Ti teniamo al sicuro.

Scopri la nuova frontiera dei sistemi anti-frode
basati sui Modelli Predittivi per i Pagamenti Cashless.

www.tasgroup.eu | solutions@tasgroup.eu

tas group
an owl company

The Fintech Startup with 30 years of history

BIG DATA E MACHINE LEARNING PER *PREVENIRE LE FRODI*

Per chi tiene le redini finanziarie di un'azienda, contrastare le frodi nei pagamenti significa tutelare il conto economico ed evitare perdite anche sostanziose, ma anche assicurare un servizio migliore al cliente finale. I modelli predittivi basati sui big data aumentano l'efficacia dei metodi di detection tradizionali e sono un'arma potente a disposizione del CFO

I modelli predittivi per il fraud management si basano su un presupposto semplice: un comportamento anomalo può essere l'indizio di una frode. Meno semplice, fino a ieri, era tradurre in pratica la semplicità di questa intuizione e, nel concreto, offrire strumenti informativi capaci di individuare l'anomalia e di associarla a una possibile truffa. Oggi il potente binomio big data - machine learning e l'aumento della capacità computazionale hanno prodotto questi strumenti, portando a maturazione il concetto di intelligenza artificiale che covava in accademia e nei laboratori di ricerca. «Il machine learning è studiato da molti anni, ma solo di recente ha trovato applicazione al servizio delle aziende e delle amministrazioni – riflette Roberto Scognamiglio, Program Manager Global Payments Solutions di TAS Group». Il gruppo, specializzato in software per l'innovazione nei sistemi di pagamento, le carte, i mercati finanziari e i processi ERP, ha da poco sviluppato un'estensione importante della propria piattaforma cl-Fraud Protect, che integra tre modelli predittivi in una soluzione creata per BancoPosta, il gigante italiano delle carte prepagate. Un sistema conforme alle raccomandazioni EBA in tema di sicurezza dei pagamenti digitali, che dal 2014 individua nell'analisi dei comportamenti degli utenti e nella loro tipizzazione in schemi caratteristici uno strumento chiave per identificare i tentativi di frode nelle transazioni. La soluzione, rilasciata in una prima tranche tra il dicembre del 2016 e l'inizio 2017, è stata premiata come la più innovativa nell'ambito di un concorso indetto dall'Associazione Prestatori di Servizi di Pagamento nel luglio 2017 ed è stata valutata con un case study da Ovum, specialista internazionale nel campo della consulenza tecnologica.

Una soluzione a moduli complementari

«I fenomeni fraudolenti sono in continua evoluzione e un sistema antifrode basato solo sull'utilizzo di regole deterministiche non sempre riesce a rispondere in maniera tempestiva ai cambiamenti dei comportamenti – osserva Scognamiglio. Per questo, abbiamo applicato il machine learning alla nostra suite antifrode per i pagamenti con carta, integrando il sistema di

regole deterministiche con un motore basato sui modelli predittivi». Grazie alla continua analisi delle transazioni in corso, il software perfeziona l'applicazione degli algoritmi e impara a riconosce i comportamenti anomali, indici di una possibile condizione fraudolenta. Gli strumenti di analisi basati sull'intelligenza artificiale e sui big data non sostituiscono ma affiancano gli algoritmi già in uso: «La suite opera attraverso due motori complementari, entrambi i quali elaborano tutte le transazioni – chiarisce Scognamiglio».

Prevedere le anomalie sconosciute

Come funzionano i modelli predittivi e in che cosa differiscono dagli algoritmi normalmente impiegati nella rilevazione delle frodi? Qual è il loro valore aggiunto? «Le regole deterministiche sono regole di monitoraggio che attraverso controlli specifici segnalano le transazioni che con maggiore probabilità nascondono una frode. I controlli implementati nelle regole derivano dall'osservazione dei fenomeni fraudolenti già avvenuti in passato – spiega Scognamiglio. I modelli predittivi, invece, sono algoritmi statistici in grado di analizzare un gran numero di informazioni e di identificare i possibili comportamenti fraudolenti. Il motore degli algoritmi predittivi individua le deviazioni dai pattern abituali di comportamento, intercettando una varietà maggiore di attacchi e rilevando velocemente nuovi fenomeni di frode». In altre parole, la regola deterministica funziona analizzando, per ogni singola transazione, elementi prestabiliti che fanno presupporre una truffa, come l'entità del pagamento o la provenienza geografica, i quali vengono determinati studiando le transazioni fraudolente note, già avvenute in passato. Il modello predittivo lavora sui dati in tempo reale, avendo come base cognitiva lo storico dei comportamenti del singolo cliente e delle singole tipologie di carta e di pagamento.

L'addestramento del motore

«I modelli predittivi integrati nella soluzione per BancoPosta si basano su una profondità storica di un anno e mezzo per ogni titolare di carta, che formano una base cognitiva di oltre due miliardi di operazioni – continua Scognamiglio. L'analisi dei dati ha richiesto un tempo lungo, circa sei mesi di lavoro. Ora puntiamo a industrializzare il processo, per ridurre il tempo di produzione dei modelli a un paio di mesi». La sostanza non cambia: un periodo di osservazione sufficientemente lungo e una base dati adeguata consentono al software di riconoscere se lo schema di comportamento in atto durante il pagamento corrisponde a transazioni genuine o può essere indice di atti fraudolenti.

Roberto Scognamiglio, Program Manager Global Payments Solutions di TAS Group

L'antifrode in due mosse

La suite viene alimentata con tutte le transazioni che arrivano alla fase autorizzante, elaborate dai due motori di analisi secondo logiche di monitoraggio differenti. Spiega ancora Scognamiglio: «Il motore SCUDO svolge un ruolo di prevention, applicando regole che bloccano la transazione se la carta o il suo intestatario compaiono nelle black list di sistema. Il blocco è temporaneo, in attesa di ulteriori controlli. Il motore BASE svolge invece un ruolo di detection, inviando la segnalazione delle transazioni sospette al centro di monitoraggio. Entrambi i motori sono assistiti da algoritmi predittivi che, lavorando sulla storia pregressa delle carte, assegnano uno score a ogni transazione. Lo score indica il livello di rischiosità dell'operazione: per le transazioni che superano un valore di soglia prestabilito, parte il blocco oppure la segnalazione».

F.R.