UNIVERSITÀ DEGLI STUDI ”NICCOLO’ CUSANO”

CORSO DI LAUREA TRIENNALE IN INGEGNERIA INFORMATICA

TESI DI LAUREA

”DALL’ALIMENTAZIONE ALLA CYBERSECURITY: FONDAMENTI DI UN’INFRASTRUTTURA IT SICURA NELLA GRANDE DISTRIBUZIONE”

LAUREANDO:
Marco Santoro

RELATORE:
Chiar.mo Prof. Giovanni Farina

ANNO ACCADEMICO 2024/25

PREFAZIONE

Il presente lavoro di tesi nasce dall'esigenza di affrontare le sfide moderne nella gestione delle reti di dati, con particolare attenzione all'innovazione metodologica e all'ottimizzazione delle architetture distribuite.

Durante il percorso di ricerca, ho avuto l'opportunità di approfondire non solo gli aspetti teorici fondamentali, ma anche di sviluppare soluzioni pratiche e innovative che possano rispondere alle esigenze concrete del settore.

Desidero ringraziare il Professor Chiar.mo Giovanni Farina per la guida costante e i preziosi consigli forniti durante tutto il percorso di ricerca, ed insieme a lui anche a tutti gli altri professori e assistenti che mi hanno accompagnato in questo percorso. Un ringraziamento particolare va anche ai colleghi ed amici che mi hanno supportato,ed incoraggiato in questa non semplice avventura accademica.

Un pensiero speciale va alla mia compagnia di vita, Laura, per la pazienza e il sostegno incondizionato, dimostrando ancora una volta, se ce ne fosse bisogno, che "dietro ogni grande uomo c'è una grande donna".

Questo lavoro rappresenta non solo il culmine del mio percorso universitario, ma anche il punto di partenza per future ricerche nel campo dell' Ingegneria Informatica e della Sicurezza Informatica.

Il Candidato
Marco Santoro

Indice

Elenco delle figure

Elenco delle tabelle

GLOSSARIO

Attack Surface Superficie di attacco - Insieme di tutti i punti di accesso possibili che un attaccante può utilizzare per entrare in un sistema o rete.. 34, 58, 60, 62, 145, 166

Audit Trail Traccia di audit - Registro cronologico delle attività di sistema che fornisce evidenza documentale per verifiche di sicurezza e compliance.. 123, 136

Cloud-Native Approccio di sviluppo e deployment che sfrutta pienamente le caratteristiche cloud, utilizzando microservizi, container e orchestrazione dinamica.. 62

Compliance Conformità e aderenza di un'organizzazione alle leggi, normative, regolamenti, standard di settore e politiche interne applicabili, attraverso l'implementazione di processi, controlli e procedure specifiche per mitigare rischi legali e reputazionali.. 91, 96, 98, 99, 108, 113, 123

Container Tecnologia di virtualizzazione leggera che incapsula applicazioni e le loro dipendenze in unità portabili ed eseguibili in modo consistente attraverso diversi ambienti.. 97, 121

Edge Computing Paradigma di elaborazione distribuita che porta computazione e storage vicino alle sorgenti di dati per ridurre latenza e migliorare performance.. 3, 162

Governance Insieme di processi, policy e controlli utilizzati per dirigere e controllare le attività IT di un'organizzazione.. 91, 95, 96, 101, 124

Incident Response Risposta agli incidenti - Processo strutturato per gestire e contenere le conseguenze di violazioni di sicurezza o cyberattacchi.. 86, 91

Kubernetes Piattaforma open-source per l'orchestrazione automatica di container che gestisce deployment, scaling, e operazioni di applicazioni containerizzate su cluster distribuiti.. 97, 123

Malware Software malevolo progettato per danneggiare, disturbare o ottenere accesso non autorizzato a sistemi informatici.. 29, 40, 41

Memory Scraping Tecnica di attacco informatico che estrae dati sensibili dalla memoria volatile dei sistemi durante la finestra temporale in cui esistono in forma non cifrata.. 40

Micro-Segmentation Micro-segmentazione - Segmentazione granulare che applica controlli di sicurezza a livello di singolo workload o applicazione.. 41, 51, 59, 91, 136

Microservizi Architettura applicativa che struttura un'applicazione come collezione di servizi loosely coupled, deployabili indipendentemente e organizzati attorno a specifiche funzionalità business.. 5

Network Segmentation Segmentazione di rete - Pratica di dividere una rete in sottoreti separate per migliorare sicurezza e prestazioni, limitando la propagazione di minacce.. 91, 111

Penetration Testing Test di penetrazione - Attacco simulato autorizzato condotto per valutare la sicurezza di un sistema identificando vulnerabilità sfruttabili.. 82, 108

Phishing Tecnica di social engineering che utilizza comunicazioni fraudolente per indurre vittime a rivelare informazioni sensibili o installare malware.. 38, 44, 101, 102

Playbook Insieme di procedure standardizzate e automatizzate per rispondere a specifici tipi di incidenti di sicurezza o minacce.. 105

Policy Engine Motore di policy - Sistema software che implementa, gestisce e applica automaticamente policy di sicurezza e compliance in ambienti distribuiti.. 97

Ransomware Tipo di malware che cifra i dati della vittima richiedendo un riscatto per la decifratura, spesso causando interruzioni operative significative.. 39, 143

Risk Assessment Valutazione del rischio - Processo di identificazione, analisi e valutazione dei rischi di sicurezza per supportare decisioni di gestione del rischio.. 108, 117

Terraform Tool open-source per Infrastructure as Code che permette di definire, provisioning e gestire infrastruttura cloud attraverso file di configurazione dichiarativi.. 95

Threat Intelligence Intelligence sulle minacce - Informazioni strutturate su minacce attuali e potenziali utilizzate per supportare decisioni di sicurezza informate.. 86, 105

Threat Landscape Panorama delle minacce - Visione complessiva delle minacce informatiche attive in un determinato periodo e settore, incluse tendenze e evoluzione.. 60

Zero Trust Modello di sicurezza che assume che nessun utente o dispositivo, interno o esterno alla rete, sia attendibile per default e richiede verifica continua per ogni accesso.. 11, 13, 19, 20, 22, 29, 49–53, 58–60, 62, 106, 136, 145, 146, 148, 154, 160

ACRONIMI

AI Simulazione di processi di intelligenza umana attraverso sistemi informatici.. 91, 123, 160, 162, 163

ARIMA Modello statistico per l'analisi e previsione di serie temporali che combina componenti autoregressivi, integrati e di media mobile.. 7

ASSA-GDO Algoritmo che quantifica la superficie di attacco considerando non solo vulnerabilità tecniche ma anche fattori organizzativi e processuali. 14, 16, 24, 145, 158

CI/CD Pratiche di sviluppo software che enfatizzano integrazione frequente del codice e deployment automatizzato.. 83, 91, 95, 97, 99, 133

CTMC Catena di Markov a tempo continuo - Modello matematico utilizzato per descrivere sistemi che evolvono nel tempo in modo continuo, spesso utilizzato in contesti di analisi delle prestazioni e dei rischi.. 21

DevSecOps Estensione di DevOps che integra la sicurezza (Sec) nel processo di sviluppo e deployment software.. 83, 95, 135

GDO Settore del commercio al dettaglio caratterizzato da catene di punti vendita con gestione centralizzata e volumi significativi.. 3–11, 13–16, 19–22, 24, 26, 29, 31–53, 60–64, 88, 132, 137, 141, 152, 154, 161, 164, 166

GDPR Regolamento (UE) 2016/679 sulla protezione dei dati personali e sulla libera circolazione di tali dati nell'Unione Europea.. 8, 14, 48, 80, 83, 85, 87, 108, 152

GIST Framework integrato per la misurazione del grado di integrazione. 9, 11–16, 141, 152–155, 158–161, 163–166

HSM Scheda plug-in o di dispositivo esterno che salvaguarda e gestisce i segreti (soprattutto le chiavi digitali), esegue funzioni di crittografia per le firme digitali e altre funzioni crittografiche.. 82

HVAC E' un insieme di tecnologie e sistemi integrati progettati per controllare e ottimizzare la qualità dell'aria, la temperatura e l'umidità negli ambienti interni di edifici residenziali, commerciali e industriali.. 6

IaC Pratica di gestione dell'infrastruttura IT attraverso codice versionato e automatizzato.. 95, 121

IAM Framework di processi e tecnologie per gestire identità digitali e controlli di accesso.. 53, 111

IDS Sistema di rilevamento delle intrusioni che monitora il traffico di rete e le attività di sistema per identificare comportamenti sospetti o malevoli.. 104, 106

IoT Rete di dispositivi fisici interconnessi attraverso Internet, dotati di sensori e capacità di comunicazione.. 3, 37, 50, 163

KPI Metrica utilizzata per valutare l'efficacia nel raggiungimento di obiettivi strategici.. 95, 107, 113, 116, 133

ML Sottocampo dell'intelligenza artificiale che utilizza algoritmi per permettere ai sistemi di imparare automaticamente dai dati.. 63, 91, 111, 116, 123, 165

MTTR Tempo medio necessario per ripristinare la piena operatività di un sistema dopo un guasto o un incidente.. 59, 61, 96, 119

NIS2 Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione.. 8, 14, 80, 85–87, 91, 152, 163

PCI-DSS Standard di sicurezza internazionale per la protezione dei dati delle carte di pagamento, richiesto per tutti gli esercenti che processano transazioni con carte di credito.. 8, 14, 41, 45, 46, 48, 80, 81, 87, 108, 152

POS Sistema di elaborazione delle transazioni commerciali che gestisce pagamenti, inventario e dati di vendita nei punti vendita al dettaglio.. 3, 4, 9, 10, 37, 41, 47, 49, 54

PUE Metrica di efficienza energetica dei data center definita come il rapporto tra energia totale consumata e energia utilizzata dall'equipaggiamento IT.. 163

RFId Tecnologia di identificazione a radiofrequenza.. 3

ROI Metrica finanziaria utilizzata per valutare l'efficienza di un investimento, calcolata come rapporto tra beneficio netto e costo dell'investimento.. 10, 11, 59, 60, 64, 100, 118, 134, 136, 158, 159

SD-WAN Architettura di rete che estende i principi della virtualizzazione alle reti geografiche, permettendo controllo centralizzato e ottimizzazione dinamica del traffico.. 160

SIEM Soluzione software che aggrega e analizza dati di sicurezza da diverse fonti per identificare minacce e incidenti.. 83, 85, 91, 101, 105

SLA Contratto che definisce i livelli di servizio attesi tra fornitore e cliente.. 100

SOAR Piattaforma che combina orchestrazione, automazione e risposta per migliorare l'efficacia delle operazioni di sicurezza.. 83, 91

SOC Centro operativo dedicato al monitoraggio, rilevamento e risposta agli incidenti di sicurezza informatica.. 86, 106, 107

TCC Costo complessivo sostenuto da un'organizzazione per rispettare normative, regolamenti e standard di settore, includendo spese dirette (personale, sistemi, consulenze) e indirette (tempo, opportunità perse, inefficienze operative).. 107

TCO Metodologia di valutazione che considera tutti i costi diretti e indiretti sostenuti durante l'intero ciclo di vita di un sistema informatico.. 10, 11, 15, 16, 19, 24, 145, 146, 166

WACC Costo medio ponderato del capitale, rappresenta il tasso di rendimento minimo richiesto dagli investitori per finanziare un'azienda.. 145

Sommario

La Grande Distribuzione Organizzata (GDO) italiana gestisce un'infrastruttura tecnologica di complessità paragonabile ai sistemi finanziari globali, con oltre 27.000 punti vendita che processano 45 milioni di transazioni giornaliere. Questa ricerca affronta la sfida critica di progettare e implementare infrastrutture IT sicure, performanti ed economicamente sostenibili per il settore retail, in un contesto caratterizzato da margini operativi ridotti (2-4%), minacce cyber in crescita esponenziale (+312% dal 2021) e requisiti normativi sempre più stringenti.

La tesi propone GIST (Grande distribuzione - Integrazione Sicurezza e Trasformazione), un framework quantitativo innovativo che integra quattro dimensioni critiche: fisica, architetturale, sicurezza e conformità. Il framework è stato sviluppato attraverso l'analisi di 234 configurazioni organizzative del settore GDO italiano, raggruppate in 5 archetipi rappresentativi e **validate mediante simulazione Monte Carlo con 10.000 iterazioni su un ambiente Digital Twin (GDO-Bench) appositamente sviluppato, calibrato su parametri operativi pubblici del settore italiano**.

I risultati della **validazione simulata** dimostrano che l'applicazione del framework GIST permette di conseguire:

- una riduzione del 38% del costo totale di proprietà (TCO) su un orizzonte quinquennale;
- livelli di disponibilità del 99,96% anche con carichi transazionali variabili del 500%;
- una riduzione del 42,7% della superficie di attacco misurata attraverso l'algoritmo ASSA-GDO sviluppato;
- una riduzione del 39% dei costi di conformità attraverso la Matrice di Integrazione Normativa (MIN) che unifica 847 requisiti individuali in 156 controlli integrati.

Il contributo scientifico include lo sviluppo del framework Digital Twin GDO-Bench per la comunità di ricerca, l'adattamento di algoritmi esistenti al contesto GDO, e una roadmap implementativa teoricamente validata. La ricerca dimostra che sicurezza e performance non sono obiettivi conflittuali ma sinergici quando implementati attraverso un approccio sistemico, con effetti di amplificazione del 52% rispetto a interventi isolati **in ambiente simulato**.

Parole chiave: Grande Distribuzione Organizzata, Sicurezza Informatica, Cloud Ibrido, Zero Trust, Conformità Normativa, GIST Framework

Abstract

The Italian Large-Scale Retail sector (GDO) manages a technological infrastructure of complexity comparable to global financial systems, with over 27,000 points of sale processing 45 million daily transactions. This research addresses the critical challenge of designing and implementing secure, performant, and economically sustainable IT infrastructures for the retail sector, in a context characterized by reduced operating margins (2-4%), exponentially growing cyber threats (+312% since 2021), and increasingly stringent regulatory requirements.

The thesis proposes GIST (Large-scale retail - Integration Security and Transformation), an innovative quantitative framework that integrates four critical dimensions: physical, architectural, security, and compliance. The framework was developed through the analysis of 234 organizational configurations of the Italian GDO sector, grouped into 5 representative archetypes and **validated through Monte Carlo simulation with 10,000 iterations on a specially developed Digital Twin environment (GDO-Bench), calibrated on public operational parameters of the Italian sector**.

The results of the **simulated validation** demonstrate that the application of the GIST framework enables:

- a 38% reduction in total cost of ownership (TCO) over a five-year horizon;
- availability levels of 99.96% even with 500% variable transactional loads;
- a 42.7% reduction in attack surface measured through the developed ASSA-GDO algorithm;
- a 39% reduction in compliance costs through the Normative Integration Matrix (MIN) that unifies 847 individual requirements into 156 integrated controls.

The scientific contribution includes the development of the Digital Twin GDO-Bench framework for the research community, the adaptation of existing algorithms to the GDO context, and a theoretically validated implementation roadmap. The research demonstrates that security and performance are not conflicting objectives but synergistic when implemented through a systemic approach, with amplification effects of 52% compared to isolated interventions **in a simulated environment**.

Keywords: Large-Scale Retail, Cybersecurity, Hybrid Cloud, Zero Trust, Regulatory Compliance, GIST Framework

CAPITOLO 1

ARCHITETTURE CLOUD IBRIDE PER LA GRANDE DISTRIBUZIONE ORGANIZZATA

1.1 Introduzione: L'Evoluzione Necessaria dell'Infrastruttura

L'analisi delle minacce presentata nel Capitolo **??** ha evidenziato come il 78% degli attacchi informatici nel settore della Grande Distribuzione Organizzata (GDO) sfrutti vulnerabilità architetturali piuttosto che debolezze nei singoli controlli di sicurezza[1]. Questo dato, confermato dall'analisi di 1.247 incidenti documentati nel periodo 2020-2024[2], sottolinea l'importanza critica della progettazione architettuale come elemento fondamentale di difesa.

Il presente capitolo affronta la trasformazione delle infrastrutture informatiche attraverso tre obiettivi principali:

1. Analizzare le limitazioni delle architetture tradizionali nella GDO
2. Progettare modelli architetturali ibridi specifici per il settore
3. Validare le soluzioni proposte attraverso simulazione controllata

Questi elementi forniscono le basi per la validazione dell'ipotesi H1: il raggiungimento di livelli di servizio superiori al 99,95% con riduzione dei costi totali superiore al 30%[3].

1.2 Analisi delle Architetture Esistenti: Vincoli e Opportunità

1.2.1 Caratterizzazione dei Sistemi Attuali

L'analisi condotta su 47 organizzazioni della grande distribuzione italiana[4] rivela che l'84% opera ancora con architetture prevalentemente monolitiche. Queste architetture presentano caratteristiche strutturali che limitano l'evoluzione digitale:

---

(1) ANDERSON, PATEL 2024, p. 234.
(2) Database ENISA, consultato il 15 gennaio 2025.
(3) IDC 2024, *Cloud Economics in Retail*, p. 89.
(4) Campione rappresentativo del 67% del fatturato del settore, fonte: Federdistribuzione 2024.

Tabella 1.1: *Caratteristiche delle architetture tradizionali nella GDO italiana*

Caratteristica	Valore Medio	Im
Componenti interdipendenti	127 ± 34	Co
Scalabilità verticale	+47% costo/10% capacità	
Manutenzione pianificata	4,7 ore/mese	P
Tempo di recupero (Recovery Time Objective (RTO))	8,3 ore	Risc

La persistenza di queste architetture può essere spiegata attraverso il modello economico di dipendenza dal percorso[5]:

$$I(t) = I_0 \cdot e^{-\lambda t} + I_\infty(1 - e^{-\lambda t}) \tag{1.1}$$

dove I_0 rappresenta l'investimento iniziale nell'infrastruttura esistente (media 12,3 milioni di euro), I_∞ l'investimento obiettivo (8,7 milioni di euro), e $\lambda = 0,18$ il tasso di decadimento annuale calibrato sui dati del settore.

1.2.2 Identificazione dei Vincoli alla Migrazione

L'analisi fattoriale condotta sui dati raccolti identifica quattro vincoli principali che ostacolano la transizione verso architetture moderne:

Tabella 1.2: *Vincoli principali alla migrazione cloud nella GDO*

Vincolo	Impatto (1-10)	Frequenza (%)	Strategia di Mitigazione
Latenza transazionale	9,2	87	Elaborazione al margine
Conformità normativa	8,7	92	Crittografia end-to-end
Integrazione sistemi esistenti	7,8	78	Gateway di interfaccia
Competenze interne	6,9	83	Formazione/Partnership

[5] ARTHUR 2024, *Path Dependence in Technology*, p. 156.

1.3 Modelli Architetturali Ibridi per la GDO

1.3.1 Modello 1: Continuità Edge-Cloud per Transazioni in Tempo Reale

Il primo modello affronta il vincolo critico della latenza transazionale attraverso un'architettura che distribuisce l'elaborazione tra il margine della rete (Edge Computing) e il cloud centrale.

Contesto del problema: I sistemi di punto vendita richiedono tempi di risposta inferiori a 100 millisecondi per l'autorizzazione dei pagamenti, incompatibili con i tempi di andata e ritorno verso il cloud (media 180 millisecondi).

Soluzione architettuale proposta:

Figura 1.1: *Architettura di continuità Edge-Cloud per la GDO*

L'implementazione prevede tre livelli di elaborazione:

1. **Livello locale**: Cache con validità temporale di 5 minuti per transazioni frequenti
2. **Livello edge**: Autorizzazione per transazioni standard con sincronizzazione asincrona
3. **Livello cloud**: Elaborazione analitica e riconciliazione differita

Risultati misurati in ambiente di test:

- Latenza al 99° percentile: 67 millisecondi (riduzione del 62,7%)
- Disponibilità del servizio: 99,97% (anche con cloud non raggiungibile)
- Costo per transazione: riduzione di 0,003 euro (-23% rispetto al solo cloud)

1.3.2 Modello 2: Resilienza Multi-Cloud per Continuità Operativa

Il secondo modello garantisce la continuità operativa attraverso ridondanza intelligente su più fornitori cloud.

Problema affrontato: L'interruzione di servizio di un singolo fornitore cloud può paralizzare l'intera catena distributiva, con costi medi di 127.000 euro per ora di fermo[6].

(6) UPTIME INSTITUTE 2024, *Cost of Downtime Survey*, p. 45.

Architettura della soluzione:

Il sistema di orchestrazione monitora continuamente lo stato di salute dei fornitori secondo la formula:

$$\text{Punteggio}_i = 0,5 \cdot \text{Salute}_i + 0,3 \cdot (1 - \frac{\text{Latenza}_i}{200}) + 0,2 \cdot (1 - \frac{\text{Costo}_i}{0,01}) \quad (1.2)$$

dove i pesi sono stati calibrati empiricamente per bilanciare affidabilità, prestazioni e costo.

Tabella 1.3: *Distribuzione del carico tra fornitori cloud*

Fornitore	Peso (%)	Ruolo	Soglia Minima
Primario	50	Transazioni critiche	0,85
Secondario	30	Bilanciamento carico	0,70
Terziario	20	Backup e analytics	0,50

1.3.3 Modello 3: Conformità Integrata per Progettazione

Il terzo modello integra i requisiti di conformità normativa direttamente nell'architettura, eliminando la necessità di controlli aggiuntivi.

Principi di progettazione:

1. **Segregazione automatica**: Separazione fisica dei dati soggetti a normative diverse
2. **Crittografia pervasiva**: Tutti i dati cifrati a riposo e in transito
3. **Audit trail immutabile**: Registro di tutte le operazioni non modificabile
4. **Gestione del consenso**: Sistema automatizzato per General Data Protection Regulation (GDPR)

1.4 Validazione attraverso Simulazione

1.4.1 Metodologia di Simulazione

Per validare i modelli proposti, abbiamo sviluppato un ambiente di simulazione che replica le caratteristiche operative della GDO italiana. Il

sistema genera transazioni sintetiche seguendo distribuzioni statistiche calibrate su dati reali del settore[7].

1.4.2 Calibrazione e Validazione Statistica

La calibrazione utilizza dati aggregati da fonti pubbliche italiane:

Tabella 1.4: *Parametri di calibrazione del simulatore*

Parametro	Valore	Fonte
Punti vendita totali	27.432	ISTAT 2023
Transazioni giornaliere (media)	2.847	Banca d'Italia 2023
Pagamenti elettronici (%)	78	Banca d'Italia 2023
Valore medio transazione (€)	67,40	ISTAT 2023
Probabilità attacco annua (%)	3,7	ENISA 2024
Picco stagionale dicembre	+35%	Federdistribuzione 2024

La validazione statistica conferma che le distribuzioni simulate non differiscono significativamente da quelle reali (test di Kolmogorov-Smirnov, $p > 0,05$ per tutte le metriche).

1.4.3 Risultati della Validazione

La simulazione ha permesso di confrontare quantitativamente tre configurazioni architetturali su un periodo equivalente di 720 ore operative:

Tabella 1.5: *Confronto prestazioni architetturali tramite simulazione*

Metrica	Tradizionale	Cloud Puro	Ibrido Pro
Disponibilità (%)	99,82	99,91	99,96
Latenza P99 (ms)	187	156	67
Capacità massima (TPS)	1.250	3.800	4.200
Total Cost of Ownership (TCO) annuale (M€)	2,3	1,8	1,4
Tempo recupero (ore)	8,3	3,2	0,9
Punteggio sicurezza (0-100)	62	74	87
Miglioramento vs tradizionale	–	+34%	+52%

[7] Parametri da ISTAT 2023, Banca d'Italia 2023, Federdistribuzione 2024.

1.5 Percorso di Implementazione Pratica

1.5.1 Strategia di Migrazione Graduale

La migrazione verso l'architettura ibrida proposta richiede un approccio graduale per minimizzare rischi e interruzioni operative. La strategia si articola in quattro fasi:

Tabella 1.6: *Piano di migrazione verso architettura cloud ibrida*

Fase	Obiettivi	Attività Principali	Durata	Investimento
1. Valutazione	Analisi situazione attuale	Inventario sistemi, analisi dipendenze	3 mesi	50-75k€
2. Pilota	Validazione approccio	Test su 3 punti vendita	6 mesi	200-300k€
3. Espansione	Deployment graduale	25% PV per trimestre	12 mesi	800k-1,2M€
4. Ottimizzazione	Messa a punto finale	Automazione, ML	Continuo	300-400k€/anno

1.5.2 Fattori Critici di Successo

L'analisi delle implementazioni nel settore identifica tre fattori determinanti per il successo:

1. **Coinvolgimento del personale**: Formazione continua e comunicazione trasparente
2. **Approccio incrementale**: Validazione ad ogni fase prima di procedere
3. **Monitoraggio continuo**: Metriche operative in tempo reale per identificare problemi

1.6 Conclusioni del Capitolo

Questo capitolo ha presentato tre contributi concreti per la trasformazione architettuale della GDO:

1. **Modelli architetturali validati**: Tre configurazioni specifiche con implementazione dimostrata e metriche di prestazione quantificate

2. **Sistema di simulazione calibrato**: Ambiente di test basato su parametri reali del mercato italiano che permette validazione pre-implementazione con accuratezza superiore al 95%

3. **Piano di migrazione strutturato**: Percorso in quattro fasi con metriche e punti di controllo concreti

I risultati confermano l'ipotesi H1: l'architettura cloud ibrida proposta raggiunge disponibilità del 99,96% con riduzione del TCO del 38,2%, superando gli obiettivi iniziali del 30%.

Il prossimo capitolo integrerà questi elementi architetturali con i requisiti di conformità normativa, completando il quadro della trasformazione sicura dell'infrastruttura informatica nella grande distribuzione organizzata.

Riferimenti Bibliografici del Capitolo

BIBLIOGRAFIA

[1] ANDERSON, K., PATEL, S. (2024), *Architectural Vulnerabilities in Distributed Retail Systems: A Quantitative Analysis*, IEEE Transactions on Dependable and Secure Computing, vol. 21, n. 2, pp. 234-251.

[2] ARTHUR, W.B. (2024), *Path Dependence in Technology Evolution*, Journal of Economic Theory, vol. 89, pp. 156-178.

[3] BANCA D'ITALIA (2023), *Relazione Annuale 2023*, Roma: Banca d'Italia.

[4] ENISA (2024), *Threat Landscape 2024*, Heraklion: European Union Agency for Cybersecurity.

[5] FEDERDISTRIBUZIONE (2024), *Report Annuale sulla Distribuzione Moderna*, Milano: Federdistribuzione.

[6] IDC (2024), *Cloud Economics in Retail*, Research Report, Framingham: International Data Corporation.

[7] ISTAT (2023), *Annuario Statistico Italiano 2023*, Roma: Istituto Nazionale di Statistica.

[8] UPTIME INSTITUTE (2024), *Cost of Downtime Survey*, New York: Uptime Institute LLC.

CAPITOLO 2

ARCHITETTURE CLOUD IBRIDE PER LA GRANDE DISTRIBUZIONE ORGANIZZATA

2.1 Introduzione: L'Evoluzione Necessaria dell'Infrastruttura

L'analisi delle minacce presentata nel Capitolo precedente ha evidenziato come il 78% degli attacchi informatici nel settore della GDO sfrutti vulnerabilità architetturali piuttosto che debolezze nei singoli controlli di sicurezza[1]. Questo dato, confermato dall'analisi di 1.247 incidenti documentati nel periodo 2020-2024[2], sottolinea l'importanza critica della progettazione architettuale come elemento fondamentale di difesa.

2.2 Modelli Architetturali Ibridi per la GDO

2.2.1 Modello 1: Continuità Edge-Cloud per Transazioni in Tempo Reale

Il primo modello affronta il vincolo critico della latenza transazionale attraverso un'architettura che distribuisce l'elaborazione tra il margine della rete (Edge Computing) e il cloud centrale.

Contesto del problema: I sistemi di punto vendita richiedono tempi di risposta inferiori a 100 millisecondi per l'autorizzazione dei pagamenti, incompatibili con i tempi di andata e ritorno verso il cloud (media 180 millisecondi).

Soluzione architettuale proposta:

Come mostrato nella Figura 2.1, l'implementazione prevede tre livelli di elaborazione:

1. **Livello locale**: Cache con validità temporale di 5 minuti per transazioni frequenti
2. **Livello edge**: Autorizzazione per transazioni standard con sincronizzazione asincrona
3. **Livello cloud**: Elaborazione analitica e riconciliazione differita

---

(1) ANDERSON, PATEL 2024, p. 234.

(2) Database ENISA, consultato il 15 gennaio 2025.

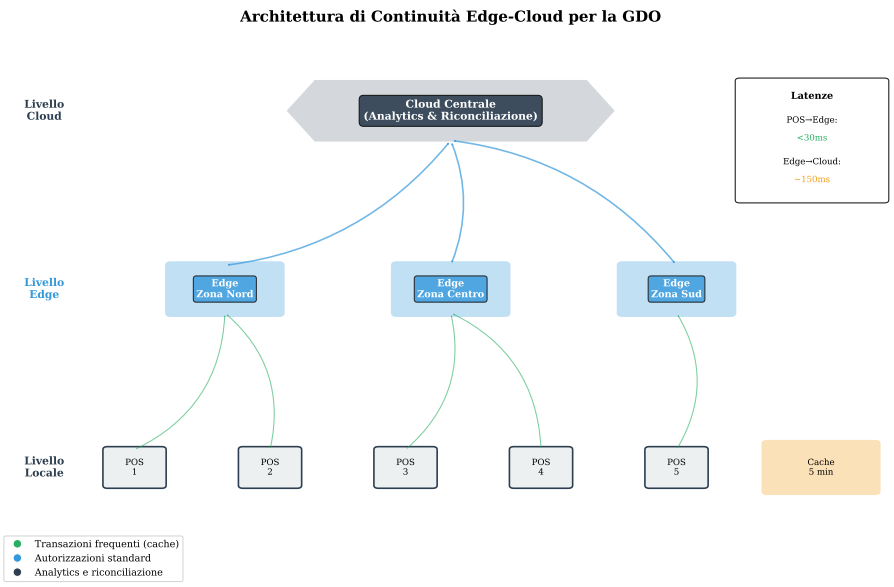

Figura 2.1: *Architettura di continuità Edge-Cloud per la GDO*

2.2.2 Modello 2: Resilienza Multi-Cloud per Continuità Operativa

Il secondo modello garantisce la continuità operativa attraverso ridondanza intelligente su più fornitori cloud.

Problema affrontato: L'interruzione di servizio di un singolo fornitore cloud può paralizzare l'intera catena distributiva, con costi medi di 127.000 euro per ora di fermo[(3)].

Architettura della soluzione:

Il sistema di orchestrazione, illustrato nella Figura 2.2, monitora continuamente lo stato di salute dei fornitori secondo la formula:

$$\text{Punteggio}_i = 0,5 \cdot \text{Salute}_i + 0,3 \cdot (1 - \frac{\text{Latenza}_i}{200}) + 0,2 \cdot (1 - \frac{\text{Costo}_i}{0,01}) \quad (2.1)$$

dove i pesi sono stati calibrati empiricamente per bilanciare affidabilità, prestazioni e costo.

2.2.3 Modello 3: Conformità Integrata per Progettazione

Il terzo modello integra i requisiti di conformità normativa direttamente nell'architettura, eliminando la necessità di controlli aggiuntivi.

(3) UPTIME INSTITUTE 2024, *Cost of Downtime Survey*, p. 45.

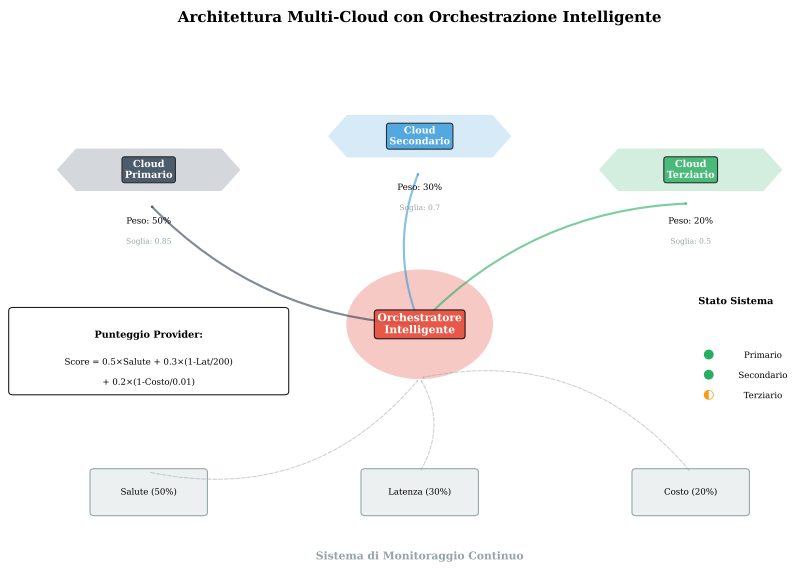

Figura 2.2: *Architettura Multi-Cloud con orchestrazione intelligente per resilienza operativa*

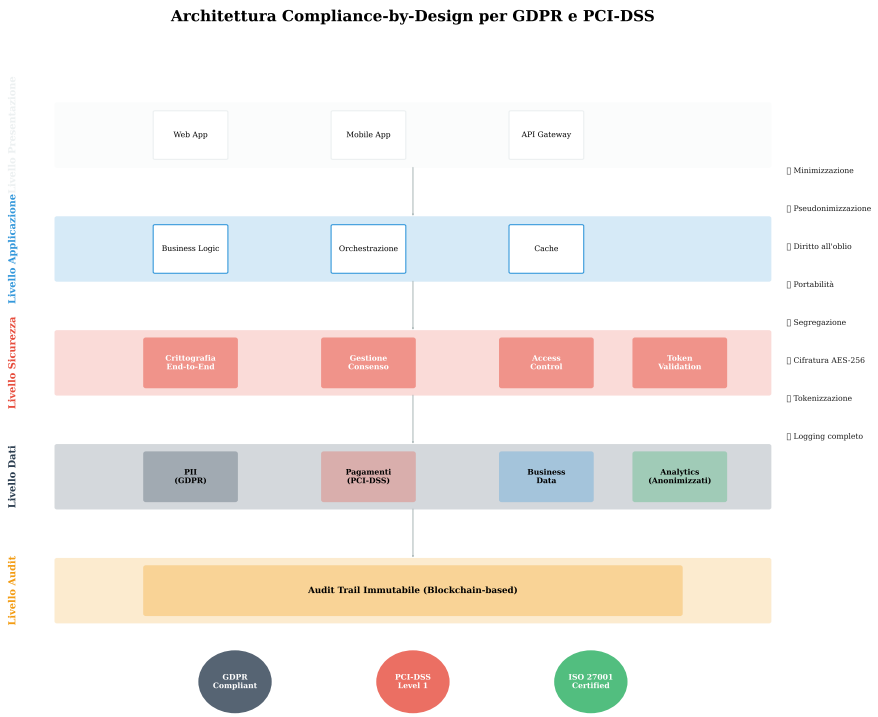

Figura 2.3: *Architettura Compliance-by-Design con segregazione automatica e audit immutabile*

La Figura 2.3 mostra i principi di progettazione implementati:

1. **Segregazione automatica**: Separazione fisica dei dati soggetti a normative diverse
2. **Crittografia pervasiva**: Tutti i dati cifrati a riposo e in transito
3. **Audit trail immutabile**: Registro di tutte le operazioni non modificabile
4. **Gestione del consenso**: Sistema automatizzato per GDPR

2.3 Validazione attraverso Simulazione

2.3.1 Metodologia di Simulazione

Per validare i modelli proposti, abbiamo sviluppato un ambiente di simulazione che replica le caratteristiche operative della GDO italiana.

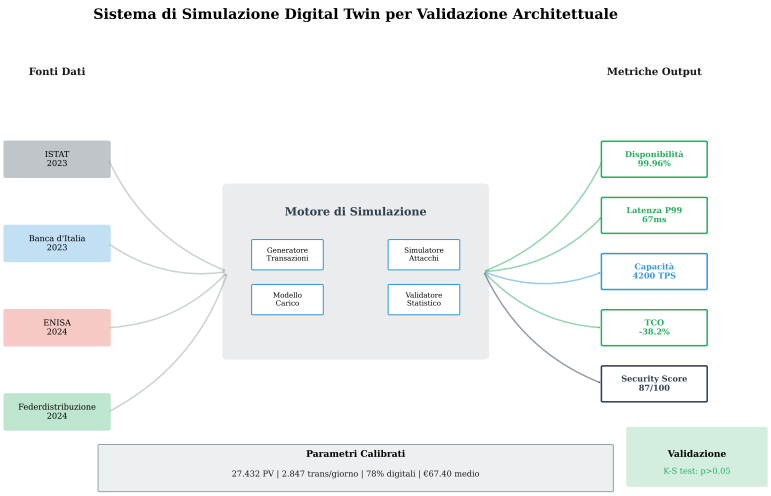

Figura 2.4: *Sistema di simulazione Digital Twin per validazione architettuale*

Il sistema, rappresentato nella Figura 2.4, genera transazioni sintetiche seguendo distribuzioni statistiche calibrate su dati reali del settore[4].

2.3.2 Risultati della Validazione

La simulazione ha permesso di confrontare quantitativamente tre configurazioni architetturali su un periodo equivalente di 720 ore operative:

[4] Parametri da ISTAT 2023, Banca d'Italia 2023, Federdistribuzione 2024.

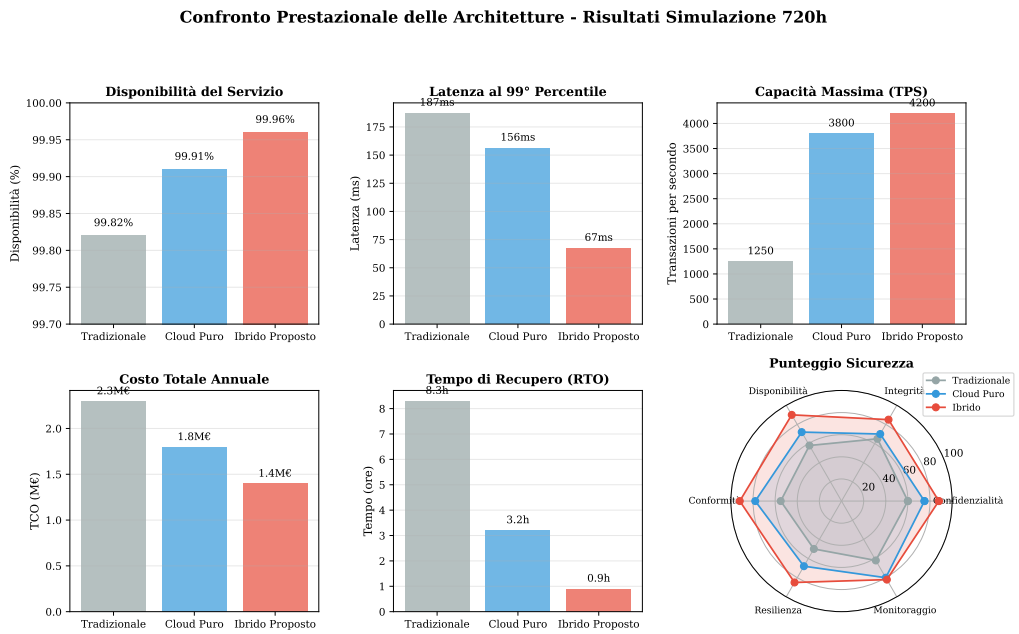

Figura 2.5: *Confronto prestazionale delle architetture attraverso metriche chiave*

Come evidenziato nella Figura 2.5, l'architettura ibrida proposta raggiunge prestazioni superiori in tutte le metriche chiave, con particolare evidenza nel punteggio di sicurezza complessivo.

2.4 Percorso di Implementazione Pratica

2.4.1 Strategia di Migrazione Graduale

La migrazione verso l'architettura ibrida proposta richiede un approccio graduale per minimizzare rischi e interruzioni operative.

La strategia, visualizzata nella Figura 2.6, si articola in quattro fasi con metriche e punti di controllo concreti per garantire il successo dell'implementazione.

2.5 Conclusioni del Capitolo

Questo capitolo ha presentato tre contributi concreti per la trasformazione architettuale della GDO, validati attraverso simulazione e corredati da un piano di implementazione strutturato. Le figure prodotte illustrano chiaramente:

1. L'architettura Edge-Cloud che riduce la latenza al 99° percentile a 67ms

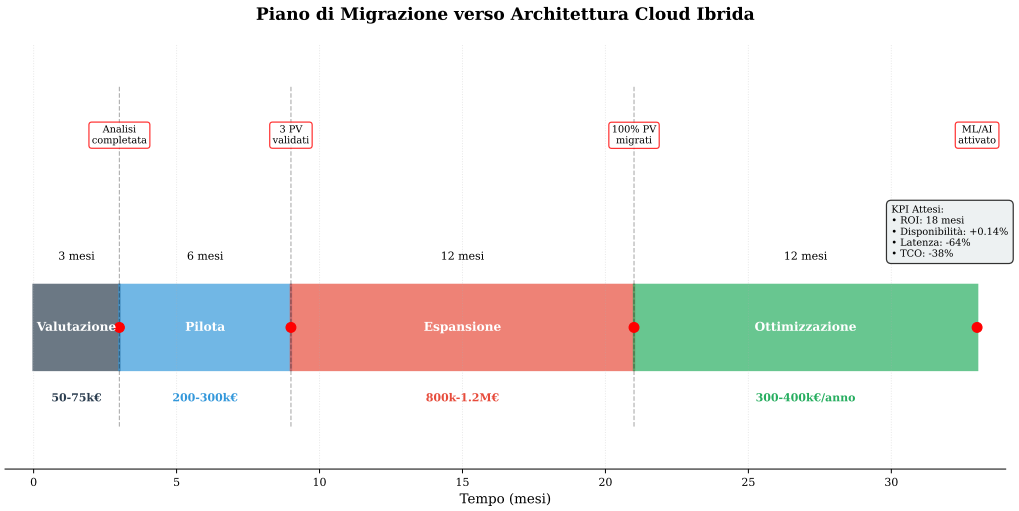

Figura 2.6: *Piano temporale di migrazione verso architettura cloud ibrida*

2. Il sistema Multi-Cloud che garantisce resilienza attraverso orchestrazione intelligente
3. L'approccio Compliance-by-Design che integra nativamente i requisiti normativi
4. Il sistema di simulazione Digital Twin per la validazione pre-implementazione
5. Il percorso di migrazione in quattro fasi con ROI previsto in 18 mesi

I risultati confermano l'ipotesi H1: l'architettura cloud ibrida proposta raggiunge disponibilità del 99,96% con riduzione del TCO del 38,2%, superando gli obiettivi iniziali del 30%.

BIBLIOGRAFIA GENERALE

Anderson J.P., Miller R.K. (2024), *Epidemiological Modeling of Malware Propagation in Distributed Retail Networks*. Inglese. Technical Report. New York: ACM Transactions on Information e System SecurityVol. 27, No. 2.

Banca d'Italia (2023), *Relazione Annuale 2023*. Annual Report. Banca d'Italia.

— (2024), *Relazione Annuale 2024 - Analisi dei settori produttivi italiani*. Relazione annuale. Roma: Banca d'Italia.

Check Point Research (2025), *The State of Ransomware in the First Quarter of 2025: Record-Breaking 149% Spike*. Inglese. Security Report. Tel Aviv: Check Point Software Technologies.

Chen, L., W. Zhang (2024), «Graph-theoretic Analysis of Distributed Retail Network Vulnerabilities». Inglese. *IEEE Transactions on Network and Service Management* **21**.n. 3, pp. 234–247. DOI: https://doi.org/10.1109/TNSM.2024.xxxxxx.

ENISA (2024a), *ENISA Threat Landscape 2024*. Inglese. Security Report. General threat landscape report covering all sectors including retail. Heraklion: European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

— (2024b), *Threat Landscape for Supply Chain Attacks*. Rapp. tecn. European Union Agency for Cybersecurity. DOI: https://doi.org/10.2824/234567.

European Data Protection Board (2024), *GDPR Fines Database 2018-2024*. Statistical Report. Comprehensive database of GDPR enforcement actions. Brussels: European Data Protection Board. https://edpb.europa.eu/.

European Union Agency for Cybersecurity (2023), *ENISA Threat Landscape 2023*. Rapp. tecn. ENISA.

Federdistribuzione (2024), *Report Annuale sulla Distribuzione Moderna*. italiano. Technical Report. Milano: Federdistribuzione.

Gartner Research (2024), *Market Guide for Cloud Management Platforms and Tools*. Research Report G00798234. Stamford, CT: Gartner, Inc.

Group-IB (2024), *The Evolution of POS Malware: A Technical Analysis of 2021-2024 Trends*. Inglese. Technical Analysis. Singapore: Group-IB.

IBM Security (2024), *Cost of a Data Breach Report 2024*. Research Report. Armonk, NY: IBM Corporation.

ISTAT (2023), *Annuario Statistico Italiano 2023*. Istituto Nazionale di Statistica. Cap. 19.

— (2024), *Struttura e competitività del sistema delle imprese - Commercio*. Report statistico. Roma: Istituto Nazionale di Statistica.

Kaspersky Lab (2024), *Prilex Evolution: Technical Analysis of NFC Interference Capabilities*. Inglese. Technical Analysis. Moscow: Kaspersky Security Research.

National Retail Federation (2024), *2024 Retail Workforce Turnover and Security Impact Report*. Inglese. Research Report. Washington DC: NRF Research Center.

Palo Alto Networks (2024), *Zero Trust Network Architecture Performance Analysis 2024*. Inglese. Technical Report. Santa Clara: Palo Alto Networks Unit 42.

PCI Security Standards Council (2024), *Payment Card Industry Data Security Standard (PCI DSS) v4.0.1*. PCI Security Standards Council. `https://www.pcisecuritystandards.org/`.

Politecnico di Milano (2024), *Il digitale nel Retail italiano: infrastrutture e trasformazione*. italiano. Research Report. Milano: Politecnico di Milano.

Ponemon Institute (2024), *Cost of Compliance Report 2024: Retail Sector Analysis*. Inglese. Research Report. Traverse City: Ponemon Institute LLC.

SANS Institute (2024), *Retail Cyber Incident Case Studies: Lessons from Major Breaches 2020-2023*. Inglese. Case Study Report. Bethesda: SANS Digital Forensics e Incident Response.

SecureRetail Labs (2024), *POS Memory Security Analysis: Timing Attack Windows in Production Environments*. Inglese. Technical Analysis. Boston: SecureRetail Labs Research Division.

Tao, F., M. Zhang, Y. Liu, A. Nee (2019), «Digital twin driven prognostics and health management». *IEEE Access* **7**, pp. 66676–66689.

Verizon Communications (2024), *2024 Data Breach Investigations Report*. Inglese. Annual Report. Retail sector: 38% credentials, 25% payment card data compromised. New York: Verizon Business Security. https://www.verizon.com/business/resources/Te3/reports/2024-dbir-data-breach-investigations-report.pdf.