Politecnico di Torino

Politecnico di Torino

Laurea Magistrale in Ingegneria Informatica

2024 - 2025

Sessione di laurea aprile 2025

Innovazione nei processi di conformità del settore fintech: automazione e intelligenza predittiva

Relatori:

Alberto Monge Roffarello

Candidato:

Matteo Busnelli

Indice

Capitolo 1

Introduzione

Il settore fintech (financial technology) si configura come un'area altamente dinamica, caratterizzata dall'integrazione di tecnologie avanzate nei servizi finanziari. Negli ultimi anni, l'evoluzione del fintech ha rivoluzionato il panorama economico globale, introducendo modelli operativi innovativi che mirano a migliorare l'efficienza, ridurre i costi e ampliare l'accesso ai servizi bancari e finanziari.

Un aspetto fondamentale del fintech è la capacità di sfruttare tecnologie quali il cloud computing, la blockchain, l'intelligenza artificiale (AI) e il machine learning per automatizzare processi esistenti e offrire soluzioni scalabili e sicure ai propri clienti. Queste tecnologie consentono di superare le rigide limitazioni dei sistemi tradizionali (legacy), che risultano poco adattabili alle esigenze del mercato odierno.

Il settore bancario, in particolare, ha beneficiato dell'adozione di innovazioni fintech attraverso la digitalizzazione di numerosi servizi: apertura di conti online, pagamenti digitali, gestione degli investimenti e prestiti personalizzati. Tuttavia, con l'espansione delle operazioni digitali, è emersa la necessità di rafforzare i controlli di conformità normativa per prevenire frodi, riciclaggio di denaro e finanziamento al terrorismo.

L'importanza strategica del fintech non si limita ai miglioramenti operativi, ma si estende alla capacità di favorire l'inclusione finanziaria. Grazie a piattaforme digitali accessibili, milioni di persone precedentemente escluse dai tradizionali sistemi bancari possono ora usufruire di servizi come prestiti, pagamenti e risparmi. Questo aspetto è particolarmente rilevante nei mercati emergenti, dove l'adozione di tecnologie mobili ha accelerato la diffusione dei servizi finanziari.

In definitiva, il settore fintech rappresenta un ecosistema complesso e in continua evoluzione, dove la collaborazione tra tecnologia e finanza genera opportunità e sfide che richiedono un costante adattamento sia tecnologico che regolamentare. Questa tesi si inserisce in questo contesto, esplorando specificamente il ruolo dell'underwriter e i processi di conformità normativa, analizzando come l'adozione di tecnologie avanzate possa risolvere le inefficienze dei sistemi tradizionali.

Durante la mia esperienza di tirocinio, ho avuto l'opportunità di lavorare attivamente a un progetto in questo settore, approfondendo le problematiche legate alla conformità normativa e contribuendo in prima persona all'analisi, allo studio e all'implementazione di soluzioni efficaci e scalabili. Durante le analisi che ho effettuato, ho concluso che l'underwriter svolge un ruolo fondamentale nella valutazione del rischio e nella verifica della conformità normativa. Questo professionista analizza i dati dei clienti e degli enti associati per assicurarsi che rispettino standard regolatori come i controlli PEP (Politically Exposed Person) e OFAC (Office of Foreign Assets Control). Tuttavia, i processi manuali, spesso utilizzati per queste attività, presentano limiti significativi: risultano lenti, costosi e inclini a errori umani. La crescente complessità delle normative richiede quindi un approccio più sistematico e tecnologico, capace di coniugare automazione ed efficienza operativa. Alla luce di queste considerazioni, ho lavorato direttamente all'implementazione di un sistema automatizzato per i controlli di conformità PEP e OFAC, progettando soluzioni in grado di ottimizzare il processo di verifica, ridurre i margini di errore e garantire un'elevata efficienza operativa. L'integrazione di tecnologie avanzate e di metodologie di automazione ha permesso di trasformare un processo tradizionalmente manuale in un sistema più affidabile, scalabile e conforme agli standard normativi.

1.1 Obiettivi della tesi

1.1.1 Analisi delle criticità dei processi attuali

Questa tesi analizza le criticità che caratterizzano i controlli di conformità nei processi manuali nel settore fintech/banking. L'attenzione è rivolta a inefficienze come la lentezza operativa, i costi elevati e l'alto rischio di errore umano, accentuati dalla complessità e dalla frequenza degli aggiornamenti normativi. Tali problematiche non solo influiscono sull'efficienza aziendale, ma possono anche compromettere la compliance regolatoria, con impatti significativi sia dal punto di vista legale che reputazionale.

1.1.2 Proposta di soluzioni tecnologiche innovative

Questa ricerca si concentra sull'adozione di soluzioni tecnologiche avanzate per superare le attuali inefficienze dei processi tradizionali. Una fase iniziale di analisi degli attuali problemi legati ai controlli di conformità, è seguita da una fase di implementazione che riguarda l'automazione dei controlli PEP e OFAC.

L'automazione di questi controlli prevede l'implementazione di sistemi software in grado di gestire in modo rapido ed efficace l'elaborazione dei dati necessari per

verificare la conformità. Grazie all'integrazione di database globali e strumenti di screening automatico, i controlli PEP e OFAC possono essere effettuati in tempo reale, riducendo drasticamente il tempo richiesto per la verifica manuale e minimizzando il rischio di errore umano. Questi sistemi permettono, ad esempio, di confrontare le informazioni di clienti o transazioni con liste di sanzioni, blacklist e registri di individui politicamente esposti, notificando immediatamente eventuali corrispondenze sospette.

Oltre alla velocità, l'automazione garantisce una maggiore standardizzazione nei processi di controllo, eliminando ambiguità interpretative e assicurando un rispetto più rigoroso delle normative internazionali. Tali sistemi possono essere ulteriormente migliorati con l'adozione di moduli di apprendimento automatico (machine learning), che consentono al software di adattarsi dinamicamente ai cambiamenti normativi e di migliorare le capacità di riconoscimento dei pattern di rischio.

Sviluppato in parallelo all'automazione, l'introduzione di sistemi di intelligenza artificiale predittiva (Predictive AI) rappresenta un ulteriore passo avanti nell'evoluzione tecnologica. Questi strumenti, basati su framework come il Knowledge Reasoning Representation (KRR), offrono la possibilità di prevedere situazioni di rischio prima che si verifichino effettivamente. La Predictive AI analizza grandi volumi di dati, tra cui transazioni finanziarie, profili di clienti e diversi contesti geopolitici, per identificare anomalie o schemi ricorrenti che possono indicare potenziali violazioni normative.

In particolare, i framework di KRR integrano capacità di ragionamento logico e semantico, migliorando l'efficacia dei sistemi predittivi nei contesti complessi tipici del settore fintech. Questo approccio consente non solo di identificare transazioni sospette in tempo reale, ma anche di generare report dettagliati che supportano gli underwriter nella valutazione dei rischi e nella gestione dei casi.

Combinando automazione e intelligenza predittiva, le soluzioni tecnologiche proposte offrono un livello di accuratezza, efficienza e scalabilità che risponde alle esigenze dei moderni ecosistemi fintech. Questo approccio rappresenta un passaggio cruciale verso l'adozione di processi completamente digitalizzati e basati sull'intelligenza artificiale, in grado di rispondere alle sfide attuali e future del settore.

1.2 Struttura della tesi

La tesi è strutturata in modo da fornire una visione organica e integrata del problema e delle soluzioni proposte:

- **Capitolo 1**: Introduzione al settore fintech e banking, con focus sull'underwriter. Obiettivi e struttura della tesi.

- **Capitolo 2**: Analisi delle motivazioni alla trasformazione digitale.
- **Capitolo 3**: Approfondimento sulla trasformazione digitale nel contesto fintech e bancario.
- **Capitolo 4**: Descrizione dettagliata dei controlli di conformità PEP e OFAC.
- **Capitolo 5**: Implementazione pratica dei controlli sviluppati durante l'esperienza di tirocinio.
- **Capitolo 6**: Implementazione e importanza dei test automatizzati nei processi di conformità.
- **Capitolo 7**: Ruolo dell'Identity and Access Management (IAM) nelle applicazioni fintech.
- **Capitolo 8**: Approfondimento sull'intelligenza artificiale e sulla predictive AI.
- **Capitolo 9**: Applicazioni della predictive AI, con particolare attenzione al settore fintech.
- **Capitolo 10**: Conclusioni e prospettive future della ricerca.

Capitolo 2

Motivazioni alla trasformazione digitale: criticità, analisi e soluzioni

2.1 Le criticità: inefficienza e manualità nei controlli svolti dagli underwriters

I processi manuali utilizzati negli attuali controlli di conformità rappresentano una significativa barriera alla competitività del settore fintech e bancario. Gli underwriters, responsabili della valutazione dei rischi e della verifica della conformità normativa, devono spesso eseguire attività complesse che implicano l'analisi di grandi quantità di dati, come elenchi di individui o entità ad alto rischio, soggetti a verifiche approfondite per garantirne la conformità.

Questi controlli manuali sono intrinsecamente limitati dalla loro natura operativa: l'elaborazione è lenta, richiede risorse significative e presenta un alto rischio di errore umano. Queste criticità non solo riducono l'efficienza aziendale, ma espongono anche le organizzazioni a potenziali sanzioni per il mancato rispetto delle normative. In uno scenario in cui la velocità e l'accuratezza sono cruciali, le procedure manuali rappresentano un ostacolo evidente.

La mancanza di automazione si traduce in inefficienze economiche e operative. Ad esempio, la necessità di verificare manualmente ogni transazione o cliente aumenta il tempo necessario per completare le procedure, generando ritardi che possono compromettere l'esperienza cliente e diminuire la competitività aziendale. Inoltre, errori derivanti da valutazioni non uniformi o omissioni possono comportare gravi implicazioni legali e reputazionali per le aziende.

Un caso reale che illustra queste problematiche è quello della Banca del Sud S.p.A., sanzionata dalla Banca d'Italia per "carenze nell'organizzazione e nei controlli interni". Durante un'ispezione, è emerso che l'istituto si affidava eccessivamente a procedure manuali per i controlli di conformità, compromettendo l'efficacia dei processi [1]. Le carenze hanno portato a una sanzione di 30.000 euro per la banca e ulteriori multe, tra i 10.000 e i 20.000 euro, per gli ex membri del Consiglio di Amministrazione e del Collegio Sindacale.

Questo esempio testimonia come l'inefficienza e la manualità nei controlli possano tradursi in sanzioni significative e danni reputazionali per le istituzioni finanziarie.

2.2 Cause delle criticità: complessità normativa, costi elevati, lentezza e suscettibilità all'errore umano

Le radici delle inefficienze nei controlli di conformità risiedono nella crescente complessità del panorama normativo globale. Negli ultimi anni, il settore finanziario è stato sottoposto a normative sempre più stringenti, volte a contrastare il riciclaggio di denaro (AML - Anti-Money Laundering) e il finanziamento del terrorismo (CFT - Combating the Financing of Terrorism). Organizzazioni internazionali come la Financial Action Task Force (FATF) e l'European Banking Authority (EBA) definiscono standard e linee guida che richiedono un costante aggiornamento dei processi interni e una maggiore granularità nei controlli delle transazioni.

Un esempio emblematico della complessità normativa è l'introduzione del regolamento europeo AMLD5 (Fifth Anti-Money Laundering Directive), che ha esteso i requisiti di conformità a settori precedentemente meno regolamentati, come le criptovalute. Questa direttiva impone alle aziende non solo di verificare l'identità dei clienti, ma anche di monitorare transazioni transfrontaliere in tempo reale, aumentando significativamente il carico di lavoro [2].

L'adeguamento a tali normative richiede risorse significative, sia in termini di personale che di infrastrutture tecnologiche. Tuttavia, il costo associato all'impiego di personale qualificato per processi manuali è estremamente elevato, specialmente per istituzioni che operano in mercati globali con un volume di transazioni elevato. Ad esempio, uno studio condotto nel 2021 ha stimato che le banche europee spendono mediamente oltre 100 milioni di euro all'anno per rispettare i requisiti di conformità normativa [3].

Oltre ai costi, la lentezza intrinseca dei processi manuali costituisce un ulteriore svantaggio. La verifica manuale di migliaia di transazioni giornaliere non è solo dispendiosa, ma limita anche la capacità delle aziende di rispondere rapidamente a nuove esigenze regolatorie o a eventi imprevisti. Questo ritardo operativo può

risultare particolarmente critico in scenari in cui il monitoraggio tempestivo è essenziale per evitare sanzioni o frodi.

Un'altra problematica fondamentale è rappresentata dalla suscettibilità all'errore umano. Anche con personale altamente qualificato, omissioni, interpretazioni errate o decisioni non uniformi sono inevitabili. Questi errori possono comportare conseguenze gravi, come l'approvazione di transazioni sospette o il blocco ingiustificato di clienti legittimi. Un caso reale di errori legati all'inefficienza manuale riguarda la banca Standard Chartered, multata per oltre 1 miliardo di dollari nel 2019 per carenze nei controlli AML. L'indagine ha rivelato che alcune transazioni sospette erano state erroneamente approvate a causa di procedure manuali poco efficaci e aggiornamenti non tempestivi delle liste di controllo [4].

2.3 Strategie di mitigazione: digitalizzazione avanzata e automazione tramite tecnologie innovative

Per affrontare le criticità sopra descritte, le organizzazioni del settore fintech e bancario stanno implementando strategie di mitigazione che si basano su soluzioni tecnologiche avanzate.

La digitalizzazione consente di trasformare dati non strutturati, come documenti cartacei o registri elettronici eterogenei, in formati standardizzati che possono essere elaborati da sistemi automatizzati. Questo processo facilita non solo la gestione delle informazioni, ma anche la loro analisi in tempo reale. Ad esempio, piattaforme di analisi basate su intelligenza artificiale possono identificare rapidamente correlazioni tra dati apparentemente non collegati, permettendo di rilevare attività sospette con maggiore tempestività.

Un esempio significativo è rappresentato dalla tecnologia di optical character recognition (OCR), utilizzata per digitalizzare documenti complessi e integrarla con algoritmi di analisi automatica. Questo approccio è stato adottato da diverse banche per migliorare il controllo di documenti di identità e transazioni estere, riducendo gli errori legati alla digitazione manuale e accelerando il processo di verifica [5].

L'intelligenza artificiale (AI) è un altro elemento cardine di queste strategie. Oltre ai vantaggi legati all'identificazione di schemi di rischio attraverso il machine learning, l'AI può essere impiegata per analizzare comportamenti sospetti in un contesto dinamico, adattandosi rapidamente ai cambiamenti normativi. Un esempio pratico è l'utilizzo di algoritmi predittivi per il monitoraggio delle transazioni in tempo reale: istituzioni come JPMorgan Chase hanno adottato soluzioni AI per migliorare la precisione dei loro controlli AML, riducendo significativamente i falsi positivi e ottimizzando l'allocazione delle risorse [6].

Un ulteriore progresso è rappresentato dai framework di Knowledge Reasoning Representation (KRR), che integrano capacità logiche e semantiche nei sistemi automatizzati. Questi framework non solo migliorano la capacità di identificare comportamenti sospetti, ma forniscono agli underwriters strumenti analitici avanzati per la gestione di casi complessi. Ad esempio, i report generati da sistemi basati su KRR possono includere dettagli contestuali che supportano decisioni più informate e rapide, riducendo il rischio di sanzioni per inadempienze normative.

Infine, l'adozione di soluzioni cloud-based ha trasformato la capacità delle aziende di gestire grandi volumi di dati. Queste piattaforme offrono scalabilità, riduzione dei costi e accesso in tempo reale alle informazioni, garantendo una maggiore resilienza operativa. Ad esempio, aziende come HSBC hanno adottato piattaforme cloud per integrare database globali di sanzioni e blacklist con i propri sistemi automatizzati, migliorando la tempestività e la precisione dei controlli [7].

Durante il mio tirocinio, una fase iniziale di analisi delle criticità sopra descritte, è stata successivamente seguita da una fase di implementazione. Tale fase ha avuto come obiettivo quello di proporre una valida soluzione ai problemi evidenziati dai sistemi preesistenti, automatizzando alcuni processi che verranno approfonditi nei capitoli successivi.

Capitolo 3

Trasformazione digitale

3.1 Differenze concettuali tra trasformazione digitale e digitalizzazione

La trasformazione digitale e la digitalizzazione sono due concetti distinti ma complementari, spesso confusi o utilizzati come sinonimi. Tuttavia, la comprensione delle loro differenze è essenziale per definire strategie mirate in qualsiasi settore che ambisca a sfruttare il pieno potenziale delle tecnologie moderne.

La digitalizzazione si riferisce al processo di conversione di informazioni, processi o strumenti analogici in formato digitale. Questo approccio si limita a sostituire strumenti tradizionali con tecnologie digitali, migliorando l'efficienza operativa senza modificare le modalità fondamentali di funzionamento. Ad esempio, digitalizzare significa adottare software per archiviare documenti, invece di utilizzare archivi fisici, o implementare un sistema di fatturazione elettronica in sostituzione di uno cartaceo.

La trasformazione digitale, invece, rappresenta un cambiamento profondo, strategico e culturale, che va ben oltre la semplice adozione di strumenti digitali. Essa implica un ripensamento radicale di processi, modelli di business, e persino della mentalità organizzativa, al fine di sfruttare appieno le opportunità offerte dalle tecnologie emergenti.

Un aspetto fondamentale della trasformazione digitale è il cambiamento culturale. L'introduzione di nuove tecnologie richiede che le persone e le organizzazioni modifichino il loro modo di lavorare e di interagire. Questo non si limita all'apprendimento di nuovi strumenti, ma include un'adesione più ampia a valori come la flessibilità, l'innovazione e la collaborazione. Ad esempio, le gerarchie tradizionali, rigide e centralizzate, sono spesso sostituite da strutture più agili e decentralizzate, che favoriscono una comunicazione bidirezionale e un approccio orientato al problem-solving collettivo [8].

Un altro elemento cruciale della trasformazione digitale è la centralità dei dati. Le organizzazioni devono imparare a raccogliere, analizzare e utilizzare i dati per guidare le decisioni strategiche. Questo richiede una mentalità basata sull'analisi continua e sulla sperimentazione, dove gli errori non sono visti come fallimenti, ma come opportunità di apprendimento [9].

In sintesi, mentre la digitalizzazione si concentra sull'efficienza operativa e sulla modernizzazione tecnologica, la trasformazione digitale abbraccia un cambiamento più ampio che coinvolge l'organizzazione nella sua totalità. Questo cambiamento non è limitato ai processi, ma investe profondamente la cultura aziendale, spingendo le persone a lavorare in modo più innovativo, adattivo e orientato al futuro.

3.2 Principali motivazioni che guidano la trasformazione digitale

La trasformazione digitale è guidata da una combinazione di fattori tecnologici, economici, sociali e competitivi, che spingono le organizzazioni a ripensare i propri modelli operativi e di business. Questi fattori non solo evidenziano le opportunità offerte dalle nuove tecnologie, ma sottolineano anche la necessità di adattarsi rapidamente per mantenere la competitività in un mercato in continua evoluzione.

Adattamento alle esigenze dei clienti

Una delle principali motivazioni della trasformazione digitale è l'evoluzione delle aspettative dei clienti. Con l'avvento delle tecnologie digitali, i consumatori si aspettano esperienze personalizzate, immediate e accessibili su più canali. Ad esempio, nel settore del retail, piattaforme come Amazon hanno rivoluzionato l'esperienza cliente offrendo suggerimenti basati sui comportamenti d'acquisto e un servizio di consegna rapida [10]. Le aziende che non riescono a soddisfare queste aspettative rischiano di perdere quote di mercato a favore di concorrenti più agili e innovativi.

Pressioni competitive

La crescente competizione rappresenta un ulteriore fattore trainante. Organizzazioni digital-first e startup tecnologiche stanno sfruttando l'agilità operativa e le tecnologie avanzate per entrare in mercati tradizionali, mettendo sotto pressione aziende consolidate. Ad esempio, nel settore assicurativo, l'ascesa delle insurtech ha costretto gli attori tradizionali a rivedere i propri processi per competere su costi, efficienza e qualità del servizio [11].

Ottimizzazione dei costi e aumento dell'efficienza

La trasformazione digitale permette alle organizzazioni di ridurre i costi operativi e aumentare l'efficienza, automatizzando processi ripetitivi e riducendo l'errore umano. Tecnologie come l'automazione robotica dei processi (RPA) e il machine learning consentono di ottimizzare attività amministrative e operative. Ad esempio, l'utilizzo di chatbot basati su intelligenza artificiale ha consentito a diverse aziende di gestire milioni di richieste dei clienti, riducendo i costi del supporto tradizionale [9].

Conformità normativa e gestione del rischio

L'evoluzione normativa richiede alle organizzazioni di adottare strumenti avanzati per garantire la conformità e ridurre i rischi. Ad esempio, i sistemi digitali che monitorano transazioni in tempo reale e analizzano grandi volumi di dati consentono di identificare comportamenti anomali, rispondendo alle stringenti normative in ambiti come la protezione dei dati (GDPR) o la prevenzione del riciclaggio di denaro [12].

Innovazione e sviluppo di nuovi modelli di business

Infine, la trasformazione digitale è spesso guidata dalla necessità di innovare e creare nuovi modelli di business. L'adozione di tecnologie emergenti come il cloud computing, la blockchain e l'intelligenza artificiale ha permesso a molte organizzazioni di sviluppare servizi innovativi, espandendo le proprie opportunità di mercato. Un esempio è rappresentato dall'industria musicale, che ha abbandonato i modelli basati sulla vendita di supporti fisici per adottare piattaforme di streaming come Spotify, trasformando radicalmente il modo in cui i consumatori accedono ai contenuti [13].

Questi fattori evidenziano come la trasformazione digitale non sia solo una scelta strategica, ma una necessità per le organizzazioni che vogliono rimanere rilevanti, competitive e pronte a rispondere ai cambiamenti di mercato. Solo attraverso un cambiamento profondo e integrato è possibile cogliere appieno i benefici delle tecnologie digitali.

3.3 Criticità legate ai sistemi legacy, alla resistenza al cambiamento e alla compliance

La trasformazione digitale comporta sfide significative, spesso derivanti da fattori strutturali, culturali e normativi. Affrontare queste criticità richiede un approccio integrato e una pianificazione strategica che bilanci innovazione tecnologica, cambiamento organizzativo e conformità normativa.

Sistemi legacy: un ostacolo tecnologico

I sistemi legacy costituiscono una delle principali barriere alla trasformazione digitale. Queste infrastrutture obsolete, pur essendo ancora operative, non sono progettate per supportare tecnologie moderne, come il cloud computing o l'intelligenza artificiale. La loro integrazione con sistemi avanzati richiede spesso investimenti significativi in termini di risorse economiche e tecniche. Inoltre, la manutenzione di questi sistemi comporta costi elevati e limita la flessibilità operativa, ostacolando l'adozione di soluzioni innovative.

Resistenza al cambiamento: una sfida culturale

La trasformazione digitale non può prescindere dal coinvolgimento delle persone. Tuttavia, molte organizzazioni si scontrano con una resistenza diffusa al cambiamento. Questo fenomeno può derivare da diverse cause, tra cui l'incertezza sul futuro, la mancanza di competenze digitali e la paura di un'eventuale perdita di ruolo. Il successo della trasformazione digitale richiede quindi non solo l'introduzione di nuove tecnologie, ma anche una profonda trasformazione culturale, che favorisca l'adozione di mentalità orientate all'innovazione, alla collaborazione e all'adattabilità.

Compliance: un equilibrio tra innovazione e regolamentazione

L'evoluzione normativa rappresenta un ulteriore ostacolo per le organizzazioni che intendono intraprendere un percorso di trasformazione digitale. Regolamenti come il GDPR o le normative AML richiedono alle aziende di garantire una gestione rigorosa dei dati, introducendo al contempo misure per la protezione della privacy e la sicurezza delle informazioni. Questo equilibrio tra innovazione e conformità normativa può risultare complesso, in quanto le nuove tecnologie comportano spesso rischi aggiuntivi, come vulnerabilità di sicurezza o possibili violazioni delle normative. Le organizzazioni devono quindi adottare strumenti avanzati che non solo supportino l'innovazione tecnologica, ma garantiscano anche un controllo efficace e trasparente.

Superare le criticità legate ai sistemi legacy, alla resistenza al cambiamento e alla compliance richiede una visione strategica e un approccio multidisciplinare. Solo attraverso una modernizzazione progressiva delle infrastrutture, un cambiamento culturale ben gestito e una rigorosa attenzione alle normative, le organizzazioni possono affrontare con successo le sfide della trasformazione digitale, cogliendone appieno i benefici.

3.4 Confronto tra approccio waterfall e agile transformation nel contesto fintech e banking

La scelta del modello di sviluppo progettuale è un aspetto cruciale per il successo della trasformazione digitale, specialmente in settori come il fintech e il banking, dove l'innovazione tecnologica e la conformità normativa si intrecciano in modo complesso. Tra le metodologie più utilizzate si annoverano l'approccio waterfall, tradizionale e sequenziale, e l'agile transformation, iterativo e flessibile. Entrambi i modelli hanno punti di forza e debolezze che li rendono più o meno adatti a specifiche tipologie di progetti e contesti operativi.

3.4.1 Approccio waterfall: un modello tradizionale per progetti strutturati

Il modello waterfall è caratterizzato da una sequenza rigida e lineare di fasi, che comprendono analisi, progettazione, sviluppo, test e implementazione. Questo approccio è stato a lungo il paradigma dominante, specialmente in settori regolamentati come il banking, dove la stabilità e la prevedibilità dei processi sono essenziali.

Una delle principali caratteristiche del modello waterfall è la definizione rigorosa dei requisiti all'inizio del progetto. Questo permette di stabilire un piano dettagliato e di evitare ambiguità durante lo sviluppo. Tuttavia, questa stessa rigidità costituisce un limite nei contesti in cui i requisiti possono evolvere rapidamente, come nel fintech, dove le innovazioni tecnologiche o le modifiche normative possono richiedere aggiustamenti continui.

L'approccio waterfall è inoltre particolarmente indicato per progetti a lungo termine, in cui la completa definizione degli obiettivi iniziali è possibile e auspicabile. Tuttavia, la sua struttura sequenziale comporta che eventuali problemi identificati nelle fasi avanzate del progetto richiedano una revisione delle fasi precedenti, aumentando così i costi e i tempi di sviluppo.

3.4.2 Agile transformation: un paradigma di adattabilità e innovazione

L'approccio agile si è affermato come risposta alle limitazioni del modello waterfall, introducendo un paradigma più flessibile e iterativo. A differenza del waterfall, l'agile si basa sulla suddivisione dei progetti in iterazioni più brevi, chiamate sprint, che producono incrementi di valore tangibili e utilizzabili. Questa metodologia consente di incorporare feedback continui e di adattarsi rapidamente ai cambiamenti dei requisiti o alle esigenze di mercato.

Nel contesto fintech, l'agile transformation ha rivoluzionato il modo in cui vengono sviluppati nuovi prodotti e servizi. Ad esempio, l'adozione di team cross-funzionali consente una collaborazione più stretta tra sviluppatori, analisti di business e stakeholder, garantendo che il prodotto finale sia allineato alle reali necessità dei clienti. Inoltre, l'approccio agile facilita l'integrazione di tecnologie emergenti, come l'intelligenza artificiale e il machine learning, che richiedono iterazioni rapide per testare e ottimizzare i modelli.

Un altro elemento distintivo dell'agile è l'enfasi sulla comunicazione continua e trasparente. Le riunioni giornaliere (daily stand-up) e le revisioni regolari degli sprint assicurano che tutti i membri del team siano costantemente allineati sugli obiettivi e sugli avanzamenti del progetto, riducendo il rischio di incomprensioni o deviazioni dagli obiettivi prefissati.

3.4.3 Confronto tra i due approcci: criteri di valutazione

Per comprendere meglio le differenze tra i due modelli, è utile analizzarli attraverso alcuni criteri chiave:

- **Gestione dei requisiti**: Nel modello waterfall, i requisiti sono definiti in modo dettagliato all'inizio del progetto e rimangono invariati, a meno di costose modifiche successive. Nell'agile, invece, i requisiti sono flessibili e possono evolvere durante lo sviluppo, rendendo il processo più adattabile a cambiamenti improvvisi.

- **Flessibilità**: L'agile è intrinsecamente più flessibile grazie alla sua struttura iterativa, mentre il waterfall offre una maggiore stabilità, utile per progetti in cui i requisiti sono fissi e ben definiti.

- **Time-to-market**: L'agile consente di rilasciare funzionalità in modo incrementale, riducendo il time-to-market e permettendo di ottenere feedback dagli utenti finali già nelle fasi iniziali. Il modello waterfall, invece, richiede il completamento di tutte le fasi prima di consegnare il prodotto.

- **Documentazione**: Il waterfall si basa su una documentazione dettagliata e rigorosa, indispensabile per settori altamente regolamentati. L'agile, pur mantenendo una documentazione essenziale, pone maggiore enfasi sulla comunicazione diretta tra i membri del team.
- **Gestione del rischio**: Il modello waterfall può risultare più rischioso in caso di cambiamenti significativi nei requisiti o nel contesto di mercato, poiché richiede la revisione delle fasi precedenti. L'agile, invece, minimizza i rischi grazie alla continua integrazione e al feedback iterativo.

3.4.4 Impatti specifici nel contesto fintech e banking

Nel settore fintech e bancario, la scelta tra approccio waterfall e agile transformation è strettamente legata alle caratteristiche del progetto e agli obiettivi strategici. Sebbene il modello waterfall offra vantaggi in termini di tracciabilità e controllo, l'approccio agile ha dimostrato un valore superiore per rispondere alle sfide del fintech, un contesto caratterizzato da innovazione rapida, alta competizione e requisiti normativi in continua evoluzione.

Adattabilità ai cambiamenti normativi e di mercato

Una delle principali sfide nel fintech è la necessità di adattarsi rapidamente ai cambiamenti, sia normativi che di mercato. L'approccio agile, grazie alla sua struttura iterativa e incrementale, consente di integrare i cambiamenti in modo continuo e progressivo, riducendo al minimo il rischio di ritardi o inefficienze. Ad esempio, nel caso di modifiche alle normative AML (Anti-Money Laundering) o alla PSD2 (Payment Services Directive), i team agili possono aggiornare le funzionalità di una piattaforma di pagamento in tempi brevi, incorporando i nuovi requisiti senza compromettere la continuità operativa.

Time-to-market e innovazione continua

Un vantaggio cruciale dell'approccio agile nel fintech è la riduzione del time-to-market. Le organizzazioni che adottano l'agile possono rilasciare funzionalità incrementali in modo più rapido rispetto al waterfall, ottenendo feedback dai clienti già nelle prime fasi dello sviluppo. Questa capacità di iterare rapidamente consente non solo di migliorare continuamente il prodotto, ma anche di rispondere alle mutevoli esigenze dei consumatori, che nel fintech sono particolarmente esigenti in termini di usabilità, sicurezza e velocità.

Ad esempio, nella creazione di una nuova app mobile per il banking, un team agile può concentrarsi inizialmente sul rilascio di funzionalità essenziali, come il monitoraggio del saldo e i trasferimenti di denaro. Le funzionalità più complesse,

come l'integrazione con strumenti di budgeting o servizi di investimento, possono essere sviluppate in iterazioni successive, garantendo al contempo una rapida penetrazione nel mercato e una progressiva ottimizzazione basata sui feedback degli utenti.

Questo approccio si chiama MVP (Minimum valuable product).

Collaborazione tra team e stakeholder

Il fintech si distingue per la necessità di integrare competenze interdisciplinari, come tecnologia, finanza, regolamentazione e user experience. L'approccio agile, grazie alla struttura dei team cross-funzionali, promuove una collaborazione continua tra sviluppatori, analisti, esperti legali e stakeholder. Questo processo iterativo garantisce che ogni componente del progetto risponda sia ai requisiti tecnici che alle esigenze normative, riducendo il rischio di discrepanze o malintesi.

Gestione del rischio e mitigazione degli errori

Nel settore fintech, il rischio operativo è una preoccupazione primaria, considerando la delicatezza delle informazioni finanziarie e la necessità di garantire elevati standard di sicurezza. L'approccio agile riduce il rischio complessivo grazie alla continua integrazione e ai test iterativi, che identificano e correggono errori nelle prime fasi dello sviluppo. Ciò è particolarmente utile per i progetti fintech, in cui anche piccoli errori possono avere conseguenze significative in termini di conformità normativa o sicurezza dei dati.

Un ulteriore beneficio è la possibilità di rilasciare aggiornamenti incrementali, limitando l'impatto di eventuali errori. Questo approccio differisce dal waterfall, dove problemi rilevati nelle fasi avanzate possono richiedere modifiche costose e ritardi significativi.

Flessibilità per integrare tecnologie emergenti

L'agile è particolarmente efficace nel contesto fintech per la sua capacità di integrare rapidamente tecnologie emergenti, come intelligenza artificiale, blockchain e machine learning. Queste tecnologie, che richiedono test frequenti e aggiornamenti continui, si sposano perfettamente con la natura iterativa dell'agile.

Cultura dell'innovazione e centralità del cliente

Infine, l'approccio agile favorisce una cultura aziendale incentrata sull'innovazione e sul cliente. Nel fintech, dove la competizione è elevata e la fidelizzazione dei clienti è essenziale, questa mentalità si traduce in prodotti che non solo soddisfano le esigenze funzionali, ma offrono anche un'esperienza utente superiore. Grazie

all'agile, le organizzazioni possono mantenere il cliente al centro del processo di sviluppo, utilizzando feedback continui per migliorare l'usabilità, la sicurezza e le prestazioni dei prodotti.

L'approccio agile offre un chiaro vantaggio competitivo, consentendo alle organizzazioni di rispondere rapidamente ai cambiamenti normativi, accelerare l'innovazione e migliorare l'esperienza cliente. La sua flessibilità, la capacità di integrare tecnologie emergenti e la promozione di una collaborazione interdisciplinare lo rendono uno strumento indispensabile per affrontare le sfide di un mercato in continua evoluzione. Tuttavia, il successo dell'agile richiede un impegno culturale significativo, un supporto tecnologico adeguato e una gestione efficace dei processi, elementi che devono essere attentamente considerati in ogni iniziativa di trasformazione digitale.

In conclusione, l'approccio waterfall e l'agile transformation rappresentano due filosofie progettuali complementari, ognuna con i propri punti di forza e limitazioni. La trasformazione digitale nel settore fintech e bancario richiede spesso una combinazione di entrambi gli approcci, adottando il modello più adatto in base alle specifiche esigenze del progetto. Una valutazione attenta dei requisiti, delle risorse disponibili e delle condizioni di mercato è fondamentale per massimizzare i benefici e mitigare i rischi associati a ciascuna metodologia.

3.5 Benefici della trasformazione digitale: scalabilità, efficienza e conformità normativa

La trasformazione digitale rappresenta un'opportunità senza precedenti per migliorare le prestazioni organizzative, ottimizzare i processi e garantire la conformità normativa. In particolare, tre benefici chiave emergono come fondamentali: la scalabilità, l'efficienza e il miglioramento delle capacità di conformità alle normative. Questi vantaggi, se ben implementati, possono trasformare le organizzazioni in entità più resilienti, competitive e innovative.

Scalabilità: un pilastro per la crescita e l'innovazione

La scalabilità rappresenta uno dei principali vantaggi della trasformazione digitale, consentendo alle organizzazioni di adattarsi rapidamente ai cambiamenti della domanda o di espandersi verso nuovi mercati. L'adozione di tecnologie basate su cloud, ad esempio, offre alle aziende la possibilità di aumentare o ridurre dinamicamente le risorse IT in base alle necessità operative, senza dover sostenere i costi fissi di infrastrutture fisiche.

Nel contesto digitale, la scalabilità non si limita alla capacità tecnologica, ma si estende ai processi aziendali. Sistemi automatizzati e flessibili permettono di gestire volumi crescenti di transazioni o richieste dei clienti senza compromettere la qualità del servizio. Questo è particolarmente cruciale nei settori come il fintech e il banking, dove l'aumento della clientela o delle transazioni richiede una capacità operativa proporzionale e immediata.

Efficienza: ottimizzazione dei processi e riduzione dei costi

Un altro beneficio fondamentale della trasformazione digitale è l'aumento dell'efficienza operativa. L'automazione dei processi, supportata da tecnologie come il robotic process automation (RPA) e l'intelligenza artificiale, consente di eliminare attività ripetitive e dispendiose in termini di tempo, riducendo al minimo l'errore umano e migliorando la produttività complessiva.

La digitalizzazione delle informazioni e dei flussi di lavoro rende inoltre possibile la gestione centralizzata dei dati, facilitando l'accesso e la condivisione tra i team. Ciò non solo accelera i processi decisionali, ma riduce anche i costi operativi legati a inefficienze come la duplicazione di dati o la mancanza di comunicazione tra reparti. Ad esempio, l'utilizzo di dashboard interattive consente ai manager di monitorare in tempo reale le performance aziendali, identificando rapidamente eventuali aree critiche da ottimizzare.

Conformità normativa: garantire trasparenza e ridurre i rischi

La crescente complessità del panorama normativo rende la conformità un aspetto critico per le organizzazioni moderne. La trasformazione digitale offre strumenti avanzati per garantire il rispetto delle normative, riducendo i rischi di non conformità che possono portare a sanzioni o danni reputazionali.

L'implementazione di soluzioni digitali, come i sistemi di gestione automatizzata della compliance, consente alle organizzazioni di monitorare e documentare ogni attività in modo trasparente e tracciabile. Inoltre, l'adozione di piattaforme di governance dei dati garantisce una gestione centralizzata e sicura delle informazioni sensibili, migliorando la capacità delle organizzazioni di rispondere alle richieste di audit e di segnalazione da parte delle autorità regolatorie. Questo approccio non solo riduce il rischio di violazioni normative, ma aumenta anche la fiducia degli stakeholder, inclusi clienti, partner e investitori.

La trasformazione digitale, con i suoi benefici in termini di scalabilità, efficienza e conformità normativa, non è più un'opzione, ma una necessità strategica per le organizzazioni moderne. Questi vantaggi, se integrati in una visione globale e supportati da una gestione efficace, possono garantire alle aziende una maggiore

competitività e una resilienza a lungo termine, permettendo di affrontare con successo le sfide di un mercato in costante evoluzione.

Capitolo 4

Controlli di conformità PEP e OFAC

In questo capitolo viene trattato il primo vero contributo sul quale ho lavorato durante l'esperienza di tirocinio. La fase di implementazione, inserita nel capitolo successivo, è stata preceduta da un'attenta e rigorosa analisi teorica riguardante i controlli PEP e OFAC, inserta in questo capitolo. Prima della fase di sviluppo, è fondamentale aver compreso a fondo l'argomento trattato per poter avere una visione logica complessiva di ciò che si sta andando ad implementare.

4.1 Definizione e ambito applicativo

I controlli di conformità PEP (Politically Exposed Person) e OFAC (Office of Foreign Assets Control) rappresentano strumenti fondamentali per garantire la sicurezza e l'integrità del sistema finanziario globale. Questi controlli sono progettati per prevenire il riciclaggio di denaro, il finanziamento del terrorismo e altre attività illecite attraverso il monitoraggio rigoroso delle transazioni finanziarie e l'identificazione di individui o entità ad alto rischio.

4.1.1 Controlli PEP: identificazione delle persone politicamente esposte

Le PEP sono definite come individui che ricoprono o hanno ricoperto ruoli pubblici di alto livello, come capi di stato, ministri, parlamentari, giudici di corti supreme o dirigenti di organizzazioni internazionali. Questi individui, a causa della loro posizione e influenza, sono considerati a rischio maggiore di coinvolgimento in attività di corruzione o riciclaggio di denaro.

I controlli PEP si concentrano sull'identificazione e sulla valutazione dei rischi associati alle transazioni o ai rapporti commerciali con queste persone. La normativa internazionale, come le raccomandazioni del GAFI (Gruppo di Azione Finanziaria Internazionale), richiede alle istituzioni finanziarie di adottare procedure specifiche per monitorare le attività delle PEP, garantendo che ogni transazione sia conforme ai requisiti normativi. L'ambito di applicazione include l'identificazione di legami familiari o stretti collaboratori delle PEP, ampliando così il raggio d'azione dei controlli [14].

4.1.2 Controlli OFAC: sanzioni economiche e monitoraggio delle transazioni

L'OFAC è un'agenzia del Dipartimento del Tesoro degli Stati Uniti responsabile dell'amministrazione e dell'applicazione delle sanzioni economiche contro stati, organizzazioni o individui coinvolti in attività illecite, come il terrorismo o il traffico di droga. Le sanzioni imposte dall'OFAC possono includere il congelamento di beni, il divieto di transazioni finanziarie o altre restrizioni economiche.

I controlli OFAC sono progettati per garantire che le istituzioni finanziarie non facilitino, intenzionalmente o meno, attività che violano le sanzioni statunitensi. Questo richiede una rigorosa verifica delle transazioni in tempo reale, utilizzando database aggiornati che elencano individui ed entità soggette a restrizioni. L'ambito applicativo degli strumenti OFAC si estende a livello globale, coinvolgendo non solo istituzioni americane, ma anche operatori stranieri che intrattengono rapporti con il sistema finanziario statunitense [15].

4.1.3 Complementarità e rilevanza globale

I controlli PEP e OFAC, sebbene distinti per natura e obiettivi, sono complementari nella lotta contro le attività illecite. Mentre i controlli PEP si concentrano sulla prevenzione della corruzione e del riciclaggio legati a persone di rilievo pubblico, i controlli OFAC mirano a proteggere il sistema finanziario globale da minacce più ampie, come il finanziamento del terrorismo e la proliferazione di armi.

Entrambi i sistemi operano su scala globale, riflettendo la crescente interdipendenza dei mercati finanziari internazionali. La loro applicazione rigorosa è cruciale non solo per garantire la conformità normativa, ma anche per preservare la fiducia degli investitori e dei consumatori nei mercati finanziari. Nel contesto della trasformazione digitale, questi controlli sono stati ulteriormente potenziati grazie all'adozione di tecnologie avanzate, come l'intelligenza artificiale e il machine learning, che migliorano l'efficienza e la precisione delle verifiche.

La definizione e l'ambito applicativo dei controlli PEP e OFAC sottolineano la loro importanza strategica per la sicurezza del sistema finanziario globale. La loro implementazione efficace richiede non solo tecnologie all'avanguardia, ma anche una profonda comprensione delle normative internazionali e delle dinamiche del rischio. Questi controlli rappresentano una risposta integrata alle sfide poste da un panorama economico e normativo in continua evoluzione.

4.2 Caratteristiche dei controlli PEP e OFAC

I controlli PEP e OFAC si distinguono per specificità operative e funzionalità, rispondendo a esigenze di compliance normative con approcci complementari. Entrambi i sistemi offrono strumenti essenziali per gestire rischi complessi e garantire l'integrità del sistema finanziario globale.

4.2.1 Specificità dei controlli PEP

I controlli PEP si concentrano sull'analisi e la gestione dei rischi legati a individui politicamente esposti, con un focus su tre aspetti fondamentali:

- *Profilazione dinamica del rischio*: le PEP sono valutate in base a parametri che includono il ruolo ricoperto, la durata dell'incarico e il contesto giurisdizionale. Questo approccio consente una classificazione del rischio più precisa e aggiornata.

- *Monitoraggio reputazionale*: l'analisi non si limita a database istituzionali, ma si estende a fonti aperte, come articoli di stampa e report investigativi, per identificare potenziali segnali di allerta.

- *Analisi delle connessioni*: attraverso strumenti avanzati, è possibile tracciare legami tra una PEP e altre entità o individui, individuando reti sospette e relazioni rilevanti.

4.2.2 Specificità dei controlli OFAC

I controlli OFAC si distinguono per la loro capacità di implementare sanzioni economiche in modo efficace e tempestivo. Le principali caratteristiche includono:

- *Efficienza operativa*: Gli algoritmi di matching identificano rapidamente transazioni e soggetti che corrispondono alle liste di sanzioni, minimizzando il rischio di errori.

- *Integrazione globale*: Le normative OFAC influenzano transazioni transfrontaliere, richiedendo una perfetta compatibilità con i sistemi di compliance internazionali.
- *Aggiornamenti costanti*: Le liste OFAC sono aggiornate regolarmente, riflettendo modifiche normative e nuove designazioni, e garantiscono una conformità continua.

4.2.3 Ruolo delle tecnologie avanzate

L'integrazione di tecnologie avanzate nei controlli PEP e OFAC ne amplifica l'efficienza e la capacità di risposta. Sistemi basati sull'intelligenza artificiale e sull'automazione offrono vantaggi significativi:

- Elaborazione in tempo reale di grandi volumi di dati, migliorando la tempestività nell'identificazione di anomalie.
- Riduzione del carico operativo dei team di compliance, che possono concentrarsi su analisi qualitative più complesse.
- Capacità predittive che consentono di anticipare rischi emergenti, grazie a modelli analitici basati su dati storici e scenari simulati.

Le caratteristiche dei controlli PEP e OFAC riflettono una combinazione unica di rigore normativo e innovazione tecnologica. La loro efficacia dipende dalla capacità di adattarsi ai cambiamenti normativi e di sfruttare strumenti tecnologici per migliorare la protezione e la trasparenza del sistema finanziario globale.

4.3 Analisi approfondita dei requisiti e delle funzionalità

L'efficacia dei controlli di conformità PEP e OFAC dipende dalla loro capacità di soddisfare requisiti normativi complessi e di implementare funzionalità tecnologiche avanzate. Questa sezione esamina nel dettaglio i principali requisiti operativi e le funzionalità chiave di entrambi i sistemi, evidenziando il loro ruolo nella gestione del rischio e nella garanzia di conformità.

4.3.1 Requisiti operativi dei controlli PEP e OFAC

I requisiti operativi sono fondamentali per assicurare che i controlli PEP e OFAC rispondano efficacemente alle aspettative normative e aziendali. Questi requisiti si articolano in:

- *Accuratezza e tempestività*: I controlli devono garantire un monitoraggio in tempo reale e un'accurata identificazione di individui, entità o transazioni ad alto rischio. L'utilizzo di database globali aggiornati e algoritmi di matching avanzati è essenziale per raggiungere questo obiettivo.

- *Tracciabilità e auditabilità*: Ogni transazione o attività di verifica deve essere documentata in modo dettagliato, consentendo una completa tracciabilità delle decisioni prese e facilitando i processi di audit.

- *Adattabilità normativa*: I sistemi devono essere in grado di integrarsi rapidamente con nuovi requisiti regolatori, come quelli legati a modifiche normative o a liste di sanzioni aggiornate.

- *Protezione dei dati*: Data la natura sensibile delle informazioni trattate, i controlli devono rispettare standard rigorosi di sicurezza e privacy, come il GDPR in Europa o le normative equivalenti in altre giurisdizioni.

4.3.2 Sfide e opportunità nell'implementazione

Nonostante i significativi progressi tecnologici, l'implementazione dei controlli PEP e OFAC presenta ancora alcune sfide, come:

- *Integrazione con sistemi esistenti*: integrare queste funzionalità con infrastrutture legacy può risultare complesso e costoso, richiedendo investimenti significativi in termini di tempo e risorse.

- *Falsi positivi*: un problema ricorrente è la generazione di falsi positivi, che possono aumentare il carico di lavoro manuale e rallentare le operazioni. Tuttavia, l'uso di algoritmi avanzati e l'automazione intelligente stanno riducendo progressivamente questo problema.

- *Compliance multi-giurisdizionale*: le organizzazioni globali devono adattare i controlli PEP e OFAC a normative diverse, garantendo che ogni transazione rispetti i requisiti locali e internazionali.

Un'analisi approfondita dei requisiti e delle funzionalità dei controlli PEP e OFAC evidenzia la loro importanza strategica nella gestione del rischio e nella conformità normativa. La loro efficacia dipende dalla capacità di integrare requisiti complessi e funzionalità avanzate in un sistema unico, che possa rispondere alle esigenze operative e regolatorie di un panorama finanziario globale in continua evoluzione.

4.4 Criticità affrontate e problemi risolti dai controlli di conformità

I controlli di conformità PEP e OFAC rappresentano strumenti indispensabili per affrontare le sfide che emergono nel sistema finanziario globale. Questi controlli sono progettati per risolvere criticità di natura operativa, normativa e reputazionale, garantendo al contempo una maggiore sicurezza e trasparenza nelle transazioni.

4.4.1 Criticità operative

Le problematiche operative sono tra le più evidenti per le istituzioni finanziarie che gestiscono un volume crescente di dati e transazioni. I processi tradizionali, spesso caratterizzati da manualità, risultano inadeguati nel contesto attuale, poiché:

- La gestione di grandi quantità di informazioni comporta un rischio elevato di errore umano.
- La lentezza nei processi manuali ostacola l'efficienza operativa e aumenta i costi aziendali.
- L'assenza di sistemi automatizzati riduce la capacità di identificare anomalie e comportamenti sospetti in tempo reale.

L'introduzione di algoritmi avanzati e l'automazione dei processi hanno permesso di superare queste limitazioni, migliorando la capacità di gestione del rischio e riducendo i tempi di elaborazione delle transazioni.

4.4.2 Criticità normative

Il contesto normativo globale è caratterizzato da requisiti sempre più complessi e da frequenti aggiornamenti legislativi. Tra le principali sfide si evidenziano:

- La necessità di garantire conformità simultanea a normative di giurisdizioni diverse, che spesso presentano differenze sostanziali.
- L'adattamento rapido a nuove regolamentazioni o a modifiche delle liste PEP e OFAC, che richiedono una revisione continua delle procedure.
- L'obbligo di garantire tracciabilità e trasparenza per soddisfare le richieste di audit e supervisione normativa.

I controlli di conformità affrontano queste problematiche integrando strumenti tecnologici capaci di adattarsi dinamicamente ai cambiamenti normativi e garantendo una conformità continua senza interruzioni operative.

4.4.3 Criticità reputazionali

La fiducia nel sistema finanziario è strettamente legata alla capacità delle organizzazioni di garantire la conformità normativa e di prevenire scandali. I rischi principali in questo ambito includono:

- Il danno reputazionale causato dall'associazione a pratiche illecite, come il riciclaggio di denaro o il finanziamento del terrorismo.
- La perdita di fiducia da parte di clienti e investitori, che può tradursi in una riduzione del valore di mercato dell'organizzazione.
- L'impatto negativo sulla fidelizzazione della clientela, soprattutto in mercati competitivi dove la sicurezza è un fattore chiave di scelta.

Grazie alla trasparenza e alla capacità di prevenzione offerte dai controlli PEP e OFAC, le organizzazioni possono mitigare significativamente questi rischi e rafforzare la loro reputazione.

4.4.4 Conclusione: problemi risolti dai controlli di conformità

In conclusione, i controlli PEP e OFAC offrono soluzioni concrete per risolvere le problematiche sopra descritte. In particolare:

- Automatizzano processi complessi, riducendo il rischio di errori umani e migliorando l'efficienza operativa.
- Consentono un adattamento rapido a cambiamenti normativi, mantenendo la conformità anche in contesti giurisdizionali complessi.
- Offrono strumenti avanzati di analisi e monitoraggio, che migliorano la capacità di rilevare e prevenire attività sospette.
- Rafforzano la fiducia degli stakeholder attraverso una maggiore trasparenza e tracciabilità delle operazioni.

Le criticità affrontate dai controlli PEP e OFAC evidenziano l'importanza di strumenti tecnologici avanzati nella gestione del rischio e nella conformità normativa. La loro implementazione non solo risolve problemi operativi, normativi e reputazionali, ma rappresenta anche un investimento strategico per costruire un sistema finanziario più resiliente e sicuro.

Capitolo 5

Implementazione dei controlli di conformità PEP e OFAC

5.1 Introduzione alle attività di implementazione

Questo capitolo illustra lo sviluppo svolto durante il tirocinio, focalizzandosi sull'implementazione pratica di controlli di conformità PEP e OFAC. Vengono descritte le soluzioni sviluppate, il loro impatto operativo e l'approccio tecnico seguito per garantire una conformità efficace e scalabile.

5.2 Illustrazione delle attività pratiche svolte durante il tirocinio

5.2.1 Obiettivi delle implementazioni

In questa sezione vengono presentati gli obiettivi specifici delle implementazioni svolte, includendo:

- Automazione dei controlli per ridurre il carico operativo manuale.
- Miglioramento dell'accuratezza nell'identificazione dei rischi PEP e OFAC.
- Gestione dei matching riscontrati durante i controlli.

Siccome le implementazioni di PEP e OFAC, dal punto di vista del codice, sono molto simili, mi concentrerò su quanto sviluppato per i controlli PEP.

5.2.2 Descrizione del contesto operativo

Il progetto su cui si è concentrato il tirocinio ha riguardato lo sviluppo e l'implementazione di una piattaforma fintech per l'elaborazione dei pagamenti e delle transazioni finanziarie. La piattaforma è stata progettata per operare in un ecosistema gerarchico composto da tre ruoli principali: acquirer, provider e merchant, ciascuno con compiti specifici e ben definiti.

- *Acquirer*: rappresenta il vertice della piramide operativa e svolge un ruolo centrale nell'autorizzazione delle transazioni. Può essere identificato, ad esempio, in una banca o in un'istituzione finanziaria che offre servizi di pagamento per conto dei merchant.
- *Provider*: agisce come intermediario tecnico e operativo: un esempio tipico di provider potrebbe essere una società di servizi tecnologici che gestisce le infrastrutture necessarie per l'elaborazione delle transazioni, come gateway di pagamento o piattaforme di tokenizzazione.
- *Merchant*: sono le aziende che forniscono beni o servizi direttamente ai clienti finali. In un caso pratico, un negozio online di e-commerce rappresenterebbe il merchant, mentre il provider sarebbe il gateway di pagamento utilizzato dal negozio per elaborare i pagamenti e l'acquirer la banca che gestisce le transazioni per conto del merchant.

La piattaforma è stata sviluppata per garantire scalabilità, sicurezza e conformità alle normative internazionali. L'architettura del sistema utilizza tecnologie avanzate per assicurare la gestione efficiente di un elevato volume di transazioni, offrendo al contempo un alto livello di integrazione tra i diversi attori coinvolti.

Nell'ambito di questo progetto, come già citato in precedenza, mi sono occupato dell'implementazione del **backend** per i controlli PEP e OFAC.

Questi controlli sono stati specificamente sviluppati per monitorare tre ruoli chiave associati ai merchants: la legal entity, il business owner e il primary account holder.

- *Legal entity*: si riferisce all'entità giuridica registrata presso il merchant, come una società o un'organizzazione. Ad esempio, una grande azienda che utilizza la piattaforma per gestire i propri pagamenti.
- *Business owner*: rappresenta il proprietario dell'azienda o il soggetto che detiene il controllo decisionale. Ad esempio, il fondatore o amministratore delegato della società registrata.
- *Primary account holder*: indica l'utente principale associato al conto aziendale, responsabile della gestione operativa delle transazioni. Un esempio potrebbe essere il responsabile finanziario o contabile dell'azienda.

Ogni volta che un nuovo utente con uno di questi ruoli viene aggiunto alla piattaforma o quando vengono apportate modifiche a un profilo esistente, vengono eseguiti automaticamente i controlli di conformità PEP e OFAC. Ad esempio, se una società registra un nuovo amministratore delegato come business owner, il sistema esegue immediatamente una verifica nei database PEP e OFAC per identificare eventuali rischi associati al soggetto.

Per gestire i controlli PEP e OFAC all'interno della piattaforma, è stata sviluppata una logica proprietaria che assegna uno status specifico a ciascun controllo eseguito. Gli status non sono generati direttamente dai database PEP e OFAC, ma sono stati definiti internamente per garantire una gestione strutturata e tracciabile delle verifiche. Gli status implementati sono i seguenti:

- *Clear*: Indica che non sono state trovate corrispondenze nelle liste PEP o OFAC per l'utente o l'entità verificata.

- *Possibile match*: Indica una possibile corrispondenza con le liste di controllo, rilevata sulla base di somiglianze nei dati (ad esempio, nome o identificativi parziali).

- *Manually cleared*: Questo status viene impostato manualmente dall'underwriter, dopo aver esaminato un possibile match e aver determinato che non rappresenta un rischio effettivo. Per ogni successivo check eseguito su quella risorsa, se la risposta da PEP e OFAC è la medesima del check precedente, lo status viene settato a *clear*, altrimenti nel caso sia stato riscontrato un match diverso dal precedente (lo determiniamo effettuando un confronto tra i due json ritornati dall'API), lo status viene settato a "possible match" nuovamente.

- *Confirmed match*: Lo status viene impostato manualmente dall'underwriter quando la corrispondenza individuata è verificata e confermata come rilevante per le liste PEP o OFAC.

Ogni volta che un controllo viene eseguito su un utente o un'entità, il sistema assegna automaticamente uno status iniziale basato sui risultati della verifica. Nel caso di uno status di *possibile match*, le API forniscono un set dettagliato di informazioni in formato JSON, che include i dati rilevanti sulla corrispondenza riscontrata. Gli underwriter analizzano ogni risorsa con i rispettivi controlli di conformità in modo approfondito e, se necessario, aggiornano manualmente lo status a *manually cleared* o *confirmed match*. Lo status *confirmed match* può anche venire settatto a seguito di un sistema di challenge che l'utente deve superare, ma questo argomento esula dalla mia attività di tirocinio.

5.2.3 Panoramica degli strumenti e tecnologie utilizzati

L'implementazione dei controlli di conformità PEP e OFAC è stata realizzata utilizzando un insieme di strumenti e tecnologie avanzate che garantiscono l'efficienza, la scalabilità e la mantenibilità del sistema. La scelta tecnologica è stata guidata dalle esigenze specifiche del progetto e dalla necessità di integrare funzionalità complesse in un ambiente strutturato e facilmente gestibile.

Linguaggio di programmazione e framework custom

Il backend dell'applicazione è stato sviluppato utilizzando **Golang**, un linguaggio noto per le sue prestazioni elevate, la semplicità sintattica e il supporto nativo alla concorrenza. Tuttavia, per rispondere alle esigenze specifiche del progetto, è stato utilizzato un framework custom che struttura il codice backend secondo un approccio modulare basato su endpoint, handler e procedure.

Ogni handler e ogni procedure all'interno del sistema è stato organizzato seguendo una sequenza di step ben definiti, che consentono di mantenere il flusso logico chiaro e facilmente estendibile:

- **New**: Inizializzazione dello stato e dei parametri necessari.
- **BeforeValidate**: Preparazione dei dati e verifica preliminare delle condizioni.
- **Validate**: Validazione delle informazioni in ingresso.
- **BeforeExecute**: Esecuzione di eventuali operazioni preparatorie.
- **Execute**: Esecuzione principale della logica di business associata alla procedure.
- **AfterExecute**: Finalizzazione e restituzione dei risultati, con eventuali operazioni post-esecuzione.

Questa struttura permette di garantire modularità, riusabilità del codice e un controllo preciso del flusso operativo.

Gestione del database

Il sistema utilizza **PostgreSQL** come database relazionale per la persistenza dei dati. L'interazione con il database è facilitata tramite un **ORM** (Object Relational Mapping) chiamato **gosql**, una libreria ottimizzata per Go che consente di astrarre le operazioni SQL e semplificare la gestione delle query.

Per mantenere un controllo rigoroso sulle modifiche apportate al database nel corso del progetto, è stato adottato un sistema di **migrations**. Questo sistema permette di gestire il versionamento del database, applicare in modo incrementale

le modifiche alla struttura delle tabelle e garantire che ogni ambiente (sviluppo, staging e produzione) utilizzi la stessa configurazione dei dati.

Containerizzazione e deployment

L'intera applicazione è stata dockerizzata per garantire un ambiente di esecuzione uniforme e indipendente dall'infrastruttura sottostante. Ogni componente del sistema viene eseguito in un container Docker separato, facilitando la scalabilità e la gestione delle risorse. La containerizzazione assicura che il sistema sia facilmente replicabile e deployabile su qualsiasi infrastruttura compatibile con Docker.

Il processo di **deploy** viene automatizzato tramite **Jenkins**, uno strumento di Continuous Integration e Continuous Deployment (CI/CD). Jenkins permette di orchestrare il rilascio dell'applicazione, eseguire test automatici e assicurare un aggiornamento continuo delle funzionalità, riducendo al minimo i tempi di fermo e garantendo l'affidabilità del sistema.

Sintesi

La combinazione di queste tecnologie — dal framework custom basato su Golang, all'ORM gosql per PostgreSQL, fino alla containerizzazione con Docker e il deploy automatizzato tramite Jenkins — ha reso possibile l'implementazione di un sistema efficiente, modulare e conforme ai requisiti di scalabilità e manutenibilità richiesti dal progetto.

5.3 Esempi concreti e documentazione delle implementazioni

5.3.1 Esempio 1: esecuzione di un PEP check su una risorsa

Nuovo handpoint

E' stato definito un nuovo endpoint per la creazione di un PEP check su una risorsa. Tale risorsa è associata ad uno specifico merchant.

```
{
    "P":
    ↪  "/merchants/<merchant_id>/resources/<resource_type_id>/pep-checks/<resource_id>",
    "M": "POST",
    "H": "screenapi.PEPCheckCreateHandler{}",
    "A": {
        "RNT": "gs:rn:merchant:$1:pep:$2",
        "RA": "create",
        "EON": "merchant.MERCHANT_UNDERWRITING"
    },
    "FF": {
        "Name": "be_pep_new",
        "HasRollout": true
    }
}
```

L'URL dell'endpoint è strutturato come segue:

`/merchants/<merchant_id>/resources/<resource_type_id>/pep-checks/<resource_id>`

- `/merchants/<merchant_id>`: Identifica l'ID del merchant proprietario della risorsa. Questo parametro è utilizzato per associare il PEP check al contesto specifico di un merchant registrato sulla piattaforma.
- `/resources/<resource_type_id>`: Specifica il tipo di risorsa che deve essere verificata. Questo parametro consente di distinguere tra diverse categorie di risorse (legal entity, business owner o primary account holder).
- `/pep-checks/<resource_id>`: Indica l'ID della risorsa (utente) da sottoporre al PEP check.

L'endpoint utilizza il metodo HTTP `POST`, poiché si tratta di un'operazione che crea una nuova risorsa lato server. L'implementazione è gestita dall'handler `screenapi.PEPCheckCreateHandler`.

La configurazione include anche un riferimento a un `feature flag`, definito come `be_pep_new`, che regola l'attivazione o meno dell'endpoint, essendo una nuova implementazione. Questo sistema permette di gestire gradualmente il rilascio della nuova funzionalità e di abilitare la nuova implementazione, secondo le necessità operative e solo dopo che il QA team ha effettuato i feature tests, con lo scopo di evitare regression.

Ruolo dell'handler PEPCheckCreateHandler

L'handler `PEPCheckCreateHandler` è responsabile dell'elaborazione della richiesta e dell'esecuzione della logica associata al PEP check. Dopo aver eseguito i controlli preliminari di validazione sull'input ricevuto, l'handler chiama la procedure specifica.

Un frammento di codice significativo all'interno dell'handler è il seguente:

```
1  func (h *PEPCheckCreateHandler) Execute() error {
2      proc := new(screenproc.PEPCheckCreateProcedure)
3      proc.AccID = h.accID
4      proc.ResourceTypeName = audit.ResourceTypeName(h.resourceType.Name)
5      proc.ResourceID = h.resourceID
6      if err := h.PX.Exec(h.Ctx, proc); err != nil {
7          return err
8      }
9
10     h.pepID = proc.PEPCheck.ID
11
12     return nil
13 }
```

Questo codice illustra come l'handler:

- Inizializza una nuova istanza della procedure `PEPCheckCreateProcedure`.
- Assegna i parametri necessari alla procedure, come l'`AccID` (merchant id), il tipo di risorsa e il suo ID.
- Esegue la procedure tramite il contesto applicativo (`h.PX.Exec`), gestendo eventuali errori.
- Recupera l'ID del PEP check appena creato (`h.pepID = proc.PEPCheck.ID`) e lo rende disponibile per ulteriori elaborazioni (partendo dall'ID, tramite una query, possiamo ritornare al frontend la view con tutte le informazioni necessarie).

Questo approccio modulare consente di separare la logica dell'handler dalla logica di business implementata nella procedure, migliorando la leggibilità e la manutenibilità del codice.

Mapping della richiesta/risposta alle API del database di PEP

Prima di analizzare nel dettaglio la logica della procedure, è necessario spiegare come sono state mappate sia la richiesta che la risposta delle API del database PEP utilizzando delle *struct* specifiche, al fine di garantire una gestione chiara e strutturata dei dati. Di seguito è riportata la definizione delle *struct* utilizzate:

```
type PEPCheckRequest struct {
        FullName    string
        BirthDate   string
        TaxIDNumber string
        Response    PEPCheckResponse
}
```

La richiesta contiene i dati principali della risorsa da verificare, inclusi nome completo, data di nascita e codice fiscale (`TaxIDNumber`), oltre alla struttura per la risposta `PEPCheckResponse`.

La risposta ricevuta dall'API è rappresentata come segue:

```
type PEPCheckResponse struct {
        Responses PEPCheckEntity `json:"responses"`
}
```

`PEPCheckResponse` include una singola proprietà `Responses`, che mappa ulteriori dettagli sul risultato del controllo, descritti nella struttura `PEPCheckEntity`:

```
type PEPCheckEntity struct {
        Entity PEPCheckEntityStatusResultsAndTotal `json:"entity"`
}
```

La struttura `PEPCheckEntityStatusResultsAndTotal` contiene tre campi principali: lo `Status` dell'entità, i `Results` del controllo e il totale delle corrispondenze trovate.

```
type PEPCheckEntityResults struct {
        Id         string                      `json:"id"`
        Schema     string                      `json:"schema"`
        Properties PEPCheckResponseProperties `json:"properties"`
        Datasets   []string                    `json:"datasets"`
        Referents  []string                    `json:"referents"`
        Target     bool                        `json:"target"`
        FirstSeen  string                      `json:"first_seen"`
        LastSeen   string                      `json:"last_seen"`
        LastChange string                      `json:"last_change"`
        Score      float32                     `json:"score"`
        Features   PEPCheckResponseFeatures    `json:"features"`
        Match      bool                        `json:"match"`
}
```

Ogni risultato include dettagli approfonditi sull'entità, come gli identificativi (`Id`), il punteggio di similarità (`Score`) e un insieme di proprietà che descrivono le caratteristiche rilevanti.

Le proprietà specifiche sono mappate tramite la struttura `PEPCheckResponseProperties`:

```
type PEPCheckResponseProperties struct {
        Position      []string `json:"position"`
        Name          []string `json:"name"`
        Alias         []string `json:"alias"`
        Notes         []string `json:"notes"`
        Gender        []string `json:"gender"`
        AddressEntity []string `json:"addressEntity"`
        BirthDate     []string `json:"birthDate"`
        ...
}
```

La struttura sopra riportata consente di catturare ogni aspetto rilevante della risorsa controllata, come alias, posizione, dati anagrafici e note di interesse.

La definizione delle *struct* per il mapping delle richieste e risposte è stata integrata nella procedure `PEPCheckCreateProcedure`. Durante il metodo `Execute`, la struttura `PEPCheckRequest` viene popolata con i dati della risorsa in verifica e inviata tramite un client HTTP. La risposta viene poi deserializzata in `PEPCheckResponse` per determinare lo stato finale del controllo (`CLEAR` o `POSSIBLE_MATCH`) e procedere alla registrazione del risultato nel database.

Esecuzione della chiamata API al database PEP

La chiamata all'API del database PEP è implementata tramite un metodo dedicato, `Exec`, definito all'interno della struttura `PEPCheckRequest`. Questo metodo si

occupa di costruire la richiesta HTTP, inviarla al servizio esterno e gestire la risposta. Di seguito è riportata l'implementazione del metodo:

```
1  func (r *PEPCheckRequest) Exec(c app.HTTPClient) error {
2
3          // JSON body
4          buf := bytes.NewBuffer(nil)
5          data := r.getPEPPayload()
6          if err := json.NewEncoder(buf).Encode(data); err != nil {
7                  return err
8          }
9          req, err := http.NewRequest("POST", app.Config.PEP.APIURL.Value, buf)
10         if err != nil {
11                 return err
12         }
13
14         req.Header.Add("Authorization", "ApiKey "+app.Config.PEP.APIKey.Value)
15
16         resp, err := c.Do(req)
17         if err != nil {
18                 return err
19         }
20         defer resp.Body.Close()
21         if resp.StatusCode != 200 {
22                 return legal.ErrPEPCheckFailed
23         }
24         return json.NewDecoder(resp.Body).Decode(&r.Response)
25 }
```

Struttura della richiesta La richiesta HTTP è costruita utilizzando il metodo POST, il cui corpo (*body*) è generato a partire dai dati della risorsa da verificare, raccolti tramite il metodo privato `getPEPPayload`. Il payload è serializzato in formato JSON tramite il pacchetto standard `encoding/json`, garantendo che i dati siano strutturati correttamente secondo i requisiti dell'API.

Autenticazione Per accedere all'API, la richiesta include un'intestazione (`header`) di autorizzazione con una chiave API (*API Key*). Questo meccanismo garantisce che solo richieste autorizzate possano interagire con il database PEP.

Gestione della risposta Il metodo `Exec` invia la richiesta utilizzando un client HTTP (`app.HTTPClient`) e attende la risposta del server. In caso di errore nella comunicazione o di codice di stato HTTP diverso da 200, il metodo restituisce un errore specifico (`legal.ErrPEPCheckFailed`). Se la risposta è valida, il contenuto del

corpo (*body*) della risposta viene deserializzato nella struttura `PEPCheckResponse`, già definita nella fase di mapping.

Ruolo della procedure PEPCheckCreateProcedure

La procedure `PEPCheckCreateProcedure` rappresenta il cuore dell'implementazione del PEP check. Essa viene invocata dall'handler `PEPCheckCreateHandler` per eseguire la logica principale, suddivisa in tre fasi: `BeforeExecute`, `Execute` e `AfterExecute`.

BeforeExecute Il metodo `BeforeExecute` ha il compito di recuperare i dati relativi alla risorsa specifica basandosi sui parametri `resource_type_id` e `resource_id`. Questi dati sono fondamentali per eseguire i controlli successivi in modo accurato, ma poiché non contiene logica critica, non viene riportato in dettaglio.

Execute Il metodo `Execute` implementa la logica principale del PEP check. Qui di seguito il codice:

```
1  func (p *PEPCheckCreateProcedure) Execute() error {
2      req := p.requestInfo
3      if err := p.HTTP.Exec(p.Ctx, req); err != nil {
4          return err
5      }
6
7      check := new(screening.PEPCheck)
8      check.ResourceID = p.ResourceID
9      check.ResourceType = p.ResourceTypeName
10     if len(req.Response.Responses.Entity.Results) > 0 {
11         check.PEPResults =
           ↪  types.GetRawJSON(req.Response.Responses.Entity.Results)
12         check.PEPStatusName = screenenum.PEP_CHECK_STATUS_POSSIBLE_MATCH
13     } else {
14         check.PEPStatusName = screenenum.PEP_CHECK_STATUS_CLEAR
15     }
16     check.PEPTotal = types.GetRawJSON(req.Response.Responses.Entity.Total)
17     check.CreatedAt = p.TIME.Now()
18     check.UpdatedAt = p.TIME.Now()
19
20     if len(req.Response.Responses.Entity.Results) > 0 {
21         if p.lastPEPCheck != nil && !p.lastPEPCheck.PEPResults.IsZero() &&
22            (p.lastPEPCheck.PEPStatusName == screenenum.PEP_CHECK_STATUS_CLEAR
               ↪  ||
23             p.lastPEPCheck.PEPStatusName ==
                ↪  screenenum.PEP_CHECK_STATUS_MANUALLY_CLEARED) {
24             var lastResults []screenhttp.PEPCheckEntityResults
```

```
25              if err := p.lastPEPCheck.PEPResults.Decode(&lastResults); err !=
                ↪  nil {
26                  return err
27              }
28              if screenutil.ComparePEPCheckEntityResults(lastResults,
                ↪  req.Response.Responses.Entity.Results) {
29                  check.PEPStatusName = screenenum.PEP_CHECK_STATUS_CLEAR
30                  check.AutomaticClear = true
31              }
32          }
33      }
34
35      if check.PEPStatusName == screenenum.PEP_CHECK_STATUS_POSSIBLE_MATCH {
36          p.possibleMatchResourceID = check.ResourceID
37          check.PossibleMatchAt = p.Time.Now()
38
39          if p.ResourceTypeName == audit.RESOURCE_TYPE_LEGAL_PRINCIPAL {
40              p.principal.PEPStatusSetByUnderwriter = false
41
42              query := new(legalsql.UpdatePrincipalQuery)
43              query.Principal = p.principal
44              if err := p.DB.Exec(p.Ctx, query); err != nil {
45                  return err
46              }
47          }
48      }
49
50      query := new(screensql.InsertPEPCheckQuery)
51      query.PEPCheck = check
52      if err := p.DB.Exec(p.Ctx, query); err != nil {
53          return err
54      }
55
56      p.PEPCheck = query.PEPCheck
57
58      return nil
59  }
```

Il metodo `Execute` esegue i seguenti passi:

- Esegue la chiamata API al database PEP come mostrato in precedneza tramite `p.HTTP.Exec`.

- Inizializza una nuova istanza di `PEPCheck` con i dati della risorsa e i risultati ottenuti. Tale istanza verrà successivamente inserita a database come nuova riga della tabella che contine tutti i PEP checks.

- Se il campo `Result` ha una lunghezza maggiore di zero, significa che è stata trovata una possibile corrispondenza nel database di PEP, per cui automaticamente settiamo lo status a `POSSIBLE_MATCH`, altrimenti a `CLEAR`.

- A questo punto viene eseguito un ulteriore controllo finalizzato a verificare, partendo dal PEP check precedente (se esistente), se quest'ultimo fosse stato già settato a `CLEAR` o `MANUALLY_CLEAR`. In caso affermativo, viene effettuato un confronto tra i due JSON, ovvero quello associato al PEP check precedente e quello relativo al PEP check corrente. L'obiettivo di questo confronto è determinare se l'API ha restituito lo stesso risultato in entrambe le occasioni. Qualora il PEP check precedente fosse stato impostato dall'underwriter su `CLEAR` o `MANUALLY_CLEAR` con le relative motivazioni, anche il PEP check corrente verrà settato a `CLEAR`, ignorando la risposta fornita dall'API.

- Infine, l'istanza di `PEPCheck` viene inserita a database con un'apposita query gosql.

AfterExecute Il metodo `AfterExecute` è responsabile della gestione delle operazioni post-esecuzione. Il codice è riportato di seguito:

```
1 func (p *PEPCheckCreateProcedure) AfterExecute() error {
2     return p.ExecFuncs(
3         p.createChangeLog,
4         p.sendPushNotifications,
5         p.sendEmailAlerts,
6         p.updateUnderwritingChallenges,
7     )
8 }
```

Le funzioni richiamate includono:

- `p.createChangeLog`: Genera log dettagliati dei cambiamenti per una maggiore tracciabilità.

- `p.sendPushNotifications`: Invia notifiche push al merchant. (Solo se è stato rilevato un `POSSIBLE_MATCH`)

- `p.sendEmailAlerts`: Genera email per notificare i risultati al merchant. (Solo se è stato rilevato un `POSSIBLE_MATCH`)

- `p.updateUnderwritingChallenges`: Aggiorna eventuali "challenge" specifiche per il processo di underwriting in base ai risultati del controllo.

5.3.2 Esempio 2: Recupero della lista di PEP checks di un merchant

Nuovo endpoint

Un nuovo endpoint è stato definito per permettere il recupero della lista di tutti i PEP checks associati a uno specifico `merchant`. Di seguito è riportata la configurazione dell'endpoint:

```
{
    "P": "/merchants/{merchant_id}/pep-checks",
    "M": "GET",
    "H": "screenapi.PEPCheckListHandler{}",
    "A": {
        "RNT": "gs:rn:merchant:$1:pep",
        "RA": "list"
    },
    "FF": {
        "Name": "be_pep_new",
        "HasRollout": true
    }
}
```

Struttura dell'URL dell'endpoint L'URL dell'endpoint è strutturato come segue:

`/merchants/{merchant_id}/pep-checks`

- `/merchants/merchant_id`: Specifica l'ID del `merchant` di cui si vogliono recuperare tutti i PEP checks.
- `/pep-checks`: Indica che l'operazione richiesta è relativa alla lista completa dei controlli PEP per il `merchant`.

L'endpoint utilizza il metodo HTTP `GET`, poiché l'operazione consiste nella lettura di dati già esistenti. L'implementazione è gestita dall'handler `PEPCheckListHandler`, che recupera i dati richiesti dal database e li ritorna al client.

Ruolo dell'handler PEPCheckListHandler

L'handler `PEPCheckListHandler` è responsabile dell'elaborazione della richiesta e della gestione della logica necessaria per recuperare la lista completa dei PEP checks associati al `merchant`. Qui di seguito è riportata l'implementazione del metodo principale, `Execute`:

```
func (h *PEPCheckListHandler) Execute() error {
    query := new(screensql.SelectPEPCheckViewListByAccQuery)
    query.Where.MerchantAccID = h.accID
    query.Filter = h.params.Filter()
    if err := h.DB.Exec(h.Ctx, query); err != nil {
        return err
    }
    h.Out.Body = web.JSONList(query.List, len(query.List))
    return nil
}
```

Logica dell'handler La logica dell'handler segue i seguenti passaggi:

- Viene costruita una query gosql (`screensql.SelectPEPCheckViewListByAccQuery`) per recuperare tutti i PEP checks associati all'ID del `merchant` specificato (`MerchantAccID`).
- La query applica eventuali filtri definiti nei parametri della richiesta (`h.params.Filter()`), che permettono di restringere i risultati in base a criteri specifici.
- I risultati della query vengono serializzati in formato JSON e ritornati come corpo (*body*) della risposta tramite `web.JSONList`.

Autenticazione e validazione dei dati Prima di eseguire la query, il metodo `BeforeExecute` verifica che il `merchant` esista nel database, effettuando un controllo sulla tabella dei merchant tramite la query `merchsql.SelectExistsMerchantByAccIDQuery`. Se il merchant non è trovato, l'handler ritorna un errore specifico (`merchant.ErrNoMerchant`).

Risultato finale L'handler ritorna una lista completa dei PEP checks associati al `merchant`, contenente informazioni dettagliate su ogni controllo.

5.3.3 Altri endpoint implementati

Oltre agli endpoint descritti nei paragrafi precedenti, durante il tirocinio ho sviluppato ulteriori endpoint per la gestione dei PEP checks, che ampliano le funzionalità della piattaforma e supportano l'interazione con gli underwriter. Di seguito, una descrizione sintetica degli endpoint implementati:

Recupero di un singolo PEP check associato a un merchant

È stato implementato un endpoint che permette di ottenere i dettagli relativi a un singolo PEP check specifico associato a un merchant. Questo endpoint, accessibile

tramite il metodo HTTP `GET`, utilizza l'ID del merchant e l'ID del PEP check per restituire al client tutte le informazioni pertinenti. Questa funzionalità è essenziale per consentire un'analisi approfondita e mirata dei controlli eseguiti sulla piattaforma, agevolando l'accesso rapido a dati specifici per la revisione.

Aggiornamento dello stato di un PEP check

Un altro endpoint implementato permette agli underwriter di aggiornare manualmente lo stato di un PEP check. Questo endpoint, accessibile tramite il metodo HTTP `PATCH`, consente di modificare lo stato di un controllo già esistente (ad esempio, passando da `POSSIBLE_MATCH` a `MANUALLY_CLEAR` o `CONFIRMED_MATCH`).

Le implementazioni di codice relative a questi due endpoint non sono state incluse in quanto non presentano particolari complessità tecniche o logiche innovative rispetto agli esempi già analizzati. Entrambi seguono strutture consolidate, sfruttando handler modulari per la gestione delle richieste e query predefinite per l'interazione con il database.

5.4 Discussione sulle implementazioni

Le implementazioni descritte in questo capitolo rappresentano un significativo avanzamento nella gestione automatizzata dei controlli di conformità PEP e OFAC. Attraverso l'adozione di una struttura modulare basata su endpoint, handler e procedure, è stato possibile ottenere un sistema scalabile e facilmente estensibile.

Uno degli aspetti più rilevanti delle implementazioni è l'integrazione di controlli avanzati per garantire l'affidabilità dei risultati. Ad esempio, l'uso di confronti tra risultati consecutivi dei PEP checks e la gestione automatica dello stato dei controlli riducono sensibilmente il carico manuale degli underwriter, migliorando l'efficienza operativa. Inoltre, la possibilità di aggiornare manualmente lo stato dei PEP checks tramite un endpoint dedicato permette di affrontare casi eccezionali con un alto grado di flessibilità.

Dal punto di vista tecnico, la combinazione di un framework custom per il backend e l'uso dell'ORM `gosql` per l'interazione con il database ha facilitato lo sviluppo di soluzioni robuste e ben integrate. L'uso di un sistema di *feature flag* ha inoltre permesso di rilasciare gradualmente le nuove funzionalità, riducendo al minimo i rischi di regressioni.

In termini di benefici per la piattaforma, queste implementazioni migliorano la capacità di monitorare e gestire i rischi di conformità, aumentando la fiducia degli utenti e degli stakeholder nel sistema. Tuttavia, alcune aree di miglioramento restano aperte, come l'ottimizzazione delle prestazioni per gestire un numero elevato

di richieste simultanee e l'automazione del processo decisionale tramite algoritmi di machine learning.

5.5 Conclusioni e prospettive future

Le implementazioni sviluppate durante il tirocinio rappresentano un passo importante verso un sistema di gestione della conformità più efficiente e scalabile.

In prospettiva futura, ci sono diverse direzioni di sviluppo che potrebbero essere intraprese:

- **Automazione avanzata**: L'integrazione di algoritmi di machine learning potrebbe migliorare ulteriormente l'accuratezza dei controlli, riducendo i falsi positivi e fornendo suggerimenti predittivi agli underwriter. Nei capitoli successivi della tesi verranno approfondite queste tematiche, con particolare attenzione all'uso di tecniche di AI predittiva combinate con framework di Knowledge Representation and Reasoning (KRR), per supportare decisioni più informate e automatizzate.
- **Miglioramento dell'esperienza utente**: L'implementazione di dashboard interattive per il monitoraggio e la gestione dei PEP checks potrebbe semplificare l'accesso ai dati e migliorare la produttività degli operatori.
- **Estensione delle funzionalità**: Lo sviluppo di endpoint aggiuntivi per la gestione automatizzata di altri tipi di controlli normativi, come l'AML (Anti-Money Laundering), amplierebbe le capacità della piattaforma.
- **Ottimizzazione delle prestazioni**: L'adozione di tecniche avanzate di caching e load balancing potrebbe garantire una maggiore efficienza, soprattutto in scenari con elevati volumi di richieste.

Questi miglioramenti non solo rafforzerebbero la competitività della piattaforma nel settore fintech, ma contribuirebbero anche a garantire una maggiore sicurezza e conformità nel panorama globale dei servizi finanziari.

Capitolo 6

Implementazione di test automatizzati

Nel contesto dei sistemi software complessi, l'implementazione di test automatizzati rappresenta un elemento essenziale per garantire la qualità, la robustezza e la conformità dei prodotti. I test automatizzati consentono di identificare rapidamente anomalie e regressioni, migliorando il ciclo di sviluppo e riducendo i costi associati ai difetti di produzione. In particolare, nei sistemi che gestiscono dati sensibili o processi critici, i test automatizzati diventano fondamentali per assicurare l'aderenza alle normative e la protezione delle informazioni.

Questo capitolo illustra l'approccio adottato per implementare test automatizzati nei vari componenti del sistema sviluppati (controlli PEP e OFAC e inoltre anche dei test sul sistema di permessi IAM integrato nella piattaforma che verrà descritto nel capitolo successivo). Verranno analizzate tre aree principali:

- **Rilevanza dei test automatizzati nei sistemi complessi**: un'analisi dei vantaggi offerti dai test automatizzati e delle metodologie adottate per affrontare le sfide specifiche di sistemi complessi e distribuiti.
- **Test sui controlli di conformità PEP e OFAC**: dettagli sull'implementazione di test automatizzati volti a verificare l'accuratezza e l'affidabilità dei controlli di conformità.
- **Validazione e verifica del sistema di gestione dei permessi**: una descrizione delle procedure utilizzate per garantire che il sistema di gestione delle identità e degli accessi funzioni in modo corretto e sicuro.

L'obiettivo è fornire una visione completa del processo di testing, evidenziando le tecniche utilizzate, gli strumenti scelti e i risultati ottenuti. Verranno inoltre inclusi esempi pratici e frammenti di codice per offrire una panoramica dettagliata delle implementazioni.

6.1 Rilevanza dei test automatizzati nei sistemi complessi

I sistemi software complessi, in particolare quelli che operano in contesti critici come il fintech e la conformità normativa, richiedono strategie di testing avanzate per garantire la qualità, l'affidabilità e la sicurezza. I test automatizzati giocano un ruolo cruciale in questo processo, fornendo strumenti per identificare rapidamente anomalie e assicurare che ogni modifica al codice non comprometta la stabilità del sistema.

Benefici dei test automatizzati

L'adozione di test automatizzati offre molteplici vantaggi nei sistemi complessi:

- **Velocità e frequenza di esecuzione**: i test automatizzati consentono di eseguire verifiche in tempi ridotti rispetto ai test manuali, favorendo un ciclo di sviluppo più rapido.
- **Riduzione dei costi di manutenzione**: rilevando i difetti nelle prime fasi dello sviluppo, i test automatizzati riducono i costi associati alla risoluzione dei problemi nelle fasi avanzate del ciclo di vita del software.
- **Miglioramento della copertura del codice**: grazie a framework avanzati, è possibile coprire un ampio spettro di scenari e garantire la conformità a requisiti tecnici e normativi.
- **Affidabilità a lungo termine**: i test automatizzati forniscono una base solida per prevenire regressioni e garantire che il sistema rimanga stabile nel tempo, anche con l'introduzione di nuove funzionalità.

Sfide nei sistemi complessi

Nonostante i numerosi vantaggi, l'implementazione di test automatizzati nei sistemi complessi presenta alcune sfide significative:

- **Gestione della complessità**: i sistemi distribuiti, come quelli basati su microservizi, richiedono strategie di testing che includano test di integrazione e di end-to-end.
- **Configurazione degli ambienti di test**: riprodurre fedelmente ambienti di produzione può essere complesso e richiedere strumenti specifici per orchestrare container e servizi.

- **Dipendenze esterne**: nei sistemi che si interfacciano con provider esterni o API, la gestione delle dipendenze è cruciale per garantire test affidabili e replicabili.

Metodologie e strumenti per il testing

Per affrontare queste sfide, è fondamentale adottare metodologie e strumenti specifici:

- **Test unitari**: verificano il corretto funzionamento di singoli componenti o moduli del sistema, garantendo che ogni unità soddisfi i requisiti specifici.
- **Test di integrazione**: assicurano che i vari moduli collaborino correttamente, testando le interazioni tra componenti e servizi.
- **Test end-to-end**: simulano scenari realistici per verificare il comportamento del sistema nella sua interezza, dal frontend al backend.
- **Strumenti CI/CD**: piattaforme come Jenkins, GitLab CI/CD o GitHub Actions automatizzano l'esecuzione dei test durante il processo di integrazione e rilascio continuo, riducendo al minimo l'intervento umano.
- **Mocking e virtualizzazione**: per gestire le dipendenze esterne, strumenti come WireMock e Postman permettono di simulare API e servizi di terze parti, garantendo test isolati e affidabili.

Impatto dei test automatizzati nel settore fintech

Nel settore fintech, dove la sicurezza e la conformità normativa sono prioritarie, i test automatizzati rappresentano un pilastro fondamentale. La capacità di simulare scenari complessi, come la gestione di transazioni finanziarie e il controllo di accesso basato su ruoli, consente alle organizzazioni di:

- Garantire la conformità a normative.
- Ridurre il rischio di frodi e violazioni di sicurezza.
- Offrire un'esperienza utente affidabile e fluida, anche in presenza di carichi elevati.

In sintesi, i test automatizzati non solo migliorano la qualità del software, ma rappresentano anche una componente strategica per affrontare le complessità dei sistemi moderni. Nelle sezioni successive, verranno presentati esempi concreti di test applicati ai controlli di conformità PEP e OFAC, nonché alla gestione delle identità e degli accessi.

6.2 Test sui controlli di conformità PEP e OFAC

I controlli di conformità PEP e OFAC rappresentano una componente critica per garantire la sicurezza e la conformità normativa delle piattaforme fintech. Per verificarne il corretto funzionamento, sono stati implementati test automatizzati utilizzando librerie avanzate come `httptest` e `webtest`, che permettono di simulare e validare le interazioni con gli endpoint del sistema.

Struttura dei test

La libreria `webtest` è stata utilizzata per definire specifiche dettagliate per ogni endpoint relativo ai controlli PEP. I test sono organizzati in gruppi (`TestGroup`), ciascuno dei quali rappresenta un endpoint, e contengono più test cases (`Test`) per coprire scenari differenti.

Esempio di definizione di un gruppo di test per l'endpoint di creazione di un PEP check:

```
var PEPChecksSpec = webtest.Spec([]*httptest.TestGroup{
    {
        E: "POST
        ↪  /merchants/{merchant_id}/resources/{resource_type_id}/pep-checks/{resource_id}",
        N: "Create PEP Checks",
        Tests: []*httptest.Test{{
            Request: httptest.Request{
                Params: httptest.Params{"merchant_id": 6800001,
                ↪  "resource_type_id": 13, "resource_id": 6800001},
            },
            Response: httptest.Response{
                StatusCode: web.StatusCreated,
                Body: httptype.JSON(screening.PEPCheckView{
                    ID:                          1,
                    ResourceID:                  6800001,
                    ResourceTypeName:            "legal_principals",
                    ResourceTypeDisplayName:     "Business Owner",
                    ResourceFullName:            "Prince Doe",
                    PrincipalOwnershipPercentage: 70,
                    PEPStatusName:
                    ↪  screenenum.PEP_CHECK_STATUS_CLEAR,
                    PEPTotal:
                    ↪  types.NewRawJSON([]byte(`{"value":0,"relation":""}`)),
                    CreatedAt:                   webtest.TimeValue,
                    UpdatedAt:                   webtest.TimeValue,
                }),
            },
        }},
```

```
25      },
26  })
```

Principali endpoint testati

Sono stati implementati test per diversi endpoint relativi ai controlli PEP, ciascuno con una finalità specifica:

- **Creazione di un nuovo PEP check**: verifica che l'endpoint crei correttamente un PEP check per una specifica risorsa associata a un merchant.
- **Recupero della lista dei PEP check**: testa la capacità dell'endpoint di restituire una lista filtrata e ordinata di PEP check.
- **Recupero di un singolo PEP check**: simula la lettura di un controllo specifico, verificando che i dati restituiti siano corretti e completi.
- **Aggiornamento dello stato di un PEP check**: valida la capacità dell'endpoint di aggiornare lo stato di un controllo esistente, ad esempio da `CLEAR` a `POSSIBLE_MATCH`.

Struttura di un test

Ogni test case include i seguenti elementi:

- `Request`: definisce i parametri, il corpo (*body*) e le query string della richiesta.
- `Response`: specifica lo stato HTTP atteso (`StatusCode`) e il formato del corpo della risposta.
- `Body`: utilizza strutture JSON per verificare che i dati restituiti siano corretti.

Esempio di test per la lista dei PEP check:

```
{
    E: "GET /merchants/{merchant_id}/pep-checks",
    N: "List PEP Checks",
    Tests: []*httptest.Test{{
        Request: httptest.Request{
            Params: httptest.Params{"merchant_id": 6800001},
            Query:  httptest.Query{"sort": {"id"}, "max": {"3"}},
        },
        Response: httptest.Response{
            StatusCode: web.StatusOK,
            Body: web.JSONList([]screening.PEPCheckView{{
                ID:                          2,
                ResourceID:                  6800001,
                ResourceTypeName:            "legal_principals",
                ResourceTypeDisplayName:     "Business Owner",
                ResourceFullName:            "Prince Doe",
                PrincipalOwnershipPercentage: 70,
                PEPStatusName:
                ↪  screenenum.PEP_CHECK_STATUS_POSSIBLE_MATCH,
                CreatedAt:                   webtest.TimeValue,
                UpdatedAt:                   webtest.TimeValue,
            }}, 3),
        },
    }},
}
```

Utilizzo di librerie e strumenti avanzati

La combinazione di `httptest` e `webtest` offre numerosi vantaggi:

- **Riproducibilità**: i test possono essere eseguiti in qualsiasi ambiente senza dipendere da configurazioni esterne.
- **Mocking avanzato**: le risposte simulate permettono di testare scenari complessi senza necessità di interagire con sistemi esterni.
- **Diagnosi immediata**: in caso di fallimento, i dump dei dettagli della richiesta e della risposta forniscono informazioni preziose per identificare e correggere i problemi (è possibile lanciare i tests specificando il parametro -v, che significa verborse, il quale stampa un errore dettagliato in caso di fallimento del test).

6.3 Validazione e verifica del sistema di gestione dei permessi

Nei sistemi complessi, la gestione dei permessi è fondamentale per garantire che solo gli utenti autorizzati possano accedere o eseguire operazioni su risorse sensibili. In questo contesto, sono stati implementati test automatizzati per verificare la correttezza delle politiche di accesso, utilizzando le medesime librerie descritte in precedenza.

Test di accesso per gli endpoint relativi agli OFAC Checks

I test automatizzati implementati verificano i permessi di accesso agli endpoint relativi ai controlli OFAC. In particolare, vengono verificati due endpoint:

- `GET /merchants/{merchant_id}/ofac-checks`: Recupero della lista di OFAC checks associati a un merchant.
- `POST /merchants/{merchant_id}/resources/{resource_type_id}/ofac-checks/{res` Creazione di un nuovo OFAC check per una risorsa specifica.

Esempio di test sull'elenco degli OFAC checks

Il seguente codice verifica se diversi ruoli all'interno di un'organizzazione, come `owner`, `admin` o `member`, possono accedere all'elenco degli OFAC checks per un merchant specifico.

```
1  var ofac_check_spec = webtest.Spec([]*httptest.TestGroup{{
2      E: "GET /merchants/{merchant_id}/ofac-checks", N: "List OFAC Checks",
3      Tests: []*httptest.Test{{
4          N: "SHOULD ALLOW: List OFAC checks by acquirer's owner",
5          Request: httptest.Request{
6              Params: httptest.Params{"merchant_id": 999720, "legal_entity_id":
                   ↪  1800001},
7              Header: webtest.CookieForUser(999705),
8          },
9          Response: ALLOW(),
10     }, {
11         N: "SHOULD DENY: List OFAC checks by acquirer's member",
12         Request: httptest.Request{
13             Params: httptest.Params{"merchant_id": 999720, "legal_entity_id":
                   ↪  1800001},
14             Header: webtest.CookieForUser(999704),
15         },
16         Response: DONT_ALLOW(999704),
```

```
    }},
}})
```

Descrizione del test

- Il primo caso di test verifica che un `owner` possa accedere correttamente alla lista degli OFAC checks per un determinato merchant, restituendo una risposta `ALLOW()`.
- Il secondo caso simula una richiesta da parte di un `member`, che non dispone dei permessi necessari. In questo caso, il sistema restituisce una risposta di errore `DONT_ALLOW(999704)`.

Esempio di test sulla creazione di un OFAC check

Questo test verifica se utenti con ruoli specifici, come `risk manager` o `underwriting executive`, possono creare un nuovo controllo OFAC per una risorsa.

```
{
    E: "POST
    ↪  /merchants/{merchant_id}/resources/{resource_type_id}/ofac-checks/{resource_id}",
    N: "Create OFAC Check",
    Tests: []*httptest.Test{{
        N: "SHOULD ALLOW: create OFAC check by acquirer's owner",
        Request: httptest.Request{
            Params: httptest.Params{"merchant_id": 999720, "resource_type_id":
            ↪  11, "resource_id": 4500001},
            Header: webtest.CookieForUser(999705),
        },
        Response: ALLOW(),
    }, {
        N: "SHOULD DENY: create OFAC check by acquirer's member",
        Request: httptest.Request{
            Params: httptest.Params{"merchant_id": 999720, "resource_type_id":
            ↪  11, "resource_id": 4500001},
            Header: webtest.CookieForUser(999704),
        },
        Response: DONT_ALLOW(999704),
    }},
}
```

Descrizione del test

- Il test verifica che solo utenti autorizzati possano creare un controllo OFAC, come `owner`, `admin` o `risk manager`.

- Gli utenti non autorizzati, come i semplici membri (`member`), ricevono un messaggio di errore e la richiesta è negata.

Questi test automatizzati garantiscono che il sistema di gestione dei permessi funzioni correttamente e rispetti le politiche di sicurezza definite. La loro implementazione consente di:

- Verificare che solo utenti con i permessi appropriati possano accedere o modificare i dati sensibili.
- Rilevare eventuali configurazioni errate o anomalie nelle policy di accesso.
- Migliorare la fiducia degli stakeholder nella piattaforma, assicurando che i controlli di accesso siano rigorosi e conformi agli standard normativi.

Capitolo 7

Identity and Access Management (IAM) e sicurezza delle transazioni finanziarie

Un'ulteriore parte fondamentale della piattaforma sulla quale ho avuto l'opportunità di lavorare è il sistema e la gestione dei permessi utente. Anche in questo caso ho condotto un'analisi prima teorica e poi pratica del sistema preesistente. La parte pratica, inserita nel capitolo precedente dei test automatizzati, ha avuto come scopo quello di identificare potenziali errori, lacune, incorrettezze nell'attuale sistema, attraverso l'esecuzione di test su specifici endpoint, in contrasto con le richieste del cliente. In questo capitolo è inserita invece la ricerca teoria che ho condotto.

7.1 Definizione e importanza dell'Identity and Access Management

L'Identity and Access Management (IAM) rappresenta un insieme di politiche, processi e tecnologie progettate per gestire in modo sicuro le identità digitali e controllare l'accesso alle risorse all'interno di un'organizzazione. L'obiettivo principale dell'IAM è garantire che solo gli utenti autorizzati possano accedere alle informazioni e ai sistemi, riducendo al minimo il rischio di violazioni di sicurezza [16].

Definizione di IAM

L'IAM si concentra sulla gestione delle identità e sull'implementazione di un accesso sicuro attraverso tre pilastri fondamentali:

- **Identificazione**: riconoscere un'entità digitale (utente, dispositivo o applicazione) tramite credenziali univoche come nomi utente, chiavi API o certificati digitali.
- **Autenticazione**: verificare che l'identità dichiarata sia valida, utilizzando meccanismi come password, autenticazione a due fattori (2FA), sistemi biometrici (impronte digitali, riconoscimento facciale) o autenticazione basata su token [17].
- **Autorizzazione**: stabilire i livelli di accesso per ogni identità, regolando quali risorse e azioni sono consentite in base a policy specifiche.

Importanza dell'IAM nella sicurezza digitale

La crescente digitalizzazione e l'adozione di architetture cloud hanno reso l'IAM un elemento cruciale per la protezione delle infrastrutture digitali. Tra i principali benefici, troviamo:

- **Riduzione del rischio di accessi non autorizzati**: l'IAM limita gli accessi alle sole risorse autorizzate ad operare, riducendo la superficie di attacco.
- **Conformità normativa**: strumenti IAM avanzati permettono alle aziende di rispettare normative complesse.
- **Miglioramento dell'efficienza operativa**: l'utilizzo di Single Sign-On (SSO) e sistemi di autenticazione avanzati consente di ottimizzare l'accesso alle risorse aziendali, migliorando l'esperienza utente [18].
- **Auditabilità e trasparenza**: l'IAM tiene traccia di ogni evento di accesso o modifica alle risorse, facilitando l'analisi degli incidenti e le attività di audit [16].

Esempi reali dell'importanza dell'IAM

Numerosi casi dimostrano come una corretta implementazione di IAM possa prevenire incidenti significativi:

- Nel 2019, una violazione di sicurezza presso *Capital One* ha compromesso dati sensibili di oltre 100 milioni di clienti. L'incidente è stato attribuito a configurazioni IAM errate, che hanno permesso un accesso non autorizzato a un

bucket Amazon. Questo evento ha evidenziato l'importanza di configurazioni IAM precise e di routine di monitoraggio [19].

- Un altro esempio riguarda *Zoom*, che durante la pandemia ha rafforzato il proprio sistema IAM per contrastare episodi di *Zoom-bombing*. L'implementazione di autenticazione basata su SSO e criteri di accesso granulari ha migliorato significativamente la sicurezza delle sessioni virtuali [20].

Sfide dell'implementazione IAM

Nonostante i benefici, l'implementazione dell'IAM presenta sfide complesse:

- **Gestione delle identità in ambienti multi-cloud**: le aziende che operano su piattaforme come AWS, Azure e Google Cloud devono garantire un'integrazione coerente tra i sistemi IAM di ogni provider [21].
- **Bilanciamento tra sicurezza e usabilità**: metodi di autenticazione avanzati, come la biometria, possono risultare complessi per alcuni utenti, richiedendo soluzioni che non compromettano l'esperienza utente [17].
- **Manutenzione continua**: la gestione di identità e credenziali richiede risorse dedicate per aggiornare le policy, revocare accessi non più necessari e rispondere a minacce emergenti [18].

IAM e trasformazione digitale

Nel contesto della trasformazione digitale, l'IAM è essenziale per proteggere le nuove architetture IT. Ad esempio:

- Con l'adozione del *Bring Your Own Device* (BYOD), le aziende devono gestire identità non solo degli utenti ma anche dei dispositivi personali, garantendo accessi sicuri alle risorse aziendali [22].
- Le tecnologie emergenti, come il 5G e l'Internet of Things (IoT), richiedono un IAM avanzato per gestire miliardi di dispositivi connessi e prevenire accessi non autorizzati [23].

Esempi di implementazioni avanzate di IAM

- *Google Identity-Aware Proxy (IAP)*: Google utilizza un proxy basato su IAM per controllare l'accesso alle sue applicazioni interne. Ogni richiesta viene autenticata e autorizzata in tempo reale, migliorando la sicurezza senza compromettere l'efficienza operativa [24].

- *Microsoft Azure Active Directory (AAD)*: Azure AAD consente alle aziende di implementare funzionalità di SSO, gestione di dispositivi e accesso condizionale. Questo approccio combina sicurezza e flessibilità, rispondendo alle esigenze di ambienti aziendali complessi [21].

In sintesi, l'IAM è un elemento imprescindibile per la sicurezza digitale e l'operatività aziendale. Nella sezione successiva, analizzeremo il ruolo cruciale dell'IAM nel settore fintech, con particolare attenzione alle sue applicazioni pratiche per garantire la protezione delle informazioni e la conformità normativa.

7.2 IAM e sicurezza delle transazioni finanziarie in un' applicazione fintech

Nel settore fintech, la sicurezza informatica non è solo una necessità operativa, ma un pilastro fondamentale per garantire la fiducia degli utenti, la conformità normativa e la protezione contro le crescenti minacce cibernetiche. Le applicazioni fintech sono particolarmente vulnerabili a causa della natura sensibile dei dati trattati e dell'elevata frequenza delle transazioni finanziarie. L'implementazione di un solido sistema di *Identity and Access Management* (IAM), combinato con protocolli di sicurezza avanzati, rappresenta una delle strategie più efficaci per mitigare i rischi.

IAM e protezione degli accessi

Nel contesto fintech, così come in altri ambiti, l'IAM svolge un ruolo cruciale nel garantire che solo utenti autorizzati possano accedere alle risorse critiche. Tra le funzionalità chiave dell'IAM applicate alla sicurezza informatica:

- **Single Sign-On (SSO)**: riduce il numero di credenziali necessarie, migliorando l'usabilità e riducendo i rischi legati al riutilizzo delle password.
- **Autenticazione a più fattori (MFA)**: aggiunge un livello di sicurezza verificando l'identità degli utenti attraverso fattori come password, dispositivi fisici o biometria.
- **Gestione delle sessioni**: sistemi avanzati monitorano le sessioni attive, terminando automaticamente quelle inattive per ridurre il rischio di accessi non autorizzati.
- **Accesso condizionale**: l'accesso viene concesso in base a parametri contestuali, come la posizione geografica, l'orario e il dispositivo utilizzato [18].

Sicurezza nelle transazioni finanziarie

Le applicazioni fintech gestiscono transazioni di importanza critica, come pagamenti, trasferimenti di fondi e gestione degli investimenti. Garantire la sicurezza di queste transazioni richiede l'adozione di protocolli specifici e standard internazionali. Tra i principali protocolli di sicurezza troviamo:

- **Transport Layer Security (TLS)**: garantisce la protezione dei dati durante il transito, prevenendo intercettazioni e manomissioni. Le versioni più recenti, come TLS 1.3, offrono miglioramenti significativi in termini di velocità e sicurezza [25].
- **Payment Card Industry Data Security Standard (PCI-DSS)**: questo standard obbliga le aziende che gestiscono informazioni sulle carte di pagamento a implementare misure di sicurezza stringenti, come la cifratura end-to-end e il monitoraggio delle attività di rete [26].
- **Strong Customer Authentication (SCA)**: introdotto da una direttiva dell'Unione Europea, richiede almeno due fattori di autenticazione per garantire l'identità del cliente durante le transazioni online [27].
- **JSON Web Token (JWT)**: utilizzato per l'autenticazione e l'autorizzazione sicura tra le parti, garantisce la protezione delle sessioni utente attraverso firme digitali [28].

Protezione contro le minacce cibernetiche

Le applicazioni fintech sono esposte a numerose minacce, come attacchi *man-in-the-middle*, phishing e *ransomware*. L'adozione di pratiche di sicurezza robuste è fondamentale:

- **Cifratura dei dati**: ogni dato sensibile, sia in transito che a riposo, deve essere cifrato utilizzando algoritmi avanzati.
- **Monitoraggio e rilevamento delle anomalie**: strumenti basati sull'intelligenza artificiale possono identificare comportamenti sospetti e rispondere in tempo reale per prevenire attacchi.
- **Protezione DDoS**: sistemi di mitigazione come *cloud firewalls* proteggono contro attacchi distribuiti che mirano a interrompere i servizi dell'applicazione.
- **Hardening delle API**: poiché molte applicazioni fintech comunicano attraverso API, queste devono essere protette contro vulnerabilità come injection e accessi non autorizzati [29].

Esempi applicativi

Diversi casi pratici dimostrano l'importanza di protocolli di sicurezza e IAM nel settore fintech:

- **PayPal**: utilizza una combinazione di autenticazione biometrica e machine learning per prevenire frodi durante le transazioni, analizzando in tempo reale milioni di parametri [30].
- **Revolut**: l'implementazione di Strong Customer Authentication ha permesso di migliorare la sicurezza delle transazioni online, riducendo le frodi legate ai pagamenti [31].
- **Stripe**: adotta TLS 1.3 e politiche rigorose di tokenizzazione dei dati per garantire la sicurezza delle transazioni globali [32].

Sfide e prospettive future

Nonostante i progressi, le applicazioni fintech affrontano sfide crescenti:

- **Scalabilità della sicurezza**: con l'aumento dei volumi di transazioni, le soluzioni IAM e i protocolli di sicurezza devono adattarsi rapidamente senza compromettere le prestazioni.
- **Integrazione multi-cloud**: la protezione delle applicazioni distribuite su più ambienti cloud richiede un IAM altamente flessibile e strumenti avanzati di gestione degli accessi.
- **Minacce emergenti**: tecnologie come l'intelligenza artificiale possono essere utilizzate sia per migliorare la sicurezza che per sviluppare nuove forme di attacco.

In conclusione, il ruolo dell'IAM e dei protocolli di sicurezza nel settore fintech non può essere sottovalutato. Con l'evoluzione delle minacce cibernetiche, l'adozione di soluzioni innovative, come l'intelligenza artificiale e i modelli predittivi, sarà essenziale per garantire la protezione delle applicazioni finanziarie e la fiducia degli utenti.

7.3 Esempi applicativi rilevanti

La sicurezza delle transazioni finanziarie è una priorità assoluta per le piattaforme fintech e i provider di pagamento. Sistemi di protezione avanzati, come quelli offerti da RS2 (che ho avuto occasione di conoscere e studiare durante la mia esperienza

di tirocinio), integrano soluzioni IAM e altre tecnologie di sicurezza per garantire un'elaborazione affidabile e conforme alle normative internazionali.

RS2 e la sicurezza delle transazioni finanziarie

RS2 è uno dei provider leader nel settore dei pagamenti, offrendo una piattaforma modulare che supporta soluzioni di pagamento end-to-end. L'integrazione di funzionalità di sicurezza avanzate include:

- **Tokenizzazione dei dati**: RS2 utilizza tecnologie di tokenizzazione per sostituire i dati sensibili delle carte di pagamento con token univoci, proteggendo le informazioni durante la trasmissione e l'archiviazione.
- **Autenticazione a due fattori (2FA)**: garantisce che solo utenti autorizzati possano accedere ai sistemi RS2 e approvare le transazioni.
- **Conformità PCI-DSS**: RS2 soddisfa pienamente gli standard del Payment Card Industry Data Security Standard (PCI-DSS), che rappresentano un riferimento per la sicurezza delle transazioni finanziarie [26].

Un esempio pratico è rappresentato dall'utilizzo di RS2 da parte di istituti finanziari per gestire l'elaborazione dei pagamenti internazionali. Grazie alla sua architettura scalabile e ai sistemi IAM integrati, RS2 consente di monitorare e proteggere le transazioni in tempo reale, identificando potenziali anomalie e prevenendo frodi [33].

Integrazione dell'IAM nella sicurezza delle transazioni

Un altro aspetto fondamentale è l'integrazione dei sistemi IAM nella sicurezza delle transazioni finanziarie. L'utilizzo di tecnologie come OAuth 2.0 e JWT (JSON Web Tokens) consente di gestire in modo sicuro l'accesso alle API dei provider di pagamento. Ad esempio:

- **OAuth 2.0**: utilizzato per autenticare e autorizzare in modo sicuro gli utenti e le applicazioni che accedono all'applicazione.
- **JSON Web Tokens (JWT)**: implementati per trasmettere dati autenticati e crittografati tra le parti coinvolte nelle transazioni [34].

7.3.1 Esempi applicativi nella prevenzione delle frodi

PayPal: Machine Learning per il rilevamento delle frodi

PayPal è uno degli esempi più avanzati di utilizzo di intelligenza artificiale e machine learning per prevenire frodi nelle transazioni finanziarie. L'azienda analizza milioni

di transazioni ogni giorno, identificando schemi anomali che potrebbero indicare attività fraudolente. I sistemi integrano tecniche IAM per limitare l'accesso e applicano protocolli avanzati di crittografia per proteggere i dati dei clienti [35].

Stripe e l'autenticazione basata sul rischio

Stripe utilizza un approccio basato sul rischio per autenticare gli utenti. Ad esempio, gli utenti con un comportamento considerato sospetto vengono sottoposti a verifiche aggiuntive, come il riconoscimento facciale o l'invio di codici OTP. Questo modello, supportato da sistemi IAM avanzati, garantisce la protezione delle transazioni senza compromettere l'esperienza utente [32].

7.3.2 Sicurezza nel contesto multi-cloud e applicazioni cross-border

Molti provider di pagamento, inclusi RS2, operano in ambienti multi-cloud per garantire scalabilità e ridondanza. Tuttavia, questo comporta sfide uniche per la sicurezza. Ad esempio:

- **Gestione centralizzata delle identità**: sistemi come Azure AD o AWS IAM offrono soluzioni centralizzate per gestire gli accessi, anche in ambienti distribuiti.
- **Crittografia end-to-end**: implementata per garantire la protezione dei dati durante le transazioni cross-border, rispettando normative locali e internazionali [36].

In sintesi, gli esempi sopra riportati evidenziano il ruolo cruciale dell'IAM e delle tecnologie di sicurezza avanzate nel proteggere le transazioni finanziarie e i dati sensibili. RS2, insieme ad altri leader del settore, rappresenta un modello di eccellenza nell'adozione di soluzioni innovative per affrontare le sfide del panorama finanziario globale.

Capitolo 8

Intelligenza artificiale e predictive AI

A questo punto della mia ricerca, le attività teorie e pratiche che ho sviluppato durante l'esperienza di tirocinio sono terminate. Nella parte restante ho condotto delle analisi su possibili ulteriori miglioramenti futuri, che superino addirittura la semplice automazione che ho implementato, e che utilizzino la tecnologia che caratterizzerà il nostro futuro: l'intelligenza artificiale.

8.1 Introduzione e classificazione dei tipi di intelligenza artificiale

L'intelligenza artificiale (IA) rappresenta uno dei pilastri fondamentali della trasformazione digitale, offrendo strumenti innovativi per affrontare sfide complesse in vari settori, tra cui quello finanziario. Attraverso la simulazione dell'intelligenza umana mediante algoritmi e tecnologie avanzate, l'IA permette di migliorare l'efficienza operativa, l'accuratezza decisionale e la capacità di gestione dei rischi. Questo capitolo esplorerà le principali tipologie di IA, fornendo una base teorica necessaria per comprendere le applicazioni avanzate trattate nelle sezioni successive.

Classificazione dell'intelligenza artificiale

L'IA può essere classificata in base al livello di complessità, autonomia e capacità di adattamento. La suddivisione più comune comprende tre principali categorie:

1. Intelligenza artificiale ristretta (ANI - Artificial Narrow Intelligence)

L'ANI si riferisce a sistemi progettati per svolgere compiti specifici in modo altamente efficiente. Questa categoria rappresenta la forma più diffusa di IA attualmente in uso. Gli esempi includono assistenti vocali come Alexa o Google Assistant, motori di raccomandazione utilizzati da piattaforme di streaming e algoritmi di analisi predittiva.

Nonostante l'elevata competenza in ambiti circoscritti, l'ANI è caratterizzata dall'incapacità di adattarsi a contesti al di fuori del suo scopo originario. Un assistente vocale, ad esempio, non può analizzare dati finanziari complessi senza essere esplicitamente programmato per farlo. Questo limita le sue applicazioni a situazioni in cui il problema è ben definito e i dati sono strutturati.

2. Intelligenza artificiale generale (AGI - Artificial General Intelligence)

L'AGI rappresenta un livello teorico di IA in cui le macchine sono in grado di apprendere e comprendere qualsiasi compito intellettuale umano. Questo tipo di intelligenza mira a raggiungere capacità di adattamento a nuovi contesti e risoluzione di problemi non previsti nel loro design iniziale.

Il raggiungimento dell'AGI è uno degli obiettivi più ambiziosi della ricerca sull'IA. La realizzazione di un'AGI richiederebbe una profonda comprensione dell'intelligenza umana, sia a livello cognitivo che emotivo, e un'infrastruttura tecnologica in grado di supportare un apprendimento continuo. Nonostante i progressi teorici, l'AGI rimane un traguardo lontano, con implicazioni etiche e sociali significative.

3. Superintelligenza artificiale (ASI - Artificial Superintelligence)

L'ASI si riferisce a un'ipotetica IA che supera di gran lunga le capacità cognitive umane in ogni aspetto, dalla creatività alla risoluzione dei problemi e al processo decisionale.

Sebbene l'ASI offra la prospettiva di risolvere problemi globali complessi, come il cambiamento climatico o le malattie incurabili, pone anche rischi enormi, inclusa la possibilità che l'umanità perda il controllo sulla tecnologia. Il dibattito su come regolare l'ASI è attualmente confinato a discussioni accademiche, ma riflette l'urgenza di affrontare le implicazioni della crescita esponenziale dell'IA.

Evoluzione storica dell'intelligenza artificiale

L'evoluzione dell'IA è stata guidata da progressi tecnologici significativi. Negli anni '50, l'IA era principalmente teorica, basata su algoritmi semplici per problemi specifici. Con l'avvento di computer più potenti, si sono sviluppati sistemi più

complessi, come reti neurali artificiali negli anni '80 e metodi di apprendimento profondo (deep learning) nel XXI secolo.

Oggi, l'IA è alimentata da tre elementi fondamentali:

- **Big Data**: La disponibilità di enormi volumi di dati strutturati e non strutturati è essenziale per addestrare modelli IA.
- **Capacità computazionale**: L'uso di GPU e TPU ha reso possibile l'elaborazione di modelli complessi in tempi ridotti.
- **Algoritmi avanzati**: I progressi negli algoritmi di apprendimento supervisionato, non supervisionato e rinforzato hanno ampliato le capacità dell'IA.

Implicazioni della classificazione dell'IA

Ogni categoria di IA trova applicazioni in contesti specifici:

- L'ANI domina gli scenari attuali, fornendo soluzioni per problemi ben definiti come la personalizzazione dell'esperienza utente per attività quotidiane.
- L'AGI rappresenta il futuro della ricerca, con il potenziale di trasformare settori complessi come la medicina o l'educazione.
- L'ASI, se realizzata, richiederà un ripensamento delle strutture economiche, politiche e sociali globali.

Nei capitoli successivi, ci concentreremo sul suo impatto nel settore fintech e sui modelli predittivi che guidano l'ottimizzazione dei processi di compliance normativa, come i controlli PEP e OFAC.

8.2 Ruolo dell'intelligenza artificiale nel settore fintech e banking

L'intelligenza artificiale (IA) sta trasformando profondamente il settore fintech e bancario, rappresentando un elemento cardine per l'innovazione e la competitività. La capacità dell'IA di analizzare grandi volumi di dati, rilevare anomalie e automatizzare processi complessi consente alle istituzioni finanziarie di migliorare la qualità dei servizi offerti, ottimizzare le operazioni interne e rispondere rapidamente alle esigenze di un mercato in continua evoluzione.

Automazione dei processi e ottimizzazione operativa

Uno dei contributi principali dell'IA nel settore finanziario è l'automazione di processi manuali ripetitivi e dispendiosi. Algoritmi di machine learning possono essere utilizzati per gestire attività come la riconciliazione dei conti, la verifica delle transazioni e il rilevamento delle frodi. Ad esempio, l'adozione di modelli predittivi basati su reti neurali consente di identificare transazioni sospette con maggiore precisione, riducendo al contempo i falsi positivi e migliorando l'efficienza complessiva del sistema.

Miglioramento della user experience

L'IA ha rivoluzionato l'esperienza utente nei servizi bancari, introducendo interfacce personalizzate e assistenti virtuali basati su chatbot. Questi sistemi, alimentati da algoritmi di elaborazione del linguaggio naturale (NLP), sono in grado di rispondere a domande, gestire richieste e fornire suggerimenti in tempo reale. Inoltre, la personalizzazione dei servizi basata sull'analisi dei dati comportamentali dei clienti consente di proporre prodotti e offerte specifiche, migliorando la soddisfazione degli utenti.

Rilevamento delle frodi e gestione del rischio

Nel contesto della gestione del rischio, l'IA si distingue per la capacità di analizzare rapidamente enormi volumi di dati transazionali e comportamentali. Gli algoritmi avanzati di machine learning possono identificare schemi fraudolenti, come transazioni anomale o accessi non autorizzati, in modo più rapido ed efficace rispetto ai metodi tradizionali. Questo approccio consente alle istituzioni di reagire tempestivamente a minacce emergenti, proteggendo sia i clienti sia l'integrità del sistema finanziario.

Supporto alla compliance normativa

Un'area cruciale di applicazione dell'IA nel settore finanziario è la gestione della conformità normativa. L'automazione dei controlli di conformità, come i controlli PEP e OFAC, permette di garantire l'aderenza ai requisiti normativi in modo efficiente. L'IA non solo accelera il processo di verifica, ma riduce anche il rischio di errore umano, migliorando la tracciabilità e l'accuratezza dei controlli.

Impatto strategico dell'intelligenza artificiale nel settore

L'adozione dell'IA non si limita a migliorare le operazioni esistenti, ma influenza anche la strategia complessiva delle istituzioni finanziarie. La capacità di adattarsi

rapidamente ai cambiamenti del mercato, di personalizzare i servizi su larga scala e di ridurre i costi operativi rende l'IA un elemento imprescindibile per affrontare le sfide di un settore in rapida trasformazione. Nei capitoli successivi, saranno analizzati più in dettaglio i modelli predittivi e le tecnologie di Knowledge Reasoning Representation (KRR) che rappresentano l'evoluzione futura delle applicazioni di IA nel fintech.

8.3 Differenze tra modelli generativi e predittivi

L'intelligenza artificiale si avvale di due principali categorie di modelli, generativi e predittivi, che si distinguono per finalità, funzionamento e ambiti di applicazione. Entrambi i tipi rappresentano pilastri fondamentali nello sviluppo di soluzioni avanzate, ma sono caratterizzati da approcci e obiettivi distinti.

Modelli generativi

I modelli generativi sono progettati per apprendere la distribuzione probabilistica dei dati di input e per generare nuovi dati simili a quelli su cui sono stati addestrati. Questi modelli non si limitano a classificare o predire, ma possono creare contenuti nuovi, come immagini, testo o musica, che ricalcano le caratteristiche del dataset originale.

Un esempio emblematico è rappresentato dalle reti generative avversarie (GAN), utilizzate per generare immagini fotorealistiche, o dai modelli linguistici avanzati, come GPT, che producono testo coerente e contestualizzato. Nel contesto aziendale, i modelli generativi trovano applicazione nella creazione di scenari simulati, nella generazione di dati per il training di altri algoritmi e nel miglioramento dell'esperienza utente tramite contenuti personalizzati [37].

Modelli predittivi

I modelli predittivi, invece, si concentrano sull'analisi dei dati esistenti per prevedere eventi futuri o identificare relazioni nascoste. Essi utilizzano tecniche di apprendimento supervisionato o non supervisionato per costruire relazioni tra le variabili di input e i risultati attesi.

Un esempio comune di modello predittivo è rappresentato dalle reti neurali profonde (DNN), impiegate per stimare il rischio di credito, prevedere fluttuazioni di mercato o identificare comportamenti fraudolenti. Questi modelli sono fondamentali nel settore fintech per prendere decisioni basate sui dati e per migliorare l'accuratezza delle previsioni [38].

Confronto tra modelli generativi e predittivi

Le differenze principali tra i modelli generativi e predittivi possono essere riassunte nei seguenti punti:

- **Finalità**: i modelli generativi si concentrano sulla creazione di nuovi dati, mentre i modelli predittivi si focalizzano sull'identificazione di relazioni e sulla previsione di eventi futuri.
- **Approccio ai dati**: i modelli generativi apprendono l'intera distribuzione probabilistica dei dati, mentre i modelli predittivi costruiscono una mappatura diretta tra input e output.
- **Applicazioni**: i modelli generativi sono utilizzati in contesti creativi, simulativi e di arricchimento dei dati, mentre i modelli predittivi trovano impiego in ambiti analitici e decisionali.
- **Complessità computazionale**: I modelli generativi tendono a essere più complessi dal punto di vista computazionale, poiché devono ricostruire l'intera distribuzione dei dati, mentre i modelli predittivi, se ben progettati, possono risultare più efficienti [39].

Complementarità tra modelli generativi e predittivi

Sebbene distinti, i modelli generativi e predittivi possono essere integrati per creare soluzioni più potenti. Ad esempio, i modelli generativi possono produrre dati sintetici per addestrare modelli predittivi, migliorandone l'efficacia in scenari con dataset limitati. Questa complementarità è particolarmente rilevante nel fintech, dove la combinazione di capacità generative e predittive consente di sviluppare strumenti avanzati per la gestione del rischio, la personalizzazione dei servizi e la simulazione di scenari finanziari complessi.

L'analisi delle differenze tra modelli generativi e predittivi evidenzia come ciascuna categoria offra vantaggi unici in base agli obiettivi e al contesto applicativo. Nei capitoli successivi, verrà approfondito l'impiego di tecnologie predittive e KRR (Knowledge Reasoning Representation) per l'ottimizzazione dei controlli di conformità e per lo sviluppo di soluzioni intelligenti nel settore fintech.

8.4 Tecnologie predictive AI e KRR (Knowledge Reasoning Representation)

L'Intelligenza Artificiale Predittiva (Predictive AI) rappresenta un'area di sviluppo tecnologico che mira a prevedere eventi futuri basandosi su schemi e correlazioni

identificati in grandi volumi di dati storici. Accanto a questa, la Knowledge Reasoning Representation (KRR) si distingue per la sua capacità di integrare il ragionamento logico con rappresentazioni strutturate della conoscenza, permettendo di affrontare problemi complessi che richiedono sia apprendimento che deduzione.

Predictive AI: una visione dettagliata

La Predictive AI si basa sull'applicazione di tecnologie avanzate di machine learning e analisi statistica. Le sue principali applicazioni includono:

- **Analisi predittiva delle frodi**: algoritmi come le reti neurali profonde (Deep Learning) analizzano transazioni in tempo reale per rilevare schemi anomali associati a potenziali attività fraudolente.
- **Ottimizzazione della gestione del rischio**: i modelli predittivi supportano le istituzioni finanziarie nella valutazione del rischio di credito e nel miglioramento della resilienza operativa.
- **Personalizzazione dei servizi**: i sistemi predittivi utilizzano dati demografici e comportamentali per creare esperienze utente altamente personalizzate, migliorando la soddisfazione del cliente.

Questi sistemi si basano su tecniche come regressione, alberi decisionali e reti neurali, che prevedono scenari futuri con un'alta precisione.

Knowledge Reasoning Representation (KRR): concetti fondamentali

La Knowledge Reasoning Representation (KRR) combina strumenti di rappresentazione della conoscenza, con capacità di ragionamento logico. A differenza della Predictive AI, che si basa principalmente su dati storici, KRR si focalizza sulla comprensione e deduzione basate su strutture formalizzate.

Elementi chiave di KRR

- **Ontologie**: forniscono una descrizione formale di concetti e relazioni all'interno di un dominio specifico, permettendo una rappresentazione uniforme della conoscenza.
- **Grafi della conoscenza**: questi grafi collegano entità e relazioni in modo che i sistemi possano inferire nuove informazioni basandosi sulle connessioni esistenti.
- **Logica descrittiva**: utilizzata per esprimere regole, vincoli e deduzioni che consentono di automatizzare molte deduzioni logiche.

Sinergia tra Predictive AI e KRR

L'integrazione tra Predictive AI e KRR offre un potente framework per affrontare scenari complessi, combinando l'analisi statistica e il ragionamento logico. Questa sinergia è cruciale in contesti in cui non basta prevedere, ma è necessario comprendere le implicazioni delle previsioni.

Esempi di applicazione

- **Fintech e conformità normativa**: predictive AI può anticipare potenziali anomalie nelle transazioni, mentre KRR identifica connessioni e relazioni tra entità per garantire la conformità alle normative.

- **Gestione del rischio**: l'unione di modelli predittivi e grafi della conoscenza consente di valutare i rischi legati a specifici attori, identificando schemi ricorrenti e deducendo nuove minacce.

- **Piattaforme di raccomandazione**: i grafi della conoscenza possono arricchire i modelli predittivi, migliorando la precisione delle raccomandazioni offerte agli utenti.

Prospettive di sviluppo

Le prospettive future per Predictive AI e KRR sono promettenti, grazie all'evoluzione di tecnologie come il cloud computing e l'elaborazione ad alte prestazioni (HPC). La Predictive AI sta progredendo verso modelli più spiegabili (Explainable AI), aumentando la fiducia degli utenti. Parallelamente, KRR si sta integrando con tecniche di Natural Language Processing (NLP), permettendo una comprensione più avanzata dei dati testuali.

L'espansione di queste tecnologie rappresenta una sfida e un'opportunità per i settori regolamentati, in cui la trasparenza e la tracciabilità delle decisioni sono fondamentali. In particolare, il loro impiego in applicazioni come i controlli PEP e OFAC potrebbe rivoluzionare l'efficienza e l'accuratezza delle verifiche, riducendo al contempo i costi operativi.

L'integrazione tra Predictive AI e KRR è destinata a diventare uno standard nei processi decisionali automatizzati, offrendo soluzioni innovative e scalabili per gestire le sfide sempre più complesse dei mercati globali.

8.5 Vantaggi dell'intelligenza artificiale nell'ottimizzazione dei controlli PEP e OFAC

L'introduzione dell'intelligenza artificiale (IA) nei controlli di conformità PEP e OFAC ha segnato un punto di svolta per l'efficienza e l'accuratezza dei processi di compliance. Grazie alla sua capacità di analizzare grandi volumi di dati e di apprendere dai modelli storici, l'IA offre vantaggi significativi in termini di velocità, scalabilità e riduzione del rischio operativo.

1. Automazione e velocità dei controlli

I tradizionali processi manuali di conformità richiedono tempi significativi per l'analisi delle transazioni e la verifica dei dati. L'IA consente di automatizzare queste operazioni, riducendo drasticamente i tempi di elaborazione. Ad esempio, algoritmi di machine learning possono analizzare in tempo reale le transazioni di grandi volumi, identificando anomalie o potenziali violazioni con una rapidità impossibile per gli operatori umani.

L'automazione basata sull'IA elimina gran parte della necessità di intervento manuale nei controlli preliminari, permettendo agli underwriter di concentrarsi su analisi più complesse e strategiche. Questo migliora non solo l'efficienza operativa, ma anche la qualità del lavoro svolto.

2. Riduzione dei falsi positivi

Uno dei principali problemi nei controlli di conformità è rappresentato dall'alto numero di falsi positivi, ovvero casi in cui un'entità o una transazione viene erroneamente segnalata come sospetta. L'intelligenza artificiale, grazie all'utilizzo di algoritmi predittivi e modelli di apprendimento supervisionato, è in grado di ridurre sensibilmente questo problema.

L'IA può apprendere dai dati storici per migliorare continuamente le proprie prestazioni, affinando i criteri di classificazione e minimizzando le segnalazioni non necessarie. Questo si traduce in un risparmio di tempo e risorse, oltre a una maggiore precisione nei risultati.

3. Analisi predittiva e identificazione delle minacce emergenti

L'intelligenza artificiale consente non solo di analizzare i dati attuali, ma anche di prevedere schemi di rischio futuri. Questo è particolarmente utile in un contesto dinamico come quello della conformità, dove le minacce evolvono rapidamente e richiedono risposte immediate.

Attraverso l'uso di tecniche avanzate di analisi predittiva, come le reti neurali e i modelli di clustering, l'IA può identificare tendenze latenti che potrebbero indicare comportamenti fraudolenti o violazioni normative. Queste capacità predittive permettono di intervenire tempestivamente, riducendo i rischi prima che si concretizzino.

4. Integrazione con sistemi di Knowledge Reasoning Representation (KRR)

Un ulteriore vantaggio dell'IA è la possibilità di integrarla con sistemi di rappresentazione della conoscenza come i KRR. Questa sinergia consente di combinare capacità predittive e ragionamento logico, migliorando l'accuratezza e la trasparenza dei controlli.

Grazie ai KRR, i sistemi basati sull'IA possono comprendere e rappresentare le complesse relazioni tra entità finanziarie, creando una visione completa e contestualizzata delle verifiche di conformità. Questo approccio aumenta la capacità di prendere decisioni informate e riduce il rischio di errori.

5. Scalabilità e adattabilità a contesti globali

L'IA offre una scalabilità senza precedenti, rendendola particolarmente adatta per gestire i crescenti volumi di dati e le esigenze di conformità in contesti globali. I sistemi basati sull'IA possono adattarsi rapidamente a nuovi requisiti normativi, garantendo una conformità continua anche in ambienti regolamentari complessi e in rapida evoluzione.

L'intelligenza artificiale consente di standardizzare i controlli su scala globale, adattandosi alle specifiche normative di ogni giurisdizione. Questo non solo riduce i costi di gestione, ma migliora anche la coerenza e l'efficacia delle operazioni di compliance.

L'adozione dell'intelligenza artificiale nei controlli di conformità PEP e OFAC rappresenta un passo decisivo verso un futuro più efficiente, sicuro e conforme. La combinazione di automazione, analisi predittiva e capacità di ragionamento logico offre una soluzione integrata per affrontare le sfide sempre più complesse del panorama finanziario globale. Questi sviluppi non solo migliorano la capacità di rilevare e prevenire attività illecite, ma contribuiscono anche a rafforzare la fiducia degli stakeholder nei mercati finanziari.

Capitolo 9

Applicazioni della predictive AI

L'intelligenza artificiale predittiva (Predictive AI) è diventata una delle tecnologie più influenti del nostro tempo, rivoluzionando innumerevoli settori grazie alla sua capacità di analizzare grandi quantità di dati, identificare schemi ricorrenti e fornire previsioni precise. Questa tecnologia consente non solo di risolvere problemi complessi, ma anche di anticipare eventi, migliorando l'efficienza operativa e la qualità delle decisioni.

Nel contesto odierno, caratterizzato da una crescente complessità e da una connessione globale, la Predictive AI si è dimostrata indispensabile per affrontare le sfide emergenti. Attraverso modelli avanzati e tecnologie innovative, offre vantaggi significativi in termini di riduzione dei costi, mitigazione dei rischi e ottimizzazione dei processi. Questo capitolo esplora le applicazioni principali della Predictive AI, analizzando settori come il finance, la sanità e la difesa, per poi approfondire il suo ruolo cruciale nel fintech.

9.1 Settori principali di applicazione

La Predictive AI è una tecnologia adottata in numerosi ambiti per affrontare problemi complessi e generare valore attraverso l'analisi predittiva dei dati. Tra i settori che ne hanno tratto maggiori benefici troviamo il finance, la sanità e il settore della difesa. Questi contesti mostrano come essa possa adattarsi a esigenze diverse, fornendo soluzioni su misura per ogni ambito.

9.1.1 Finance, fintech e banking

Il settore finanziario è uno dei principali beneficiari della Predictive AI, che viene impiegata per ottimizzare la gestione del rischio, garantire la conformità normativa e migliorare l'efficienza operativa. Le principali applicazioni includono:

- **Rilevamento delle frodi**: la Predictive AI analizza milioni di transazioni al secondo, identificando schemi sospetti che potrebbero indicare attività fraudolente. Ad esempio, PayPal utilizza algoritmi di machine learning per rilevare comportamenti anomali in tempo reale, riducendo significativamente le perdite finanziarie dovute a frodi [40].
- **Valutazione del credito**: sistemi predittivi analizzano dati storici, comportamentali e demografici per stimare con maggiore precisione la capacità di rimborso dei richiedenti, migliorando i tassi di accettazione dei prestiti senza aumentare i rischi.
- **Gestione degli investimenti**: i robo-advisor, basati su algoritmi predittivi, offrono analisi personalizzate e strategie di investimento ottimizzate, consentendo anche agli investitori meno esperti di accedere a soluzioni finanziarie avanzate.
- **Compliance normativa**: sistemi come quelli per i controlli PEP e OFAC, già trattati nei capitoli precedenti, rappresentano esempi concreti di come la Predictive AI possa essere utilizzata per anticipare potenziali violazioni normative, automatizzando processi complessi e garantendo una maggiore efficienza.

Queste applicazioni evidenziano come l'Predictive AI sia fondamentale per migliorare la competitività, mitigare i rischi e rispondere alle sfide di un settore in continua evoluzione.

9.1.2 Sanità

La Predictive AI sta trasformando profondamente il settore sanitario, migliorando la diagnosi, l'efficienza operativa e la qualità dell'assistenza. Tra le applicazioni principali troviamo:

- **Prevenzione delle malattie**: modelli predittivi analizzano dati clinici, genetici e ambientali per identificare pazienti a rischio di sviluppare malattie croniche o rare. Ad esempio, algoritmi avanzati sono utilizzati per prevedere l'insorgenza di malattie cardiovascolari o diabetiche, consentendo interventi preventivi mirati [41].

- **Diagnosi precoce**: l'intelligenza artificiale supporta i medici nell'interpretazione di immagini mediche, come TAC e risonanze magnetiche, identificando con maggiore accuratezza tumori o altre anomalie rispetto ai metodi tradizionali.

- **Ottimizzazione delle risorse**: gli ospedali utilizzano algoritmi predittivi per prevedere il flusso di pazienti, migliorando la gestione del personale, delle attrezzature e delle scorte di medicinali. Ad esempio, durante la pandemia di COVID-19, modelli predittivi hanno aiutato a stimare la domanda di posti letto in terapia intensiva.

- **Medicina personalizzata**: la Predictive AI consente di sviluppare trattamenti su misura, basati sull'analisi dei dati genetici e clinici di ciascun paziente.

Case Study: Previsione delle complicazioni diabetiche tramite modelli predittivi

Il diabete rappresenta una delle patologie croniche più diffuse a livello globale, con milioni di pazienti a rischio di sviluppare complicazioni severe come insufficienza renale, neuropatia e malattie cardiovascolari. Per affrontare queste sfide, l'intelligenza artificiale predittiva ha dimostrato di essere uno strumento chiave nella prevenzione e gestione dei rischi associati.

Un esempio significativo è rappresentato dal progetto *Diabetes Predict*, un'iniziativa che utilizza algoritmi di *machine learning* per analizzare dati clinici storici, tra cui livelli glicemici, pressione arteriosa, dieta e fattori genetici. Grazie a questa analisi avanzata, il sistema identifica i pazienti con un'elevata probabilità di sviluppare complicazioni gravi, consentendo ai medici di pianificare interventi tempestivi e personalizzare i trattamenti [42].

I principali passaggi implementati includono:

- **Raccolta dei dati**: un ampio dataset di pazienti diabetici, contenente parametri medici, anamnesi e risultati di esami di laboratorio.

- **Addestramento del modello**: Un modello predittivo basato su reti neurali ricorrenti (RNN), progettato per identificare correlazioni complesse tra i fattori di rischio.

- **Classificazione del rischio**: i pazienti vengono suddivisi in categorie di rischio (basso, medio, alto) con livelli di confidenza associati, migliorando l'efficienza degli interventi clinici [43].

- **Monitoraggio continuo**: tramite un'app mobile, i pazienti possono registrare parametri quotidiani come glicemia e dieta. Questi dati vengono integrati automaticamente nel sistema per aggiornare il profilo di rischio in tempo reale.

I risultati ottenuti da *Diabetes Predict* sono stati particolarmente significativi:

- Una riduzione del 30% nelle ospedalizzazioni legate a complicazioni diabetiche [44].

- Un miglioramento dell'aderenza ai trattamenti grazie a notifiche personalizzate inviate ai pazienti a rischio.

- Una gestione più efficiente delle risorse sanitarie, con un focus mirato sui pazienti più vulnerabili.

Questi dati dimostrano come la predictive AI non solo migliori la qualità delle cure, ma riduca anche i costi complessivi del sistema sanitario, offrendo un modello scalabile per la gestione di altre patologie croniche [45].

9.1.3 Settore della difesa

Nel settore della difesa, la predictive AI gioca un ruolo fondamentale, migliorando la sicurezza e l'efficienza delle operazioni. Le principali applicazioni includono:

- **Previsione delle minacce**: gli algoritmi predittivi analizzano dati geopolitici, movimenti di truppe e attività sospette per identificare potenziali conflitti o attacchi imminenti. Ad esempio, il Pentagono utilizza sistemi avanzati per monitorare le minacce cibernetiche e fisiche in tempo reale.

- **Manutenzione predittiva**: l'IA viene impiegata per monitorare in modo continuo lo stato degli equipaggiamenti militari, prevedendo guasti e riducendo i tempi di inattività operativa.

- **Ottimizzazione della logistica**: algoritmi predittivi supportano la pianificazione di missioni e la gestione delle risorse, garantendo che i materiali critici siano consegnati in modo tempestivo e sicuro.

- **Supporto decisionale**: la Predictive AI viene integrata nei centri di comando per fornire analisi in tempo reale, aiutando i comandanti a prendere decisioni informate durante le operazioni.

Case Study: Prevenzione degli attacchi informatici con sistemi predittivi

Nel settore della difesa, la protezione da attacchi informatici rappresenta una priorità assoluta. Con l'evoluzione delle minacce, le tradizionali tecniche di rilevamento basate su regole statiche si sono rivelate insufficienti a fronte di attacchi sempre più sofisticati. La Predictive AI ha introdotto un cambio di paradigma, offrendo strumenti avanzati per identificare minacce imminenti e prevenire violazioni di sicurezza [46].

Un esempio di applicazione di successo è il sistema *CyberShield*, sviluppato per il monitoraggio e la protezione delle infrastrutture critiche. Questo sistema utilizza modelli di *machine learning* e analisi comportamentale per identificare attività sospette all'interno della rete.

I principali componenti implementati includono:

- **Monitoraggio in tempo reale**: analizza in modo continuo il traffico di rete, cercando anomalie rispetto al comportamento abituale degli utenti e dei sistemi.
- **Modelli predittivi basati su reti neurali**: gli algoritmi analizzano grandi volumi di dati storici per prevedere schemi di attacco ricorrenti, come tentativi di accesso non autorizzato o esfiltrazione di dati sensibili [47].
- **Risposta automatizzata**: in caso di rilevamento di una minaccia, il sistema attiva contromisure automatiche, come il blocco di IP sospetti, la disconnessione di dispositivi compromessi o la limitazione del traffico su determinati canali.
- **Integrazione con sistemi di intelligence**: si collega a database globali di minacce per aggiornare costantemente i modelli di rilevamento.

Grazie a questa architettura, *CyberShield* ha dimostrato di essere un sistema altamente efficace. Alcuni risultati ottenuti includono:

- Una riduzione del 40% nel tempo medio necessario per rilevare e rispondere a un attacco [48].
- Una diminuzione dei falsi positivi, migliorando la precisione del 30% rispetto ai sistemi tradizionali.
- Un incremento della resilienza complessiva delle infrastrutture difensive, con una prevenzione proattiva di attacchi ransomware e DDoS.

Questi risultati sottolineano il ruolo strategico della predictive AI nel settore della difesa, non solo per la protezione delle reti informatiche ma anche per l'ottimizzazione delle risorse e la risposta rapida alle emergenze. Con l'ulteriore sviluppo di tecnologie basate su AI, il settore della difesa può raggiungere un nuovo livello di sicurezza, anticipando le minacce invece di reagire a incidenti già avvenuti [49].

Capitolo 10

Conclusioni

10.1 Sintesi dei risultati raggiunti

Il percorso affrontato in questa tesi ha permesso di analizzare e sviluppare soluzioni avanzate per la gestione dei controlli di conformità PEP e OFAC, sfruttando tecnologie innovative come l'intelligenza artificiale e l'automazione. Tra i principali risultati conseguiti:

- **Implementazione dei controlli di conformità**: sono stati progettati e realizzati endpoint dedicati per la gestione automatizzata dei controlli PEP e OFAC, integrando feature flag per un rilascio graduale e sicuro delle funzionalità.
- **Ottimizzazione dei processi di conformità**: l'adozione di un sistema automatizzato ha ridotto i tempi di elaborazione, migliorato l'accuratezza dei controlli e minimizzato i rischi associati a errori umani.
- **Sviluppo di test automatizzati**: sono stati creati test robusti per verificare il corretto funzionamento degli endpoint e la gestione dei permessi, garantendo l'affidabilità del sistema.
- **Approfondimenti teorici**: sono stati esaminati i vantaggi dell'intelligenza artificiale, con un focus sull'applicazione di tecnologie predittive e sistemi di Knowledge Reasoning Representation (KRR), evidenziandone il ruolo cruciale nel settore fintech.

Questi risultati dimostrano come l'integrazione di tecnologie moderne e una progettazione accurata possano contribuire significativamente al miglioramento della sicurezza, della conformità normativa e dell'efficienza operativa nei sistemi finanziari.

10.2 Prospettive di sviluppo futuro

L'evoluzione tecnologica e le crescenti esigenze normative offrono molteplici opportunità per il miglioramento e l'espansione dei sistemi di conformità e sicurezza. Tra le principali prospettive di sviluppo futuro:

- **Intelligenza artificiale avanzata**: l'implementazione di modelli predittivi più sofisticati, combinati con l'elaborazione semantica avanzata (KRR), potrebbe migliorare ulteriormente l'accuratezza dei controlli di conformità, riducendo i falsi positivi e fornendo analisi predittive.
- **Integrazione con blockchain**: l'uso della tecnologia blockchain potrebbe garantire una tracciabilità immutabile dei controlli effettuati, aumentando la fiducia e la trasparenza nel sistema.
- **Espansione a nuovi ambiti di applicazione**: le soluzioni implementate potrebbero essere adattate a settori diversi dal fintech, come la sanità e la difesa, dove la gestione delle identità e dei controlli di conformità è altrettanto critica.
- **Automazione delle verifiche globali**: lo sviluppo di sistemi in grado di integrare normative e liste di sanzioni globali in tempo reale rappresenta un passo avanti verso la standardizzazione dei controlli di conformità.
- **Miglioramento dell'esperienza utente**: l'integrazione di interfacce intuitive per gli underwriter e report personalizzati potrebbe semplificare ulteriormente la gestione delle operazioni, riducendo la curva di apprendimento e migliorando l'efficienza operativa.

In conclusione, il lavoro svolto rappresenta un importante contributo verso la costruzione di un sistema finanziario più sicuro, conforme e tecnologicamente avanzato. Le prospettive delineate sottolineano il potenziale di ulteriori innovazioni, che potranno contribuire a ridefinire gli standard operativi e di sicurezza in un settore in continua evoluzione.

Bibliografia

[1] Noi Notizie. *Carenze nell'organizzazione e nei controlli interni: sanzionata Banca del Sud*. 2022. URL: https://www.noinotizie.it/28-06-2022/carenze-nellorganizzazione-e-nei-controlli-interni-sanzionata-banca-del-sud/ (cit. a p. 6).

[2] European Commission. *Fifth Anti-Money Laundering Directive*. 2022. URL: https://ec.europa.eu/anti-money-laundering (cit. a p. 6).

[3] Deloitte Insights. *The Cost of Compliance in Financial Services*. 2021. URL: https://www2.deloitte.com (cit. a p. 6).

[4] Reuters. *Standard Chartered fined 1 billion for Anti−Money Laundering Failures*. 2019. URL: https://www.reuters.com (cit. a p. 7).

[5] McKinsey Company. «The Future of AML Compliance: Leveraging Technology for Better Outcomes». In: *McKinsey Insights* (2020). URL: https://www.mckinsey.com (cit. a p. 7).

[6] JPMorgan Chase. *How AI is Transforming Compliance in Banking*. 2022. URL: https://www.jpmorganchase.com (cit. a p. 7).

[7] HSBC. *Cloud Transformation in Financial Compliance*. 2021. URL: https://www.hsbc.com (cit. a p. 8).

[8] George Westerman, Didier Bonnet e Andrew McAfee. *Leading Digital: Turning Technology into Business Transformation*. Boston, MA: Harvard Business Review Press, 2021 (cit. a p. 9).

[9] McKinsey Company. «How Automation is Driving Efficiency». In: *McKinsey Insights* (2020). URL: https://www.mckinsey.com (cit. alle pp. 10, 11).

[10] Forrester Research. «The Evolution of Digital Customer Expectations». In: *Forrester Insights* (2022). URL: https://www.forrester.com (cit. a p. 10).

[11] Gartner. «Digital Transformation in Banking: A Strategic Imperative». In: *Gartner Research* (2021). URL: https://www.gartner.com (cit. a p. 10).

[12] European Banking Authority. *Guidelines on Anti-Money Laundering and Counter-Terrorist Financing*. 2023. URL: https://www.eba.europa.eu (cit. a p. 11).

[13] Spotify. *Transforming the Music Industry through Digital Innovation*. Spotify Corporate Report. 2020. URL: https://newsroom.spotify.com (cit. a p. 11).

[14] Financial Action Task Force. *Guidance on Politically Exposed Persons*. 2022. URL: https://www.fatf-gafi.org (cit. a p. 21).

[15] Office of Foreign Assets Control. *Sanctions Compliance Guidance for the Banking Industry*. 2021. URL: https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information (cit. a p. 21).

[16] Deloitte. *The Future of Compliance: Leveraging Technology for Enhanced Risk Management*. 2023. URL: https://www2.deloitte.com (cit. alle pp. 53, 54).

[17] NIST. *Digital Identity Guidelines*. 2020. URL: https://www.nist.gov (cit. alle pp. 54, 55).

[18] Forrester. *State of IAM 2020*. 2020. URL: https://www.forrester.com (cit. alle pp. 54–56).

[19] AWS. *Case Study: Capital One Data Breach*. 2019. URL: https://aws.amazon.com/security (cit. a p. 55).

[20] Zoom. *Zoom's Security Enhancements during COVID-19*. 2020. URL: https://blog.zoom.us (cit. a p. 55).

[21] Microsoft. *Azure Active Directory (AAD): Features and Benefits*. 2022. URL: https://azure.microsoft.com (cit. alle pp. 55, 56).

[22] Deloitte. *BYOD and Security: The Next Evolution*. 2023. URL: https://www2.deloitte.com (cit. a p. 55).

[23] McKinsey. *Securing the IoT Landscape: Challenges and Opportunities*. 2022. URL: https://www.mckinsey.com (cit. a p. 55).

[24] Google. *Identity-Aware Proxy Overview*. 2021. URL: https://cloud.google.com/iap (cit. a p. 55).

[25] IETF. *The Transport Layer Security (TLS) Protocol Version 1.3*. 2020. URL: https://datatracker.ietf.org/doc/html/rfc8446 (cit. a p. 57).

[26] PCI Security Standards Council. *Payment Card Industry Data Security Standard (PCI DSS)*. 2023. URL: https://www.pcisecuritystandards.org (cit. alle pp. 57, 59).

[27] European Commission. *Payment Services Directive 2 (PSD2) - Strong Customer Authentication (SCA)*. 2018. URL: `https://ec.europa.eu/finance` (cit. a p. 57).

[28] JWT. *JSON Web Tokens - Overview and Implementation*. 2020. URL: `https://jwt.io` (cit. a p. 57).

[29] OWASP. *OWASP API Security Top 10*. 2021. URL: `https://owasp.org/www-project-api-security/` (cit. a p. 57).

[30] PayPal. *Fraud Prevention with Machine Learning*. 2022. URL: `https://www.paypal.com/security` (cit. a p. 58).

[31] Revolut. *Enhanced Security with Strong Customer Authentication*. 2022. URL: `https://blog.revolut.com` (cit. a p. 58).

[32] Stripe. *Global Payment Security with Tokenization*. 2023. URL: `https://stripe.com/security` (cit. alle pp. 58, 60).

[33] RS2. *RS2 Payment Processing Solutions*. 2023. URL: `https://www.rs2.com` (cit. a p. 59).

[34] OAuth. *OAuth 2.0 Framework*. 2020. URL: `https://oauth.net/2/` (cit. a p. 59).

[35] PayPal. «How AI is Revolutionizing Fraud Prevention at PayPal». In: *PayPal Insights* (2021). URL: `https://www.paypal.com` (cit. a p. 60).

[36] Amazon Web Services. *AWS Security Best Practices*. 2023. URL: `https://aws.amazon.com` (cit. a p. 60).

[37] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville e Yoshua Bengio. «Generative adversarial networks». In: *arXiv preprint arXiv:1406.2661* (2014). URL: `https://arxiv.org/abs/1406.2661` (cit. a p. 65).

[38] Trevor Hastie, Robert Tibshirani e Jerome Friedman. *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*. 2nd. Springer, 2009 (cit. a p. 65).

[39] Christopher M. Bishop. *Pattern Recognition and Machine Learning*. 2006. URL: `https://www.springer.com/gp/book/9780387310732` (cit. a p. 66).

[40] MIT Technology Review. *How Predictive AI is Revolutionizing Fraud Detection*. 2023. URL: `https://www.technologyreview.com/` (cit. a p. 72).

[41] World Health Organization. *Artificial Intelligence in Healthcare: Trends and Challenges*. 2023. URL: `https://www.who.int/` (cit. a p. 72).

[42] Diabetes Predict Initiative. *Machine Learning for Diabetes Complications Prevention*. Diabetes Predict Organization, 2023. URL: `https://www.diabetespredict.org` (cit. a p. 73).

[43] The Lancet Digital Health. «Artificial Intelligence in Chronic Disease Management: A Review». In: *The Lancet* 3.5 (2021), e315–e325. URL: https://www.thelancet.com (cit. a p. 73).

[44] World Health Organization. «Diabetes Facts: Chronic Disease Management and Complications». In: *WHO Reports* (2022). URL: https://www.who.int/diabetes (cit. a p. 74).

[45] National Institutes of Health. *AI Applications in Healthcare: Progress and Challenges*. 2023. URL: https://www.nih.gov (cit. a p. 74).

[46] Cyber Defense Magazine. «AI-Driven Cybersecurity: How Predictive Models Are Revolutionizing Defense». In: *Cyber Defense Quarterly* (2022). URL: https://www.cyberdefensemagazine.com (cit. a p. 75).

[47] Deloitte. *Enhancing Cybersecurity with AI and Predictive Analytics*. 2023. URL: https://www2.deloitte.com (cit. a p. 75).

[48] Gartner. *Predictive Analytics in Financial Services*. 2022. URL: https://www.gartner.com/ (cit. a p. 75).

[49] National Institute for Advanced Defense. *AI for National Security: Applications and Challenges*. 2023. URL: https://www.niad.org (cit. a p. 75).

Ringraziamenti

Ringrazio la mia famiglia, *mamma*, *papà*, *Martina* e *Buddy*, mi avete sempre supportato e messo nelle condizioni di condurre questo percorso con la massima serenità.

Ringrazio *Andrea* per la tua disponibilità e generosità, mi hai permesso di portare avanti, con successo, sia studio che lavoro.

Ringrazio *me stesso*. La determinazione, l'impegno e la costanza sono state la chiave di questo traguardo.