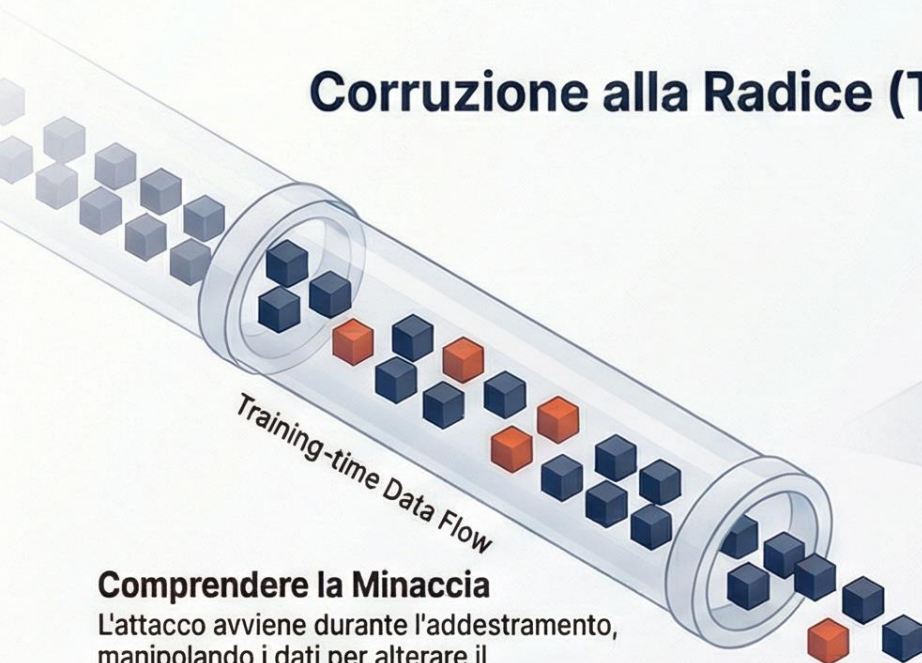


Data Poisoning: La Minaccia Invisibile all'Integrità dell'IA

Corruzione alla Radice (Training-time)



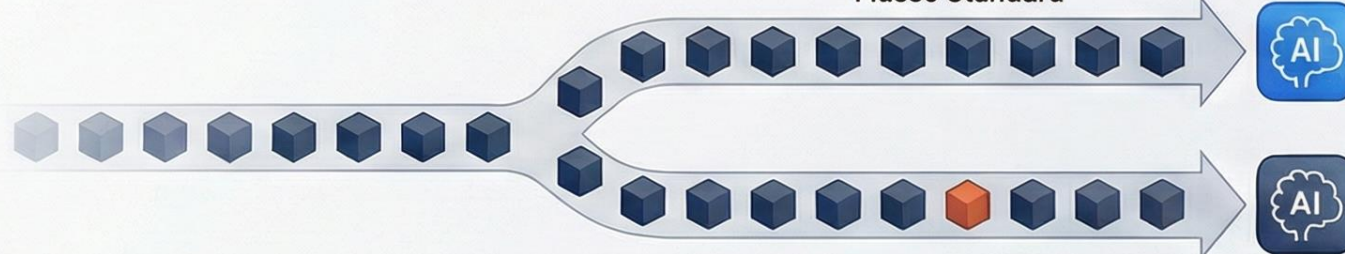
Comprendere la Minaccia

L'attacco avviene durante l'addestramento, manipolando i dati per alterare il comportamento futuro del modello.

Il Pericolo del "Clean-Label"

I dati contraffatti appaiono legittimi e coerenti, rendendo l'attacco quasi invisibile ai controlli standard.

Flusso Standard



Backdoor e Trojan nell'IA

L'attaccante può inserire "trigger" che attivano comportamenti malevoli solo in circostanze specifiche e desiderate.

Impatto Strategico e Difesa



Rischi in Finanza e Supply Chain

Può causare frodi invisibili nei sistemi di credit scoring o sabotare le decisioni logistiche aziendali.



L'Obbligo della Compliance (EU AI Act)

Entro il 2026, la robustezza e la governance dei dati saranno requisiti legali obbligatori.



Verifica dell'Origine



Sanitizzazione Automatizzata



Protezione End-to-End

È necessario verificare l'origine dei dati (provenance) e implementare sistemi di sanitizzazione automatizzata.