(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 048 840***

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **16 52007**

(51) Int Cl[8] : ***H 04 L 29/02*** *(2017.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 10.03.16.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 15.09.17 Bulletin 17/37.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *Amadeus S.A.S.* — FR.

(72) **Inventeur(s) :** FLORIMOND CEDRIC, ANDREVON THIBAUD, LE MARIER MATHIEU et EL KAOUI HANANE.

(73) **Titulaire(s) :** Amadeus S.A.S..

(74) **Mandataire(s) :** SAMSON & PARTNER PATENTANWALTE MBB.

(54) SYSTEME DE CONTROLE DE BASES DE DONNEES.

(57) Les systèmes, les procédés et les produits de programme informatique pour surveiller une première base de données. Un système de contrôle de bases de données reçoit des données indiquant des évènements de changement lié aux enregistrements dans la première base de données et stocke les évènements dans une seconde base de données. De plus, le système de contrôle de bases de données identifie les enregistrements associés aux transactions frauduleuses et définit un ensemble d'entraînement qui inclut les transactions frauduleuses. Un réseau neuronal est entraîné pour détecter des modèles d'évènements indiquant une fraude à l'aide de l'ensemble d'entraînement et des évènements correspondants stockés dans la seconde base de données. En réponse au réseau neuronal entraîné détectant un modèle d'évènements frauduleux associé à un enregistrement de base de données active, le système de contrôle de bases de données analyse la transaction sous-jacente pour déterminer si la transaction est frauduleuse. Un affichage graphique peut être généré sur la base des données extraites du réseau neuronal et peut représenter un ou plusieurs sommets correspondant aux évènements associés aux transactions frauduleuses.

FR 3 048 840 - A1

SYSTÈME DE CONTRÔLE DE BASES DE DONNÉES

CONTEXTE

[0001] De façon générale, la présente invention concerne les ordinateurs et les systèmes informatiques et, notamment les systèmes, les procédés et les produits de programmes informatiques qui détectent une manipulation frauduleuse des enregistrements de données.

[0002] Les paiements des produits de voyage sont typiquement perçus avant la date prévue d'utilisation des produits. Ces paiements sont souvent faits en facturant le coût des produits de voyage achetés sur un compte de carte de crédit fourni par le voyageur, le vendeur agissant comme le marchand. Les transactions par carte de crédit comprennent typiquement un processus d'autorisation et de règlement en deux étapes. Au moment de la transaction, les informations afférentes telles que le montant de l'achat, l'identité du marchand, le numéro de compte de carte de crédit et la date d'expiration sont transmises du marchand vers une banque émettrice. La banque émettrice peut ensuite contrôler le compte pour vérifier que la carte de crédit est valable et que la limite de crédit est suffisante pour autoriser la transaction. Si la banque approuve la transaction, le marchand termine la transaction et émet un billet pour le voyageur. Pour recevoir le paiement, le marchand peut envoyer une série d'autorisations approuvées à une « banque acquéreuse » à la fin d'un jour ouvré. La banque acquéreuse peut ensuite rapprocher et transmettre les autorisations aux banques émettrices, typiquement via un réseau de cartes ou un centre d'échange d'informations et déposer les fonds sur le compte du marchand. Les fonds sont ensuite transférés de la banque émettrice à la banque acquéreuse, et une facture envoyée au titulaire de la carte par la banque émettrice.

[0003] Malheureusement, les cartes de crédit sont souvent utilisées pour l'achat frauduleux de billets d'avion par des escrocs qui utilisent des cartes de crédit obtenues irrégulièrement ou volées pour faire des achats non autorisés. Quand le véritable titulaire de la carte de crédit remarque l'achat non autorisé, il peut contester les frais auprès de la banque émettrice. Cela donne typiquement lieu à un « rejet de débit » délivré au marchand pour le coût de la transaction. Les rejets de débit peuvent être reçus jusqu'à plusieurs moins après la survenue de la transaction, période pendant laquelle les produits de voyage ont normalement été utilisés. Les transactions frauduleuses de carte de crédit nuisent ainsi fortement aux marchands et aux fournisseurs de produits de voyage qui ne peuvent en général pas recouvrer les coûts de produits de voyage.

[0004] Par conséquent, des systèmes, des procédés et des produits de programmes informatiques améliorés d'analyse des opérations pour détecter la fraude sont nécessaires afin de réduire l'incidence des frais frauduleux et réduire les pertes subies par les marchands et les fournisseurs de produits de voyage en raison des achats frauduleux de produits de voyage.

RÉSUMÉ

[0005] Dans un mode de réalisation de l'invention, un système est fourni ; il inclut un ou plusieurs processeurs et une mémoire couplée au processeur. La mémoire inclut un code de programme qui, lorsqu'il est exécuté par un ou plusieurs processeurs, amène le système à détecter un changement dans un enregistrement de voyage après qu'un itinéraire défini dans l'enregistrement de voyage a été réservé et, en réponse à la détection du changement, il détermine un modèle de changements apportés à l'enregistrement de voyage. De plus, le code du programme amène le système à déterminer si le modèle correspond à un modèle potentiellement frauduleux et, en réponse au modèle correspondant à un modèle potentiellement frauduleux, il signale l'enregistrement de voyage comme potentiellement frauduleux.

[0006] Dans un autre mode de réalisation de l'invention, un procédé est fourni. Le procédé inclut la détection du changement dans l'enregistrement de voyage après que l'itinéraire défini dans l'enregistrement de voyage a été réservé et, en réponse à la détection du changement, la détermination du modèle de changements apportés à l'enregistrement de voyage. De plus, le procédé inclut le fait de déterminer si le modèle correspond au modèle potentiellement frauduleux et, en réponse au modèle correspondant au modèle potentiellement frauduleux, la signalisation de l'enregistrement de voyage comme potentiellement frauduleux.

[0007] Dans un autre mode de réalisation de l'invention, un programme informatique est fourni ; il inclut un support de stockage, lisible par ordinateur, non transitoire incluant le code de programme. Le code de programme est configuré, lorsqu'il est exécuté par un ou plusieurs processeurs, pour amener un ou plusieurs processeurs à détecter le changement dans l'enregistrement de voyage après que l'itinéraire défini dans l'enregistrement de voyage a été réservé et, en réponse à la détection du changement, pour déterminer le modèle de changements apportés à l'enregistrement de voyage. De plus, le code de programme permet à un ou plusieurs processeurs de déterminer si le modèle correspond au modèle potentiellement frauduleux et, en réponse au modèle correspondant au modèle frauduleux, signaler l'enregistrement de voyage comme potentiellement frauduleux.

BRÈVE DESCRIPTION DES DESSINS

[0008] Les dessins annexés qui sont inclus dans et font partie de cette spécification, illustrent divers modes de réalisation de l'invention et, avec la description générale de l'invention ci-dessus et la description détaillée des modes de réalisation données ci-dessous, ils servent à expliquer les modes de réalisation de l'invention.

[0009] La FIG. 1 est une vue schématique d'un exemple d'environnement d'exploitation pour un système de contrôle de bases de données, l'environnement d'exploitation incluant une pluralité de systèmes informatiques qui communiquent via un réseau.

[0010] La FIG. 2 est une vue schématique d'un exemple de système informatique de la FIG. 1.

[0011] La FIG. 3 est une vue schématique d'un système de contrôle de bases de données de la FIG. 1 montrant un moteur de contrôle de bases de données.

[0012] La FIG. 4 est une vue graphique illustrant un réseau neuronal qui peut être utilisé par le moteur de contrôle de bases de données de la FIG. 3 pour détecter les modèles de modification de bases de données indiquant une fraude.

[0013] La FIG. 5 est une vue graphique d'une version simplifiée du réseau neuronal de la FIG. 4.

[0014] La FIG. 6 est une vue graphique illustrant une amélioration de la capacité du réseau neuronal des FIG. 3 ou 4 à détecter les modèles dans un échantillon d'entraînement.

[0015] La FIG. 7 est une vue graphique illustrant un effet des règles d'agrégation sur la probabilité qu'une opération soit frauduleuse.

[0016] La FIG. 8 est une vue graphique d'une interface utilisateur graphique qui utilise une pluralité de sommets reliés par des bords pour communiquer les modèles de fraude à un utilisateur du système.

DESCRIPTION DÉTAILLÉE

[0017] Les modes de réalisation de l'invention concernent des systèmes, des procédés et des produits de programme informatique qui déterminent si une transaction précédemment effectuée pour un produit est frauduleuse ou non. Cette détermination peut impliquer l'identification d'un modèle de changements après l'achat sur un ou plusieurs enregistrements de bases de données indiquant une fraude. Les modes de réalisation de l'invention peuvent être mis en œuvre par un système de contrôle de bases de données comprenant un ou plusieurs ordinateur(s) ou serveur(s)

en réseau. Les ordinateurs en réseau peuvent inclure un Système mondial de distribution (GDS) et peuvent fournir des fonctions de traitement et de base de données pour les systèmes et modules liés au voyage qui analysent les enregistrements de base de données pour identifier des transactions qui peuvent être frauduleuses. Les enregistrements de base de données peuvent inclure, par exemple, des enregistrements de voyage tels que des enregistrements de noms de passagers (PNR), des enregistrements de paiement, des titres de transport et/ou des profils clients. Si le système de contrôle de bases de données détecte une activité de réservation post-réservation suspicieuse, le système peut signaler la transaction comme étant potentiellement frauduleuse, demander une détection anti-fraude supplémentaire et/ou annuler la réservation.

[0018] Nous faisons maintenant référence à la FIG. 1, un environnement d'exploitation 10 conformément à un mode de réalisation de l'invention peut comprendre un Système mondial de distribution (GDS) 12, un système de réservation 14, un système vendeur 16, un système de paiement 18, un système de contrôle de bases de données 20, un système de détection anti-fraude 22 et une base de données d'enregistrements de voyages 24. Le GDS 12, le système de réservation 14, le système vendeur 16, le système de paiement 18, le système de contrôle de bases de données 20, le système de détection anti-fraude 22 et la base de données d'enregistrements de voyages 24 peuvent communiquer via un réseau 26. Le système de réservation 14 peut inclure un Système de réservation par ordinateur (CRS) qui permet au GDS 12 ou au système vendeur 16 de réserver et de payer des billets d'avion. Le système de réservation 14 peut également interagir avec d'autres systèmes de réservation (non présentés), soit directement, soit via le GDS 12 pour permettre à un transporteur officiel de vendre des billets pour des sièges fournis par un transporteur effectif. Le transporteur effectif peut ensuite facturer les produits fournis au transporteur officiel. La facturation entre les vendeurs et les fournisseurs de produits de voyage peut être fournie ou autrement facilitée par le système de paiement 18. Le réseau 26 peut inclure un ou plusieurs réseaux privés ou publics (par ex. Internet) qui permet l'échange de données entre les systèmes.

[0019] Le GDS 12 peut être configuré pour faciliter la communication entre le système de réservation 14 et le système vendeur 16 par des agents de voyage habilités, des transporteurs officiels ou d'autres vendeurs afin de faire des réservations sur le système de réservation 14 via le GDS 12. Le GDS 12 peut conserver des liens avec plusieurs systèmes de réservation via le réseau 26 qui permet au GDS 12 d'acheminer les demandes de réservation du système vendeur

16 au fournisseur correspondant du produit de voyage réservé. Le système vendeur 16 peut ainsi réserver des produits de voyage auprès de nombreux fournisseurs de produits via une seule connexion au GDS 12.

[0020] Le système de paiement 18 peut être configuré pour traiter les moyens de paiement liés à l'achat de produits par le client. Le système de paiement 18 peut être configuré pour échanger des données avec un ou plusieurs systèmes bancaires (non présentés), tels qu'un système bancaire émetteur et/ou un système bancaire acquéreur pour autoriser le paiement et le transfert de fonds entre des comptes. En cas d'achat payé au moins en partie par carte de crédit ou de débit, au moment de la transaction, le système de paiement 18 peut transmettre une demande d'autorisation au système bancaire émetteur qui peut être déterminé à partir du numéro d'identification de l'émetteur de la carte. En réponse à la réception d'une demande d'autorisation, le système bancaire émetteur peut vérifier que le compte est valable et que le compte dispose de fonds suffisants pour couvrir le montant de la transaction.

[0021] Le système bancaire émetteur peut ensuite transmettre une réponse d'autorisation au système de paiement 18 indiquant que la transaction a été approuvée, rejetée ou que de plus amples informations sont requises. Si de plus amples informations sont requises, le système de paiement 18 demande au système de détection anti-fraude 22 de réaliser un contrôle de sécurité sur le mode de paiement. Une fois que la transaction est terminée, le système vendeur 16 peut transmettre les données caractérisant la transaction au système bancaire acquéreur. Ces données peuvent être transmises comme faisant partie d'un fichier séquentiel à la fin d'une période, comme la fin d'un jour ouvré. Le système bancaire acquéreur peut ensuite déposer les fonds sur un compte du vendeur, et recouvrer les fonds de la banque correspondante, émettrice des cartes de crédit utilisées pour acheter les produits de voyage.

[0022] Le système de détection anti-fraude 22 peut être exploité par un prestataire de services d'authentification qui fournit une détection prédictive anti-fraude. La détection prédictive anti-fraude peut utiliser un ou plusieurs modèles prédictifs pour détecter la fraude au moment de la vente en appliquant les modèles prédictifs aux informations de la transaction. Les informations de la transaction peuvent être transmises au système de détection anti-fraude par le système vendeur 16 et/ou le système de paiement 18, qui peut ensuite attendre une réponse du système de détection anti-fraude 22 avant de terminer la transaction. Dans certains cas, le système de détection anti-fraude 22 peut être exploité par la banque émettrice pour le moyen de

paiement utilisé pour acheter le produit de voyage ou par un prestataire de service sous contrat avec la banque émettrice.

[0023] La base de données d'enregistrements de voyages 24 peut être fournie par un système autonome, le GDS 12 ou le système de réservation 14. La base de données d'enregistrements de voyage 24 peut comprendre une base de données d'enregistrements de voyages, tels que des enregistrements de noms de passagers (PNR). Chaque enregistrement de voyage peut inclure un ou plusieurs enregistrements de réservation qui contiennent l'itinéraire et les informations sur le voyageur associé à un ou plusieurs produits réservés. Un ou plusieurs enregistrements de réservation peuvent inclure des données définissant l'itinéraire d'un voyage en particulier, le passager ou le groupe de passagers. L'itinéraire défini peut inclure des produits de voyage provenant de nombreux fournisseurs de produits de voyage, tels que les transporteurs aériens, les hôtels, les agences de location de véhicules ou tout autre fournisseur de produits de voyage. Pour faciliter la localisation des enregistrements de voyage dans la base de données d'enregistrements de voyages 24, un localisateur d'enregistrements ou un autre identificateur approprié peut être associé à chaque enregistrement de voyage.

[0024] Nous faisons maintenant référence à la FIG. 2, le GDS 12, le système de réservation 14, le système vendeur 16, le système de paiement 18, le système de contrôle de bases de données 20, le système de détection anti-fraude 22, la base de données d'enregistrements de voyages 24 et le réseau 26 de l'environnement d'exploitation 10 peuvent être mis en œuvre sur un ou plusieurs dispositifs ou systèmes informatiques, tels que l'exemple d'ordinateur 30. L'ordinateur 30 peut inclure un processeur 32, une mémoire 34, un dispositif de stockage de mémoire de masse, une interface d'entrée/sortie (I/O) 38 et une Interface homme machine (HMI) 40. L'ordinateur 30 peut également être couplé de manière fonctionnelle à une ou plusieurs ressources externes 42 via le réseau 26 ou l'interface I/O 38. Les ressources externes peuvent inclure mais sans s'y limiter, des serveurs, des bases de données, des dispositifs de stockage de masse, des dispositifs périphériques, des services de réseau en nuage ou toute autre ressource informatique appropriée qui peut être utilisée par l'ordinateur 30.

[0025] Le processeur 32 peut inclure un ou plusieurs dispositifs sélectionnés parmi des microprocesseurs, des microcontrôleurs, des processeurs de signaux numériques, des microordinateurs, des unités centrales de traitement, des réseaux de portes programmables par l'utilisateur , des dispositifs logiques programmables, des machines à états, des circuits logiques,

des circuits analogiques, des circuits numériques ou tout autre dispositif qui manipule des signaux (analogiques ou numériques) basés sur des instructions opérationnelles qui sont stockées en mémoire 34. La mémoire 34 peut comprendre un dispositif de mémoire unique ou pluralité de dispositifs de mémoire, notamment mais sans s'y limiter, une mémoire morte (ROM), une mémoire vive (RAM), une mémoire volatile, une mémoire non volatile, une mémoire vive statique (SRAM), une mémoire vive dynamique (DRAM), une mémoire flash, une mémoire cache ou tout autre dispositif capable de stocker des données. Le dispositif de mémoire de stockage de masse 36 peut inclure des dispositifs de stockage de données tels qu'un disque dure, un lecteur optique, un lecteur de bande, un dispositif volatile ou non volatile à semi-conducteur ou tout autre dispositif capable de stocker des données.

[0026] Le processeur 32 peut fonctionner sous le contrôle d'un système d'exploitation 44 qui réside dans la mémoire 34. Le système d'exploitation 44 peut gérer les ressources informatiques, de sorte que le code de programme informatique se présentant sous forme d'une ou plusieurs applications logicielles informatiques, telles que l'application 46 résidant dans la mémoire 34, peut avoir des instructions exécutées par le processeur 32. Le processeur 32 peut également exécuter l'application 45 directement, auquel cas le système d'exploitation 44 peut être omis. Une ou plusieurs applications logicielles informatiques peuvent inclure un exemple en fonctionnement d'une application comprenant un serveur, qui peut accepter des demandes de et fournir des réponses à, une ou plusieurs applications clients correspondantes. Une ou plusieurs structures de données 48 peuvent également résider dans la mémoire 34 et peuvent être utilisées par le processeur 32, le système d'exploitation 44 et/ou l'application 46 pour stocker et/ou manipuler des données.

[0027] L'interface I/O 38 peut fournir une interface machine qui couple de manière opérationnelle le processeur 32 à d'autres dispositifs et systèmes, tels que le réseau 26 ou la ressource externe 42. L'application 46 peut ainsi fonctionner en coopération avec le réseau 26 ou la ressource externe 42 en communiquant via l'interface I/O 38 pour fournir les différentes fonctionnalités, fonctions, applications, processus ou modules comprenant les modes de réalisation de l'invention. L'application 46 peut également avoir un code de programme qui est exécuté par une ou plusieurs ressources 42 ou qui s'appuie autrement sur les fonctions ou signaux fournis par d'autres composants système ou réseau externe à l'ordinateur 30. En effet, étant donné les configurations matérielles et logicielles possibles presque sans fin, il faut

comprendre que les modes de réalisation de l'invention peuvent inclure des applications qui sont situées à l'extérieur de l'ordinateur 30, réparties entre de multiples ordinateurs ou d'autres ressources externes 42 ou fournies par des ressources informatiques (matérielles et logicielles) qui sont fournies comme un service sur le réseau 26, comme un service informatique en nuage.

[0028] La HMI 40 peut être couplée de manière fonctionnelle au processeur 32 de l'ordinateur 30 pour permettre à un utilisateur d'interagir directement avec l'ordinateur 30. La HMI 40 peut inclure des écrans vidéo ou alphanumériques, un écran tactile, un haut-parleur et/ou tout autre indicateur audio et visuel approprié capable de fournir les données à l'utilisateur. La HMI 40 peut également inclure des dispositifs d'entrée et des contrôles tel qu'un clavier alphanumérique, un dispositif de pointage, des claviers, des boutons, des boutons de commande, des microphones, etc., capables d'accepter des instructions ou une entrée de l'utilisateur et de transmettre l'entrée effectuée au processeur 32.

[0029] Une base de données 50 peut résider dans le dispositif de stockage de mémoire de masse 36 et peut être utilisé pour collecter et organiser les données utilisées par les différents systèmes et modules décrits dans les présentes. La base de données 50 peut inclure des données et des structures de données de support qui stockent et organisent les données. La base de données 50 peut notamment être agencée avec toute organisation ou structure de base de données y compris mais sans s'y limiter une base de données relationnelle, une base de données hiérarchique, une base de données de réseau, une base de données orientée objet ou des combinaisons de celles-ci.

[0030] Un système de gestion de bases de données sous la forme d'une application logicielle informatique qui exécute les instructions sur le processeur 32 peut être utilisé pour accéder aux données stockées dans les enregistrements de la base de données 50 en réponse à une demande. La demande peut être déterminée dynamiquement et exécutée par le système d'exploitation 44, d'autres applications 46 ou un ou plusieurs modules. Bien que les modes de réalisation de l'invention puissent être décrits dans les présentes en utilisant une terminologie de base de données relationnelle, hiérarchique, de réseau, orientée objet ou autre dans des cas spécifiques, il faut comprendre que les modes de réalisation de l'invention peuvent utiliser tout modèle de gestion de bases de données approprié et ne sont pas limités à un type de base de données en particulier.

[0031] Le système de détection anti-fraude 22 peut tenter de prévenir la fraude liée au paiement en évaluant le risque de fraude au moment du paiement et rejeter la carte si le risque de fraude est trop élevé. Cependant, même en détectant la fraude avant la vente, le taux de fraude peut être supérieur à zéro et peut être typiquement de 10 % ou plus. Afin de contourner le système de détection anti-fraude 22, les fraudeurs peuvent créer un contexte d'achat qui manque d'indicateurs de fraude au moment du paiement. Le fraudeur peut ensuite modifier la réservation ultérieurement pour commettre la fraude, par exemple en réservant un nouveau vol moins cher et en empochant la différence. Un fraudeur peut réaliser ce type de fraude en achetant un billet d'avion avec une carte de crédit volée et en demandant un remboursement plus tard sur une carte de crédit appartenant au fraudeur. Dans ce cas, la transaction peut empêcher la détection par le système de détection anti-fraude 22 basé sur l'utilisation de la carte du fraudeur, étant donné que les détections anti-fraude ne sont typiquement pas réalisées sur le remboursement d'un billet.

[0032] Une autre manière pour un fraudeur d'éviter la détection par le système de détection anti-fraude 22 est d'avoir émis le billet du vol au nom du titulaire de la carte volée au moment de la réservation. Les systèmes de détection anti-fraude avant achat qui traitent les noms des titulaires de cartes et de passagers qui ne correspondent pas comme un indicateur de fraude éventuelle peuvent ainsi être dupés en autorisant la transaction. Une fois le paiement effectué avec la carte de crédit volée, le fraudeur peut modifier le nom sur le billet avec le nom de la personne qui utilisera en réalité le billet.

[0033] Les produits peuvent être disponibles dans différentes classes de service et certaines classes de services peuvent être sujettes à des règles de détection anti-fraude plus clémentes que pour d'autres classes de service. Pour tirer avantage de ces différences, les fraudeurs peuvent réserver un vol dans une classe de service, de sorte que le système de détection anti-fraude 22 applique les règles de détection les plus clémentes pour cette catégorie, puis, après acceptation du paiement, ils peuvent modifier la classe de service en une autre classe de service. Les règles de détection anti-fraude peuvent être plus clémentes pour certaines classes de service que pour d'autres parce que refuser la vente du billet représente un plus gros manque à gagner pour la classe où les règles sont plus clémentes. Par exemple, un fraudeur peut réserver un billet en classe affaires et une fois que le billet a été réservé, réserver à nouveau le billet en classe économique en échange du billet en classe affaires. Puisque le prix d'un billet en classe économique est normalement plus bas qu'un billet en classe affaire sur le même vol, les

paiements par carte de crédit peuvent ne pas être requis. Par conséquent, la détection anti-fraude ne sera typiquement pas appliquée à l'échange du billet en classe affaires pour un billet en classe économique.

[0034] Un autre procédé qui peut être utilisé pour éviter le signalement d'une transaction par le système de détection anti-fraude 22 est l'achat d'un billet utilisant un numéro de carte grand voyageur. Les règles de détection anti-fraude peuvent être plus clémentes avec les grands voyageurs, s'ils sont considérés comme étant plus fiables et/ou précieux que les clients réguliers par le transporteur. De plus, les prestataires tiers de détection anti-fraude ne peuvent typiquement pas vérifier si la carte d'un grand voyageur est valable ou si le nom sur la carte grand voyageur correspond au nom sur la carte de crédit. Le fraudeur peut acheter et payer le vol avec la carte de crédit volée, puis supprimer la carte de grand voyageur après que le paiement a été réalisé.

[0035] Nous faisons maintenant référence à la FIG. 3, le système de contrôle de bases de données 20 peut comprendre un moteur de contrôle de base de données 60, une base de données d'enregistrement des réservations 62, une base de données d'enregistrement des paiements 64, une base de données des fraudes 66, un moteur d'analyse a posteriori 68, un moteur d'apprentissage de machine 70 et une Interface de programmation d'application (API) 72. La base de données des fraudes 66 peut comprendre une base de données de modèles frauduleux connus. L'API 72 peut être, par exemple, une API Web qui permet aux utilisateurs d'accéder au système de contrôle de bases de données 20 à partir de systèmes externes, tels que le système vendeur 16 ou un autre système utilisateur, en utilisant une demande d'accès tel qu'un navigateur Web. Le moteur de contrôle de base de données 60 peut recevoir une alimentation d'enregistrements de réservations 74 du système de réservation 14 et une alimentation d'enregistrements de paiements d'un système de paiement 18. Dans un mode de réalisation de l'invention, un ou plusieurs système(s) de réservation 14, système(s) de paiement 18 et système(s) de contrôle de bases de données 20 peuvent être hébergés ou autrement fournis par le GDS 12.

[0036] Le moteur de contrôle de base de données 60 peut stocker les enregistrements de réservations reçus sur l'alimentation d'enregistrements de réservations 74 dans la base de données d'enregistrements de réservations 62 et les enregistrements de paiements reçus sur l'alimentation d'enregistrements de paiements 76 dans la base de données d'enregistrements de

paiements. La base de données d'enregistrements de réservations 62 et la base de données d'enregistrements de paiements 64 peuvent fournir des bases de données historiques des paiements et des évènements d'enregistrement de voyages qui peuvent être utilisés par le moteur de contrôle de base de données 60 pour prévoir la fraude.

[0037] Le moteur d'analyse a posteriori 68 peut gérer le moteur d'apprentissage de machine 70 qui peut comprendre, par exemple, un réseau neuronal. Le moteur d'apprentissage de machine 70 peut être configuré pour détecter automatiquement (c-à-d sans intervention humaine) un comportement présumé frauduleux fondé sur l'activité de réservation qui apparaît après réalisation du paiement. Le moteur d'analyse a posteriori 68 peut également fournir des modèles de comportement de réservation après paiement qui semblent être liés à une activité frauduleuse sous une forme lisible par l'homme sur l'API 72.

[0038] Le moteur d'apprentissage de machine 70 peut être configuré pour fonctionner dans un mode d'apprentissage ou un mode de détection. La détection de la fraude par le moteur d'apprentissage de machine 70 dans le mode de détection peut être réalisée par un cadre transversal commun. Ce cadre peut permettre à différents clients de définir différentes typologies de fraude pour différentes zones touchées. Le cadre peut également automatiquement identifier les enregistrements de voyage qui apparaissent comme frauduleux, en utilisant un algorithme d'apprentissage de machine, par ex. un algorithme d'entrainement du réseau neuronal. En plus des enregistrements de voyage, les typologies d'analyse de la fraude peuvent analyser d'autres types d'enregistrements, tels que les enregistrements de paiement et les profils utilisateurs, pour affiner encore la détection de modèles frauduleux.

[0039] Tandis que le moteur d'apprentissage de machine 70 est en mode apprentissage, le moteur d'analyse a posteriori 68 peut utiliser un apprentissage supervisé pour entraîner le moteur d'apprentissage de machine 70 en utilisant des enregistrements pour les transactions actuelles connues pour être frauduleuses. Les transactions frauduleuses connues peuvent faire partie d'un ensemble d'entraînement de transactions stockées dans la base de données des fraudes 66. Les transactions frauduleuses connues peuvent être identifiées, par exemple, en utilisant des rapports de rejets de débit produits par le système vendeur 16, le système de paiement 18 ou tout autre système approprié. Pour chaque opération déterminée comme frauduleuse, le moteur de contrôle de base de données 60 peut extraire un enregistrement de voyage connexe (par ex. PNR) de la base de données d'enregistrements de voyage 24 et l'historique de l'enregistrement de voyage de

la base de données d'enregistrements de réservations 62 et/ou de la base de données d'enregistrements de paiements 64. L'historique de l'enregistrement de voyage peut inclure un historique des évènements qui se sont produits pendant la vie de l'enregistrement de voyage, notamment la création de l'enregistrement de voyage, chaque changement suivant apporté à l'enregistrement de voyage et les dates auxquelles chaque évènement s'est produit.

[0040] Dans le cadre du processus d'entraînement, le moteur d'analyse a posteriori 68 peut filtrer l'historique des évènements pour générer un historique filtré des évènements. Ce filtrage peut exclure les évènements provenant de l'historique filtré des évènements considérés comme étant sans rapport avec la détection de fraude (c-à-d qui ne sont pas considérés comme utiles pour un fraudeur) tels que l'ajout d'une remarque sur l'enregistrement de voyage. L'historique filtré des évènements et les transactions frauduleuses associées peuvent être utilisés pour remplir un ensemble d'apprentissage utilisé pour entraîner le moteur d'apprentissage de machine 70. Le moteur d'apprentissage de machine 70 peut générer un arbre de décision de détection de fraude et optimiser l'arbre de décision en utilisant l'ensemble d'apprentissage. L'entraînement peut être réalisé à l'aide d'une analyse de l'arbre de décision, d'une analyse des forêts aléatoires ou d'une analyse de la concentration des modèles frauduleux connus. À titre d'exemple de l'utilisation de l'analyse de l'arbre de décision pour filtrer les évènements, le moteur d'analyse a posteriori 68 peut déterminer qu'en cas d'évènement de changement de nom suivi d'un évènement d'annulation de nom avant le paiement, seul l'évènement d'annulation de nom devrait être retenu.

[0041] La détection de la fraude basée sur la modification après-vente des enregistrements de voyage peut utiliser une classification globale des modèles frauduleux. Les alertes de comportements frauduleux peuvent ensuite varier en fonction du marché, la définition du marché variant en fonction des enregistrements analysés. Pour les enregistrements liés à la distribution de billets, les marchés peuvent se baser sur le bureau de vente ou le guichet. Pour les enregistrements générés par les systèmes porteurs, les marchés peuvent se baser sur le comptoir de vente de l'aéroport, le guichet en ville et/ou la présence de la compagnie aérienne dans le bureau. Le système de contrôle de bases de données 20 peut inclure différents niveaux de rapports sélectionnables, tels que les rapports périodiques, les rapports sur alerte, les rapports ascendants et/ou la diffusion descendante.

[0042] Les données de la transaction frauduleuse stockées dans la base de données des fraudes 66 peuvent être utilisées pour fournir la notation des canaux de vente. A cette fin, le moteur d'analyse a posteriori 68 peut calculer un score pour chaque canal de vente basé sur les Indicateurs de performance clés (KPI) des ventes et de la fraude. Le score des canaux de vente peut peser et regrouper des KPI sélectionnés pour déterminer un score pour chaque canal de vente dans une zone fonctionnelle donnée. Les canaux de vente peuvent passer dans une catégorie de score supérieure ou inférieure en fonction du résultat du calcul. Le passage d'une catégorie à une autre peut déclencher automatiquement l'ajustement des systèmes en aval, tels que le point de vente, l'intégrité du produit, la disponibilité du produit avec évaluation active (RAAV), la tarification, et les systèmes basés sur l'e-commerce.

[0043] Du point de vue du paiement, le système de contrôle de bases de données 20 peut identifier des utilisateurs frauduleux qui modifient légèrement les paramètres de la transaction pour duper le système de détection anti-fraude 22 au moment du paiement, et procéder à des révisions ultérieures de la réservation pour terminer la fraude. En analysant le contenu des enregistrements et des évènements de réservation avec les enregistrements de paiement, le moteur de contrôle de base de données 60 peut détecter un modèle d'évènements potentiellement frauduleux et demander au système de détection anti-fraude 22 d'analyser de nouveau la transaction après le paiement. Un rapport des modèles potentiellement frauduleux peut être produit pour prévenir les marchands d'un comportement suspicieux et aider à améliorer la sécurité.

[0044] Les évènements analysés pour des modèles suspects peuvent inclure des changements de dates de vols. Par exemple, les changements de dates de vols effectués peu de temps après la réservation du vol (par ex., moins d'une journée) peuvent indiquer une fraude. De plus, la probabilité de fraude peut augmenter de manière inversement proportionnelle à la période située entre la date de réservation du vol et la date de demande de changement. Changer la date de vol de la date de départ initialement planifiée (par ex. plusieurs jours/semaines/mois dans le futur) à une date plus immédiate (par ex. le même jour où le changement est demandé) peut également indiquer une fraude. Dans ce cas, la probabilité de fraude peut être liée à la taille du changement. Des changements de date de départ avec un intervalle de temps plus grand indiquent une probabilité plus élevée de fraude que des changements de date de départ avec un intervalle de temps plus court. Les changements qui déplacent la date de départ peu de temps

après la date de demande de changement (par ex. départ le même jour que le jour de demande de changement) peut également indiquer une fraude. La probabilité de fraude augmente de manière inversement proportionnelle à la période située entre la date de demande de changement et la date de départ demandée. En réponse à la détection d'un changement de date de vol suspect, le système de contrôle de bases de données 20 peut demander au système de détection anti-fraude 22 d'analyser de nouveau la transaction en utilisant de nouvelles valeurs pour les dates de réservation et de départ.

[0045] Le moteur d'apprentissage de machine 70 peut analyser les changements des enregistrements de voyage en utilisant un réseau neuronal qui comprend une pluralité de neurones artificiels ou « nœuds » interconnectés de manière analogue à un réseau neuronal biologique constitué de neurones et de synapses. Les nœuds peuvent être agencés en une pluralité de couches. Chacune comprend un ou plusieurs nœuds et les nœuds dans chaque couche sont connectés à un ou plusieurs nœuds dans des couches adjacentes par des liens pondérés.

[0046] La FIG. 4 est un exemple de réseau neuronal 80 composé d'une couche d'entrée 82, une couche cachée 84 et d'une couche de sortie 86. Chaque couche comprend un ou plusieurs nœuds 88. La couche d'entrée 82 peut recevoir une pluralité de signaux d'entrée 90 (par ex. quatre) de l'extérieur du réseau neuronal 80. La couche d'entrée 82 peut coupler les signaux reçus à la couche cachée 84 sur les liens pondérés 92. Chaque nœud 88 dans la couche cachée 84 additionne les signaux pondérés reçus des nœuds 88 de la couche d'entrée 82.

[0047] Les signaux additionnés de chaque nœud 88 de la couche cachée 84 peuvent de plus être couplés à chaque nœud 88 de la couche de sortie 86 sur les liens pondérés 94 pour fournir au moins un signal de sortie 96. Le signal de sortie 96 peut de plus être couplé à une fonction d'activation 98 qui peut comparer le signal de sortie 96 avec un seuil de 100 et produire un signal de sortie 102 ayant une valeur logique = 0 (c-à-d, « vraie ») ou une valeur logique = 1 (c-à-d, « fausse») en fonction de la valeur du signal de sortie 96 par rapport au seuil 100.

[0048] Bien qu'présenté avec trois couches à des fins d'exemples, le réseau neuronal 80 peut comporter plus de trois couches (par ex. en ajoutant des couches cachées supplémentaires) ou moins de trois couches. Par exemple, la FIG. 5 montre un mode de réalisation d'un réseau neuronal 80 avec des nœuds 88 de la couche d'entrée 82 couplés directement au nœud 88 de la couche de sortie 86. Pour le réseau neuronal 80, si la somme pondérée des signaux d'entrée 90 est au-dessus du seuil 100, le signal de sortie 102 de la fonction d'activation 98 peut être la

valeur logique 1. Pour le réseau neuronal 80, si la somme pondérée des signaux d'entrée 90 est au-dessus du seuil 100, le signal de sortie 102 de la fonction d'activation 98 peut être une valeur logique 0.

[0049] Les pondérations des liens 92, 94 connectant les nœuds 88 d'une couche cachée 84 aux nœuds 88 des couches d'entrée et de sortie 82 et 86 peuvent être ajustés par des algorithmes d'entraînement qui optimisent la sortie pour fournir des résultats corrects connus (par ex., fraude = vrai/faux) en réponse aux paramètres d'entrée (par ex. évènement de changement de nom = vrai/faux) qui ont produit le résultat connu. Par exemple, le moteur d'analyse a posteriori 68 peut utiliser un réseau neuronal d'apprentissage profond pour entraîner le réseau neuronal 80.

[0050] Le moteur de contrôle de base de données 80 peut utiliser le moteur d'apprentissage de machine 70 pour reconnaître les modèles et évaluer la probabilité que le modèle reconnu indique une fraude. Parce que le moteur d'apprentissage de machine 70 peut en réalité apprendre des modèles complexes de manière autonome, une fois entraîné, le moteur d'apprentissage de machine 70 peut fonctionner comme une « boîte noire » qui prédit la fraude basée sur les alimentations de l'enregistrement de réservation et/ou de l'enregistrement de paiement

[0051] Pour configurer le moteur d'apprentissage machine 70 afin qu'il identifie des modèles de réservation frauduleux, un réseau neuronal sur mesure peut être construit à l'aide de techniques telles que le pré-entraînement par auto-encodage. Cela peut être réalisé, par exemple, en analysant les résultats de la fraude pour des opérations historiques qui incluent des transactions dans lesquelles un rejet de débit a été reçu (c-à-d des opérations frauduleuses connues) et les transactions pour lesquelles un rejet de débit n'a pas été reçu (c-à-d des opérations légitimes connues). L'exemple d'un ensemble historique d'échantillons peut inclure un nombre de transactions frauduleuses connues (par ex. 4 500) et un nombre de transactions légitimes connues (par ex. 100 000). À partir de cet ensemble historique d'échantillons de transactions, un ensemble d'entraînement peut être défini. Il inclut un nombre de transactions frauduleuses connues (par ex. 4 000), un nombre de transactions connues légitimes (par ex. 8 000) et un ensemble de tests incluant un nombre de transactions (par ex. 4 000) sélectionnées de manière aléatoire à partir de l'échantillon historique. Le moteur d'analyse a posteriori 68 peut extraire des caractéristiques des transactions à utiliser comme entrées vers le réseau neuronal 80. Ces caractéristiques peuvent inclurent des informations générales telles que la ville ou de la région à base IP et peut inclure un grand nombre (par ex. 732) de variables binaires.

[0052] Nous faisons maintenant référence à la FIG. 6 et à des fins d'illustration uniquement, l'exemple de graphique 120 inclut un axe horizontal 122 correspondant à l'indice du lot et un axe vertical 124 correspondant à la valeur d'une fonction erreur à entropie croisée. Il faut comprendre que les échelles de l'axe horizontal 122 et de l'axe vertical 214 peuvent être déformées pour décrire plus clairement les modes de réalisation de l'invention. Le graphique 120 comprend une pluralité de points d'échantillonnage 126. Chacun représente une transaction dans l'échantillon. Un lot 128 représente une valeur moyenne de la fonction erreur à entropie croisée. Le réseau neuronal 80 peut être entraîné en construisant des mini lots aléatoires de données d'entraînement et en laissant le réseau neuronal 80 s'auto-ajuster pour minimiser l'erreur à entropie croisée. Comme on peut le voir en regardant le graphique 120, la tendance selon laquelle le lot 128 bouge de la gauche vers la droite montre une baisse de la valeur moyenne de la fonction à entropie croisée. Cette baisse peut montrer que le réseau neuronal 80 a appris comment résoudre environ 50 % de l'entropie totale (disparité) des données d'entraînement. Un réseau plus complexe avec un grand nombre de nœuds et de niveaux ainsi que des paramètres d'entraînement mieux réglés peuvent fournir des résultats améliorés.

TABLEAU 1 : PERFORMANCE DU RÉSEAU NEURONAL

		VALEURS ACTUELLES	
		PAS DE FRAUDE	FRAUDE
PRÉDICTION DE MODÈLE	PAS DE FRAUDE	3360	70
	FRAUDE	158	112

[0053] Le tableau 1 illustre les résultats de tests sur 4 000 échantillons de transactions incluant 3 818 (3360 + 158) transactions non frauduleuses connues et 182 (70 + 122) transactions frauduleuses connues à l'aide d'un réseau neuronal expérimental construit comme décrit ci-dessus. Le réseau neuronal expérimental a atteint un taux de précision général de 94,3 % ((3660 + 122))/(4000)) en identifiant si une transaction était frauduleuse ou non. Le réseau neuronal a également atteint un taux négatif erroné de 38,5 % (70/ (70 + 112)).

Autrement dit, le réseau neuronal a détecté 61,5 % de transactions frauduleuses connues dans l'échantillon. Le taux positif erroné s'élève à 4,14 % (158/ (3660 + 158)).

[0054] Parce que le réseau neuronal 80 opère comme une sorte de boîte noire, il peut être difficile d'extraire des informations du moteur d'apprentissage de machine 70 sous une forme lisible par les humains. Pour fournir aux utilisateurs des informations sur la manière dont le moteur d'apprentissage machine 70 détecte la fraude, le moteur d'analyse a posteriori 68 peut générer un affichage graphique qui illustre les relations entre les évènements d'enregistrement de voyage et les transactions frauduleuses dans le moteur d'apprentissage de machine 70.

[0055] Nous faisons maintenant référence à la FIG. 7, une pluralité de relations 130, 132, 134 peut être définie dans le moteur d'apprentissage de machine 70. La relation 130 peut associer la présence de la condition A (par ex. un changement de date de départ, le même jour que celui de réservation du vol) avec une probabilité de 50 % que la transaction soit frauduleuse. La relation 132 peut associer la présence des conditions A et B (par ex. un changement de date de départ le même jour que celui de réservation du vol et un changement de nom sur la réservation) avec une probabilité de 80 % que la transaction soit frauduleuse. La relation 134 peut associer la présence des conditions A, B et C (par ex. un changement de date de départ le même jour que celui de réservation du vol, un changement de nom sur la réservation et un changement dans la réservation de la première classe à la classe économique) avec une probabilité de 85 % que la transaction soit frauduleuse.

[0056] Ces relations 130, 132, 134 peuvent former un modèle qui peut être représenté par un graphique 140. Le graphique 140 peut comprendre une pluralité de sommets 142, 1444, 146 connectés par des arêtes 148, 150, 152. Chaque sommet 142, 144, 146 peut représenter une entrée ou une condition d'enregistrement de voyage et peut avoir une pondération correspondant à un lien entre la fréquence à laquelle la condition est présente dans l'historique des enregistrements de voyage et le fait que la transaction correspondante soit frauduleuse. La présence d'une arête reliant une paire de sommets i et j peut indiquer que les conditions représentées par la paire de sommets (i,j) contribuent à la probabilité de fraude de manière cumulative ou synergique, lorsque les deux conditions sont présentes.

[0057] La FIG. 8 est un exemple de graphique 160 qui peut être un graphique orienté par des forces et qui inclut une pluralité de sommets 162 interconnectés par une pluralité d'arêtes 164. Chaque sommet 162 peut représenter une condition, telle qu'une entrée particulière dans un

champ de données d'un enregistrement de voyage et chaque arête 164 peut représenter un lien entre les conditions représentées par les sommets connectés. Des exemples d'entrées d'enregistrements de voyage qui peuvent être représentés par un sommet 162 peuvent inclure mais sans s'y limiter

amount=[378, 763]
amount=[763, 74203]
ccblob_RiskManagementData_PaymentInfo_FareAmount=[375, 755]
ccblob_RiskManagementData_PaymentInfo_FareAmount=[755, 74203]
ccblob_RiskManagementData_PaymentInfo_FeeValue=0.00
ccblob_RiskManagementData_PaymentInfo_FeeValue=[0.82, 4319.85]
ccblob_RiskManagementData_Result=False
ccblob_StringBom_Original_Provider=BN
ccblob_StringBom_Original_Provider=BP
ccblob_StringBom_rm_response=OK
recloc_InternetIndicator=N
root_xmlblob_avsResultCode=none
root_xmlblob_avsResultCode=U
root_xmlblob_cvvOrgCode=none
root_xmlblob_cvvResultCode=none
root_xmlblob_dslink=VIDSSSL
root_xmlblob_isfAmount=[88.8, 209.0]
root_xmlblob_isfAmount=[0.0, 88.8]
root_xmlblob_isnAmount=[144, 9564]
root_xmlblob_nbinstal=[3, 6]
root_xmlblob_nbinstal=[0, 3]
root_xmlblob_nbinstal=[6, 12]
root_xmlblob_paymentmethod=41
root_xmlblob_taxamount=0.00
root_xmlblob_taxamount=[1.48, 1934.83]

[0058] Chaque sommet 162 peut avoir une caractéristique graphique, telle qu'un diamètre, une forme ou une couleur qui indique une caractéristique de la condition représentée, telle

qu'une « masse » ou une pondération de la condition concernant les transactions frauduleuses. Par exemple, les sommets qui ont une masse relativement plus élevée que d'autres sommets peuvent être affichés sous la forme d'un cercle ayant un diamètre plus grand que les autres sommets.

[0059] La masse $\mu(R)$ d'un sommet représentant une condition R pour un graphique non-orienté avec une valeur maximale locale N, ou des sommets, peut être déterminée à l'aide de l'équation suivante :

$$\mu(R) = P(F|R)Supp(R) \quad Eqn.1$$

ou $Supp(R)$ retourne l'ensemble des sommets pour lesquels R n'est pas zéro, et $P(F \mid R)$ retourne une probabilité de fraude pour les transactions incluant R.

[0060] L'agrégation sur un sommet peut être déterminée en utilisant l'équation suivante :

$$M(e_i) = \frac{1}{\sum_{r \in R} \alpha(r)\mu(r)} \sum_{\substack{r \in R \\ e_i \in R}} \alpha(r) \frac{\mu(r)}{\|r\|} \quad Eqn.2$$

ou $\alpha(r)$ fournit une fonction d'agrégation qui peut être une unité dans certains modes de réalisation, r est un vecteur d'arête et e_i est le sommet pour lequel la masse est agrégée.

[0061] Le graphique 160 peut être généré à partir des sommets et des liens qui ont été élagués, de sorte que le graphique 10 affiche uniquement les sommets les plus pertinents. L'élagage peut être réalisé avec l'équation suivante :

$$\sigma(e_i, e_j) = \sum_R \delta_{i,R}\delta_{j,R}$$

ou $\sigma(e_i,e_j)$ est la pondération cumulée des sommets agrégés e_i et e_j, et $\delta_{(i,R)}$ et $\delta_{(j,R)}$ représentent la longueur idéale des arêtes reliant les nœuds i et j sans utiliser une force répulsive séparée.

[0062] Lors de l'inspection du graphique 160, un utilisateur peut déterminer que les conditions représentées par les sommets plus grands sont associées à un nombre relativement élevé de rejets de débit. Par exemple, un ou plusieurs grand(s) sommet(s)connecté(s) peut révéler qu'un nombre disproportionné de transactions frauduleuses inclut un enregistrement de voyage définissant un itinéraire acheté via un canal hors ligne, sans valeur de vérification de carte (CVV) et sans vérification de l'adresse. Cela peut, par exemple, permettre à l'utilisateur d'identifier rapidement une stratégie employée par les fraudeurs. D'autres associations de conditions, telles que l'identité du fournisseur Internet, les billetteries, les types de cartes de crédit, les lieux de départ et d'arrivée, les aéroports ainsi que la fréquence à laquelle les

associations apparaissent sur différentes périodes peuvent ainsi fournir à l'utilisateur les premières indications d'une attaque frauduleuse.

[0063] En général, les routines exécutées pour mettre en œuvre les modes de réalisation de l'invention, si elles sont mises en œuvre dans le cadre d'un système d'exploitation ou d'une application, d'un composant, d'un programme, d'un objet, d'un module spécifique, d'une séquence d'instructions ou d'un sous-ensemble correspondant peuvent être désignées dans les présentes par « code de programme informatique » ou simplement « code de programme ». Le code de programme comprend typiquement des instructions lisibles par ordinateur résidant à divers moments dans divers dispositifs de mémoire et de stockage dans un ordinateur et qui, si elles sont lues et exécutées par un ou plusieurs processeurs dans un ordinateur, font réaliser à cet ordinateur des opérations nécessaires pour exécuter les transactions et/ou éléments englobant les différents aspects des modes de réalisation de l'invention. Les instructions de programme lisibles par ordinateur pour effectuer les transactions des modes de réalisation de l'invention peuvent être, par exemple, du langage d'assemblage ou du code source ou du code objet écrit en associant un ou plusieurs langages de programmation.

[0064] Un code de programme varié décrit dans les présentes peut être identifié sur la base d'une application dans laquelle il est mis en œuvre dans des modes de réalisation de l'invention spécifiques. Cependant, il faut considérer que toute nomenclature de programme particulière suivante est utilisée simplement par commodité et par conséquent, l'invention ne devrait pas se limiter à la seule utilisation dans toute application spécifique identifiée et/ou sous-entendue par une telle nomenclature. De plus, étant donné le nombre en général sans fin de manières avec lesquelles les programmes informatiques peuvent être organisés en routines, procédures, procédés, modules, objets et autres, et les différentes manières avec lesquelles la fonctionnalité du programme peut être attribuées à diverses couches logicielles résidant dans un ordinateur type (par ex. les systèmes d'exploitation, les librairies, les API, les applications, les microprogrammes, etc.), il faut considérer que les modes de réalisation de l'invention ne sont pas limités à l'organisation spécifique et à l'attribution de fonctionnalités de programme décrites dans les présentes.

[0065] Le code de programme incorporé dans toute application/module décrit(e) dans les présentes peut être distribué individuellement ou collectivement en tant que produit de programme sous différentes formes. Le code de programme peut notamment être distribué en

utilisant un support de stockage lisible par ordinateur avec des instructions de programme lisibles par ordinateur sur celui-ci pour amener le processeur à effectuer des aspects des modes de réalisation de l'invention.

[0066] Un support de stockage lisible par ordinateur qui est intrinsèquement non transitoire peut inclure un support tangible volatile et non volatile, mobile et immobile mise en œuvre dans tout procédé ou technologie de stockage de données, telles que les instructions lisibles sur ordinateur, les structures des données, les modules de programme ou d'autres données. Le support de stockage lisible sur ordinateur peut de plus inclure une mémoire vive (RAM), une mémoire morte (ROM), une mémoire morte effaçable et programmable (EPROM), une mémoire morte programmable effaçable électriquement (EEPROM), une mémoire flash ou une autre technologie de mémoire à semi-conducteur, une disque compact à mémoire morte (CD-ROM), ou autre stockage optique, des cassettes magnétiques, une bande magnétique, le stockage sur disque magnétique ou autre dispositif de stockage magnétique, ou tout autre support qui peut être utilisé pour stocker les données souhaitées et qui peut être lu par un ordinateur. Un support de stockage lisible par ordinateur ne devrait pas être interprété comme des signaux transitoires en soi (par ex., des ondes radio ou autres ondes électromagnétiques, des ondes électromagnétiques se propageant via un support de transmission tel qu'un guide d'ondes ou des signaux électriques transmis par un fils). Les instructions du programme lisible par ordinateur peuvent être téléchargées sur un ordinateur, un autre type d'appareil de traitement de données programmables ou un autre dispositif provenant d'un support de stockage lisible par ordinateur ou vers un ordinateur externe ou un dispositif de stockage externe via un réseau.

[0067] Les instructions du programme lisible par ordinateur stockées sur un support lisible par ordinateur peuvent être utilisées pour diriger un ordinateur, d'autres types d'appareils de traitement de données programmables ou d'autres dispositifs pour fonctionner d'une manière particulière, de sorte que les instructions stockées sur un support lisible par ordinateur produisent un article de fabrication comprenant des instructions qui mettent en œuvre les fonctions, les actes et/ou les transactions précisées dans les organigrammes, diagrammes de séquence et/ou les schémas fonctionnels. Les instructions du programme informatique peuvent être fournies à un ou plusieurs processeurs d'un ordinateur à usage général, d'un ordinateur spécialisé ou d' un autre appareil de traitement de données programmables pour produire une machine, de sorte que les instructions, exécutées via un ou plusieurs processeurs provoquent une série de calculs à

effectuer pour mettre en œuvre les fonctions, les actes et/ou les transactions précisées dans les organigrammes, les diagrammes de séquence et/ou les schémas fonctionnels.

[0068] Dans certains autres modes de réalisation, les fonctions, les actes et/ou les transactions précisé(e)s dans les organigrammes, les diagrammes de séquence et/ou les schémas fonctionnels peuvent être réordonnés, traités en série, et/ou traités simultanément conformément aux modes de réalisation de l'invention. De plus, tout organigramme, diagramme de séquence et/ou schéma fonctionnel peut inclure plus ou moins de blocs que ceux cités en exemple conformément aux modes de réalisation de l'invention.

[0069] La terminologie utilisée dans les présentes a pour fin de décrire des modes de réalisation particuliers uniquement et n'est pas destinée à limiter les modes de réalisation de l'invention. Comme utilisé dans les présentes, les formes au singulier « un » et « le » incluent également les formes plurielles, sauf si le contexte indique clairement le contraire. Il est de plus entendu que les termes « comprend » et/ou « comprenant » lorsqu'ils sont utilisés dans la présente spécification, indiquent la présence de caractéristiques énoncées, entiers, actions, étapes, opérations, éléments et/ou composants mais n'excluent pas la présence ou l'ajout d'une ou de plusieurs caractéristiques, entiers, actions, étapes, opérations, éléments, composants et/ou groupes correspondants. De plus, dans la mesure où les termes « inclut », « ayant », « a », « avec » « composé de » ou leurs variantes sont utilisés soit dans la description détaillée soit dans les revendications, lesdits termes sont destinés à être inclusifs de la même manière que le terme « comprenant ».

[0070] Tandis que toute l'invention a été illustrée par la description de divers modes de réalisation et tandis que ces modes de réalisation ont été décrits de manière très détaillée, le Demandeur n'a pas l'intention de restreindre ou de quelque manière que ce soit de limiter la portée des revendications ci-jointes à de tels détails. Des avantages ou des modifications supplémentaires seront familiers pour les spécialistes en la matière. Par conséquent, l'invention dans ses aspects plus larges ne se limite pas aux détails spécifiques, à l'appareil et au procédé représentatifs et aux exemples montrés et décrits. Il est donc possible de s'écarter desdits détails sans s'écarter de l'esprit ou de la portée du concept inventif général du Demandeur.

REVENDICATIONS

1. Un procédé de détection de modèles comprenant :

la détection, par un serveur, d'un changement apporté à un premier enregistrement de voyage après qu'un premier itinéraire défini dans un premier enregistrement de voyage a été réservé ;

en réponse à la détection du changement, la détermination, par le serveur, d'un premier modèle de changements apportés au premier enregistrement de voyage ;

la détermination, par le serveur, de la concordance du premier modèle avec un modèle potentiellement frauduleux ; et

en réponse au premier modèle qui correspond au modèle potentiellement frauduleux, le signalement du premier enregistrement de voyage comme potentiellement frauduleux.

2. Le procédé selon la revendication 1 comprenant par ailleurs :

en réponse au premier enregistrement de voyage signalé comme potentiellement frauduleux, la transmission des données qui caractérisent une opération d'achat du premier itinéraire à un système de détection anti-fraude.

3. Le procédé de la revendication 2 dans lequel la transaction est caractérisée au moins en partie par le premier modèle.

4. Le procédé selon les revendications 2 ou 3 comprend par ailleurs :

en réponse au système de détection anti-fraude, l'indication que la transaction est frauduleuse, l'annulation de la réservation du premier itinéraire.

5. Le procédé selon toute revendication 1 à 4 comprenant par ailleurs :

la réception d'un rejet de débit associé à un second itinéraire ;

l'identification d'un second enregistrement de voyage qui définit le second itinéraire ;

l'extraction d'un historique des évènements du second enregistrement de voyage ;

la détermination d'un second modèle de changements sur le second enregistrement de voyage basé sur l'historique des évènements ; et

le stockage du second modèle dans une base de données de modèles frauduleux connus.

6. Le procédé selon la revendication 5 dans lequel la détermination de la concordance du premier modèle avec un modèle potentiellement frauduleux comprend :

la comparaison du premier modèle avec un ou plusieurs modèles frauduleux connus ; et

la définition du premier modèle comme correspondant au modèle potentiellement frauduleux en réponse au premier modèle correspondant à un ou plusieurs modèles frauduleux connus.

7. Le procédé selon les revendications 5 ou 6 comprend par ailleurs :

l'entraînement d'un algorithme pour détecter des modèles potentiellement frauduleux utilisant des modèles frauduleux connus dans la base de données des modèles frauduleux connus.

8. Le procédé selon les revendications 7 dans lequel l'entraînement de l'algorithme comprend :

le filtrage de l'historique des évènements pour supprimer des évènements classés comme étant non pertinents pour une analyse de la fraude ; et

l'utilisation du l'historique filtré des évènements pour entraîner l'algorithme.

9. Le procédé selon la revendication 7 ou la revendication 8 dans lequel l'algorithme est basé sur une analyse de l'arbre de décision, une analyse des forêts aléatoires ou une analyse de la concentration des modèles frauduleux connus.

10. Le procédé selon toute revendication 1 - 9 comprenant par ailleurs :

en réponse au premier modèle signalé comme potentiellement frauduleux, l'ajout du premier modèle à un rapport de modèles potentiellement frauduleux ; et

la transmission du rapport des modèles potentiellement frauduleux à un système utilisateur.

11. Le procédé de toute revendication 1 - 10 dans lequel le changement apporté au premier enregistrement de voyage est une date d'utilisation d'un produit réservé, l'identité d'un passager,

une classe de service du produit réservé, le remboursement d'un billet, la nouvelle réservation du billet ou l'échange du billet.

12. Le procédé de toute revendication 1 - 11 dans lequel le premier modèle inclut des changements puisque le premier enregistrement de voyage a été créé dans une base de données d'enregistrements de voyage.

13. Un système de détection anti-fraude comprenant :

un ou plusieurs processeurs ; et

une mémoire en communication avec un ou plusieurs processeurs, la mémoire stockant le code de programme configuré pour, s'il est exécuté par un ou plusieurs processeurs, que le système :

détecte un changement apporté à un premier enregistrement de voyage après qu'un premier itinéraire défini dans un premier enregistrement de voyage a été réservé ;

en réponse à la détection du changement, détermine un premier modèle de changements apportés au premier enregistrement de voyage ;

détermine, par le serveur, si le premier modèle correspond à un modèle potentiellement frauduleux ; et

en réponse au premier modèle qui correspond au modèle potentiellement frauduleux, signale le premier enregistrement de voyage comme potentiellement frauduleux.

14. Le système de détection anti-fraude de la revendication 13 dans lequel le code de programme, s'il est exécuté par au moins un des processeurs, amène le système à réaliser le procédé de toute revendication 2 - 12.

15. Un programme informatique pour détecter les modèles frauduleux qui, s'ils sont exécutés par un ou plusieurs processeurs, amène un ou plusieurs processeurs à :

détecte un changement apporté à un premier enregistrement de voyage après qu'un premier itinéraire défini dans un premier enregistrement de voyage a été réservé ;

en réponse à la détection du changement, détermine un premier modèle de changements apportés au premier enregistrement de voyage ;

détermine, par le serveur, si le premier modèle correspond à un modèle potentiellement frauduleux ; et

en réponse au premier modèle qui correspond au modèle potentiellement frauduleux, signale le premier enregistrement de voyage comme potentiellement frauduleux.

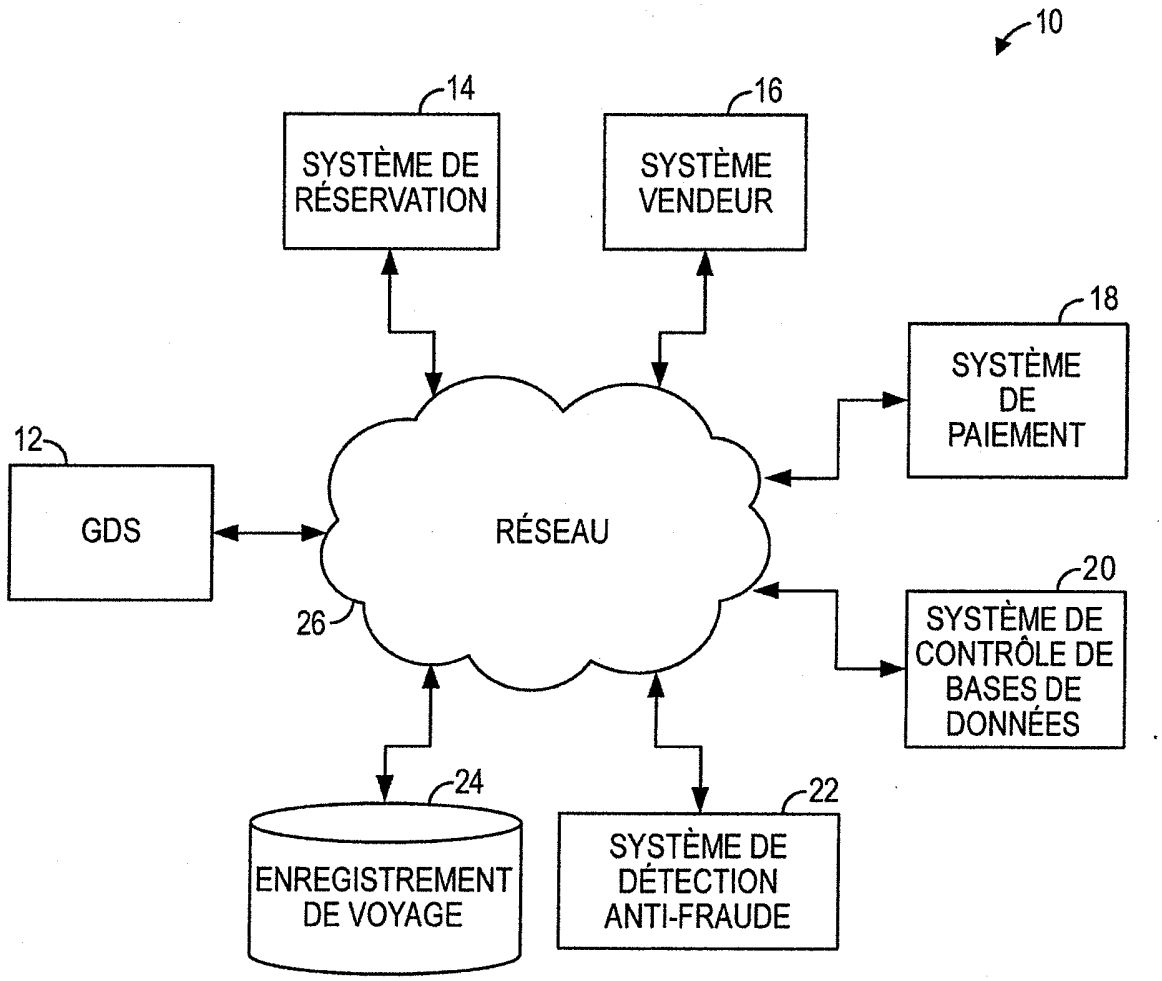
10
14
SYSTÈME DE RÉSERVATION
16
SYSTÈME VENDEUR
18
SYSTÈME DE PAIEMENT
12
GDS
RÉSEAU
26
20
SYSTÈME DE CONTRÔLE DE BASES DE DONNÉES
24
ENREGISTREMENT DE VOYAGE
22
SYSTÈME DE DÉTECTION ANTI-FRAUDE

FIG. 1

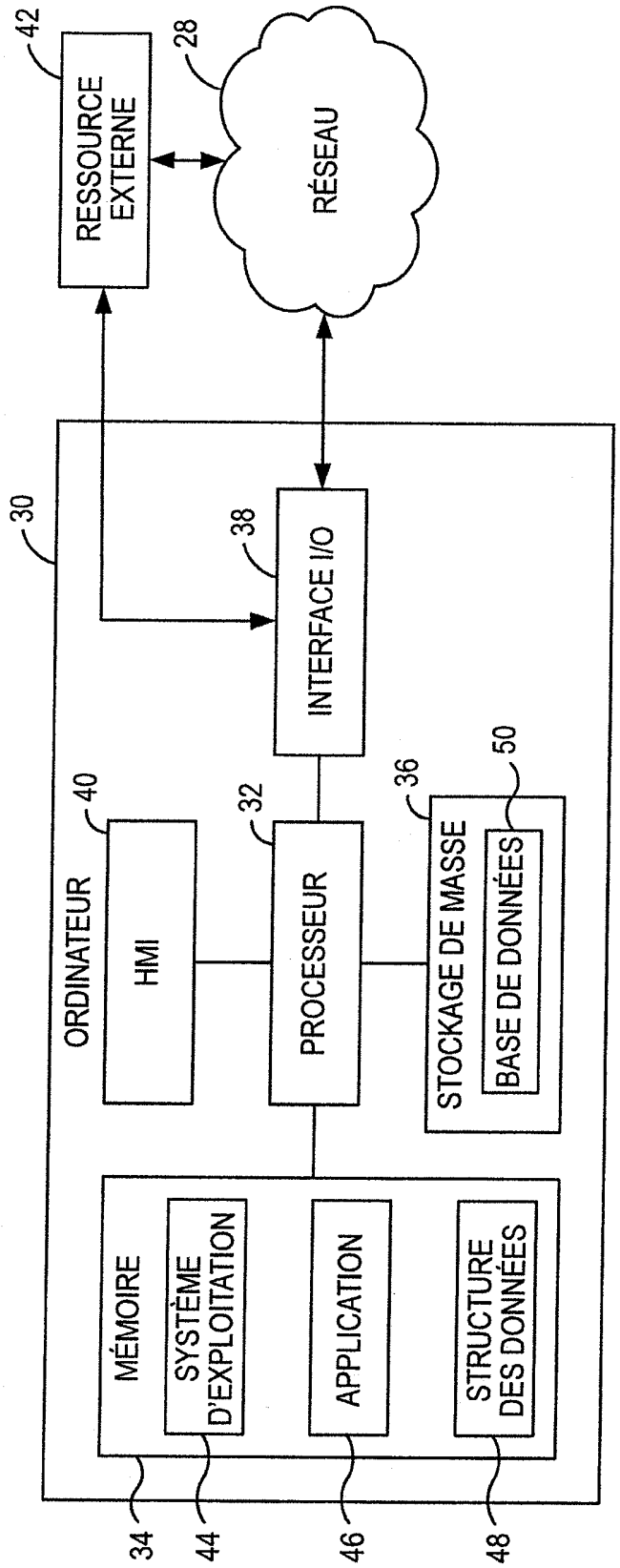
42
RESSOURCE EXTERNE
28
RÉSEAU
30
38
INTERFACE I/O
ORDINATEUR
40
HMI
32
PROCESSEUR
36
STOCKAGE DE MASSE
50
BASE DE DONNÉES
MÉMOIRE
SYSTÈME D'EXPLOITATION
APPLICATION
STRUCTURE DES DONNÉES
34
44
46
48

FIG. 2

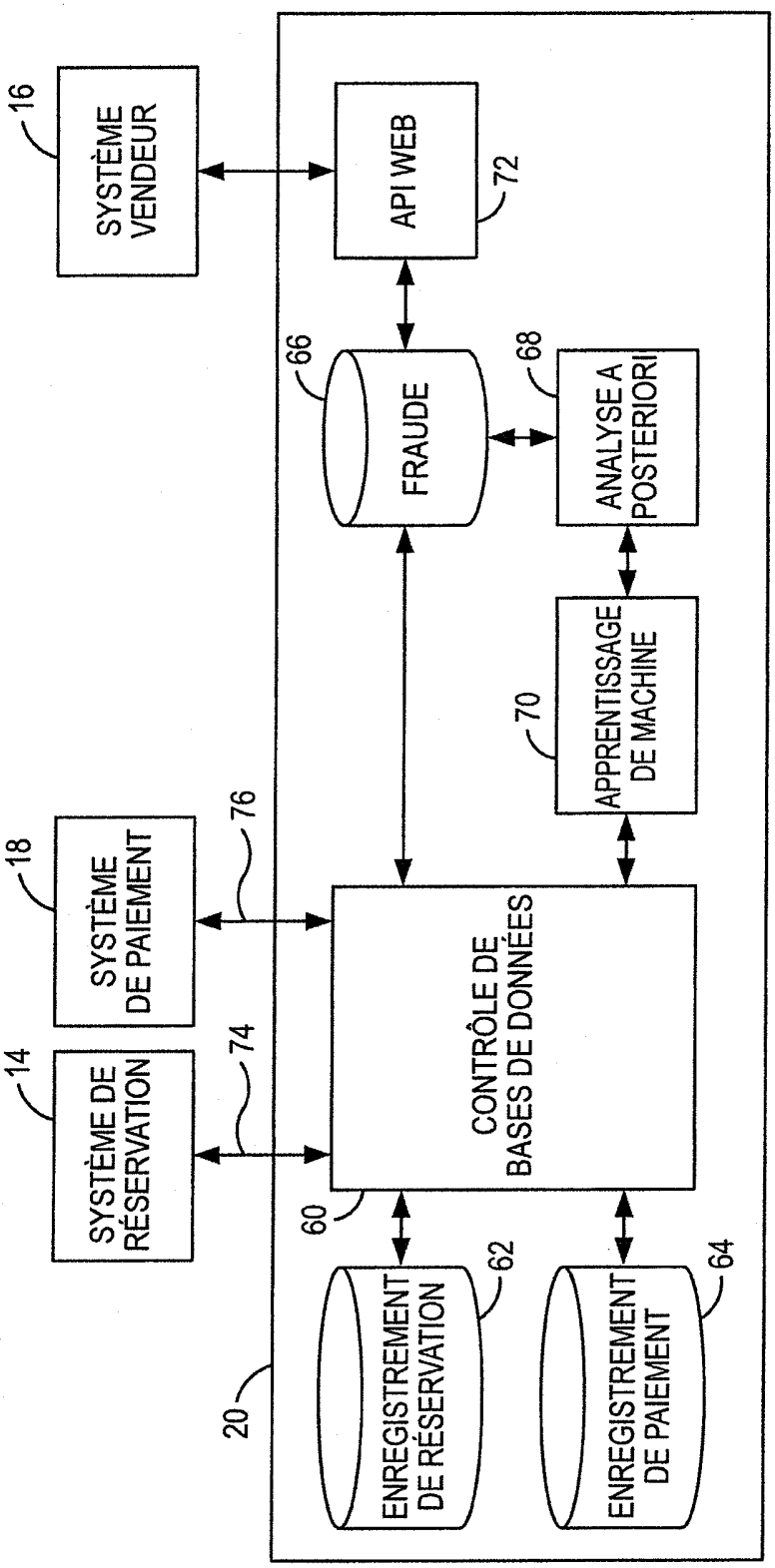
16
SYSTÈME VENDEUR
API WEB
72
66
FRAUDE
68
ANALYSE A POSTERIORI
APPRENTISSAGE DE MACHINE
70
18
SYSTÈME DE PAIEMENT
76
14
SYSTÈME DE RÉSERVATION
74
CONTRÔLE DE BASES DE DONNÉES
60
62
ENREGISTREMENT DE RÉSERVATION
64
ENREGISTREMENT DE PAIEMENT
20

FIG. 3

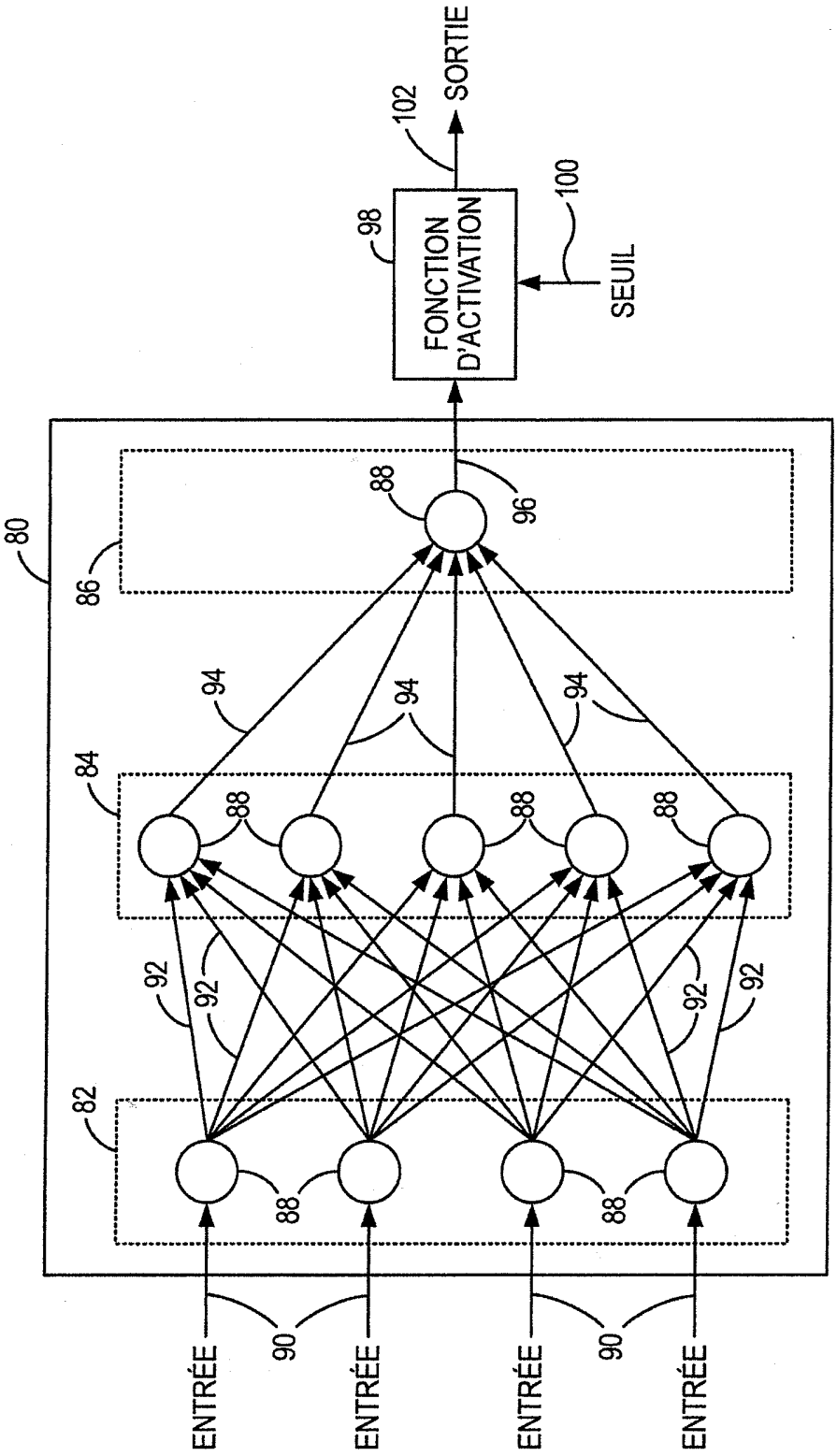
ENTRÉE
ENTRÉE
ENTRÉE
ENTRÉE
90
90
82
84
86
80
88
92
94
96
98
100
102
FONCTION D'ACTIVATION
SEUIL
SORTIE

FIG. 4

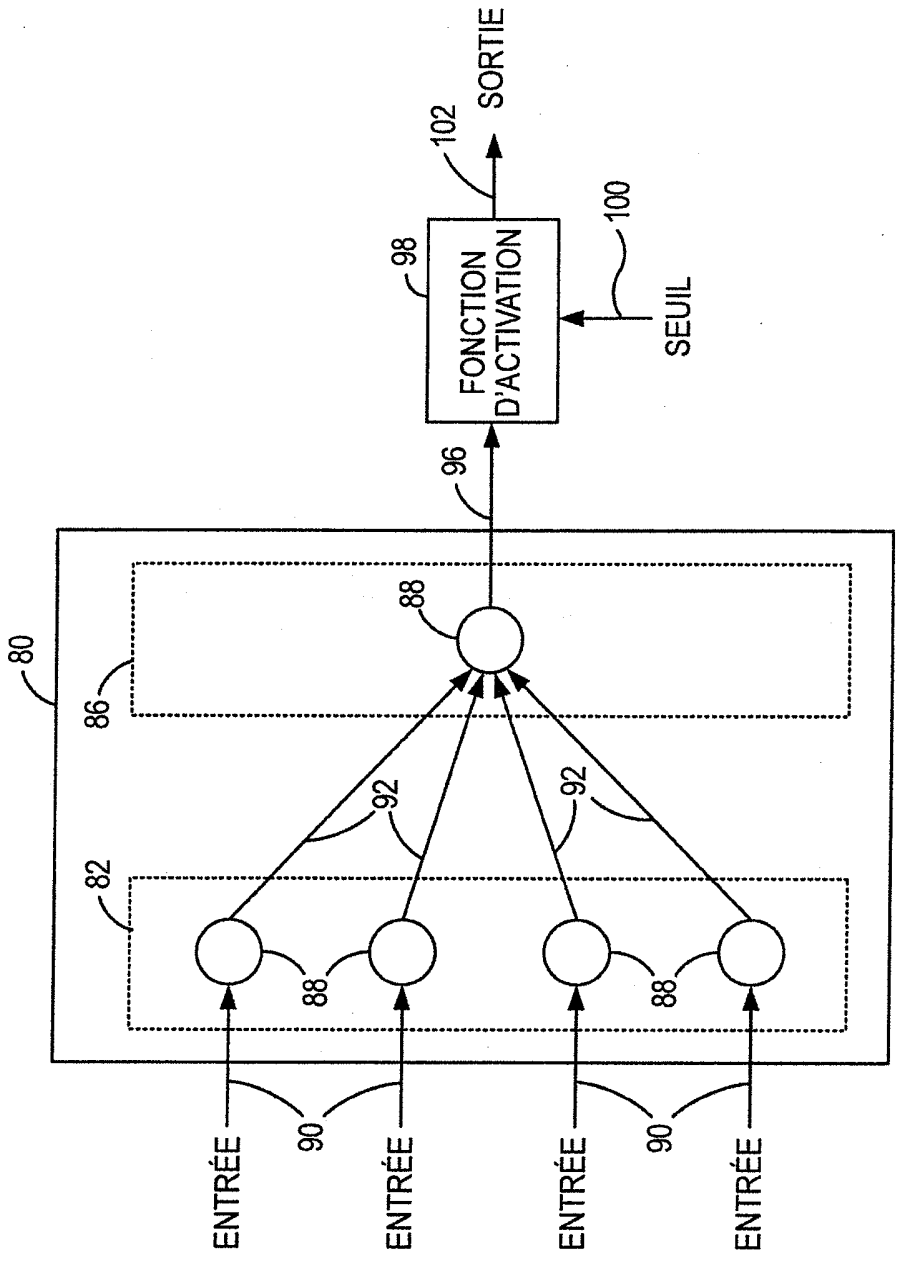
SORTIE
102
100
98
FONCTION D'ACTIVATION
SEUIL
96
80
86
88
92
92
82
88
88
90
90
ENTRÉE
ENTRÉE
ENTRÉE
ENTRÉE

FIG. 5

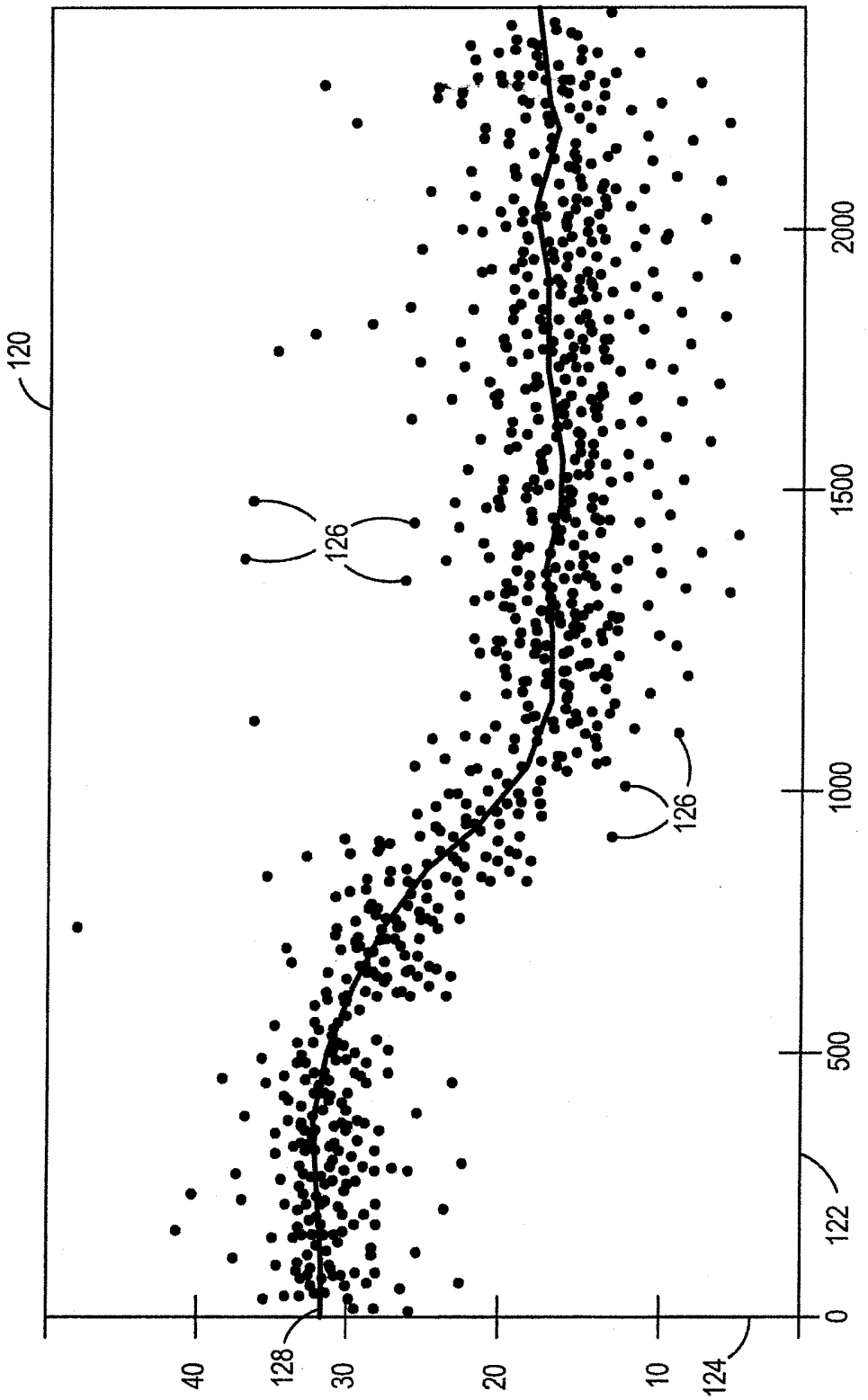

FIG. 6

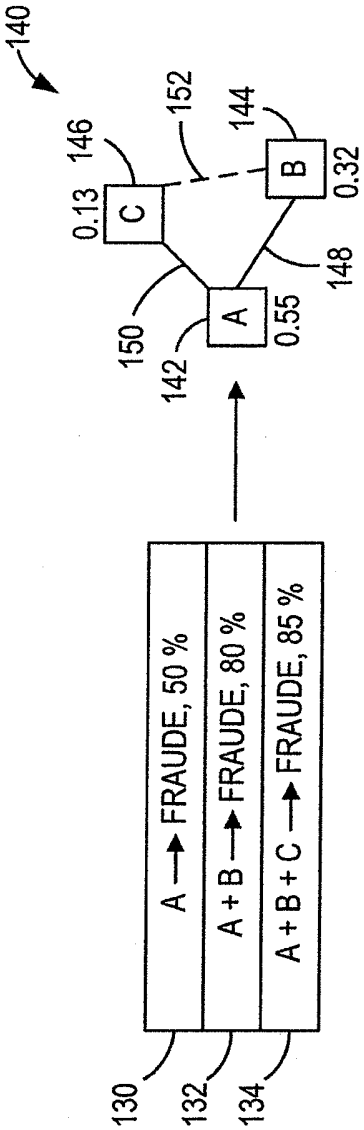
140
146
152
144
0.13
C
B
0.32
148
150
A
0.55
142
A → FRAUDE, 50 %
A + B → FRAUDE, 80 %
A + B + C → FRAUDE, 85 %
130
132
134

FIG. 7

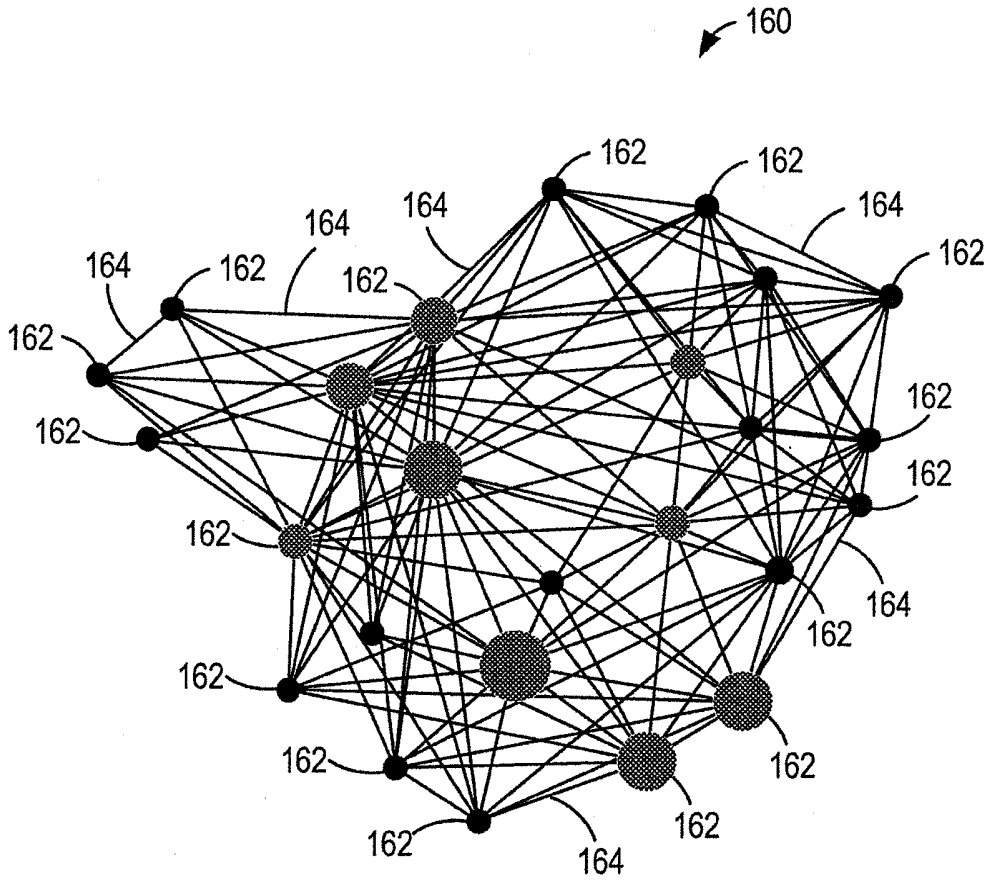
160
162
162
164
164
164
162
162
162
162
162
162
162
162
162
162
162
162
162
164
164

FIG. 8

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 825143
FR 1652007

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X Y	US 2009/271302 A1 (HAMPER LYNN C [US]) 29 octobre 2009 (2009-10-29) * alinéas [0047] - [0052], [0077] * -----	1-4, 13-15 5-12	H04L29/02
X Y	US 2012/158585 A1 (GANTI VISWESWARARAO [US]) 21 juin 2012 (2012-06-21) * alinéas [0019] - [0020], [0045], [0049], [0054], [0105] * -----	1-15 5-12	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06Q

Date d'achèvement de la recherche	Examinateur
24 novembre 2016	Veillas, Erik

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1652007 FA 825143

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 24-11-2016
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2009271302 A1	29-10-2009	US 2009271302 A1	29-10-2009
		US 2013211981 A1	15-08-2013
		WO 2010114882 A1	07-10-2010
US 2012158585 A1	21-06-2012	US 2012158585 A1	21-06-2012
		US 2014236829 A1	21-08-2014

EPO FORM P0465