DOCUMENTAÇÃO TÉCNICA | OUTUBRO DE 2014

Autenticação 3D-Secure usando modelos avançados

Os modelos usados para a autenticação com base em riscos e comportamentos de transações de comércio eletrônico podem reduzir as perdas e fornecer check-out sem empecilhos para transações de baixo risco.

Paul Dulany
Hongrui Gong
Kannan Shah
CA Technologies, análise avançada e ciência de dados

ca technologies

Sumário

Resumo executivo

Desafio

Os emissores precisam encontrar um equilíbrio entre a segurança da transação de pagamento de comércio eletrônico e uma experiência de check-out tranquila para o cliente. A questão principal é como proporcionar uma experiência de check-out perfeita para clientes legítimos, para que eles não abandonem a transação ou usem outra forma de pagamento e, ao mesmo tempo, impedir tentativas ilegítimas de transação. O uso da autenticação com base em comportamentos para determinar quais transações devem ser impactadas, exigindo que o cliente passe por meios adicionais de autenticação, é fundamental para reduzir os empecilhos para os clientes e aumentar a garantia de que a transação é legítima. As regras são um componente importante ao fornecer essa autenticação com base em riscos e comportamentos. Quando os modelos são adicionados e usados para orientar a aplicação de regras com base em riscos, o impacto nas tentativas de autenticação ilegítima pode aumentar consideravelmente, ao passo que o impacto nos clientes legítimos é reduzido, proporcionando uma melhor experiência para o titular do cartão e reduzindo as perdas do emissor.

Oportunidade

O serviço 3D-Secure oferece muitas oportunidades para os emissores. Em uma época marcada pelo aumento significativo de fraudes no comércio eletrônico, além da mudança de responsabilidade, a autenticação 3D-Secure fornece uma defesa de primeiro nível para os emissores. No entanto, é importante usar essa defesa de primeiro nível com sabedoria e da melhor maneira possível. O CA Risk Analytics fornece a oportunidade de examinar as transações de comércio eletrônico durante a autenticação usando informações exclusivas, que não estão disponíveis para sistemas de detecção de fraude de autorização, a fim de evitar uma transação ilegítima. Uma avaliação do risco de autenticação deve ser feita a fim de proporcionar uma experiência ininterrupta de check-out para a maioria dos titulares legítimos. Com o uso do CA Risk Analytics, os emissores podem reduzir as perdas e limitar os empecilhos para os clientes.

Benefícios

O CA Risk Analytics ajuda os emissores a avaliarem o nível de risco das atividades online em estabelecimentos comerciais com o 3D-Secure. Ele avalia com transparência e em tempo real se há risco de que uma transação de comércio eletrônico esteja sendo realizada por alguém que não é o legítimo titular do cartão. O CA Risk Analytics identifica uma parcela significativa de tentativas de transação legítima e permite que os clientes prossigam a compra, sem impacto, enquanto identifica da mesma forma as tentativas de transação ilegítima que devem ser interrompidas. A identificação de dispositivo, a localização geográfica, as características da conexão e os padrões históricos podem ser usados para avaliar o risco de cada tentativa de transação.

Um aspecto essencial do CA Risk Analytics é a disponibilidade de modelos regionais avançados que avaliam o nível de risco de uma determinada tentativa de transação usando uma análise sofisticada, incluindo um modelo de rede neural comportamental, e fornecem uma pontuação que indica o grau de risco dessa tentativa. Em seguida, as regras do CA Risk Analytics podem combinar a pontuação desse modelo com outros fatores de negócios para determinar o melhor tratamento para uma determinada tentativa de transação, resultando em um aumento significativo da eficácia da solução.

Seção 1

O 3D-Secure fornece a base para a redução das perdas de comércio eletrônico

O protocolo 3D-Secure fornece aos emissores muitas oportunidades de aproveitar a proteção e todos os benefícios oferecidos pelo serviço 3D-Secure.

O serviço 3D-Secure se concentra em autenticar as tentativas de transação de comércio eletrônico. É importante compreender a diferença entre autenticação e autorização. Autenticação é a tentativa de confirmar que a pessoa que inicia uma transação (ou outra atividade) é o legítimo e genuíno titular do cartão. Autorização é a tentativa de validar que o titular do cartão (confirmado) tem autoridade para fazer a transação (com base em diretivas, saldos disponíveis, status da conta e outras questões). Saiba que a fraude pode ocorrer e ser detectada tanto na etapa de autorização quanto na de autenticação, mas existem diferenças importantes; por exemplo, a autenticação não impede diretamente a fraude do próprio titular do cartão. No entanto, independentemente do tipo de fraude, a autenticação da pessoa que está tentando fazer uma transação é o ponto de partida para garantir que a transação é válida.

Para as transações de cartão presente, a presença física do cartão é aceita há muito tempo como um componente-chave de autenticação. Como os usuários ilegítimos tornaram-se mais sofisticados, os emissores responderam com o aumento da segurança nos cartões (tarja magnética, CVV/CVC/CID e cartões inteligentes). Esses dados, ou os resultados de autenticação com esses dados, geralmente são enviados no pedido de autorização.

Para as transações de CNP (Card Not Present - Cartão Não Presente), a autenticação física por meio do cartão não é mais possível, e a responsabilidade tem sido geralmente do estabelecimento comercial. Com o advento do comércio eletrônico, no entanto, tornou-se necessário desenvolver uma autenticação robusta de transações de comércio eletrônico. Os dados do pedido de autorização, embora sejam suficientes para autorizar uma transação, são insuficientes para a autenticação de uma transação de comércio eletrônico. Por isso, surgiu a transação 3D-Secure, com informações diferentes daquelas contidas no pedido de autorização e projetada para autenticar a pessoa que tentar fazer uma transação. Essa tarefa, que é fundamentalmente diferente da autorização, exige uma perspectiva exclusiva. No entanto, os resultados dessa autenticação podem ser utilizados no fluxo de autorização para fornecer um melhor contexto para o sistema de autorização.

Quando mencionamos fraude neste documento, nos referimos especificamente à fraude de autenticação nas transações 3D-Secure de comércio eletrônico.

Usando o protocolo 3D-Secure, há a oportunidade de examinar as tentativas de autenticação de comércio eletrônico com as informações exclusivas não disponíveis para sistemas de detecção de fraude de autorização e, desse modo, impedir uma transação ilegítima antes que ela crie um pedido de autorização. Ao usar o sistema CA Risk Analytics, essas informações exclusivas incluem uma identificação exclusiva para cada dispositivo (ID do dispositivo), um URL que é acessado pelo titular do cartão para fazer a transação (URL do estabelecimento comercial), o atual endereço IP do dispositivo e informações auxiliares de provedores de dados de terceiros, incluindo a localização do dispositivo, a velocidade de conexão, o tipo e a identificação do proxy anônimo, bem como outras informações. Essas informações ampliam significativamente (mas não substituem) as informações tradicionais, como o valor, a moeda, o nome e a ID do estabelecimento comercial, o identificador do cartão e outras informações. Com esse aumento, os modelos de autenticação 3D-Secure podem oferecer mais benefícios do que os modelos de autorização que têm acesso apenas às informações tradicionais, proporcionando detecção avançada das tentativas de autenticação ilegítima e impactando apenas uma pequena parcela das tentativas legítimas.

O serviço 3D-Secure fornece informações em tempo real para analisar transações de autenticação. Em particular, temos a oportunidade de atualizar as informações sobre o cartão, o dispositivo ou outras entidades principais na transação em tempo real. Isso permite que qualquer transação subsequente aproveite os benefícios da maior quantidade de informações e de contexto quando o risco de autenticação for avaliado. Essa opção pode ser especialmente vantajosa ao avaliar entidades de vários bancos em um ambiente de software como serviço na nuvem.

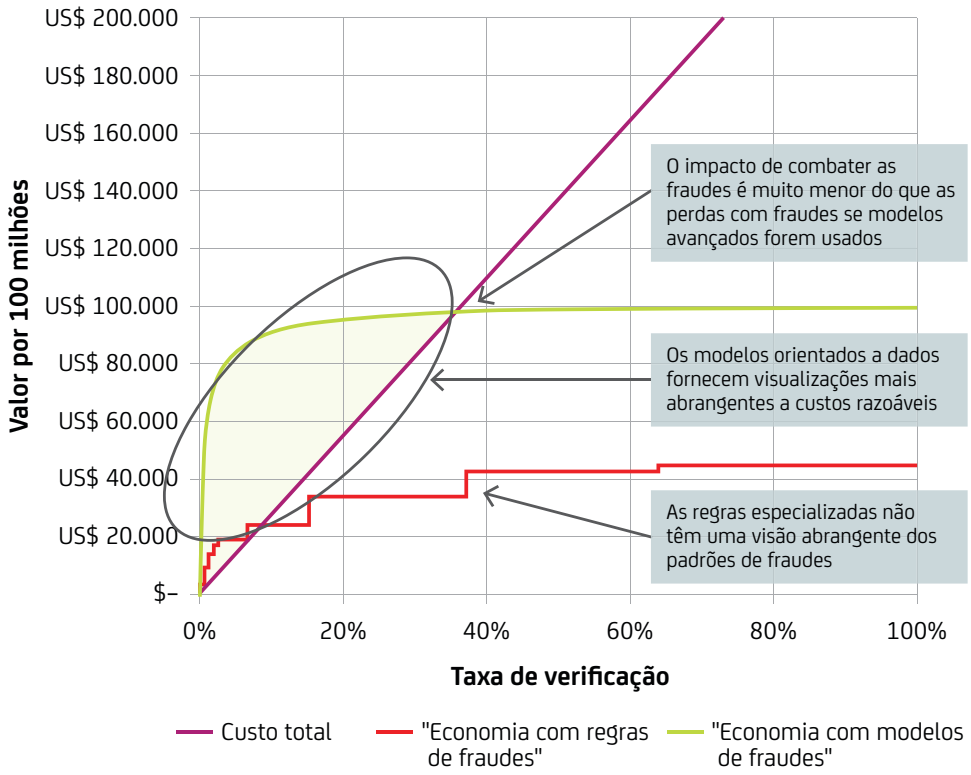
Também há a oportunidade de eliminar praticamente todos os empecilhos das compras de comércio eletrônico. As primeiras implementações do 3D-Secure apresentavam perguntas de verificação para todos os compradores de estabelecimentos comerciais com 3D-Secure. Se as perguntas forem difíceis, como o uso de OTP (One-Time-Passwords - Senhas de Uso Único), essa abordagem poderá ser razoavelmente eficaz; se as perguntas de verificação forem fáceis, como a solicitação de informações necessárias para realizar a própria transação (data de validade ou CVV2), essa abordagem não ajudará muito a impedir as perdas. No entanto, há um efeito secundário: a apresentação de perguntas de verificação para os titulares de cartão gera um "empecilho" na transação — aumentando a resistência para concluir a transação e causando um impacto negativo na experiência do cliente.

O impacto negativo do empecilho na experiência do cliente não é puramente qualitativo — também há um componente quantitativo: ele aumenta significativamente as taxas de abandono e de "falsas falhas". O abandono resulta na perda das taxas de intermediação, além de causar impactos maiores, como a perda do saldo rotativo de cartões de crédito ou a possível perda dos clientes, que é uma questão importante para as contas de débito e crédito. Esses fatos permitem quantificar parte do impacto que uma experiência negativa do cliente causa nos emissores e fornecem uma grande motivação para reduzir os empecilhos da transação. No caso extremo de apresentar perguntas de verificação a todos os clientes, os custos do abandono podem superar qualquer redução de perdas. Portanto, é fundamental avaliar o risco de uma determinada transação e interferir no processo apenas quando houver uma boa justificativa. A melhor maneira de fazer isso é usando uma autenticação com base em comportamentos.

A Figura 1, na página seguinte, mostra um exemplo do custo total da detecção de fraudes (incluindo perda de oportunidade devido ao abandono) (a linha roxa), a economia de um sistema de regras típico (linha vermelha) e a economia de um Modelo Regional típico do CA Analytics (linha verde). Observe que, à medida que a taxa de verificação aumenta, o custo de operação do sistema também aumenta. Com um sistema de regras, que geralmente não tem uma visão abrangente da fraude, o custo de operação do sistema pode superar rapidamente a economia das regras. Com um modelo avançado orientado a dados, uma visão abrangente da fraude pode ser obtida a um custo razoável. A região sombreada em verde mostra a vantagem de um modelo em comparação com as regras.

Figura 1.

O custo total da detecção de fraudes.



Seção 2

Autenticação com base em comportamentos

A autenticação com base em comportamentos envolve observar a transação atual dentro do contexto dos padrões habituais dos titulares de cartão, estabelecimentos comerciais e atividades do dispositivo do pagador para confirmar se apenas essas informações podem oferecer uma garantia confiável de que o pagador é o verdadeiro titular do cartão. Se esse for o caso, não haverá necessidade de incomodar o pagador no meio de sua transação, e a transação poderá ser realizada sem impacto, reduzindo significativamente os empecilhos e a probabilidade de abandono, além de melhorar a experiência dos titulares de cartão[1]. Como alternativa, se houver uma garantia confiável de que esse não é o verdadeiro titular do cartão, a transação poderá ser imediatamente negada, evitando um pedido de autorização ou de pagamento e eliminando a possibilidade de fraude por completo, mesmo que o fraudador saiba as informações de autenticação. Por fim, para aquelas transações nas quais não há uma garantia confiável de legitimidade nem de ilegitimidade, a aplicação de uma autenticação forte para interação com o titular do cartão pode ser recomendável. A ideia principal da autenticação com base em comportamentos é utilizar os padrões de comportamento para reduzir a incerteza de que a pessoa que está tentando fazer a autenticação é o legítimo titular do cartão e, portanto, simultaneamente (a) reduzir o número de transações legítimas impactadas por uma autenticação secundária, (b) garantir que mais fraudes entrem na autenticação secundária e (c) negar imediatamente mais fraudes.

Modelos como autenticadores com base em comportamentos

Os modelos regionais do CA Risk Analytics são criados com os dados de emissores regionais que permitem que seus dados sejam usados no CA eCommerce Consortium e que contribuem com "dados verdadeiros"[2]. Esses dados incluem transações 3D-Secure com cartão de crédito e de débito.

Os modelos regionais abrangem uma série de elementos diferentes. Em primeiro lugar, os modelos utilizam as informações da transação atual. Elas incluem a data e a hora, o valor, a localização da pessoa que está tentando autenticar uma transação (computador ou dispositivo móvel, no caso de comércio eletrônico, do titular do cartão), o nome do estabelecimento comercial, a ID e o URL, informações sobre o endereço IP do dispositivo, as características da conexão e informações auxiliares de provedores de dados de terceiros. Essas informações são fundamentais para que o modelo entenda a transação atual. No entanto, não são suficientes para a compreensão dos comportamentos envolvidos.

Em segundo lugar, os modelos utilizam as informações de comportamentos anteriores para as entidades principais da atual tentativa de autenticação, como o cartão, o dispositivo ou o estabelecimento comercial. As informações de comportamentos anteriores são refinadas para encontrar os fatores importantes e observar os padrões de comportamento. Essas informações incluem dados como: quais estabelecimentos comerciais foram visitados, os valores, os locais, os dispositivos utilizados em cada uma dessas visitas e quais dispositivos exclusivos foram usados com esse cartão. Padrões similares também são observados em outras entidades principais. Essas "informações refinadas principais", como são chamados os históricos, são atualizadas após cada tentativa observada de autenticar uma transação.

Em terceiro lugar, os modelos utilizam variáveis complexas, incluindo minimodelos, que isolam os padrões de comportamento das entidades principais envolvidas na transação, além de determinar como e se a transação atual se encaixa nesses padrões. Essas variáveis podem ser simples, como aquelas para identificar se há um novo dispositivo para uso com um determinado cartão ou estabelecer a velocidade de gastos em um cartão ou dispositivo. No entanto, elas também podem ser complexas, utilizando o número de vezes que um determinado titular de cartão visitou um estabelecimento comercial e fez compras mais de uma vez e comparando essa tendência com os mesmos padrões de outras pessoas.

Em quarto lugar, os modelos utilizam tabelas criadas com dados históricos. Essas tabelas fornecem informações sobre as últimas tendências de transações fraudulentas e legítimas nos dados históricos, incluindo as métricas de tendência e de Bayes Ingênuo.

Por fim, todos esses diferentes elementos são apresentados em um modelo numérico não linear que avalia suas diversas previsões sobre as anomalias de comportamento e o risco de tentativas ilegítimas. Esses modelos capturam os comportamentos não lineares: relacionamentos importantes entre as variáveis e a probabilidade de fraude que não são relacionamentos lineares simples. Eles comparam indicadores de risco com fatores atenuantes (por exemplo, estabelecimento comercial e valor com alto índice de fraude, mas a pessoa já fez esse tipo de transação no mesmo dispositivo), observando muitos relacionamentos diferentes.

A maneira como esses diferentes fatores são avaliados é determinada usando um algoritmo de treinamento em um grande conjunto de dados de transações históricas e "dados verdadeiros", ou seja, esses tipos de modelo são inerentemente "orientados a dados". Isso permite que os modelos descubram relacionamentos não triviais que não são fáceis de capturar em regras e apresentem a melhor estimativa da probabilidade de que a transação seja ilegítima.

A saída desses modelos é um número que fornece uma estimativa da probabilidade de que uma tentativa de autenticação seja *ilegítima.* Com isso, é possível fazer uma classificação das transações de autenticação, permitindo que diferentes medidas sejam tomadas e que seja possível priorizar essas medidas. Em particular, isso permite a "autenticação silenciosa" das transações, sem afetar o titular do cartão, com base nos padrões de comportamento dos dados que mostram uma baixa probabilidade de ilegitimidade.

Modelagem numérica não linear usando redes neurais feed-forward

Entre as muitas abordagens de modelagem numérica disponíveis, as FFNNs (Feed-Forward Neural Networks - Redes Neurais Feed-Forward) fornecem a combinação ideal de desempenho, flexibilidade e viabilidade.

As redes neurais feed-forward são extremamente flexíveis, pois não exigem premissas estruturais ou distribucionais sobre o espaço de características de entrada. Elas apresentam um desempenho avançado até mesmo nos dados mais não lineares, pois são aproximadoras universais de funções. Além disso, independentemente do tamanho ou da complexidade dos dados, elas treinam em tempo linear e pontuam em tempo constante, o que as torna muito práticas, até mesmo para conjuntos de dados extremamente grandes.

Estrutura da rede neural

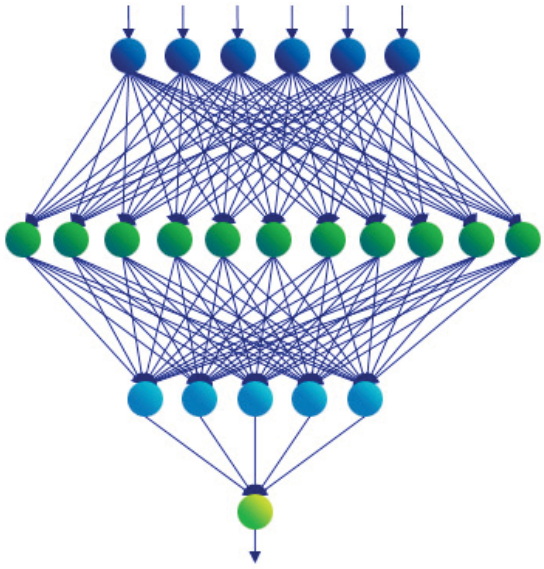
Uma FFNN é essencialmente um gráfico acíclico não linear direcionado de fluxo de sinais, cuja entrada é uma representação numérica da transação, conforme capturada pelas técnicas mencionadas acima, e cuja saída, no presente contexto, é interpretada como uma medida ordinal da probabilidade de que a tentativa de autenticação seja fraudulenta (a pontuação).

Mais especificamente, é possível considerar que as FFNNs são compostas de uma sequência de "camadas", cada uma delas composta de um conjunto de "neurônios" (veja a Figura 2). A tentativa de autenticação de entrada é apresentada para a primeira camada (entrada), na qual ela começa sua propagação pela rede. Essa propagação segue pelas camadas internas ("camadas ocultas") e, por fim, chega até a camada de saída. Cada camada executa uma transformação não linear em sua entrada e passa o resultado para a camada subsequente. Cada camada pode ter um número arbitrário de neurônios, mas, no presente contexto, a camada final (saída) tem um único neurônio (que produz a pontuação).

O poder expressivo das FFNNs encontra-se nessas transformações não lineares sequenciais, que coletivamente permitem que a FFNN modele qualquer função de sua entrada.

Figura 2.

Um exemplo de FFNN.



Seção 3

Vantagens dos modelos avançados

Desempenho do modelo

Os modelos regionais da CA permitem a negação ou a autenticação elevada na maioria das transações fraudulentas, afetando apenas uma pequena parcela das transações legítimas. O desempenho geral é mostrado na Figura 3. O modelo maximiza a detecção de fraudes, minimizando o impacto nos clientes. Observe que o gráfico não exibe a curva completa, concentrando-se apenas na área operacional da curva.

Figura 3.

A detecção de fraudes do modelo como uma função da porcentagem de todas as transações sinalizadas pelo modelo. Observe que o gráfico abrange apenas uma parcela da população, concentrando-se na área operacional da curva.

Regras e pontuações de modelos

As regras são muito boas para o direcionamento de indicadores precisos e conhecidos de fraude. Elas são rápidas de implementar e fáceis de entender. No entanto, elas não são orientadas a dados e, portanto, são limitadas pelo conhecimento do escritor das regras quanto aos possíveis sinais de fraude. As regras não conseguem captar comportamentos complexos com facilidade e não permitem que vários riscos sejam combinados prontamente em uma única decisão. Por fim, elas não conseguem classificar as operações para permitir que a recusa, a autenticação secundária e os volumes de casos sejam ajustados.

Os modelos capturam padrões complexos utilizando variáveis sofisticadas. As variáveis baseiam-se na transação atual e nas informações refinadas principais (informações importantes de transações passadas de identificadores principais nas transações, que foram refinadas). Por meio de variáveis não lineares e lineares, além de técnicas de treinamento consagradas, os modelos permitem a avaliação de diferentes fatores, usando uma abordagem orientada a dados, e produzem uma classificação das transações com base na probabilidade de fraude. No entanto, os modelos não agem isoladamente; as regras são um complemento essencial para os modelos.

Regras e modelos juntos

Levando em conta os diferentes pontos fortes de modelos e regras, a melhor abordagem é usá-los juntos. Primeiro, utilize um modelo forte para separar aquilo que é fraude daquilo que não é e classifique as transações usando uma pontuação. Segundo, escreva regras que utilizem essa pontuação de algumas maneiras: (i) pontuações altas indicam uma grande probabilidade de fraude e devem ser usadas para tomar medidas, ajustando o limite de pontuação para atingir a magnitude e os volumes de fraude desejados pela instituição, e (ii) pontuações mais baixas podem ser usadas em conjunto com regras de fraude ou outras regras, filtrando aquelas com uma alta probabilidade de não fraude e permitindo que as regras operem em um pool de dados mais sofisticado. Por fim, haverá regras de diretiva, que são independentes da probabilidade de fraude implementada pela instituição — talvez exigindo uma autenticação secundária para novos dispositivos, independentemente da probabilidade de fraude.

Seção 4

Conclusão

O uso da autenticação com base em comportamentos para determinar quais transações devem ser impactadas pela autenticação ou negação é essencial para reduzir o impacto nos clientes (ou seja, os empecilhos) e aumenta a garantia de que a transação é legítima. As regras são um componente importante ao fornecer essa autenticação com base em riscos e comportamentos. No entanto, elas têm uma série de limitações. Quando modelos sofisticados com base em comportamentos são adicionados e usados para orientar a aplicação de regras com base em riscos, o impacto nas tentativas ilegítimas pode aumentar consideravelmente, ao passo que o impacto nos clientes legítimos é reduzido, proporcionando uma melhor experiência para o titular do cartão e reduzindo as perdas do emissor.

Seção 5

Sobre os autores

Paul Dulany trabalha na área de análise avançada e ciência de dados há 14 anos. Ele entrou na CA Technologies em 2013 e liderou o desenvolvimento da infraestrutura de modelagem analítica e do primeiro modelo produzido pela equipe de ciência de dados da CA. Antes de ingressar na CA Technologies, trabalhou no SAS Institute por mais de oito anos, como parte da equipe que desenvolveu os primeiros modelos para a solução de gerenciamento de fraudes corporativas do SAS, bem como líder do desenvolvimento dos primeiros modelos de cartão de débito e de muitas novas técnicas. Antes do SAS, Paul trabalhou na HNC e na Fair Isaac por mais de cinco anos, como cientista e, mais tarde, como gerente da equipe de modelagem do instrumento de previsão de fraudes, desenvolvendo uma série de modelos de cartão de pagamento Falcon, além de trabalhar em outras áreas. Paul detém patentes da época em que trabalhou na HNC e no SAS e tem um doutorado em Física Teórica.

Hongrui Gong tem uma vasta experiência na área de análise avançada e ciência de dados. Ele entrou na CA Technologies em abril de 2013 e desempenhou uma função fundamental nos esforços de criação de uma infraestrutura de modelagem e de desenvolvimento de modelos de produtos 3D-Secure. Antes de ingressar na CA, ele trabalhou por mais de 15 anos em proeminentes empresas de análise (SAS, FICO, HNC) para desenvolver modelos de produtos, como detecção de fraudes de cartão pagamento, detecção de fraudes de seguro, identificação de sonegação fiscal para o governo federal e estadual, antilavagem de dinheiro, previsão de perda de empréstimo, gerenciamento de risco de empréstimo marginal e classificação de risco de crédito para empresas públicas e privadas. Hongrui tem um doutorado

em Fluidodinâmica Computacional e passou quatro anos no Laboratório Nacional de Los Alamos, concentrando-se na pesquisa de modelagem teórica e simulações computacionais de fluxo turbulento de fluidos. Ele detém uma série de patentes de seus trabalhos anteriores.

Kannan Shah trabalha no setor de análise avançada e ciência de dados há seis anos. Ele entrou na CA Technologies em 2013 e contribuiu para o desenvolvimento da infraestrutura de modelagem analítica e do primeiro modelo produzido pela equipe de ciência de dados da CA. Antes de ingressar na CA Technologies, ele era um cientista sênior do SAS Institute, onde desenvolveu técnicas e modelos estatísticos e forneceu suporte ao cliente para a solução de gerenciamento de fraudes corporativas do SAS. Ele contribuiu para o desenvolvimento de modelos de detecção de fraudes para cartões de pagamento e transferências bancárias e de compensação automatizada, implantados nos EUA, no Reino Unido, no México e na região da Ásia-Pacífico. Kannan detém uma série de patentes da época em que trabalhou no SAS. Kannan tem um mestrado em Engenharia Elétrica pela Universidade de Drexel, na Filadélfia. As áreas de foco durante seus estudos acadêmicos incluíram detecção e estimativa, processamento estocástico de sinais, inteligência artificial, reconhecimento estatístico de padrões, redes neurais, teoria da informação, análise espectral de ordem superior e projeto e complexidade de algoritmos.

1 Nas regiões em que ocorreram esforços significativos para instruir os titulares de cartão a procurar por indicadores 3D-Secure, a exibição de uma janela para informar que a transação é protegida por 3D-Secure pode tranquilizá-los.

2 O termo "dados verdadeiros" refere-se a informações de nível de transação e cartão para identificar as transações que o processo de autenticação deve interromper.

CS200_94860_1014