Combattre la fraude financière grâce à une plateforme de données en temps réel

La fraude financière est un problème qui prend rapidement de l'ampleur. La capacité à traiter les données rapidement et à identifier des modèles avec l'IA et l'apprentissage automatique peut aider vos programmes de détection des fraudes à relever de nouveaux défis.

Introduction

La fraude et les autres cybercrimes constituent une menace permanente, et la situation ne cesse d'empirer. L'enquête mondiale sur la criminalité et la fraude économiques menée en 2020 par PwC a révélé que 47 % des entreprises avaient été victimes de fraude au cours des deux dernières années, pour un coût total estimé à 42 milliards de dollars.

Avec l'augmentation de l'utilisation des services bancaires en ligne, la fraude a également pris de l'ampleur. Plus d'un tiers (35 %) des clients des services bancaires aux particuliers ont augmenté leur utilisation des services bancaires en ligne pendant la pandémie de Covid-19, et on peut présumer sans risque de se tromper que cela pourrait devenir une nouvelle norme. Étant donné que le secteur des paiements continue d'optimiser les transactions aux fins qu'elles soient réalisées à une vitesse maximale, les plateformes de détection des fraudes ont encore moins de temps pour réagir.

Compte tenu des coûts élevés associés à la correction de la fraude financière après coup, les entreprises travaillent d'arrache-pied pour améliorer leur capacité à détecter et à prévenir la fraude. Les mesures KYC et de la lutte contre le blanchiment d'argent jouent depuis longtemps un rôle important dans la détection de la fraude, mais les criminels trouvent constamment de nouveaux moyens de contourner le système. Les entreprises qui ne peuvent se permettre de déployer les derniers outils visant à devancer les acteurs malveillants risquent d'être ciblées plus souvent.

Le secteur reconnaît clairement qu'il fait face à un problème, et les sociétés de services financiers investissent dans des outils avancés pour le résoudre. Forrester prévoit que les dépenses des entreprises en matière d'outils de sécurité dans le Cloud, par exemple, atteindront 12,6 milliards de dollars d'ici 2023, contre 5,6 milliards de dollars en 2018. Mais dans quels outils doivent-ils investir et sur quelles tendances doivent-ils se concentrer ? Ce livre blanc examine les dernières tendances en matière de fraude financière, suggère des domaines dans lesquels les entreprises peuvent lutter efficacement, et explique comment Redis aide les entreprises à réaliser ces objectifs.

47 % des entreprises ont été victimes de fraude au cours des deux dernières années, pour un coût total estimé à

$42 milliards

Fraude sur les transactions

Avec la rapidité et l'ampleur croissantes des services bancaires en ligne, les fraudes de tous types sont de plus en plus fréquentes. Les pertes dues aux prises de contrôle de comptes ont augmenté de 72 % entre 2018 et 2019 et, la même année, l'usurpation d'identité a atteint son plus haut niveau depuis 2013, représentant des pertes de 16,9 milliards de dollars en 2019. Les détaillants et les prestataires de services financiers doivent également lutter contre la fraude liée aux débits compensatoires, la fraude des commerçants et la fraude liée aux paiements internationaux. Cette dernière est particulièrement difficile à tracer, car les entreprises n'ont souvent pas une vue unifiée des transactions sur tous les marchés et parce que les outils et méthodes de détection de la fraude diffèrent souvent d'un pays à l'autre.

Tout cela aboutit à un nombre croissant de transactions frauduleuses, et de nombreux services existants de détection des fraudes en ligne ne peuvent pas traiter les données assez rapidement pour identifier ces transactions au moment où elles se produisent. Par conséquent, de nombreuses entreprises se tournent vers l'intelligence artificielle (IA) et l'apprentissage automatique (ML) pour fournir une cotation automatisée des transactions, conçue pour la vitesse et l'échelle des services bancaires en ligne. Quelques 70 % des entreprises de services financiers utilisent déjà l'apprentissage automatique pour prévoir les transactions, ajuster les cotes de crédit et détecter les fraudes. Mais, pour être efficaces, l'IA et le ML devront être appliqués plus rapidement et à plus grande échelle en raison de la nature même du problème.

Comme le suggère cette métaphore, il existe de nombreuses transactions légitimes pour chaque transaction frauduleuse, et le contrôle de chaque transaction demande des efforts et a un coût. Et aucun système n'est parfait. Les entreprises doivent souvent décider s'il est rentable de contrôler un plus grand nombre de transactions en détail ou de se résoudre à accepter un certain niveau de fraude. Les institutions financières choisissent systématiquement la seconde solution. L'analyse statistique avancée est la clé pour prendre ce type de décisions de la manière la plus précise possible.

En examinant efficacement les modèles dans les données afin de déterminer la probabilité qu'une transaction soit frauduleuse, les plateformes basées sur l'IA peuvent automatiser la prise de décision. Dans certains cas, elles sont jusqu'à 40 % plus rapides que les systèmes de détection des fraudes basés sur des règles plus simples, avec le même taux de faux positifs. Dans le cas de ***l'apprentissage supervisé***, les données étiquetées (qui sont organisées d'une certaine manière, par exemple, pour identifier le nom, l'adresse et le numéro de téléphone) sont utilisées pour former un modèle d'IA afin de prédire si une transaction est frauduleuse ou non. ***L'apprentissage non supervisé***, quant à lui, utilise des données non étiquetées (lorsque les données ne sont pas organisées ou expliquées, par exemple des enregistrements audio ou des photos) et il est meilleur pour trouver de nouveaux modèles de fraude. Pour rendre ce type de détection possible, le moteur de l'IA doit avoir un accès permanent à des données de référence (sous la forme de détails des transactions, de profils d'utilisateurs, d'informations géospatiales, de métadonnées des appareils, etc.) qui lui indiquent à quoi ressemble une activité frauduleuse.

> " De nombreux services existants de détection des fraudes en ligne ne peuvent pas traiter les données assez rapidement pour identifier ces transactions au moment où elles se produisent. "

Toutefois, plus les données sont éloignées (en termes d'Internet) du moteur de l'IA, plus le processus est long. Les différences en termes humains sont infimes, mais les criminels peuvent lancer des milliers d'attaques par seconde. Le stockage des données d'inférence aussi près que possible des systèmes servant les modèles d'IA pour la cotation des transactions élimine une quantité importante de frais généraux en matière de calculs et de réseau, ce qui donne aux plateformes de cotation des transactions une meilleure chance de suivre le rythme.

Pour ceux qui construisent des systèmes de cotation des transactions basés sur l'IA, **RedisAI** offre la possibilité de servir des modèles d'apprentissage profond directement sur les données stockées dans Redis Enterprise, plutôt que de s'appuyer sur un serveur de modèles qui doit interroger un magasin de données distinct. La conservation des données localement dans Redis Enterprise et l'utilisation de RedisAI comme serveur de modèles permettent non seulement d'améliorer la cotation des transactions, mais aussi de simplifier l'architecture de production.

Les applications peuvent également utiliser les filtres Bloom pour vérifier si un élément est présent ou non dans un ensemble donné d'éléments. Par exemple, il est possible d'utiliser un filtre Bloom pour déterminer si un identifiant de transaction donné est présent dans une liste de modèles frauduleux connus, ou pour suivre les mots de passe des clients et empêcher la réutilisation d'anciens mots de passe. **RedisBloom** prend en charge les filtres Bloom qui permettent aux utilisateurs d'interroger efficacement les données afin de déterminer l'appartenance à un ensemble dans Redis sans stocker directement des informations sensibles. Cela peut aider les plateformes de détection des fraudes à filtrer de gros volumes de transactions en temps réel, sans compromettre les informations relatives aux clients. L'accélération des transactions rend l'automatisation indispensable. Il est impossible d'éliminer complètement la fraude, mais l'IA et le ML permettent aux sociétés de services financiers de construire la meilleure défense possible.

Offrez un service de détection des fraudes en temps réel grâce à Redis Enterprise

ENTREES

Informations sur les transactions

Biométrie comportementale

Identité du client

ENREGISTRER

RedisStreams

Acquérez et analysez de grandes quantités de transactions en temps réel.

ACCEDER

Redis Enterprise

Créez une identité numérique du client et mettez-la à jour de manière dynamique.

FILTRER

RedisBloom

Les filtres Bloom sont interrogés pour savoir si une transaction particulière est présente dans une liste de modèles frauduleux connus.

COTER

RedisAI

Exploitez le service d'IA et le traitement des données sans serveur aux fins d'améliorer la vitesse et la précision de la détection.

RESULTAT

Cotation des transactions en temps réel

Validation de l'identité numérique

Détection des anomalies

Know Your Customer (Connaître son client)

À la mi-2014, un homme nommé Rojo Filho a ouvert au moins 17 comptes bancaires à son nom et, selon les procureurs, il les a utilisés pour mettre en place un système d'investissement frauduleux. Filho avait déjà été condamné pour fraude avant d'ouvrir l'un de ces comptes et il aurait dû être détecté par les règles KYC, conçues pour limiter le blanchiment d'argent, la fraude, la corruption et le financement d'organisations illégales. Son cas illustre la facilité avec laquelle même un criminel condamné peut passer entre les mailles du filet.

Les banques sont tenues de respecter la réglementation KYC depuis un certain temps. Elles sont essentielles à la prévention de la fraude et au maintien de la confiance des clients. Cependant, beaucoup s'appuient encore sur l'authentification basée sur la connaissance (KBA), qui utilise des attributs comme les noms, les adresses, les numéros de sécurité sociale et les questions de sécurité pour vérifier l'identité d'une personne. Ces dites « informations statiques » sont relativement peu souvent mises à jour et sont vulnérables aux violations et aux vols de données.

C'est pourquoi les banques se tournent vers des moyens de plus en plus sophistiqués pour vérifier l'identité, en combinant ces données avec les informations existantes sur les clients. Par exemple, la vérification de documents et les enregistrements de visages ou d'empreintes digitales peuvent être combinés avec des modèles comportementaux, comme les types de transactions qu'un client effectue le plus fréquemment ou la façon dont il tape sur un téléphone à écran tactile. En combinant les informations traditionnelles sur les clients avec des sources de données alternatives, les institutions financières peuvent créer une identité numérique pour leurs clients qui est non seulement plus difficile à falsifier, mais qui peut être mise à jour de manière dynamique.

Avec les multiples sources et types de données qui composent une identité numérique, le défi consiste à tout mettre à jour assez rapidement afin de devancer les criminels et éviter de frustrer les clients. Plus l'identité numérique d'un client pourra être mise à jour rapidement, plus elle sera efficace.

" Avec les multiples sources et types de données qui composent une identité numérique, le défi consiste à tout mettre à jour assez rapidement afin de devancer les criminels et éviter de frustrer les clients. "

Malheureusement, si l'identité numérique est devenue plus sophistiquée, il en va de même pour la capacité des criminels à la voler ou à la falsifier. L'usurpation d'identité synthétique, où des informations réelles sont combinées à de fausses informations aux fins de créer une nouvelle identité, était à l'origine de 20 % des pertes de crédit des prêteurs américains en 2016. Elle a été décrite comme le type de criminalité financière à la croissance la plus rapide aux États-Unis. Le mélange de plusieurs éléments d'informations réelles sur le client dans des identités totalement nouvelles donne lieu à des fraudes pratiquement impossibles à détecter à l'aide des techniques KYC traditionnelles. Étant donné qu'il n'existe pas de consommateur réel pour signaler une activité frauduleuse, les fraudeurs peuvent gérer des comptes de carte de crédit et de prêt en toute légalité pendant suffisamment longtemps pour paraître légitimes et améliorer leur réputation de solvabilité, puis épuiser la ligne de crédit et disparaître.

Les bases de données graphiques sont particulièrement utiles pour lutter contre l'usurpation d'identité synthétique et améliorer les procédures KYC. La représentation et le stockage des données sous la forme d'une série de nœuds et d'arêtes qui modélisent les relations entre les points de données peuvent être plus rapides et plus souples que les bases de données traditionnelles pour certains types de requêtes, notamment l'identification des transactions suspectes. Les bases de données graphiques sont fondées sur les relations entre les entités, ce qui les rend très utiles pour découvrir des modèles suspects ou des connexions entre des entités suspectes.

Redis Enterprise offre un certain nombre d'options aux institutions financières qui cherchent à renforcer leurs procédures KYC et à lutter contre la fraude d'identité sophistiquée. Tout d'abord, il peut agir comme une base de données en mémoire rapide pour offrir la faible latence et le débit d'écriture élevé nécessaires à la mise à jour des identités numériques en temps réel. BioCatch, une société israélienne qui fournit une technologie de biométrie comportementale utilisée pour protéger les ouvertures de compte et prévenir l'usurpation d'identité, utilise Redis Enterprise comme base de données traitant une variété d'informations essentielles pour l'entreprise, notamment les données comportementales capturées pendant les sessions d'utilisateurs actifs, les profils prédéterminés sur les comportements frauduleux, les données de géolocalisation et les configurations du système.

Pour prendre en charge des formes plus sophistiquées de vérification d'identité, comme la reconnaissance faciale, RedisAI permet aux modèles d'intelligence artificielle d'être servis directement aux données stockées dans Redis Enterprise, éliminant ainsi les frais de calcul et de mise en réseau liés à l'interrogation des données de référence stockées dans un emplacement distinct ou à leur translation entre les systèmes. En outre, **RedisGraph** permet le traitement des graphiques en temps réel dans Redis Enterprise jusqu'à 600 fois plus vite que d'autres bases de données graphiques.

L'utilisation d'outils multiples offre aux sociétés de services financiers leur meilleure chance d'identifier correctement les clients. Bien que l'identification des acteurs frauduleux soit un problème difficile, les entreprises qui y parviendront de la manière la plus efficace réduiront le nombre de transactions frauduleuses qu'elles traitent, soulageant ainsi d'autres aspects de leurs activités.

RedisAI permet de servir des modèles d'intelligence artificielle directement aux données stockées dans Redis Enterprise.

RedisGraph permet le traitement des graphiques en temps réel dans Redis Enterprise jusqu'à 600 fois plus vite que d'autres bases de données graphiques.

RedisBloom prend en charge les filtres Bloom qui permettent aux utilisateurs d'interroger efficacement les données afin de déterminer l'appartenance à un ensemble dans Redis sans stocker directement des informations sensibles.

Lutte contre le blanchiment d'argent

La lutte contre le blanchiment d'argent est une exigence réglementaire pour les institutions financières et les sanctions en cas de non-respect sont sévères. Les régulateurs américains ont traditionnellement adopté une position dure, mais, en 2019, les autorités européennes ont prononcé des sanctions pénales dépassant celles infligées par les États-Unis. Il est estimé que pas moins de 5 % du PIB mondial, soit jusqu'à 2 000 milliards de dollars, sont blanchis chaque année dans le monde.

Le défi pour les institutions consiste à identifier le bénéficiaire effectif ultime (la personne qui contrôle ou bénéficie réellement d'une transaction) et son activité, tout en surveillant le comportement des clients pour identifier les activités suspectes. En outre, les entreprises doivent gérer des bases de données et des systèmes disparates et faire face à un niveau élevé de faux positifs dans la détection des transactions illicites : plus de 95 % selon certaines estimations.

Certaines banques adoptent des approches de plus en plus sophistiquées pour identifier les activités suspectes, en fonction des profils de risque des entreprises, par exemple en créant ou en renforçant des cellules internes de renseignement financier chargées d'identifier les menaces financières illicites plus complexes et stratégiques. Les banques étudient également la manière dont l'intelligence artificielle et les technologies d'identité numérique peuvent être appliquées aux programmes de conformité en matière de lutte contre le blanchiment d'argent. Ces innovations peuvent renforcer les approches de conformité à la législation anti-blanchiment et améliorer les systèmes de surveillance des transactions.

La segmentation de la clientèle et l'évaluation du risque sont souvent utilisées pour lutter contre le blanchiment d'argent, mais elles peuvent souvent être inexactes. Les entreprises cherchent donc de nouveaux moyens de réduire les faux positifs et négatifs. L'analyse de réseau peut aider à trouver des liens cachés entre les entités qui pourraient être manqués par les modèles traditionnels, et la cotation des transactions devient plus intelligente grâce à la technologie de l'IA.

Un système de surveillance des transactions en temps réel est la pierre angulaire d'un programme efficace de conformité à la législation anti-blanchiment. Une solution de lutte contre le blanchiment d'argent doit être capable de coter les transactions par cartes de crédit, de débit, de guichet automatique et prépayées (notamment les portefeuilles numériques) pour les paiements avec ou sans présence de la carte, ainsi que les transactions par chambre de compensation automatisée (ACH), les virements électroniques et les transactions pair-à-pair. Comme pour les autres cas d'utilisation de la lutte contre la fraude, le traitement rapide et précis de grandes quantités d'informations représente un défi majeur. C'est là qu'une base de données en mémoire rapide, comme Redis Enterprise, peut vous aider.

Toutefois, il peut être difficile pour une entreprise de s'attaquer seule au problème mondial du blanchiment d'argent, quelle que soit la technologie disponible. Mais si de nouvelles solutions de lutte contre le blanchiment d'argent sont développées, les entreprises de services financiers pourraient bénéficier d'une plus grande collaboration pour les aider à identifier et à prévenir le problème.

> " Il est estimé que pas moins de 5 % du PIB mondial, soit jusqu'à **2 000 milliards de dollars, sont blanchis chaque année dans le monde** "

Lutter contre la fraude tout en gardant les clients satisfaits

Les institutions financières doivent constamment trouver un équilibre entre la nécessité de détecter la fraude et la cybercriminalité et celle de garantir aux clients légitimes un service rapide et efficace. La capacité de traiter rapidement les données et d'identifier des modèles est essentielle pour lutter contre tous les types de fraude décrits dans ce livre blanc.

Redis Enterprise fournit aux plateformes de détection des fraudes l'accès en temps réel aux données dont les institutions financières ont besoin pour examiner rapidement les modèles des transactions, renforcer leurs programmes KYC grâce à de nouveaux outils d'identité numérique et lutter contre la lutte contre le blanchiment d'argent et d'autres formes plus sophistiquées de criminalité financière. Un partenariat avec Redis peut permettre à votre entreprise de se concentrer sur l'innovation rapide, plutôt que sur le travail routinier.

Le défi de la fraude financière continuera à persister alors que de plus en plus d'opérations bancaires se déroulent dans le monde numérique, mais les entreprises qui gèrent le mieux leur réponse aujourd'hui obtiendront un avantage concurrentiel immédiat et se prépareront à développer des systèmes de détection de la fraude encore plus robustes à l'avenir.

> "Redis Enterprise fournit aux plateformes de détection des fraudes l'accès en temps réel aux données dont les institutions ont besoin pour lutter contre la criminalité financière."

Pour en savoir plus sur la façon dont les entreprises alimentent les plateformes de détection des fraudes avec Redis Enterprise, consultez notre page **Redis Enterprise pour la détection des fraudes**.

Pour commencer, essayez Redis Enterprise dans le Cloud, ou téléchargez le logiciel Redis Enterprise pour un essai gratuit dès maintenant.

redis.com/try-free

À propos de Redis

Les entreprises modernes dépendent de la puissance des données en temps réel. Grâce à Redis, les entreprises peuvent offrir des expériences instantanées de manière hautement fiable et évolutive.

Redis est le berceau de Redis, la base de données en mémoire la plus populaire au monde et le fournisseur commercial de Redis Enterprise, qui offre des performances supérieures, une fiabilité incomparable et une flexibilité inégalée pour la personnalisation, l'apprentissage automatique, l'IdO, la recherche, le commerce électronique, les réseaux sociaux et des solutions de mesure dans le monde entier.

Redis, régulièrement classé comme un leader dans les principaux rapports d'analystes sur NoSQL, les bases de données en mémoire, les bases de données opérationnelles et la base de données en tant que service (DBaaS), est approuvé par plus de 7 400 entreprises clientes, dont cinq sociétés du Fortune 10, trois des quatre émetteurs de cartes de crédit, trois des cinq premières sociétés de communication, trois des cinq premières sociétés de soins de santé, six des huit premières sociétés technologiques et quatre des sept premiers détaillants.

Redis Enterprise, disponible en tant que service dans les clouds publics et privés, en tant que logiciel téléchargeable, dans des conteneurs et pour les déploiements hybrides cloud/sur site, fournit les cas d'utilisation populaires de Redis tels que les transactions à grande vitesse, la gestion des tâches et des files d'attente, les magasins de sessions utilisateur, l'acquisition de données en temps réel, les notifications, la mise en cache de contenu et les données de séries chronologiques.

redis.com