado di rubare e distribuire informazioni riservate.
Attack 2 Flow	Il malware è in grado di modificare dati come immagini e misure
Response and Postconditions	
Mitigations	Antivirus.
Non Functional Requirements	Antivirus.

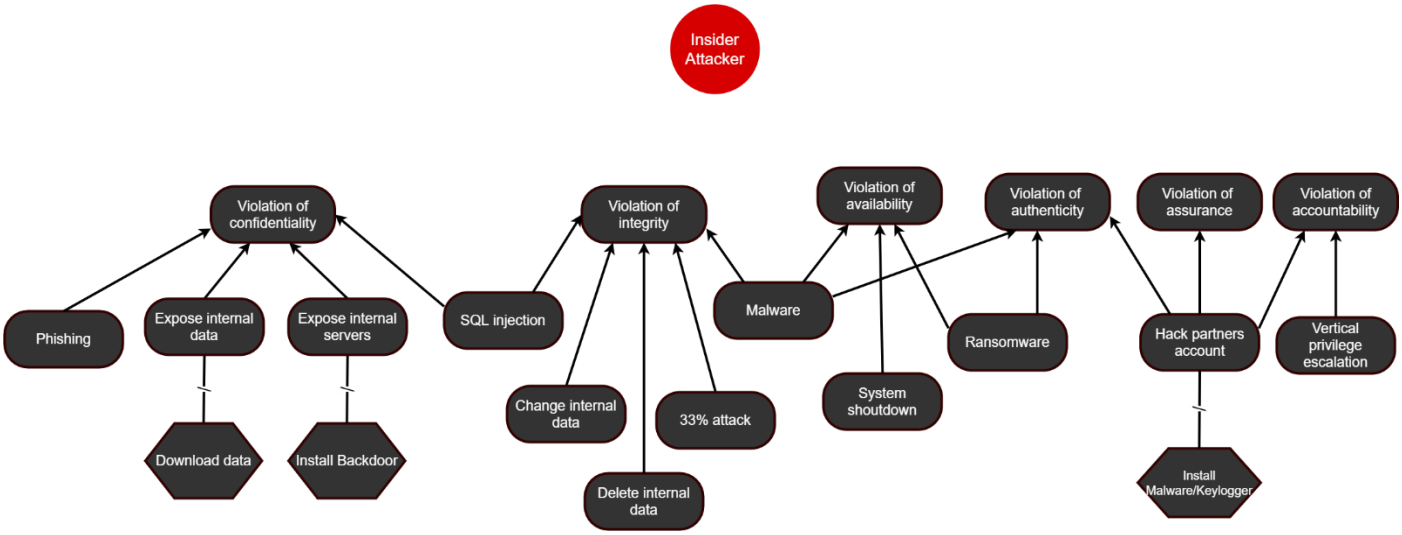
Use case ID: AT-01-08 Use case Name: Ransomware	
Actors	Modulo direttore dei lavori, Outsider Attacker.
Description	Un ransomware infetta il sistema
Data (asset)	Giornale dei lavori, misure, immagini, DB.
Stimulus and Preconditions	Dispositivi non adeguatamente protetti.
Attack 1 Flow	Il ransomware infetta i dispositivi e ne limita l'utilizzo criptando i dati.
Attack 2 Flow	
Response and Postconditions	
Mitigations	Log.
Non Functional Requirements	Log, miroring, distribuzione, diversità

Use case ID: AT-01-09 Use case Name: Phishing	
Actors	Modulo direttore dei lavori, Outsider Attacker.
Description	Truffa effettuata su internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.
Data (asset)	Giornale dei lavori, misure, immagini, DB.
Stimulus and Preconditions	Non adeguata informazione sulle truffe di phishing.
Attack 1 Flow	Il malintenzionato contatta il direttore dei lavori con una comunicazione falsa che lo invita a comunicare le credenziali d'accesso.
Attack 2 Flow	C'è un malware nell'email tramite cui viene infettato il sistema
Response and Postconditions	
Mitigations	Formazione ai dipendenti.
Non Functional Requirements	Adeguata informazione sulle truffe di phishing.

Use case ID: AT-01-10 Use case Name: SQL Injection	
Actors	Modulo direttore dei lavori, Outsider Attacker.
Description	Iniezione di codice sql tramite un form dell'applicazione web volto a modificare dati nel DB o a leggerne il contenuto.
Data (asset)	DB.
Stimulus and Preconditions	Applicazione web non resiliente ad attacchi sql injection
Attack 1 Flow	L'attaccante invia del codice sql tramite un form web per leggere le informazioni presenti nel database
Attack 2 Flow	L'attaccante invia del codice sql tramite un form web peralterare le informazioni presenti nel database
Response and Postconditions	
Mitigations	Rendere l'applicativo resiliente ad attacchi sql injection
Non Functional Requirements	Rendere l'applicativo resiliente ad attacchi sql injection

Insider attack tree

Viene qui rappresentato attack tree relativo ad un attaccante interno.



Abuse case specification - Insider attacker

Nelle seguenti tabelle sono rappresentati i possibili attacchi riferiti all'insider attacker e le mitigazioni scelte in base all'analisi del rischio riportata successivamente.

Use case ID: AT-02-01 Use case Name: Expose internal data	
Actors	Modulo direttore dei lavori, Insider Attacker.
Description	L'attaccante interno può esporre i dati aziendali all'esterno dell'azienda e quindi renderli pubblici.
Data (asset)	Giornale dei lavori, misure, immagini.
Stimulus and Preconditions	I dati sono già presenti nel sito che gestisce la blockchain.
Attack 1 Flow	Il dipendente o il direttore dei lavori si collega con il proprio account al sito per gestire il giornale dei lavori, scarica i dati e li pubblica online.
Attack 2 Flow	Il dipendente o il direttore dei lavori si collega con il proprio account al sito per gestire il giornale dei lavori, salva i dati e successivamente li rende disponibili ad esterni.
Response and Postconditions	
Mitigations	Non permettere il download dei dati.
Non Functional Requirements	Non permettere il download dei dati.

Use case ID: AT-02-02 Use case Name: Expose internal server	
Actors	Modulo direttore dei lavori, Insider Attacker.
Description	L'attaccante interno può esporre i server aziendali all'esterno rendendoli vulnerabili ad attacchi.
Data (asset)	Giornale dei lavori, misure, immagini, DB.
Stimulus and Preconditions	I dati sono già presenti nel sito che gestisce la blockchain e quindi nei server aziendali.
Attack 1 Flow	Il dipendente o il direttore dei lavori può installare delle backdoor sui server aziendali usando dei trojan o altri malware esponendo a minacce, data breach ed esecuzione remota questi ultimi.
Attack 2 Flow	
Response and Postconditions	
Mitigations	Log.
Non Functional Requirements	Log.

Use case ID: AT-02-03 Use case Name: Change internal data	
Actors	Modulo direttore dei lavori, Insider Attacker.
Description	L'attaccante interno può modificare i dati nel giornale dei lavori, prima che siano scritti nella blockchain, o può modificare l'immagine sul database a cui si riferisce un singolo blocco della blockchain.
Data (asset)	Giornale dei lavori, Misure, immagini, DB.
Stimulus and Preconditions	I dati sono già presenti nel sito che gestisce la blockchain e non ci sono duplicati.
Attack 1 Flow	Il dipendente o il direttore dei lavori può modificare le misure prima che siano inserite all'interno della blockchain ad esempio manomettendo il servizio di fotogrammetria, sfruttando vulnerabilità nel codice del Modulo direttore dei lavori modificando la foto nel database, in modo tale che l'hash sarà calcolato sulla foto modificata.
Attack 2 Flow	Il dipendente o il direttore dei lavori può modificare le foto all'interno del database, anche se l'hash è già stato calcolato ed è già presente nella blockchain del blocco relativo. Quindi si avrà una situazione in cui avendo l'hash salvato nella blockchain si sa che la foto salvata nel database non è l'originale ma senza poter risalire a quella originale.
Response and Postconditions	
Mitigations	Log.
Non Functional Requirements	Log, mantenere i sistemi aggiornati, distribuzione

Use case ID: AT-02-04 Use case Name: Delete internal data	
Actors	Modulo direttore dei lavori, Servizio di fotogrammetria, Insider Attacker.
Description	Le misure ricevute dal servizio di fotogrammetria e le immagini prese dall'api possono essere cancellate da un insider attacker.
Data (asset)	Giornale dei lavori, Misura, immagine, DB.
Stimulus and Preconditions	Le immagini e le misure non sono replicate.
Attack 1 Flow	Il dipendente o il direttore dei lavori cancella alcune foto, già presenti nella blockchain, dal database.
Attack 2 Flow	l dipendente o il direttore dei lavori cancella alcune foto o misure prima che siano inserite nella blockchain e salvate nel DB.
Response and Postconditions	
Mitigations	Log.
Non Functional Requirements	Log, mantenere i sistemi aggiornati, distribuzione

Use case ID: AT-02-05 Use case Name: Hack partners account	
Actors	Modulo direttore dei lavori, Insider Attacker.
Description	Un insider attacker accede all'account di un collega.
Data (asset)	Giornale dei lavori, Misura, Immagine, DB.
Stimulus and Preconditions	Un utente con privilegi non custodisce le credenziali o sono deboli, le lascia in buona vista o accede su uno spoof server creato dall'insider attacker.
Attack 1 Flow	Un insider attacker accede ad un account di un collega ricavando le sue credenziali e attua delle operazioni.
Attack 2 Flow	
Response and Postconditions	
Mitigations	Controllo robustezza password.
Non Functional Requirements	Aggiungere un sistema di controllo delle password in fase di registrazione, formazione del personale.

Use case ID: AT-02-06 Use case Name: System shutdown	
Actors	Modulo direttore dei lavori, Insider Attacker.
Description	L'attaccante interno può fare lo shutdown del sistema.
Data (asset)	Giornale dei lavori, DB, immagini.
Stimulus and Preconditions	L'attaccante interno accede al hardware del sistema.
Attack 1 Flow	L'attaccante invia un comando di shoutdown al sistema.
Attack 2 Flow	
Response and Postconditions	
Mitigations	I sistemi devono essere aggiornati per rendere il sistema meno vulnerabile.
Non Functional Requirements	Controllare I nuovi aggiornamenti disponibili dei sistemi operativi, tenendo conto i cambiamenti dei nuovi aggiornamenti.

Use case ID: AT-02-07 Use case Name: 33% Attack	
Actors	Modulo direttore dei lavori, Insider Attacker.
Description	Un outsider attacker è in grado di apportare modifiche alla blockchain prendendo il possesso di più del 33% dei nodi calcolatori.
Data (asset)	Giornale.
Stimulus and Preconditions	Uso di Quorum.
Attack 1 Flow	L'insider attacker sfruttando vulnerabilità nei nodi calcolatori ne prende il possesso e può modificare la blockchain.
Attack 2 Flow	
Response and Postconditions	
Mitigations	Controllo sulla concessione dei validatori.
Non Functional Requirements	High-availability designs.

Use case ID: AT-02-08 Use case Name: Malware	
Actors	Modulo direttore dei lavori, Insider Attacker.
Description	I dispositivi del direttore dei lavori sono infettati da malware.
Data (asset)	Giornale dei lavori, misure, immagini, DB.
Stimulus and Preconditions	Dispositivi non adeguatamente protetti.
Attack 1 Flow	Il malware è in grado di rubare e distribuire informazioni riservate.
Attack 2 Flow	Il malware è in grado di modificare dati come immagini e misure
Response and Postconditions	
Mitigations	Antivirus.
Non Functional Requirements	Antivirus.

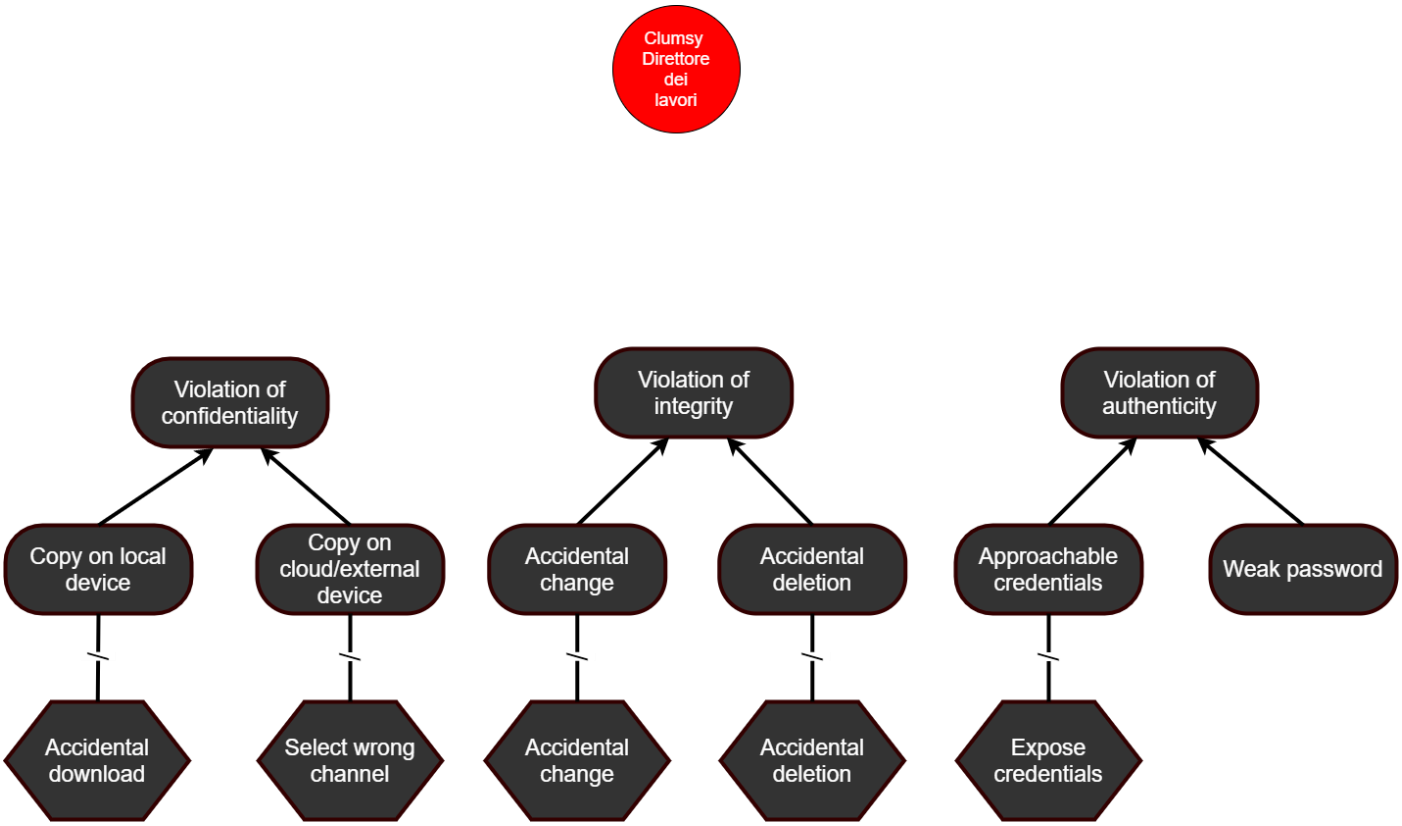
Use case ID: AT-02-09 Use case Name: Ransomware	
Actors	Modulo direttore dei lavori, Insiderr Attacker.
Description	Un ransomware infetta il sistema
Data (asset)	Giornale dei lavori, misure, immagini, DB.
Stimulus and Preconditions	Dispositivi non adeguatamente protetti.
Attack 1 Flow	Il ransomware infetta i dispositivi e ne limita l'utilizzo criptando i dati.
Attack 2 Flow	
Response and Postconditions	
Mitigations	Log.
Non Functional Requirements	Log, miroring, distribuzione, diversità

Use case ID: AT-02-10 Use case Name: Phishing	
Actors	Modulo direttore dei lavori,Insider Attacker.
Description	Truffa effettuata su internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.
Data (asset)	Giornale dei lavori, misure, immagini, DB.
Stimulus and Preconditions	Non adeguata informazione sulle truffe di phishing.
Attack 1 Flow	Il malintenzionato contatta il direttore dei lavori con una comunicazione falsa che lo invita a comunicare le credenziali d'accesso.
Attack 2 Flow	C'è un malware nell'email tramite cui viene infettato il sistema
Response and Postconditions	
Mitigations	Formazione ai dipendenti.
Non Functional Requirements	Adeguata informazione sulle truffe di phishing.

Use case ID: AT-02-11 Use case Name: SQL Injection	
Actors	Modulo direttore dei lavori, Insider Attacker.
Description	Iniezione di codice sql tramite un form dell'applicazione web volto a modificare dati nel DB o a leggerne il contenuto.
Data (asset)	DB.
Stimulus and Preconditions	Applicazione web non resiliente ad attacchi sql injection
Attack 1 Flow	L'attaccante invia del codice sql tramite un form web per leggere le informazioni presenti nel database
Attack 2 Flow	L'attaccante invia del codice sql tramite un form web peralterare le informazioni presenti nel database
Response and Postconditions	
Mitigations	Rendere l'applicativo resiliente ad attacchi sql injection
Non Functional Requirements	Rendere l'applicativo resiliente ad attacchi sql injection

Misuse attack tree

Di seguito è rappresentato l'attack tree relativo ad un direttore dei lavori maldestro.



Misuse case specification

Nelle seguenti tabelle sono rappresentati i possibili attacchi riferiti ad un direttore dei lavori maldestro, e le mitigazioni scelte in base all'analisi del rischio.

Use case ID: AT-03-01 Use case Name: Copy on local device	
Actors	Modulo direttore dei lavori, Clusmy direttore dei lavori.
Description	Il direttore dei lavori scarica dati presenti nel giornale dei lavori.
Data (asset)	Misure, immagini.
Stimulus and Preconditions	Il direttore dei lavori utilizza un visualizzatore dei dati non autorizzato.
Attack 1 Flow	Il direttore dei lavori effettua il download con tale visualizzatore, i file scaricati vengono intercettati.
Attack 2 Flow	
Response and Postconditions	
Mitigations	Creare un visualizzatore per i file contenuti nel giornale.
Non Functional Requirements	Creare un visualizzatore per i file contenuti nel giornale.

Use case ID: AT-03-02 Use case Name: Copy on cloud/external device	
Actors	Modulo direttore dei lavori, Clusmy direttore dei lavori.
Description	Il direttore dei lavori scarica una copia del giornale e la carica erroneamente in un cloud pubblico o in un hd non autorizzato.
Data (asset)	Misure, immagini.
Stimulus and Preconditions	Il direttore dei lavori utilizza un visualizzatore dei dati non autorizzato.
Attack 1 Flow	Il direttore dei lavori utilizza tale visualizzatore con un computer esterno alla società e scarica i dati aziendali. Il computer utilizzato ha un malware che preleva tali dati.
Attack 2 Flow	Il direttore dei lavori utilizza tale visualizzatore e scarica i dati aziendali. Il computer usato è sincronizzato ad un cloud che preleva i dati, successivamente l'account del cloud viene hackerato.
Response and Postconditions	
Mitigations	Creare un visualizzatore per i file contenuti nel giornale che consente la condivisione.
Non Functional Requirements	Creare l'impostazione per condividere i file contenuti nel giornale.

Use case ID: AT-03-03 Use case Name: Accidental change	
Actors	Modulo direttore dei lavori, Clusmy direttore dei lavori.
Description	Il direttore dei lavori modifica erroneamente degli assets.
Data (asset)	Misure, immagini.
Stimulus and Preconditions	Il direttore dei lavori è disattento
Attack 1 Flow	Il direttore dei lavori erroneamente cambia degli dei files con degli altri, non è più possibile verificare la validità dei nuovi asset.
Attack 2 Flow	Il direttore dei lavori erroneamente cambia degli asset con degli altri prima che vengono caricati nella blockchain, tali asset risultano attendibili ma incoerenti con la situazione reale.
Response and Postconditions	
Mitigations	Log.
Non Functional Requirements	Aggiungere la tracciabilità di tutte le modifiche effettuate. Ogni modifica consiste in un nuovo inserimento nella blockchain.

Use case ID: AT-03-04 Use case Name: Accidental delete	
Actors	Modulo direttore dei lavori, Clusmy direttore dei lavori.
Description	Il direttore dei lavori elimina erroneamente degli assets.
Data (asset)	Misure, immagini.
Stimulus and Preconditions	Il direttore dei lavori è disattento
Attack 1 Flow	Il direttore dei lavori elimina erroneamente asset, non è più possibile ottenere l'asset associato ad un determinato hash del giornale dei lavori.
Attack 2 Flow	
Response and Postconditions	
Mitigations	Log.
Non Functional Requirements	Aggiungere la tracciabilità di tutte le cancellazioni effettuate.

Use case ID: AT-03-05 Use case Name: Approachable credentials	
Actors	Modulo direttore dei lavori, Clusmy direttore dei lavori.
Description	I dati di autenticazione del direttore dei lavori vengono rubati.
Data (asset)	Giornale dei lavori, immagini, misure.
Stimulus and Preconditions	Il direttore dei lavori ha diffuso le proprie credenziali di accesso.
Attack 1 Flow	Chiunque può accedere al sistema tramite le chiavi di accesso del direttore dei lavori, dopo essersi falsamente autenticati si ha la possibilità di modificare le informazioni nel sistema.
Attack 2 Flow	
Response and Postconditions	
Mitigations	Formazione ai dipendenti.
Non Functional Requirements	Stabilire dei tempi con I dipendenti per instruirli dei rischi e dell'importanza della sicurezza informatica.

Use case ID: AT-03-06 Use case Name: Weak password	
Actors	Modulo direttore dei lavori, Clusmy direttore dei lavori.
Description	La password di autenticazione utilizzata dal direttore dei lavori è debole.
Data (asset)	Giornale dei lavori, immagini, misure.
Stimulus and Preconditions	Non sono state scelte password robuste, un utente malintenzionato ha già il nome utente della vittima.
Attack 1 Flow	Un utente malintenzionato effettua un attacco brute force ed ottiene la password, ora l'utente malintenzionato potrà accedere al sistema fingendo di essere il direttore dei lavori.
Attack 2 Flow	
Response and Postconditions	
Mitigations	Controllo robustezza password.
Non Functional Requirements	Aggiungere un sistema di controllo delle password in fase di registrazione.

Risk Assessment and Mitigation Table

Sono rappresentate in questa sezione le tipologie di attacco per ogni asset, i valori di probabilità, di impatto e di rischio, le possibili modalità di controllo per ogni attacco e il relativo costo, e la fattibilità con relativi valori di impatti, probabilità di attacco e rischio residui per ogni possibile soluzione.

Inoltre, per ogni asset è riportato il rischio totale.

Asset	Spoofing	Tampering	Repudation	Information Disclusure	Dos	Elevation of privilege	Danger	Unreliability	Absence of Resilience	Attack	Probability	Impact	Risk	Control	Cost	Feasibility	Residual attack likelihood / Residual Impact	Residual Risk
Giornale	X				X					System shutdown	2	6	12	- I sistemi devono essere aggiornati per rendere il sistema meno vulnerabile	1	- Tecnicamente fattibile, ma da svolgere periodicamente	1	6
	X			X						Sniffing	5	2	10	- PKI systems such as SSL/TLS and certificates	5	- Tecnicamente fattibile, ma dipendente dalla rete di comunicazione	2	4
														- Encryption	3	- Tecnicamente fattibile, ma la chiave deve essere rinnovata periodicamente	2	4
				X		X				Unauthorized access	5	3	15	- Cookie authentication avanzata	2	- Tecnicamente fattibile ma non è apprezzato da gran parte degli utenti	3	9
														- 2FA	6	- Tecnicamente fattibile ma potrebbe non essere apprezzato dagli utenti	1	3
	X			X				X		Spoofing admin account	4	5	20	- ACL	4	- Tecnicamnete fattibile, ma bisogna assegnare correttamente le risorse ai giusti ruoli	3	15
														- 2FA	6	- Tecnicamente fattibile ma potrebbe non essere apprezzato dagli utenti	1	5
														- Rilevazioni di accessi non autorizzati	5	- Tecnicamente fattibile, ma potrebbe essere complessa l'implementazione	2	10
					X				X	DDoS	4	6	24	- Filtering	4	- Tecnicamente fattibile, ma bisogna impostare bene il filtro	2	12
														- Captcha	1	- Tecnicamente fattibile, ma potrebbe incontrare la resistenza degli utenti	2	12
		X	X							33% Attack	2	7	14	- Controllo sulla concessione dei validatori	1	- Non è un problema del software, ma un problema della organizzazione della blockchain	1	7
				X						Expose internal data	4	1	4	- Non permettere il download dei dati	1	- Tecnicamente fattibile, ma potrebbe essere troppo restittivo	1	1
				X	X				X	Expose internal server	3	2	6	- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	1	3
														- Antivirus	3	- Tecnicamente fattibile, ma deve essere aggiornato frequentemente	1	2

Asset	Spoofing	Tampering	Repudation	Information Disclusure	Dos	Elevation of privilege	Danger	Unreliability	Absence of Resilience	Attack	Probability	Impact	Risk	Control	Cost	Feasibility	Residual attack likelihood / Residual Impact	Residual Risk
Giornale	X			X						Hack partners account	6	3	18	- Formazione ai dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	3	9
														- Controllo robustezza password	2	- Tecnicamente fattibile, alcune password fragili potrebbero non essere rilevate	4	12
														- 2FA	6	- Tecnicamente fattibile ma potrebbe non essere apprezzato dagli utenti	1	3
				X				X		Approachable credentials	5	3	15	- 2FA	6	- Tecnicamente fattibile ma potrebbe non essere apprezzato dagli utenti	1	3
														- Rilevazioni di accessi non autorizzati	5	- Tecnicamente fattibile, ma potrebbe essere complessa l'implementazione	3	9
														- Formazione ai dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	2	6
				X						Weak password	7	3	21	- Formazione ai dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	5	15
														- Controllo robustezza password	2	- Tecnicamente fattibile, alcune password fragili potrebbero non essere rilevate	3	9
		X			X			X	X	Malware	4	6	24	- Antivirus	3	- Tecnicamente fattibile, ma deve essere aggiornato frequentemente	1	6
														- Controllo degli accessi e blocco degli eseguibili in determinate locazioni di memoria	3	- Tecnicamente fattibile, può creare problemi in caso di installazione di aggiornamenti	2	14
					X			X		Ransomware	4	7	28	- Auto Backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	3	12
														- Log	3	- Tecnicamente fattibile, ma da consultare continuamente	4	16
	X			X		X				Phishing	5	4	20	- Formazione ai dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	2	10
														- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	4	12
			X					X		Change internal data	3	6	18	- Auto backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	2	6
														- I sistemi devono essere aggiornati per rendere il sistema meno vulnerabile	1	- Tecnicamente fattibile, ma probabilitàa di errori con versioni precedenti	1	6
			X					X		Delete internal data	3	5	15	- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	4	12
														- Auto backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	2	6
										TOTAL RISK			264/784					

Asset	Spoofing	Tampering	Repudation	Information Disclusure	Dos	Elevation of privilege	Danger	Unreliability	Absence of Resilience	Attack	Probability	Impact	Risk	Control	Cost	Feasibility	Residual attack likelihood / Residual Impact	Residual Risk
Misure	X			X						Sniffing	5	1	5	- PKI systems such as SSL/TLS and certificates	5	- Tecnicamente fattibile, ma dipendente dalla rete di comunicazione	2	2
														- Encryption	3	- Tecnicamente fattibile, ma la chiave deve essere rinnovata periodicamente	2	2
		X	X	X			X	X		Unauthorized access	5	6	30	- Encryption	3	- Tecnicamente fattibile ma non è apprezzato da gran parte degli utenti	3	18
														- 2FA	6	- Tecnicamente fattibile ma potrebbe non essere apprezzato dagli utenti	1	6
				X						Expose internal data	4	2	8	- Non permettere il download dei dati	1	- Tecnicamente fattibile, ma potrebbe essere troppo restittivo	1	2
		X		X				X		Expose internal server	3	6	18	- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	2	6
														- Antivirus	3	- Tecnicamente fattibile, ma deve essere aggiornato frequentemente	1	6
		X		X			X	X		Change internal data	3	6	18	- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	4	12
														- Auto backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	2	6
														- I sistemi devono essere aggiornati per rendere il sistema meno vulnerabile	1	- Tecnicamente fattibile, ma probabilità di errori con versioni precedenti	1	6
		X		X			X	X		Delete internal data	3	5	15	- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	4	12
														- Auto backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	2	6
	X		X	X			X			Hack partners account	6	6	36	- Formazione ai dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	3	18
														- Controllo robustezza password	2	- Tecnicamente fattibile, alcune password fragili potrebbero non essere rilevate	4	24
														- 2FA	6	- Tecnicamente fattibile ma potrebbe non essere apprezzato dagli utenti	1	6
				X						Copy on local device	3	1	3	- Creare un visualizzatore per i file contenuti nel giornale	3	- Tecnicamente fattibile, deve essere reso compatibile su diversi sistemi	1	1

Asset	Spoofing	Tampering	Repudation	Information Disclusure	Dos	Elevation of privilege	Danger	Unreliability	Absence of Resilience	Attack	Probability	Impact	Risk	Control	Cost	Feasibility	Residual attack likelihood / Residual Impact	Residual Risk
Misure				X						Copy on cloud/external device	2	2	4	- Creare un visualizzatore per i file contenuti nel giornale che consente la condivisione	3	- Tecnicamente fattibile, ma aumenta la probabilità di intercept, deve essere periodicamente aggiornato	1	2
		X					X	X		Accidental change	5	5	25	- Hash	3	- Tecnicamente fattibile, ma consumo della memoria periodicamente	1	5
														- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	4	20
														- Auto backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	2	10
		X					X	X		Accidental delete	5	4	20	- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	3	15
														- Auto backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	2	10
		X	X	X			X			Approachable credentials	5	3	15	- 2FA	6	- Tecnicamente fattibile ma potrebbe non essere apprezzato dagli utenti	1	3
														- Rilevazioni di accessi non autorizzati	5	- Tecnicamente fattibile, ma potrebbe essere complessa l'implementazione	3	9
														- Formazione dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	2	6
		X	X	X			X			Weak password	7	3	21	- Formazione ai dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	5	15
														- Controllo robustezza password	2	- Tecnicamente fattibile, alcune password fragili potrebbero non essere rilevate	3	9
		X						X		Malware	4	6	24	- Antivirus	3	- Tecnicamente fattibile, ma deve essere aggiornato frequentemente	1	6
														- Controllo degli accessi e blocco degli eseguibili in determinate locazioni di memoria	3	- Tecnicamente fattibile, può creare problemi in caso di installazione di aggiornamenti	2	14
								X		Ransomware	4	7	28	- Auto Backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	3	12
														- Log	3	- Tecnicamente fattibile, ma da consultare continuamente	4	16
	X			X			X			Phishing	5	4	20	- Formazione ai dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	2	8
										TOTAL RISK			290/560					

Asset	Spoofing	Tampering	Repudation	Information Disclusure	Dos	Elevation of privilege	Danger	Unreliability	Absence of Resilience	Attack	Probability	Impact	Risk	Control	Cost	Feasibility	Residual attack likelihood / Residual Impact	Residual Risk
Immagine	X			X						Sniffing	5	1	5	- PKI systems such as SSL/TLS and certificates	5	- Tecnicamente fattibile, ma dipendente dalla rete di comunicazione	2	2
														- Encryption	3	- Tecnicamente fattibile, ma la chiave deve essere rinnovata periodicamente	2	2
		X	X	X				X		Unauthorized access	5	2	10	- Cookie authentication avanzata	2	- Tecnicamente fattibile ma non è apprezzato da gran parte degli utenti	3	6
														- 2FA	6	- Tecnicamente fattibile ma potrebbe non essere apprezzato dagli utenti	1	2
				X						Expose internal data	4	1	4	- Non permettere il download dei dati	1	- Tecnicamente fattibile, impone un limite all'uso del software	1	1
		X		X				X		Expose internal server	3	4	12	- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	2	6
														- Antivirus	3	- Tecnicamente fattibile, ma deve essere aggiornato frequentemente	1	4
		X		X				X		Change internal data	3	4	12	- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	3	9
														- Auto backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	2	6
														- I sistemi devono essere aggiornati per rendere il sistema meno vulnerabile	1	- Tecnicamente fattibile, ma probabilità di errori con versioni precedenti	1	4
		X		X				X		Delete internal data	3	4	12	- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	3	9
														- Auto backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	2	6
	X		X	X						Hack partners account	6	3	18	- Formazione ai dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	3	9
														- Controllo robustezza password	2	- Tecnicamente fattibile, alcune password fragili potrebbero non essere rilevate	4	12
														- 2FA	6	- Tecnicamente fattibile ma potrebbe non essere apprezzato dagli utenti	1	3
				X						Copy on local device	3	1	3	- Creare un visualizzatore per i file contenuti nel giornale	3	- Tecnicamente fattibile, ma complesso	1	1
				X						Copy on cloud/external device	4	1	4	- Creare un visualizzatore per i file contenuti nel giornale che consente la condivisione	3	- Tecnicamente fattibile, ma complesso	1	1

Asset	Spoofing	Tampering	Repudation	Information Disclusure	Dos	Elevation of privilege	Danger	Unreliability	Absence of Resilience	Attack	Probability	Impact	Risk	Control	Cost	Feasibility	Residual attack likelihood / Residual Impact	Residual Risk
Immagine		X						X		Accidental change	5	3	15	- Hash	3	- Tecnicamente fattibile, ma consumo della memoria periodicamente	1	5
														- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	2	10
														- Auto backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	1	5
		X						X		Accidental delete	5	3	15	- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	2	10
														- Auto backup	3	- Tecnicamente fattibile, ma deve essere aggiornato frequentemente	1	5
		X	X	X						Approachable credentials	5	3	15	- 2FA	6	- Tecnicamente fattibile ma potrebbe non essere apprezzato dagli utenti	1	3
														- Rilevazioni di accessi non autorizzati	5	- Tecnicamente fattibile, ma potrebbe essere complessa l'implementazione	3	9
														- Formazione dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	2	6
		X	X	X						Weak password	7	2	14	- Formazione ai dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	5	10
														- Controllo robustezza password	2	- Tecnicamente fattibile, alcune password fragili potrebbero non essere rilevate	10	6
		X						X		Malware	4	6	24	- Antivirus	3	- Tecnicamente fattibile, ma deve essere aggiornato frequentemente	1	6
										Ransomware	4	7	28	- Controllo degli accessi e blocco degli eseguibili in determinate locazioni di memoria	3	- Tecnicamente fattibile, può creare problemi in caso di installazione di aggiornamenti	2	14
								X						- Auto Backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	3	12
														- Log	3	- Tecnicamente fattibile, ma da consultare continuamente	4	16
	X			X						Phishing	5	4	20	- Formazione ai dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	2	8
										TOTAL RISK			211/672					

Asset	Spoofing	Tampering	Repudation	Information Disclusure	Dos	Elevation of privilege	Danger	Unreliability	Absence of Resilience	Attack	Probability	Impact	Risk	Control	Cost	Feasibility	Residual attack likelihood / Residual Impact	Residual Risk
Database	X				X					System shutdown	3	6	18	- I sistemi devono essere aggiornati per rendere il sistema meno vulnerabile	1	- Tecnicamente fattibile, ma da svolgere periodicamente	1	6
	X			X						Sniffing	5	1	5	- PKI systems such as SSL/TLS and certificates	5	- Tecnicamente fattibile, ma dipendente dalla rete di comunicazione	2	2
														- Encryption	3	- Tecnicamente fattibile, ma la chiave deve essere rinnovata periodicamente	2	2
	X			X						Unauthorized access	5	3	15	- Cookie authentication avanzata	2	- Tecnicamente fattibile ma non è apprezzato da gran parte degli utenti	3	9
														- 2FA	6	- Tecnicamente fattibile ma potrebbe non essere apprezzato dagli utenti	1	3
	X			X						Spoofing admin account	4	4	16	- ACL	4	- Tecnicamnete fattibile, ma bisogna assegnare correttamente le risorse ai giusti ruoli	3	12
														- 2FA	6	- Tecnicamente fattibile ma potrebbe non essere apprezzato dagli utenti	1	4
														- Rilevazioni di accessi non autorizzati	5	- Tecnicamente fattibile, ma potrebbe essere complessa l'implementazione	2	8
				X	X					Expose internal server	5	4	20	- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	3	15
														- Antivirus	3	- Tecnicamente fattibile, ma deve essere aggiornato frequentemente	2	8
		X		X				X		Change internal data	3	6	18	- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	4	12
														- Auto backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	2	6
														- I sistemi devono essere aggiornati per rendere il sistema meno vulnerabile	1	- Tecnicamente fattibile, ma probabilitàa di errori con versioni precedenti	1	6

Asset	Spoofing	Tampering	Repudation	Information Disclusure	Dos	Elevation of privilege	Danger	Unreliability	Absence of Resilience	Attack	Probability	Impact	Risk	Control	Cost	Feasibility	Residual attack likelihood / Residual Impact	Residual Risk
Database		X		X				X		Delete internal data	3	6	18	- Log	2	- Tecnicamente fattibile, ma da consultare continuamente	4	12
														- Auto backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	2	6
	X			X				X		Hack partners account	6	4	24	- Formazione ai dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	3	12
														- Controllo robustezza password	2	- Tecnicamente fattibile, alcune password fragili potrebbero non essere rilevate	4	16
														- 2FA	6	- Tecnicamente fattibile ma potrebbe non essere apprezzato dagli utenti	1	4
		X			X			X	X	Malware	4	6	24	- Antivirus	3	- Tecnicamente fattibile, ma deve essere aggiornato frequentemente	1	6
										Ransomware	4	7	28	- Controllo degli accessi e blocco degli eseguibili in determinate locazioni di memoria	3	- Tecnicamente fattibile, può creare problemi in caso di installazione di aggiornamenti	2	14
					X			X						- Auto Backup	3	- Tecnicamente fattibile, ma uso delle risorse sempre più elevato	3	12
														- Log	3	- Tecnicamente fattibile, ma da consultare continuamente	4	16
	X			X						Phishing	5	4	20	- Formazione ai dipendenti	2	- Tecnicamente fattibile, non necessita di implementazione, ma richiede tempo	2	8
		X		X				X		SQL Injection	4	6	24	- Rendere l'applicativo resiliente ad attacchi sql injection	2	- Tecnicamente fattibile, ma da aggiornare nel tempo	1	4
										TOTAL RISK			230/504					

Mitigation table

Di seguito delle tabelle che mostrano, per ogni asset, le modalità di controllo con i relativi risk ratio, value to cost ratio e rischio residuo (calcolato per quella specifica soluzione di controllo sul rischio massimo totale).

Asset	Control	Cost	Residual Risk	Risk Ratio	Value to cost Ratio	Risk Ratio	Value to cost Ratio
Giornale	I sistemi devono essere aggiornati per rendere il sistema meno vulnerabile	1	246/784	31.38%	7.00	BASSO	ALTO
	PKI systems such as SSL/TLS and certificates	5	258/784	32.91%	1.40	BASSO	MEDIO
	Encryption	3	258/784	32.91%	2.33	BASSO	ALTO
	Cookie authentication avanzata	2	258/784	32.91%	3.50	BASSO	ALTO
	2FA	6	210/784	26.79%	1.17	BASSO	MEDIO
	ACL	4	259/784	33.04%	1.75	MEDIO	MEDIO
	Rilevazioni di accessi non autorizzati	5	248/784	31.63%	1.40	BASSO	MEDIO
	Filtering	4	252/784	32.14%	1.75	BASSO	MEDIO
	Captcha	1	252/784	32.14%	7.00	BASSO	ALTO
	Controllo sulla concessione dei validatori	1	257/784	32.78%	7.00	BASSO	ALTO
	Non permettere il download dei dati	1	261/784	33.29%	7.00	MEDIO	ALTO
	Log	2	240/784	30.61%	3.50	BASSO	ALTO
	Antivirus	3	242/784	30.87%	2.33	BASSO	ALTO
	Formazione ai dipendenti	2	230/784	29.34%	3.50	BASSO	ALTO
	Controllo robustezza password	2	246/784	31.38%	3.50	BASSO	ALTO
	Auto Backup	3	227/784	28.95%	2.33	BASSO	ALTO
	Controllo degli accessi e blocco degli eseguibili in determinate locazioni di memoria	3	250/784	31.89%	2.33	BASSO	ALTO

Asset	Control	Cost	Residual Risk	Risk Ratio	Value to cost Ratio	Risk Ratio	Value to cost Ratio
Misure	PKI systems such as SSL/TLS and certificates	5	287/560	51.25%	1.00	MEDIO	MEDIO
	Encryption	2	275/560	49.11%	2.50	MEDIO	ALTO
	2FA	6	212/560	37.86%	0.83	MEDIO	MEDIO
	Non permettere il download dei dati	1	284/560	50.71%	5.00	MEDIO	ALTO
	Log	2	247/560	44.11%	2.50	MEDIO	ALTO
	Antivirus	3	260/560	46.43%	1.67	MEDIO	MEDIO
	Auto backup	3	228/560	40.71%	1.67	MEDIO	MEDIO
	I sistemi devono essere aggiornati per rendere il sistema meno vulnerabile	1	278/560	49.64%	5.00	MEDIO	ALTO
	Formazione ai dipendenti	2	245/560	43.75%	2.50	MEDIO	ALTO
	Controllo robustezza password	2	266/560	47.50%	2.50	MEDIO	ALTO
	Creare un visualizzatore per i file contenuti nel giornale	3	288/560	51.43%	1.67	MEDIO	MEDIO
	Creare un visualizzatore per i file contenuti nel giornale che consente la condivisione	3	288/560	51.43%	1.67	MEDIO	MEDIO
	Hash	3	270/560	48.21%	1.67	MEDIO	MEDIO
	Rilevazioni di accessi non autorizzati	5	284/560	50.71%	1.00	MEDIO	MEDIO
	Controllo degli accessi e blocco degli eseguibili in determinate locazioni di memoria	3	276/560	49.29%	1.67	MEDIO	MEDIO

Asset	Control	Cost	Residual Risk	Risk Ratio	Value to cost Ratio	Risk Ratio	Value to cost Ratio
Immagine	PKI systems such as SSL/TLS and certificates	5	208/672	30.95%	1.20	BASSO	MEDIO
	Encryption	3	208/672	30.95%	2.00	BASSO	MEDIO
	Cookie authentication avanzata	2	207/672	30.80%	3.00	BASSO	ALTO
	2FA	6	176/672	26.19%	1.00	BASSO	MEDIO
	Non permettere il download dei dati	1	208/672	30.95%	6.00	BASSO	ALTO
	Log	2	177/672	26.34%	3.00	BASSO	ALTO
	Antivirus	3	185/672	27.53%	2.00	BASSO	MEDIO
	Auto backup	3	163/672	24.26%	2.00	BASSO	MEDIO
	I sistemi devono essere aggiornati per rendere il sistema meno vulnerabile	1	203/672	30.21%	6.00	BASSO	ALTO
	Formazione ai dipendenti	2	177/672	26.34%	3.00	BASSO	ALTO
	Controllo robustezza password	2	197/672	29.32%	3.00	BASSO	ALTO
	Creare un visualizzatore per i file contenuti nel giornale	3	209/672	31.10%	2.00	BASSO	MEDIO
	Creare un visualizzatore per i file contenuti nel giornale che consente la condivisione	3	208/672	30.95%	2.00	BASSO	MEDIO
	Hash	3	201/672	29.91%	2.00	BASSO	MEDIO
	Rilevazioni di accessi non autorizzati	5	205/672	30.51%	1.20	BASSO	MEDIO
	Controllo degli accessi e blocco degli eseguibili in determinate locazioni di memoria	3	197/672	29.32%	2.00	BASSO	MEDIO

Asset	Control	Cost	Residual Risk	Risk Ratio	Value to cost Ratio	Risk Ratio	Value to cost Ratio
Database	I sistemi devono essere aggiornati per rendere il sistema meno vulnerabile	1	218/504	43.25%	6.00	MEDIO	ALTO
	PKI systems such as SSL/TLS and certificates	5	227/504	45.04%	1.20	MEDIO	MEDIO
	Encryption	3	227/504	45.04%	2.00	MEDIO	MEDIO
	Cookie authentication avanzata	2	224/504	44.44%	3.00	MEDIO	ALTO
	2FA	6	186/504	36.90%	1.00	MEDIO	MEDIO
	ACL	4	226/504	44.84%	1.50	MEDIO	MEDIO
	Rilevazioni di accessi non autorizzati	5	222/504	44.05%	1.20	MEDIO	MEDIO
	Log	2	201/504	39.88%	3.00	MEDIO	ALTO
	Antivirus	3	200/504	39.68%	2.00	MEDIO	MEDIO
	Auto backup	3	190/504	37.70%	2.00	MEDIO	MEDIO
	Formazione ai dipendenti	2	206/504	40.87%	3.00	MEDIO	ALTO
	Controllo robustezza password	2	222/504	44.05%	3.00	MEDIO	ALTO
	Rendere l'applicativo resiliente ad attacchi sql injection	2	210/504	41.67%	3.00	MEDIO	ALTO
	Controllo degli accessi e blocco degli eseguibili in determinate locazioni di memoria	3	216/504	42.86%	2.00	MEDIO	MEDIO

Classificando il value to cost come:

- Alto se value to cost > 2.00
- Medio se 0.75 > Value to cost < 2.00
- Basso se value to cost < 0.75

Classificando il rischio come:

- Alto se rischio > 66%
- Medio se 34 % < rischio < 66%
- Basso se rischio < 33 %

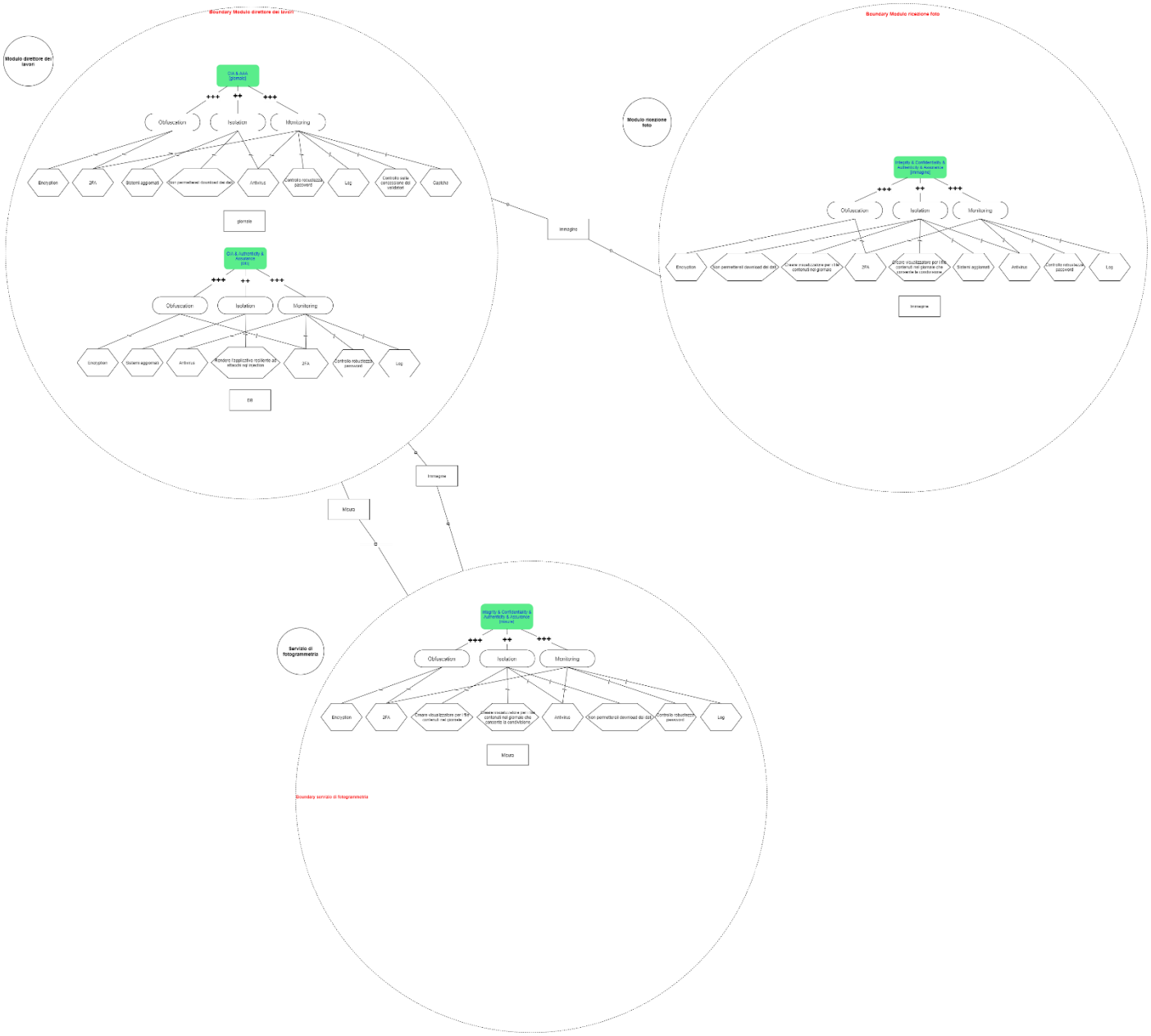
Si sono scelte le contromisure che qualitativamente consentono di ottenere il minor costo nella curva totale del rischio.

In particolare, per ogni attacco si è scelta la contromisura più conveniente usando una tabella di questo tipo:

Le contromisure scelte ed il modo in cui aiutano a raggiungere gli obiettivi di sicurezza sarà mostrato nel seguente paragrafo.

Security requirement definition

Una volta scelto per ogni possibile attacco la contromisura da adottare tramite l'analisi del rischio si possono stilare le definizioni dei requisiti di sicurezza, in modo tale da poter constatare come ogni singola contromisura aiuti un certo obiettivo di sicurezza ed in che modo.



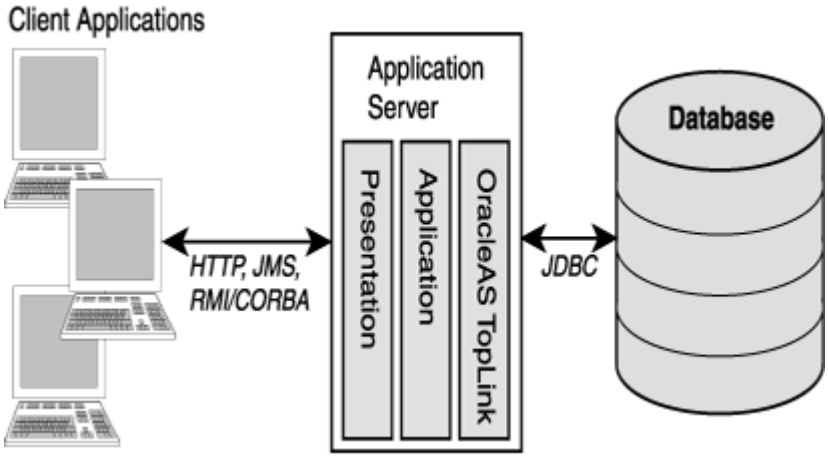
Software Security Engineering

Design

I design pattern implementati nel progetto sono stati pensati tenendo conto le qualità di modularità, semplicità, replicabilità e sicurezza.

Data la limitatezza delle risorse hardware è stato deciso di usare un design client – server in cui i nodi della blockchain, il DBMS ed il web server sono sullo stesso terminale.

L'architettura sarà del tipo Three tier cioè un'architettura client-server in cui la logica del processo funzionale, l'accesso ai dati, l'archiviazione dei dati del computer e l'interfaccia utente sono sviluppati e mantenuti come moduli indipendenti su piattaforme separate. Nel nostro caso ci sarà anche una piattaforma propria per il giornale, separando cosi il server web, il DB e l'interfaccia dell'utente.



Nella realtà la piattaforma sarà in un web server con un dominio ed il direttore potrà accedervi tramite internet da qualsiasi luogo, e sarà un **SAAS** avendo quindi i vantaggi di poter scalare facilmente e di avere a disposizione molto storage distribuito in modo tale da aumentare l'affidabilità e la sicurezza.

Si è deciso di procedere facendo uso di un'architettura di protezione a strati, in modo da isolare, offuscare e monitorare al meglio, oltre che l'applicazione stessa, anche i componenti software esterni che ne entrano in contatto.

Come visto negli abuse case e misuse case a livello di sistema è stato deciso di fare uso di un Antivirus.

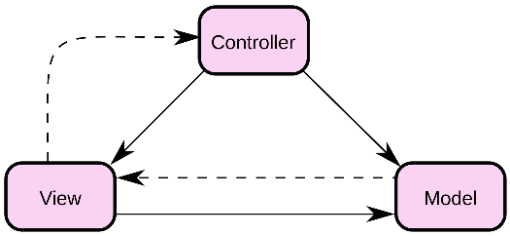
A livello di applicativo, l'accesso all'applicazione avviene tramite username e password, inoltre si farà uso di ACL, 2FA e Captcha e Log, come risultato dall'analisi del rischio.

A livello di dati, il loro accesso deve essere sempre limitato ad account abilitati, tutti i dati inseriti nel database e nella blockchain risultano criptati, inoltre si farà uso di crittografia nella comunicazione client server.

A livello di codice usiamo il factory pattern per creare oggetti senza esporre la logica di creazione al client e ci riferiamo a oggetti appena creati utilizzando delle interfacce, in modo tale da rendere più sicuro, modulare il codice, oltre a facilitarne la manutenzione.

È stato deciso di utilizzare il design pattern Model-View-Controller perché separa la logica di presentazione dei dati dalla logica di elaborazione dell'applicazione e dal modello dei dati.

MVC pattern architetturale molto diffuso ed attuale, che rende il codice più modulare ed in certi aspetti più sicuro ed affidabile, ma soprattutto più facile da manutenere.



Scelte tecnologiche

Sono in seguito riportati i principali strumenti utilizzati nello sviluppo di questa applicazione e i motivi della loro scelta.

Abbiamo scelto Java come linguaggio di programmazione, perché la maggior parte dei componenti del gruppo avevano lavorato precedentemente con tale linguaggio. Alcuni non avevano una vasta conoscenza del linguaggio ma avendo lavorato con linguaggi simili Java è risultato semplice da apprendere.

Inoltre, Java permette di usare il paradigma ad oggetti che è molto diffuso e più sicuro del paradigma classico grazie all'incapsulamento ed all'information hiding.

Per il Database abbiamo usato MySQL e per l'installazione abbiamo usato XAMPP, perché rende semplice l'installazione di un Database ed è compatibile sia con Microsoft che con Linux, inoltre permette di gestire in maniera semplice il DB tramite Tomcat ed il browser.

Per gestire la blockchain abbiamo usato Docker come proposto nelle lezioni e per la sua compatibilità con Microsoft e Linux. Per interfacciare il contratto in Solidity con l'applicazione web abbiamo usato Web3j, libreria di Java per il collegamento tra Java e Etherium/Solidity.

Come gestore di progetti è stato usato Maven, per i vantaggi che offre nel controllo delle librerie e dipendenze tramite il POM.

Per la gestione delle versioni e un fruttuoso lavoro in squadra è stato usato Git, in specifico la piattaforma di GitHub.

Blockchain

La blockchain consiste in un registro distribuito su diversi nodi, permette quindi la distribuzione dei dati sui diversi dispositivi che la andranno a costituire. Ogni nodo che ne fa pare possiede una copia in memoria dell'intera blockchain scongiurando quindi Single Point Of Failure in quanto la struttura è totalmente decentralizzata.

Ogni nodo validatore ha il compito di validare le transazioni in ingresso vedendo se è coerente con il resto delle transazioni lungo la propria copia della catena.

C'è un meccanismo di votazione che permette di "far vincere" la fork che riceve più voti se ci sono delle incongruenze, in modo da impedire eventuali tentativi di modifica e preservando la coerenza e l'integrità delle transazioni.

La blockchain usa primitive criptografiche, in particolare gli hash e la crittografia, solo chi fa parte delle blockchain può leggere il contenuto delle transazioni, a meno che non siano transazioni private tra due nodi come permette di fare Quorum.

Negli anni sono state sviluppate diverse tipologie di blockchain. Nell'implementazione di questa app, considerando le specifiche del progetto, è stata scelta Quorum.

Quorum

Quorum nasce come fork di Ethereum: piattaforma open source basata su blockchain, che consente l'implementazione di smart contract, ovvero un protocollo di transazione computerizzato che esegue i termini di un contratto, che va inserito all'interno della blockchain in modo da poterlo utilizzare in maniera distribuita. Quorum, diversamente da Ethereum, permette la creazione e la gestione di blockchain private: coloro che possono accedervi devono essere necessariamente abilitati a farlo, inoltre permette l'occultamento di transazioni e del loro contenuto, che può essere criptato, a coloro che non vi partecipano. Dato lo scopo di questa applicazione, vi è una necessità di privacy assoluta per tutelare le organizzazioni che potrebbero farne uso, inoltre è richiesta l'immutabilità dei dati inseriti per scongiurare procedure illecite. Per i motivi sopra elencati si è stabilito di scegliere Quorum.

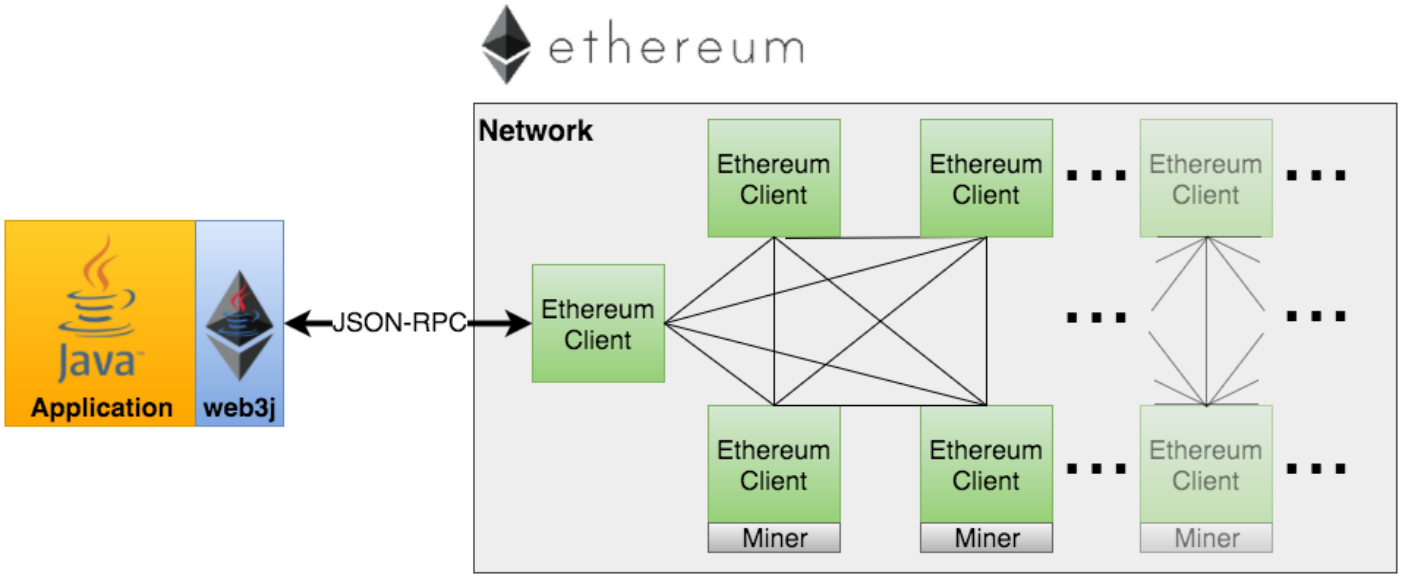
Solidity

I contratti da inserire nella blockchain Ethereum devono essere necessariamente scritti e compilati in Solidity: linguaggio tipizzato sviluppato appositamente per lo sviluppo di smart contract compatibili con la Ethereum Virtual Machine.

Per questo progetto si è usata la versione 0.6 di Solidity.

Web3j

Web3j è una libreria Java necessaria all'implementazione degli smart contract e all'interazione con la rete di nodi della blockchain Ethereum: partendo da un contratto compilato in Solidity, dà la possibilità di creare la rispettiva classe Java in modo da poter interagire con la blockchain tramite Java Application.



Java Spring

Fondamentalmente Spring è un framework che va al di sopra di Java ed è composto da strumenti e utilità che aiutano lo sviluppatore a creare applicazioni web in Java per il back-end.

Offre come elemento chiave il supporto dell'infrastruttura a livello applicativo, fornendo un modello completo sia per la configurazione che per la programmazione delle applicazioni aziendali sviluppate sotto Java, senza discriminazioni riguardo all'implementazione della piattaforma.

Tutto ciò porta un grande vantaggio, poiché consente ai team di sviluppo di concentrarsi direttamente sulla logica di business richiesta dall'applicazione, rendendo il processo più breve, veloce ed efficiente, risparmiando righe di codice evitando attività ripetitive.

Inoltre, presenta diverse classi e metodi implementati in maniere sicura, ad esempio per fare query verso il Database senza rischiare l'iniezione di codice SQL.

Design assets

Come design assets abbiamo scelto principalmente le linee guida OWASP perché l'applicazione sarà un'applicazione web, inoltre abbiamo preso anche alcuni punti dalla linea guida di Sommerville che abbiamo reputato utili inserire.

1. **Minimizzare la superficie d'attacco**: Verranno implementate solo le interfacce strettamente necessarie e saranno disponibili solo agli utenti con determinate autorizzazioni. In particolare, solo l'account del direttore dei lavori potrà visualizzare il giornale dei lavori ed inserirvi i lavori, gestire le immagini e avere modo di calcolare le misure richiamando il servizio di fotogrammetria. Solo all'account drone sarà data la possibilità di caricare nuove immagini nel sistema.

2. **Stabilire default sicuri**: Le impostazioni di sicurezza saranno impostate sicure di default, e non potranno essere modificate dagli utenti. Ad esempio, non sarà consentita l'eliminazione di immagini dal database una volta salvate nella blockchain e come già specificato ogni utente potrà accedere solo alle risorse di propria competenza. Inoltre, le password degli utenti dovranno rispettare un certo formato di sicurezza, quindi usare determinati caratteri ed avare una certa lunghezza minima, ecc…

3. **Principio dei privilegi minimi**: Ogni utente avrà i privilegi minimi per le attività che dovrà eseguire, in modo tale da evitare di apportare danni intenzionali o accidentali al sistema, riducendo quindi la superficie d'attacco. Come scritto precedentemente, ogni utente potrà eseguire solo le attività strettamente inerenti al ruolo che svolge.

4. **Difesa in profondità**: Il sistema sarà dotato di più meccanismi di difesa, in modo tale da rendere più difficili eventuali attacchi e per gestire al meglio eventuali errori da parte di utenti maldestri. Quindi saranno presenti dei controlli nel front-end, nel back-end e nello smart contract, ad esempio per verificare che i dati che si stanno caricando siano corretti e che l'utente abbia i permessi per lavorare con la blockchain.

5. **Fallire in maniera sicura**: La sicurezza deve essere presente anche in situazioni di errore di sistema, saranno presenti meccanismi di gestione delle eccezioni nei vari componenti dell'applicazione che lanceranno specifiche eccezioni se si verificheranno determinate situazioni di errore.

6. **Non fidarsi dei servizi terzi**: L'applicazione si appoggia ad un servizio terzo di fotogrammetria, ci saranno dei controlli per far in modo che venga richiamato sempre il servizio giusto e che le misure ritornate rispettino un determinato formato.

7. **Separazione di compiti**: Ogni utente avrà specifiche mansioni, diverse da quelle degli altri utenti, quindi ruoli e permessi diversi. Anche i vari moduli dell'applicazione seguiranno la stessa logica, ogni modulo si occuperà di un compito ben determinato e differente dagli altri.

8. **Evitare sicurezza per oscurità**: Sia per questioni di trasparenza, sia per questioni di sicurezza il progetto sarà open design ed open source, così eventuali bug saranno scoperti e quindi corretti nel minor tempo possibile. Tutto il progetto, compreso il codice sarà reso pubblico sul repository di GitHub.

9. **KISS**: A parità di features sarà scelta sempre la soluzione più semplice in modo tale da diminuire eventuali bug nel codice e nella progettazione e quindi restringere le superfici d'attacco. Inoltre, le soluzioni più semplici rendono il codice più chiaro per la manutenzione e più performante.

10. **Fixare correttamente i bug di sicurezza**: Una volta scoperti i bug saranno fixati correttamente capendo in profondità i motivi che li scatenano.

11. **Basare le decisioni su precise policy di sicurezza**: Il drone avrà il solo permesso di caricare nuove immagini, il direttore dei lavori avrà solo i permessi per lavorare con il giornale dei lavori e di gestire le immagini prima che vengano salvate nel giornale dei lavori.

12. **Evitare single point of failure**: Grazie alla tecnologia blockchain distribuita su nodi diversi si riesce ad evitare il SPOF a tale livello, ma bisogna evitarla anche a livello di DBMS, web server a livello applicativo e a livello dati, ad esempio facendo mirroring dei dati in automatico o usare il cloud computing come detto in precedenza.

13. **Bilanciare sicurezza ed usabilità**: L'usabilità deve comunque avere un ruolo importante, quindi a volte conviene avere un software leggermente meno sicuro ma molto più user-friendly. Infatti, non si sono considerate soluzioni drastiche come, ad esempio, il riconoscimento biometrico durante l'analisi.

14. **Fare il log delle azioni degli utenti**: Verrà fatto un log delle varie azioni eseguite dagli utenti ed apportate al sistema, come già detto in precedenze e risultato dall'analisi del rischio.

15. **Usare ridondanza e diversità**: Il progetto nasce con l'intento di usare una blockchain che di per sé è una tecnologia ridondante, inoltre come già visto nella parte precedente nella realtà si userà il cloud computing. Per soddisfare questo requisiti anche a livello di codice, si dovrebbe implementare il servizio con più linguaggi di programmazione.

16. **Specificare il formato di ogni input al sistema**: Ci saranno dei controlli negli input del programma, in particolare nei web form con relativa sanificazione per prevenire attacchi come SQL Injection. Inoltre, ci saranno dei controlli per verificare che le informazioni inserite siano corrette e coerenti, ad esempio si controllerà il formato delle immagini prima che vengano caricate, l'hash per evitare i duplicati, il nome, ecc…