Sarà una frode? Il chatbot lo chiede al cliente

TAS sta investendo sulle soluzioni antifrode basate sull'intelligenza artificiale, anche generativa, per rispondere alle crescenti insidie dei frodatori. Che riescono a ingannare clienti e imprese con deep fake e attacchi di social engineering

@ Roberto Scognamiglio, Program Manager di TAS

Il cliente dispone una transazione, ad esempio un bonifico istantaneo, e il chatbot entra in scena chiedendo maggiori informazioni per essere certo che non si tratti di una frode. È una delle ultime frontiere della intelligenza artificiale generativa applicata al mondo dell'antifrode, che vede la GenAI entrare in campo di propria iniziativa per bloccare una potenziale truffa. «Stiamo assistendo a una rapida evoluzione delle vulnerabilità alle quali vanno incontro banche e clienti – racconta Roberto Scognamiglio, Program Manager di TAS. Da un lato per via della tecnologia, che abilita di continuo nuove forme di pagamento, dall'altro per il cambiamento dei comportamenti sociali, oggi non è infrequente incontrare persone che si affidano a un reel su Instagram per investire i propri risparmi, rischiando di essere coinvolti in una truffa».

Gli algoritmi di AI per i modelli predittivi

Per questo motivo è necessario mettere in campo nuovi strumenti antifrode basati su algoritmi di intelligenza artificiale, che sono capaci di identificare e prevenire queste possibili truffe analizzando tutti i dati a disposizione. Tra le più utilizzate, compaiono le soluzioni basate su modelli predittivi, supervisionati e non supervisionati. «I modelli predittivi supervisionati analizzano tutto il traffico transazionale pregresso per identificare pattern di frode specifici – spiega Scognamiglio. Quando il cliente dispone un pagamento, quindi, questi modelli riescono a intercettare il pattern sospetto e a bloccare la transazione. I modelli non supervisionati, invece, non sono addestrati: gli algoritmi hanno il compito di scoprire criteri con cui aggregare i dati per fare emergere fenomeni altrimenti sconosciuti».

LA BANCA CONSERVATIVA E I SUOI TIMORI

«Le banche hanno spesso un approccio conservativo ma il fenomeno dell'AI, dell'AI generativa in particolare, si sta affacciando in maniera prepotente – premette Scognamiglio. La banca tradizionale è cauta verso questa tecnologia e un certo timore esiste anche nelle Istituzioni; al riguardo lo scorso 2 agosto è entrato in vigore in Europa l'AI Act proprio per fissare delle regole e mettere dei paletti per evitare che l'AI diventi pericolosa. L'AI Act non fa che rinforzare la ritrosia degli istituti bancari: preoccupati per gli aspetti di compliance, di sicurezza dei dati e ancor più per i rischi legati all'uso dell'intelligenza artificiale. Senza dimenticare il tema del ROI: quali sono i concreti vantaggi offerti da una soluzione di AI? La proposta di TAS è per un approccio incrementale che permetta alla banca di adattarsi gradualmente, di acquisire fiducia nella tecnologia, di calcolarne i vantaggi. Questo dovrebbe ridurre il rischio percepito e permettere un miglior controllo del cambiamento».

L'AI spiegabile

Con l'AI è possibile analizzare i dati su finestre temporali mobili e con un approccio di sequential covering riuscire a estrapolare regole di contrasto a eventi fraudolenti. «Si tratta di soluzioni che vengono integrate gradualmente – continua Scognamiglio – con un approccio di continuous improvement della nostra piattaforma antifrode per la quale, peraltro, abbiamo introdotto anche il concetto di explainability, per capire come e perché l'AI è arrivata a indicare un determinato score di rischio».

L'intelligenza generativa nelle mani dei frodatori

Ma oggi anche i frodatori utilizzano l'intelligenza artificiale generativa per i loro scopi e hanno tra i propri obiettivi sia il Corporate sia il Retail. Da un lato, andando a sofisticare sempre di più gli attacchi di social engineering, l'AI può colpire internamente un'azienda nutrendosi, ad esempio, di informazioni raccolte nelle mail. Dall'altro invece, ad esempio con un deep fake, l'AI può ingannare le persone e volatilizzarne i risparmi verso sedicenti piattaforme di investimento, non registrate presso le autorità competenti oppure con sede nei paradisi fiscali. «Sono casi reali, che gestiamo quotidianamente con il nostro servizio di back office frodi – evidenzia Scognamiglio. Per intercettare queste situazioni abbiamo introdotto i modelli comportamentali: tutti i clienti della banca, nel rispetto delle regole di compliance, vengono profilati e clusterizzati insieme alle categorie di pagamento più usuali per quel preciso utente. Non appena arriva una richiesta di pagamento insolita, si accende un allarme: si solleva uno score di rischio e questo è sufficiente a segnalare la transazione che sarà poi approfondita dal fraud manager. Si tratta di modelli comportamentali adattivi che recepiscono il cambiamento nel tempo delle abitudini di spesa del cliente, senza soluzioni di continuità».

Crediti immagine: ZinetroN/shutterstock

Il chatbot che allerta il cliente

Un altro sviluppo promettente è infine quello che vede l'impiego della Generative AI per creare un chatbot che contatta direttamente il cliente mettendolo in allerta sui rischi di un pagamento. «L'esperienza d'uso più comune che ognuno di noi ha con l'AI è di fare una domanda a ChatGPT e ottenere una risposta. In TAS abbiamo ribaltato questo paradigma – sottolinea Scognamiglio. Se un cliente della banca dispone un pagamento che viene intercettato dalle regole antifrode, allora riceve sullo smartphone una notifica da un chatbot specializzato. Attraverso l'AI prende quindi il via il dialogo con il cliente, al quale sono sottoposte una serie di domande. Le prime sono mirate a capire se lo smartphone è nelle mani del frodatore, nel qual caso la transazione viene immediatamente interrotta. Una volta accertato che è proprio il cliente genuino a essere in possesso dello smartphone, le domande successive sono finalizzate a capire se il cliente sta agendo per effetto di una manipolazione da parte del frodatore. Il chatbot è un software attivo 24/7 e, se non ci fosse, sarebbe necessario un help desk presidiato e altamente qualificato per la gestione delle transazioni sospette. Si tratta quindi di un'iniziativa che, guardando anche ai prossimi obblighi cui le banche dovranno ottemperare riguardo ai bonifici istantanei, riteniamo essere molto interessante».

G.C.

LA BUSINESS INTELLIGENCE PER REPORT PIÙ ESTESI

Oltre alla reportistica obbligatoria per la segnalazione delle frodi alle autorità di vigilanza, le banche possono costruire numerose tipologie di report grazie alla business intelligence, capace di analizzare nell'interezza tutte le transazioni effettuate e disposte dai clienti, andando a clusterizzare per caratteristiche comuni i pagamenti e i clienti stessi. «Questi algoritmi sono differenti da quelli specializzati per l'individuazione dei pattern di frode o per l'anomaly detection – precisa Scognamiglio – e possono essere applicati per far emergere degli elementi di rischio quali, ad esempio, dei riferimenti geografici, delle fasce d'età, il livello di istruzione di una popolazione».