WHITE PAPER | OTTOBRE 2014

Autenticazione 3D Secure basata su modelli avanzati

I modelli utilizzati per l'autenticazione basata sul rischio e sui comportamenti delle operazioni di commercio elettronico possono ridurre le perdite e fornire acquisti senza attrito per le transazioni a basso rischio.

Paul Dulany
Hongrui Gong
Kannan Shah
CA Technologies, Advanced Analytics and Data Science

ca technologies

Sommario

Riepilogo

Sfida

Gli emittenti devono trovare un equilibrio tra sicurezza delle transazioni di pagamento elettronico e un'esperienza di pagamento lineare per la clientela. Il nocciolo della questione è come fornire una perfetta esperienza di pagamento ai clienti legittimi, evitando che abbandonino la transazione o utilizzino una diversa forma di pagamento, bloccando allo stesso tempo i tentativi illegittimi di portare a termine le transazioni. L'uso dell'autenticazione basata sul comportamento per determinare quali transazioni devono essere influenzate, richiedendo al cliente di sottoporsi a passaggi di autenticazione ulteriori, è essenziale per ridurre l'attrito e al contempo per garantire al meglio la legittimità della transazione. Le regole sono una componente importante dell'erogazione di questa autenticazione basata sul rischio e sul comportamento. Quando si aggiungono i modelli, e li si utilizza per l'applicazione di regole basate sul rischio, l'impatto sui tentativi illegittimi di autenticazione può essere notevolmente aumentato, mentre si riduce quello sui clienti legittimi, offrendo un'esperienza migliore per il titolare della carta e una riduzione delle perdite per l'emittente.

L'opportunità

Il canale 3D Secure presenta numerose opportunità per gli emittenti. Con l'aumento significativo delle frodi collegate al commercio elettronico, combinate con la modifica dell'attribuzione di responsabilità, l'autenticazione 3D Secure offre una prima linea di difesa agli emittenti. Tuttavia, è importante utilizzare questa prima linea di difesa in modo sensato e ottimizzato. CA Risk Analytics offre l'opportunità di esaminare le transazioni di commercio elettronico durante l'autenticazione, mediante informazioni univoche non disponibili ai sistemi di rilevamento delle frodi di autorizzazione, evitando così transazioni illegittime. Una valutazione del rischio di autenticazione deve essere eseguita per offrire un'esperienza di acquisto senza interruzioni alla maggior parte dei titolari legittimi. Con CA Risk Analytics in funzione, gli emittenti possono ridurre le perdite e limitare l'attrito per i clienti.

Vantaggi

CA Risk Analytics consente agli emittenti di valutare il livello di rischio delle attività online per i commercianti che hanno implementato 3D Secure. Valuta in modo trasparente il rischio del tentativo di esecuzione di una transazione di commercio elettronico da parte di un soggetto diverso dal titolare legittimo della carta, in tempo reale. È in grado di identificare una quota significativa dei tentativi di transazione legittimi e consentire ai clienti di continuare con l'acquisto senza impatto, e al contempo identificare i tentativi di transazione illegittimi che è necessario bloccare. Identificazione del device, geolocalizzazione, caratteristiche della connessione e schemi storici possono essere utilizzati per valutare il rischio di ogni tentativo di transazione.

Un aspetto essenziale di CA Risk Analytics è la disponibilità di modelli regionali avanzati che valutano il livello di rischio di un determinato tentativo di transazione mediante analisi sofisticate, incluso un modello comportamentale di rete neurale, e che forniscono un punteggio che indica il livello di rischio di questo tentativo. Le regole all'interno di CA Risk Analytics possono quindi combinare il punteggio generato da questo modello con altri fattori di business, per determinare come gestire al meglio un determinato tentativo di transazione, con conseguente aumento significativo dell'efficacia della soluzione.

Sezione 1

3D Secure fornisce la base per la riduzione delle perdite nel commercio elettronico

Il protocollo 3D Secure offre agli emittenti numerose opportunità sfruttabili per ottenere tutti i vantaggi e la protezione offerti dal canale 3D Secure.

Il canale 3D Secure si concentra sull'autenticazione dei tentativi di transazione di commercio elettronico. È importante comprendere la differenza tra autenticazione e autorizzazione. L'autenticazione consiste nel tentativo di confermare che la persona che avvia una transazione (o un'altra attività) è il titolare legittimo ed effettivo della carta. L'autorizzazione consiste nel tentativo di verificare che il titolare (confermato) della carta abbia la facoltà di effettuare la transazione (in base a policy, saldo disponibile, stato del conto e altri elementi). È importante notare che la frode può avvenire ed essere rilevata sia in fase di autorizzazione che di autenticazione, ma con alcune differenze fondamentali; ad esempio, l'autenticazione non contrasta direttamente la frode first-party. Tuttavia, indipendentemente dal tipo di frode, autenticare il soggetto che tenta di eseguire una transazione è il punto di partenza per garantirne la validità.

Per le transazioni con carta presente, la presenza fisica della carta è stata a lungo accettata come una componente chiave dell'autenticazione. Alla sempre maggiore sofisticazione degli utenti illegittimi, gli emittenti hanno risposto con una maggiore sicurezza integrata nelle carte (banda magnetica, CVV/CVC/CID e smart card). Questi dati, o i risultati dell'autenticazione basata su di essi, vengono generalmente trasmessi insieme alla richiesta di autorizzazione.

Per le transazioni con carta non presente (CNP), l'autenticazione fisica tramite la carta non è più possibile, e in generale la responsabilità ricade sul commerciante. Tuttavia, con l'avvento del commercio elettronico, è diventato necessario sviluppare una forma di autenticazione robusta per le operazioni di commercio elettronico. I dati collegati alla richiesta di autorizzazione sono sufficienti per autorizzare una transazione, ma non lo sono per l'autenticazione di una transazione di commercio elettronico. Ecco quindi che è stata creata la transazione 3D Secure, con informazioni diverse rispetto alla richiesta di autorizzazione e progettata per autenticare il soggetto che tenta di eseguire una transazione. Questa attività, essenzialmente diversa dall'autorizzazione, richiede una prospettiva specifica. Tuttavia i risultati di tale autenticazione possono essere utilizzati all'interno del flusso di autorizzazione, per fornire un migliore contesto per il sistema di autorizzazione stesso.

Per chiarire, quando parliamo di frode in questo documento ci riferiamo alla frode a livello di autenticazione per le transazioni di commercio elettronico 3D Secure.

Mediante il protocollo 3D Secure, esiste l'opportunità di esaminare i tentativi di autenticazione di commercio elettronico, sfruttando informazioni univoche non disponibili ai sistemi di rilevamento delle frodi di autorizzazione ed evitando così transazioni illegittime prima che generino una richiesta di autorizzazione. Quando si utilizza il sistema di CA Risk Analytics, queste informazioni univoche includono un ID univoco per ogni device (ID device), un URL cui il titolare della carta accede per effettuare la transazione (URL commerciante), l'indirizzo IP corrente del device e informazioni aggiuntive da fornitori di dati terzi, inclusi posizione del device, velocità di connessione, tipo, identificazione anonymizer e altre. Queste informazioni ampliano in modo significativo (ma non sostituiscono) quelle tradizionali, come importo, valuta, nome del commerciante e ID, identificativo della carta e altro ancora. Tale ampliamento rende i modelli di autenticazione 3D Secure più vantaggiosi rispetto ai modelli di autorizzazione, in grado di accedere solo alle informazioni tradizionali, fornendo una rilevazione avanzata dei tentativi di autenticazione illegittimi e, al contempo, andando a incidere solo su una piccola parte dei tentativi legittimi.

Il canale 3D Secure fornisce informazioni in tempo reale per l'analisi delle operazioni di autenticazione; in particolare, è possibile aggiornare le informazioni relative alla carta, al device o ad altre entità cardine della transazione in tempo reale. Questo consente a qualsiasi transazione successiva di sfruttare i benefici di un incremento delle informazioni e del contesto quando ne viene valutato il rischio di autenticazione. Ciò risulta essere particolarmente utile quando si esaminano entità interbancarie in un ambiente SaaS cloud.

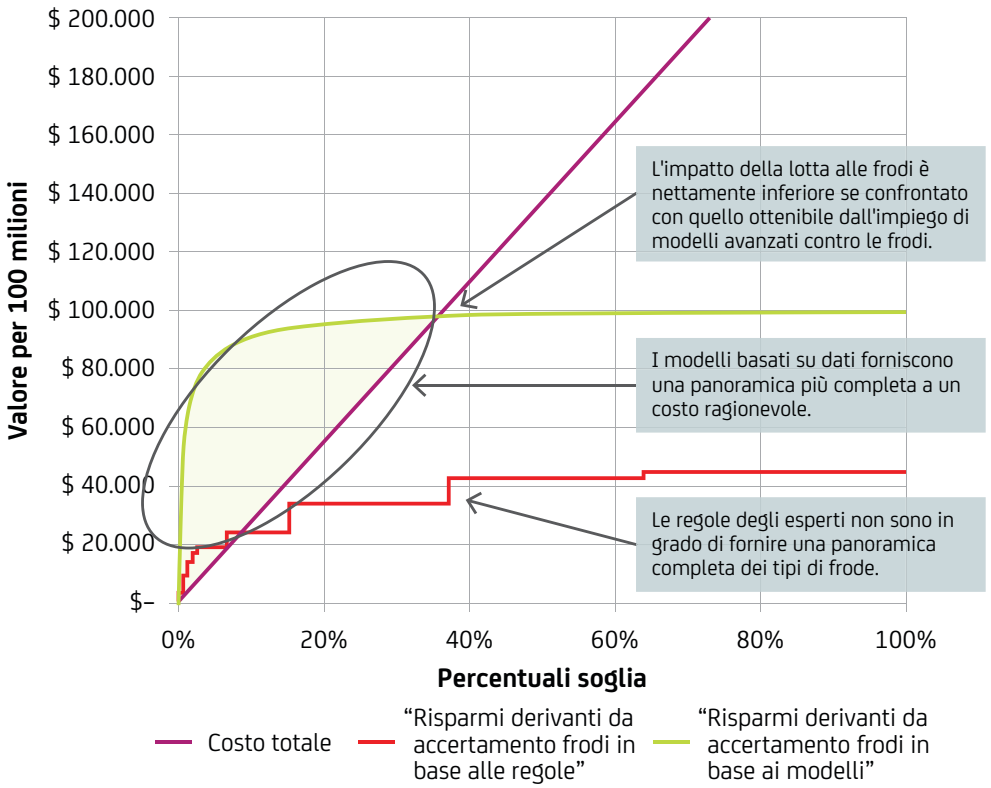
Esiste anche la possibilità di svolgere operazioni di commercio elettronico relativamente prive di attrito. Le prime implementazioni 3D Secure pongono domande di sicurezza a tutti gli acquirenti presso i commercianti 3D Secure. Se il meccanismo di sicurezza è solido, come nel caso dell'utilizzo di password monouso (OTP), può essere ragionevolmente efficace; ma se le domande di sicurezza sono poco valide, ad esempio consistono nel richiedere le informazioni necessarie per eseguire la transazione (data di scadenza o CVV2), allora risultano ben poco utili per contrastare eventuali perdite. Si produce tuttavia anche un effetto secondario: porre ai titolari delle carte domande di sicurezza introduce una forma di attrito nell'operazione, aumentando la resistenza al completamento della transazione e influenzando negativamente la customer experience.

L'impatto negativo dell'attrito sulla customer experience non è puramente qualitativo, ma ha anche una componente quantitativa: incrementa notevolmente i livelli di abbandono e le commissioni "false failure". L'abbandono determina perdita di commissioni interbancarie così come effetti più ampi, come l'incidenza sul saldo revolving per carte di credito o il possibile attrito da parte del cliente, un problema significativo per i conti di debito e di credito. Questi effetti consentono di quantificare in parte l'impatto sugli emittenti di una customer experience negativa e forniscono una motivazione forte per ridurre l'attrito della transazione. Nei casi estremi, in cui l'ulteriore livello di sicurezza viene imposto a tutti i clienti, il costo degli abbandoni può superare le eventuali perdite evitate. Pertanto, è fondamentale valutare il rischio di una determinata operazione e intervenire nel processo solo quando ha senso farlo. Questo avviene in modo ottimale utilizzando l'autenticazione basata sul comportamento.

La Figura 1, nella pagina seguente, mostra un esempio del costo totale del rilevamento delle frodi (compresa la perdita di opportunità dovuta all'abbandono) (linea viola), i risparmi derivanti da un sistema tradizionale basato su regole (linea rossa) e quelli collegati a un modello regionale tipico di CA Risk Analytics (linea verde). Si noti che, all'aumentare dei livelli di interazione imposta al cliente, aumenta anche il costo di funzionamento del sistema. Con un sistema basato su regole, che in genere non ha una visione completa della frode, i costi di funzionamento del sistema possono superare rapidamente i risparmi ottenuti. Con un modello avanzato basato sui dati, una vista completa della frode può essere ottenuta a un costo ragionevole. L'area verde ombreggiata indica il vantaggio rispetto a un modello basato su regole.

Figura 1.

Il costo totale del rilevamento delle frodi.



Sezione 2

Autenticazione basata sul comportamento

L'autenticazione basata sul comportamento comporta l'esame della transazione corrente nel contesto degli schemi abituali di attività del titolare della carta, del commerciante e del device del pagatore, per verificare se queste informazioni da sole possano generare un livello di attendibilità elevato rispetto all'identificazione del pagatore come titolare della carta. Se è così, non è necessario infastidire il pagatore nel corso della transazione, che procederà senza impatto, riducendo in modo significativo l'attrito e la probabilità di abbandono e migliorando in tal modo l'esperienza del titolare della carta[1]. In alternativa, se è elevata la probabilità che il pagatore non sia il titolare della carta, l'operazione può essere bloccata direttamente, impedendo in tal modo una richiesta di autorizzazione o di liquidazione ed eliminando completamente il rischio di frodi, anche se il truffatore è in possesso delle informazioni di autenticazione. Infine, per le transazioni in cui né la legittimità né l'illegittimità è (quasi) certa, può essere consigliabile passare a un'interazione di strong authentication con il titolare della carta. L'idea chiave da cui parte l'autenticazione basata sul comportamento è utilizzare dei modelli di comportamento per ridurre l'incertezza relativa all'identificazione della persona che tenta l'autenticazione come legittimo titolare della carta, e quindi contemporaneamente (a) ridurre la parte delle transazioni legittime per le quali viene richiesta una forma di autenticazione secondaria, (b) garantendo che per più tentativi di frode venga richiesta tale autenticazione e (c) bloccare direttamente un maggior numero di frodi.

I modelli come elementi dell'autenticazione basata sul comportamento

I modelli regionali di CA Risk Analytics sono costruiti utilizzando i dati di emittenti regionali che consentono l'impiego dei loro dati nell'ambito del CA eCommerce Consortium, al quale contribuiscono con dati sicuramente affidabili[2]. Questi dati includono transazioni 3D Secure con carte di debito e di credito.

I modelli regionali comprendono una serie di diversi elementi. Anzitutto, i modelli utilizzano informazioni derivanti dalla transazione corrente. Queste includono data e ora, importo, ubicazione della persona che tenta di autenticarsi per una transazione (computer o device mobile del titolare della carta in caso di commercio elettronico), nome, ID e URL del commerciante, informazioni riguardanti l'indirizzo IP del device, caratteristiche della connessione e informazioni di complemento da fornitori di dati terzi. Queste informazioni sono fondamentali perché il modello possa comprendere la transazione corrente. Tuttavia, non bastano per la comprensione dei comportamenti coinvolti.

In secondo luogo, i modelli utilizzano informazioni collegate al comportamento precedente delle entità cardine coinvolte nel tentativo di autenticazione corrente, come ad esempio carta, device o commerciante. Le informazioni derivate dai comportamenti passati vengono distillate in fattori essenziali per l'esame dei modelli di comportamento. Questi includono informazioni come i commercianti visitati, gli importi, i luoghi e i device utilizzati per ciascuna di queste visite e quali device unici sono stati utilizzati con la carta. Modelli simili vengono esaminati anche su altre entità cardine. Questi "distillati cardine", come vengono chiamati, vengono aggiornati a ogni tentativo osservato di autenticazione per una transazione.

In terzo luogo, i modelli utilizzano variabili complesse, inclusi mini-modelli, che isolano i modelli di comportamento delle entità cardine coinvolte nella transazione, e determinano se e come la transazione corrente corrisponde a quei modelli. Queste variabili possono essere semplici, come l'identificazione dell'utilizzo di un nuovo device con una determinata carta, o la velocità di spesa su una carta o device; ma possono anche essere complesse, ad esempio confrontando la tendenza di un dato titolare ad acquisti ripetuti e il numero di visite a un determinato commerciante, con gli stessi schemi di altri soggetti.

In quarto luogo, i modelli utilizzano tabelle create utilizzando i dati storici. Queste tabelle forniscono informazioni sulle tendenze passate per transazioni legittime e non, nei dati storici, inclusi metriche su tendenze e Naïve-bayesiane.

Infine, tutti questi diversi elementi sono rappresentati in un modello numerico non lineare che ne pondera le diverse previsioni relativamente ad anomalie comportamentali e il rischio di tentativi illegittimi. Questi modelli acquisiscono i comportamenti non lineari: relazioni importanti tra le variabili e il rischio di frodi non costituite da una semplice relazione lineare. Essi confrontano indicatori di rischio con fattori attenuanti (un commerciante e un importo a rischio elevato, ma un soggetto che ha già effettuato questo tipo di operazione da questo device), prendendo in considerazione più rapporti diversi.

La ponderazione dei diversi fattori dipende dall'utilizzo di un algoritmo di formazione su un insieme ampio di dati di transazione storici e di dati sicuramente affidabili; ovvero, questi tipi di modelli sono intrinsecamente basati sui dati. Questo consente ai modelli stessi di individuare relazioni non banali, difficili da trasformare in regole, e di presentare una valutazione ottimale della probabilità di illegittimità della transazione.

Il risultato generato da questi modelli è un numero che indica la probabilità stimata che il tentativo di autenticazione sia *illegittimo.* Questo consente un ordinamento delle operazioni di autenticazione, consentendo di attuare misure diverse e di definirne la priorità interna. In particolare, consente l'autenticazione silenziosa delle transazioni senza impatto sul titolare della carta, in base a modelli di comportamento nei dati che mostrano una scarsa probabilità di illegittimità.

Modellazione numerica non lineare tramite reti neurali feed-forward

Tra i molti approcci di modellazione numerica disponibili, le reti neurali feed-forward (FFNN) forniscono la combinazione ideale tra performance, flessibilità e fattibilità.

Le reti neurali feed-forward sono estremamente flessibili, dato che non richiedono presupposti strutturali e distributivi nello spazio di input-feature. Esse mostrano performance all'avanguardia anche sui dati meno lineari, in quanto approssimatori di funzione universali. Inoltre, indipendentemente dalla dimensione o dalla complessità dei dati, vengono addestrate a tempo lineare e generano il punteggio di rischio a tempo costante, il che le rende molto pratiche anche per insiemi di dati estremamente ampi.

Struttura delle reti neurali

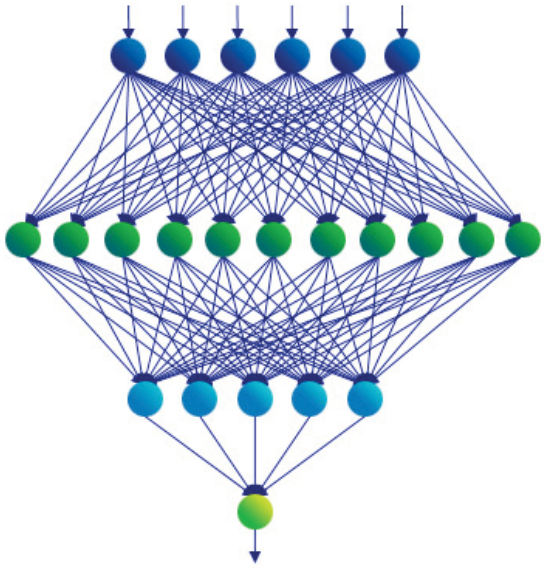
Una FFNN è essenzialmente un grafico di flusso-segnale diretto aciclico non lineare, il cui input è una rappresentazione numerica della transazione come acquisita mediante le tecniche di cui sopra, e il cui output, nel presente contesto, viene interpretato come misura ordinale della probabilità che il tentativo di autenticazione sia fraudolento (il punteggio di rischio).

In altri termini, le FFNN possono essere pensate come composte da una sequenza di "livelli", ciascuno dei quali è composto da un insieme di "neuroni" (vedere la Figura 2). Il tentativo di autenticazione iniziale viene presentato al primo livello (input), dove inizia la sua propagazione attraverso la rete. Questa propagazione continua attraverso i livelli interni ("nascosti") per arrivare poi al livello di output. Ogni livello opera una trasformazione non lineare sul dato di input e trasmette il risultato al livello successivo. Ogni livello può includere un numero arbitrario di neuroni, ma, nel contesto presente, il livello finale (output) include un neurone singolo (che genera il punteggio).

La potenza espressiva delle FFNN risiede in queste trasformazioni non lineari sequenziali, che consentono collettivamente alle FFNN di modellare qualsiasi funzione del proprio input.

Figura 2.

Un esempio di rete neurale feed-forward (FFNN).



Sezione 3

Vantaggi dei modelli avanzati

Performance del modello

I modelli regionali di CA Technologies consentono di rifiutare o di incrementare l'autenticazione su una maggioranza di operazioni fraudolente, influenzando solo una piccola parte di quelle legittime. La performance generale è rappresentata nella Figura 3. Il modello massimizza la rilevazione delle frodi, riducendo al minimo l'impatto sui clienti. Si noti che il grafico non visualizza tutta la curva, concentrandosi invece sull'area operativa della stessa.

Figura 3.

Il rilevamento delle frodi del modello come funzione della percentuale di tutte le transazioni segnalate dal modello stesso. Si noti che il grafico copre soltanto una porzione della popolazione, concentrandosi invece sull'area operativa della curva.

Punteggi e regole del modello

Le regole funzionano particolarmente bene nell'individuare indicatori di frode noti e precisi. Sono estremamente rapide da implementare e di facile comprensione. Tuttavia, non sono basate sui dati, e quindi risultano limitate dalle conoscenze dell'autore della regola in merito ai possibili indicatori di frode. Le regole non sono in grado di acquisire comportamenti complessi in modo semplice e non consentono di combinare facilmente più rischi in un'unica decisione. Infine, non possono ordinare le operazioni per consentirne blocco o autenticazione secondaria, né l'adeguamento dei volumi di ticket.

I modelli acquisiscono schemi complessi utilizzando variabili sofisticate. Le variabili si basano sulla transazione corrente, nonché sui distillati cardine (informazioni chiave che sono state distillate da operazioni passate sugli identificatori cardine nelle transazioni). Utilizzando variabili lineari e non lineari e tecniche di addestramento collaudate, i modelli consentono la ponderazione dei diversi fattori usando un approccio basato sui dati e producono un ordinamento delle operazioni in base al rischio di frode. Tuttavia, i modelli di per se stessi non agiscono; le regole rappresentano quindi un complemento essenziale ai modelli stessi.

Combinazione tra regole e modelli

Dati i diversi punti di forza di modelli e regole, l'approccio migliore consiste nell'utilizzarli in combinazione. In primo luogo, utilizzare un modello forte per separare frodi e non e ordinare le operazioni mediante un punteggio di rischio. In secondo luogo, scrivere regole che utilizzano questo punteggio in una serie di modi: (i) i punteggi più alti indicano una forte probabilità di frode e devono essere utilizzati per intervenire, adeguando la soglia di punteggio per raggiungere i volumi e il livello di sofisticazione delle frodi desiderati dall'istituzione e (ii) i punteggi più bassi possono essere utilizzati in combinazione con flash-fraud o altre regole, filtrando quelli con una forte probabilità di essere legittimi e consentendo alle regole di operare in un pool di dati più ricco. Infine, l'istituto potrà implementare regole di policy che prescindono dal rischio di frode, richiedendo eventualmente l'autenticazione secondaria per i nuovi device, indipendentemente dal livello di rischio.

Sezione 4

Conclusioni

L'utilizzo dell'autenticazione basata sul comportamento per determinare su quali operazioni si deve intervenire tramite autenticazione o blocco è fondamentale per ridurre l'impatto sul cliente (ovvero l'attrito) e al contempo garantire meglio la legittimità della transazione. Le regole sono una componente importante dell'erogazione di questa autenticazione basata sul rischio e sul comportamento. Tuttavia, presentano una serie di limitazioni. Quando si aggiungono modelli sofisticati basati sul comportamento e li si utilizza per l'applicazione delle regole basate sul rischio, l'impatto sui tentativi illegittimi di autenticazione può essere notevolmente aumentato, mentre si riduce quello sui clienti legittimi, generando un'esperienza migliore per il titolare della carta e una riduzione delle perdite per l'emittente.

Sezione 5

Informazioni sugli autori

Paul Dulany lavora nell'ambito Advanced Analytics e Data Science da 14 anni. È entrato in CA Technologies nel 2013 e ha guidato lo sviluppo dell'infrastruttura di modellazione analitica e il primo modello prodotto dal team Data Science di CA Technologies. Prima di entrare in CA Technologies, ha operato presso il SAS Institute per oltre 8 anni, come membro del team che ha sviluppato i primi modelli per la soluzione SAS Enterprise Fraud Management e come leader nello sviluppo dei primi modelli di carte di debito e di molte nuove tecniche. Prima di SAS, Paul ha fatto parte di HNC e Fair Isaac per oltre 5 anni, come scienziato e poi come responsabile del team di modellazione Fraud Predictor, sviluppando una serie di modelli di carte di pagamento Falcon e operando anche in altri ambiti. Paul è titolare di alcuni brevetti registrati durante il periodo trascorso presso HNC e SAS e ha un dottorato di ricerca in Fisica teorica.

Hongrui Gong ha una vasta esperienza in materia di analisi avanzata e Data Science. È entrato in CA Technologies nel mese di aprile 2013 assumendo un ruolo chiave nelle iniziative di creazione di un'infrastruttura di modellazione e nello sviluppo di modelli per i prodotti 3D Secure. Prima di entrare in CA Technologies, ha lavorato per oltre 15 anni con importanti società di analisi (SAS, FICO e HNC) allo sviluppo di modelli per prodotti quali il rilevamento delle frodi tramite carte di pagamento, il rilevamento delle frodi assicurative, l'identificazione degli evasori fiscali per il governo federale e statale, l'anti-riciclaggio di denaro, la previsione delle perdite sui prestiti, la gestione del rischio collegato ai margini di mediazione e la valutazione del rischio di credito per aziende pubbliche e private. Hongrui ha conseguito un

dottorato di ricerca in Dinamica dei fluidi computazionale e ha trascorso quattro anni presso il National Laboratory di Los Alamos dedicandosi alla ricerca sulla modellazione teorica e sulle simulazioni tramite computer del flusso turbolento di fluidi. Durante le sue mansioni precedenti ha conseguito una serie di brevetti.

Kannan Shah lavora nell'ambito Advanced Analytics e Data Science da 6 anni. È entrato in CA Technologies nel 2013, e ha contribuito allo sviluppo dell'infrastruttura di modellazione analitica e al primo modello prodotto dal team Data Science di CA Technologies. Prima di entrare in CA Technologies, è stato Senior Staff Scientist presso il SAS Institute, dove ha sviluppato modelli e tecniche statistiche e ha fornito supporto alla clientela per la soluzione SAS Enterprise Fraud Management. Ha contribuito allo sviluppo di modelli di individuazione delle frodi tramite carte di pagamento, trasferimenti ACH e bonifici, distribuiti negli Stati Uniti, in Regno Unito, Messico e nella regione dell'Asia-Pacifico. Durante la sua attività presso SAS ha conseguito una serie di brevetti. Kannan ha conseguito la laurea specialistica in Ingegneria elettronica presso la Drexel University di Philadelphia. Le sue aree di specializzazione durante gli studi accademici includono rilevamento e stima, elaborazione dei segnali stocastici, intelligenza delle macchine, riconoscimento dei modelli statistici, reti neurali, teoria dell'informazione, analisi spettrale degli ordini superiori, progettazione e complessità di algoritmi.

1 Nelle regioni caratterizzate da una formazione significativa dei titolari delle carte in relazione alla ricerca di indicatori 3D Secure, per il titolare può risultare rassicurante visualizzare una finestra che indica che la transazione è protetta da 3D Secure.

2 L'espressione "dati sicuramente affidabili" si riferisce alle informazioni a livello di transazione e di carta per individuare le operazioni che il processo di autenticazione dovrebbe bloccare.

CS200_94860_1014