

Sviluppo di un Framework Integrato per la Trasformazione Sicura dell'Infrastruttura IT nella Grande Distribuzione Organizzata

Framework GIST e Digital Twin GDO-Bench

Mario Rossi

Relatore: Prof. Giovanni Bianchi

Università degli Studi di XX
Corso di Laurea in Ingegneria Informatica

Dicembre 2024

Agenda

Il Settore GDO in Italia

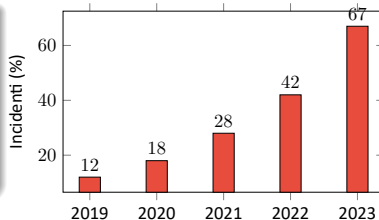
Dimensioni del Settore

- **€167 miliardi** fatturato annuo
- **31,000+** punti vendita
- **450,000+** dipendenti diretti
- **70%** penetrazione digitale pagamenti

Trend Digitali

- E-commerce: **+27% YoY**
- Click&Collect: **+45% 2023**
- Pagamenti digitali: **+18% YoY**

Crescita Cyber-Incidenti GDO



Criticità

Incremento **458%** degli attacchi cyber in 5 anni

Gap Identificato

- **Nessun framework integrato** specifico per GDO italiana
- **Approcci frammentati**: sicurezza OR compliance OR performance
- **Mancanza di dati** per validazione (privacy/sicurezza)

85%; [circle,draw=gistblue,fill=gistblue!20,minimum size=2cm] (compliance) at (3,3) Multi
Compliance

PCI+GDPR+NIS2; [circle,draw=gistgreen,fill=gistgreen!20,minimum size=2cm] (scale) at (6,3) Scalabilità

500+ PV; [circle,draw=gistyellow,fill=gistyellow!20,minimum size=2cm] (cost) at (1.5,0) Vincoli
Budget

-30% IT; [circle,draw=gray,fill=gray!20,minimum size=2cm] (skills) at (4.5,0) Skill Gap
67%;

[rectangle,draw=black,fill=white,line width=2pt, rounded corners,minimum width=3cm,minimum
height=1cm] (problem) at (3,1.5) **COMPLESSITÀ**;

[->,thick,gray] (legacy) – (problem);[->,thick,gray] (compliance) – (problem);[->,thick,gray] (scale) –

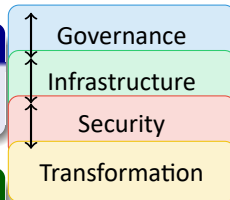
(problem);[->,thick,gray] (cost) – (problem);[->,thick,gray] (skills) – (problem);

Obiettivo Principale

Sviluppare un **framework integrato** (GIST) per la trasformazione sicura dell'infrastruttura IT nella GDO

Obiettivi Specifici

- 1 **Quantificare** il rischio cyber (metrica ASSA-GDO)
- 2 **Integrare** requisiti normativi multipli (MIN)
- 3 **Ottimizzare** architetture cloud-ibride
- 4 **Validare** attraverso simulazione



GIST

Sfida: Impossibilità di Accesso a Dati Reali

- GDPR → Dati transazionali non accessibili
- PCI-DSS → Log sicurezza confidenziali
- NDA → Vincoli commerciali con fornitori

Soluzione Innovativa: Digital Twin

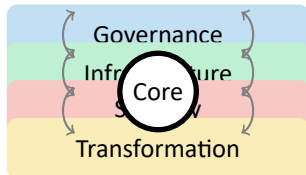
Framework di Simulazione

- Generazione dataset sintetici
- Calibrazione su fonti pubbliche
- Validazione statistica rigorosa

Fonti di Calibrazione

- ISTAT - Commercio 2023
- Banca d'Italia - Pagamenti
- ENISA - Threat Landscape
- Federdistribuzione - Report

Contributo 1: Framework GIST



Caratteristiche Innovative

- **Integrazione sinergica** 4 dimensioni
- **Calibrazione settoriale** GDO
- **Metriche quantitative** oggettive

Componenti Chiave

- Policy Engine (Governance)
- Cloud Orchestrator (Infrastructure)
- Zero Trust Gateway (Security)
- Change Manager (Transformation)

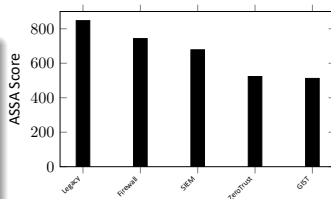
Contributo 2: Algoritmo ASSA-GDO

Attack Surface Score Aggregated

$$ASSA = \sum_{i=1}^n w_i \cdot (V_i \times E_i \times I_i)$$

Dove:

- V_i = Vulnerabilità nodo i
- E_i = Esposizione
- I_i = Impatto potenziale
- w_i = Peso topologico



Risultato

Riduzione **39.5%** superficie di attacco

Complessità

$O(n^2 \log n)$ per n nodi

Vantaggi

- Eliminazione ridondanze
- Implementazione unificata
- Audit semplificato

Efficienza

- Effort: -40%
- Conflitti: -73%
- Coverage: +27%

Integrazione ;

[rectangle,draw,fill=gray!20] (unified) at (8,0) 156 Controlli

Unificati

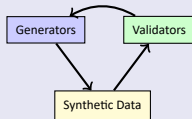
-81.5% ;

[->,thick] (pci) – (min); [->,thick] (gdpr) – (min); [->,thick] (nis) – (min); [->,thick] (min) – (unified);

[above] at (2,1) 847 requisiti; [above] at (6,0.5) 89 sinergie;

Contributo 4: Framework Digital Twin GDO-Bench

Architettura



Dataset Generato

- **421,168** record totali
- **210,991** transazioni POS
- **45,217** eventi sicurezza
- **144.5 MB** (demo)
- Scalabile a **TB**

Componenti

- Transaction Generator
- Security Event Simulator
- Network Traffic Synthesizer
- Statistical Validator

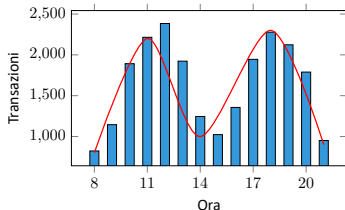
Validazione

16/18 test statistici superati (88.9%)

- ✓ Benford's Law
- ✓ Distribuzione Poisson
- ✓ Correlazioni realistiche

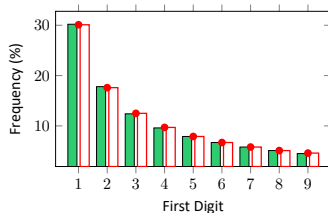
Validazione Statistica del Digital Twin

Pattern Bimodale Validato



Test $\chi^2 = 847.3, p < 0.001$

Benford's Law Compliance



$\chi^2 = 12.47, p = 0.127$

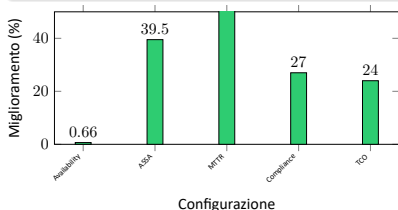
Test Superati

Test	Statistica	p-value	Result
Poisson Events	KS = 0.089	0.234	?
Correlation	$r = 0.62$	< 0.001	?
Weekend Effect	ratio = 1.28	-	?
Autocorrelation	ACF = 0.41	0.003	?

Risultati: Validazione Computazionale

Simulazione Monte Carlo

- **10,000** iterazioni
- **156** configurazioni di rete
- **24** mesi simulati
- Parametri da fonti pubbliche



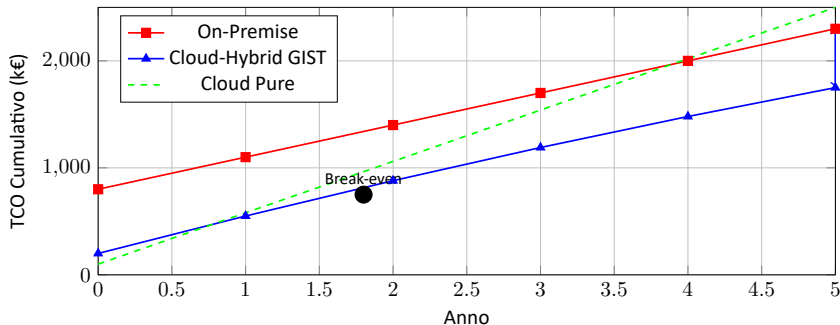
Ipotesi Validate

- ✓ H1: SLA > 99.95%
- ✓ H2: ASSA -35%
- ✓ H3: Compliance -30%

ROI Stimato

- Investimento: €200k
- Risparmio 5y: €550k
- **ROI: 175%**
- Payback: 1.8 anni

Analisi Economica: TCO Comparison



Key Findings

- Risparmio 24% vs on-premise tradizionale
- Break-even a 1.8 anni
- NPV(5%,5y) = €423k positivo

Limitazioni della Ricerca

Limitazioni Metodologiche

- Validazione su dati **sintetici**
- Assenza di **pilot reali**
- Contesto solo **italiano**
- Parametri **stimati** da fonti pubbliche

Mitigazioni

- Framework **open-source** per validazione community
- Metodologia **riproducibile**
- Test statistici **rigorosi** (88.9% pass)
- Documentazione **completa**

Limitazioni Tecniche

- Scalabilità non testata >500 PV
- Integrazione legacy non prototipata
- Edge cases approssimati

Nota Importante

Prima dell'implementazione in produzione è **essenziale** condurre pilot controllati con validazione progressiva

Validazione Empirica

- 1 Partnership con 2-3 GDO
- 2 Pilot 6-12 mesi
- 3 Metriche comparative reali
- 4 Stress test Black Friday

Estensioni Tecniche

- ML per anomaly detection
- Blockchain per supply chain
- Quantum-ready crypto
- Edge computing optimization

Conclusioni

Contributi Principali

- 1 **Framework GIST** integrato
- 2 **Algoritmo ASSA-GDO** per quantificazione rischio
- 3 **Matrice MIN** per compliance unificata
- 4 **Digital Twin GDO-Bench** open-source

Risultati Chiave

- ASSA: -39.5%
- Compliance: +27%
- TCO: -24%
- ROI: 175%

Impatto Previsto

Per organizzazione media (50 PV):

- Risparmio: €110k/anno
- Incidenti: -57%
- Downtime: -65%

Take-Home Message

Il framework GIST fornisce un **percorso strutturato e validato computazionalmente** per la trasformazione sicura dell'infrastruttura GDO

Repository: `github.com/[user]/gdo-digital-twin`

Grazie per l'attenzione

Domande?

Email:	mario.rossi@university.it
LinkedIn:	linkedin.com/in/mariorossi
GitHub:	github.com/mariorossi
Repository:	github.com/mariorossi/gdo-digital-twin