(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 105 489***
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **19 15258**

(51) Int Cl[8] : ***G 06 F 21/62*** *(2019.12), G 06 F 21/31, G 06 F 21/55*

(12) **CERTIFICAT D'UTILITÉ** **B3**

(54) DISPOSITIF ET PROCEDE DE DETECTION DE FRAUDE.

(22) **Date de dépôt :** 20.12.19.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 25.06.21 Bulletin 21/25.

(45) **Date de la mise à disposition du public du certificat d'utilité :** 31.12.21 Bulletin 21/52.

(56) **Les certificats d'utilité ne font pas l'objet d'un rapport de recherche.**

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

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *AMADEUS SAS Société Par Actions Simplifiée* — FR.

(72) **Inventeur(s) :** AMAR Virginie, BARLET Jeremie, CAMPORA Marc, EL HAYEK Joseph, PEICLE Romain, THONNARD Olivier et ZOUAOUI Jihane.

(73) **Titulaire(s) :** AMADEUS SAS Société Par Actions Simplifiée.

(74) **Mandataire(s) :** Marks & Clerk France.

FR 3 105 489 - B3

Description

Titre de l'invention : Dispositif et procédé de détection de fraude

Domaine technique

[0001] L'invention concerne de manière général les dispositifs et procédé de détection de fraudes.

Contexte

[0002] Les systèmes informatiques modernes sont souvent amenés à stocker ou manipuler des informations sensibles, tel que des clés secrètes, des données personnelles ou confidentielles, ou des informations de paiement.

[0003] Un utilisateur malveillant peut chercher à accéder à de telles informations à des fins de fraudes. Dans un contexte où les systèmes informatiques modernes sont amenés à prendre en charge des données de plus en plus volumineuses (Big Data), la détection de telles fraudes devient un enjeu essentiel.

[0004] Une fraude (ou 'action anormale') fait référence à un comportement ou à des actions utilisateur malicieux vis-à-vis d'un système donné. Une fraude est classiquement caractérisée au moyen d'informations expérimentales (par exemple, moyen et/ou canal par lequel une fraude a été commise, finalités de la fraude, etc.).

[0005] Les dispositifs de détection de fraude existants mettent généralement en œuvre des règles ou conditions permettant de tester des paramètres pour identifier ou non la présence d'une fraude donnée. Par ailleurs, de tels dispositifs peuvent mettre en œuvre une action correctrice adaptée en réponse à la détection d'une fraude pour limiter ou interrompre la fraude.

[0006] Des exemples de solutions de détection de fraude ont été décrits par exemple dans :

- Tom Fawcett and Foster Provost. Adaptive fraud detection. Data mining and knowledge discovery, 1997.
- Sushmito Ghosh and Douglas L Reilly. Credit card fraud detection with a neural-network. In System Sciences, 1994. Proceedings of theTwenty-Seventh Hawaii International Conference on, 1994.
- J. P. Magalhaes and L. M. Silva, "Detection of Performance Anomalies in Web-Based Applications," 2010 Ninth IEEE International Symposium on Network Computing and Applications, Cambridge, MA, 2010, pp. 60-67.

[0007] Généralement, l'identification/la caractérisation des différents types de fraudes pouvant être réalisées sur un système donné est réalisée par des experts techniques, à chaque fois qu'une fraude a été rencontrée sur le système ou un système similaire. Les mêmes experts techniques élaborent ensuite les règles de détection de fraude devant être mise en œuvre par le dispositif en fonction de la caractérisation des fraudes.

[0008] Cependant, selon cette approche supervisée (basée sur l'expérience des actions

passées utilisée par un expert technique), les règles de détection de fraude sont déterminées *a posteriori*, donc après la mise en œuvre de la fraude. Par ailleurs, selon cette approche, les règles de détection sont créées et chargées statiquement dans le système par l'expert technique. Ainsi, lorsqu'une situation de fraude est détectée, un intervalle de temps allant de quelques minutes à plusieurs jours est souvent nécessaire avant de pouvoir implémenter de nouvelles règles dans le système qui permettent de détecter la fraude.

[0009] En outre, de tels dispositifs de détection de fraudes supervisés reposent sur la capacité des experts techniques à caractériser et identifier des actions frauduleuses, ce qui crée une faille de sécurité importante. De telles approches supervisées ont donc des limitations significatives dans des dispositifs ou environnements en perpétuelle évolution.

[0010] D'autres approches de détection de fraude sont connues dans le cadre de systèmes de paiement en ligne ou de courrier électronique (par exemple dans les systèmes de e-commerce ou bancaires). De tels dispositifs de détection de fraude permettent de détecter des accès anormaux au système par des utilisateurs présumés non autorisés. Ces dispositifs de détection d'accès anormaux utilisent un agent qui détecte les connexions inhabituelles à travers une combinaison d'IP (acronyme pour « Internet Protocol » signifiant Protocole Internet) et un navigateur web.

[0011] Cependant, ces dispositifs de détection d'accès anormaux sont basés sur des règles statiques relatives au nombre d'accès à un compte par exemple.

[0012] Il existe donc un besoin pour un dispositif de détection de fraudes capable d'empêcher en temps réel les attaques par tout type de fraude.

Définition générale de l'invention

[0013] L'invention vient améliorer la situation. A cet effet, elle propose un dispositif de détection de fraude comprenant un module de détection configuré pour détecter une fraude sur un système informatique cible comprenant un ensemble d'applications exécutables, le module de détection comprenant :

- un module de génération de modèle de comportement utilisateur configuré pour déterminer un modèle de comportement utilisateur pour chaque caractéristique extraite de traces d'événements reçues d'au moins une application exécutée sur le système cible pendant une session d'un utilisateur connecté au système cible via un dispositif client ;
- un moteur de calcul de poids d'anomalie configuré pour calculer un poids d'anomalie élémentaire pour chaque modèle de comportement utilisateur associé à une caractéristique donnée ;
- au moins une fonction d'agrégation configurée pour calculer un poids d'anomalie globale à partir des poids d'anomalie élémentaires calculés pour les modèles de comportement utilisateur associé aux caractéristiques extraites.

[0014] Avantageusement, le dispositif de détection étant configuré pour détecter une fraude à partir du poids d'anomalie global calculé et le module de détection de fraude détermine la présence d'une fraude de l'utilisateur sur le système cible en fonction du résultat de la comparaison effectuée par le comparateur.

[0015] Dans un mode de réalisation, le module de génération de modèle de comportement utilisateur peut être configuré pour appliquer une méthode statistique choisie à chaque caractéristique extraite pour générer le modèle de comportement utilisateur.

[0016] Le moteur de calcul de poids d'anomalie peut être configuré pour appliquer une fonction de calcul de poids choisie en fonction de la méthode statistique appliquée à la caractéristique par le module de génération de modèle de comportement utilisateur.

[0017] Dans un mode de réalisation, le moteur de calcul de poids d'anomalie peut être configuré pour agréger les poids d'anomalie élémentaires associés aux modèles de comportement basés sur la même caractéristique d'entrée, ce qui fournit un poids d'anomalie élémentaire commun, et pour affecter le poids d'anomalie élémentaire aux modèles de comportement utilisateur.

[0018] En particulier, les poids d'anomalie élémentaires et le poids d'anomalie globale peuvent avoir une valeur comprise entre 0 et 1.

[0019] Les fonctions d'agrégation peuvent être basées sur une technique CDMA.

[0020] Dans un mode de réalisation, le dispositif peut être configuré pour déterminer si la valeur de poids global satisfait une condition de fraude liée à au moins une valeur de référence, une fraude étant détectée si la condition de fraude n'est pas satisfaite.

[0021] Le dispositif de détection peut en outre comprendre un moteur d'intervention configuré pour déclencher une action d'intervention en fonction de la valeur de poids global.

[0022] Il est également proposé un procédé de détection de fraude sur un système informatique cible comprenant un ensemble d'applications exécutables, le procédé de détection comprenant les étapes consistant à :

- déterminer un modèle de comportement utilisateur pour chaque caractéristique extraite de traces d'événements reçues d'au moins une application exécutée sur le système cible pendant une session d'un utilisateur connecté au système cible via un dispositif client ;
- calculer un poids d'anomalie élémentaire pour chaque modèle de comportement utilisateur associé à une caractéristique donnée ;
- appliquer au moins une fonction d'agrégation pour calculer un poids d'anomalie globale à partir des poids d'anomalie élémentaires calculés pour les modèles de comportement utilisateur associé aux caractéristiques extraites.

[0023] Le procédé de détection détecte une fraude à partir du poids d'anomalie global calculé.

[0024] Les modes de réalisation de l'invention permettent de détecter toute action frauduleuse de manière dynamique tout en empêchant l'action frauduleuse.

Brève description des dessins

[0025] D'autres caractéristiques et avantages de l'invention apparaîtront à l'aide de la description qui suit et des figures des dessins annexés dans lesquels :

[0026] [fig.1] représente un système de détection de fraude, selon certains modes de réalisation ;

[0027] [fig.2] est un organigramme représentant le procédé de détection de fraude selon un mode de réalisation ;

[0028] [fig.3] est un organigramme représentant le procédé de détection de fraude selon un autre mode de réalisation.

[0029] Les dessins pourront non seulement servir à mieux faire comprendre la description, mais aussi contribuer à la définition de l'invention, le cas échéant.

Description détaillée

[0030] La figure 1 représente un système 100 (dit système cible) comprenant un dispositif de détection de fraude 10, selon certains modes de réalisation.

[0031] Telle qu'utilisée ici, une fraude (encore appelé « processus frauduleux ») fait référence à une action ou une série d'actions malveillantes exercées à l'encontre du système cible 100 ayant pour but d'impacter négativement ou de détourner le fonctionnement d'au moins une partie du système cible 100. Une fraude peut résulter d'une action non frauduleuse en soi, mais de plusieurs actions, chacune légitime en soi, qui effectuées selon une certaine séquence peuvent conduire à un détournement du fonctionnement du système cible 100.

[0032] Le système cible 100 peut être tout type de système informatique manipulant (échangeant, recevant, transmettant, traitant et/ou stockant) des données.

[0033] Le système 100 peut être connecté via un réseau de communication 4 à un ou plusieurs dispositifs utilisateurs 5 ou à d'autres systèmes.

[0034] Le réseau de communication 4 peut inclure un ou plusieurs réseaux privés et/ou publics (par ex., Internet) qui permettent d'échanger des données, tels qu'Internet, un réseau local (LAN), un réseau étendu (WAN), un réseau de voix/données cellulaire, une ou plusieurs connexions de bus à grande vitesse et/ou d'autres types de réseaux de communication. Le réseau de communication 4 peut utiliser les technologies de communication standards et/ou les protocoles tels que 4G, Ethernet, 802.11, TCP/IP (protocole de commande de transmission/protocole Internet), HTTP (protocole de transport hypertexte), FTP (protocole de transfert de fichier), etc. Les données peuvent être échangées via le réseau 4 selon les différentes technologies d'échange de données et/ou formats tels que le langage de balisage hypertexte (HTML) et le langage de

balisage extensible (XML).

[0035] Le dispositif de détection de fraudes 10 comprend un module de détection 101 configuré pour détecter en temps réel une fraude et un moteur d'intervention 102 configuré pour sélectionner une ou plusieurs actions (par exemple action correctrice ou déclenchement d'une alarme), en réponse à la détection d'une fraude et à déclencher l'exécution de la ou des actions sélectionnées.

[0036] Le module de détection 101 est configuré pour apprendre dynamiquement de manière non supervisée le comportement d'un utilisateur, sur la base d'un procédé d'apprentissage. Le module de détection 101 peut être connecté à une pluralité d'applications exécutables dans le système cible pour recevoir des données d'apprentissage telles que des événements de différentes applications. Le module de détection 101 peut en outre mettre en œuvre des fonctions de filtrage et/ou d'agrégation des données reçues des applications. Le module de détection 101 peut comprendre un module de modélisation de comportement 1010 (encore appelé « module d'apprentissage de comportement utilisateur ») configuré pour déterminer un modèle de comportement utilisateur pendant une session utilisateur. Le module de détection 101 peut comprendre en outre un comparateur 1011 configuré pour comparer le modèle de comportement utilisateur déterminé par le module 1010 avec un modèle de référence de comportement utilisateur pour détecter une fraude.

[0037] Le module de détection 101 peut mettre en œuvre un procédé de détection tel que représenté sur la figure 2 pour apprendre le modèle de comportement utilisateur relatif à un comportement utilisateur pendant une session utilisateur.

[0038] A l'étape 200, des événements sont reçus d'une ou plusieurs applications.

[0039] A l'étape 202, les événements sont agrégés en temps réel, à chaque session utilisateur, en appliquant un ou plusieurs algorithmes statistiques d'agrégation sur la session, ce qui permet d'apprendre (et ainsi de déterminer) le modèle de comportement de l'utilisateur.

[0040] A l'étape 204, le résultat obtenu sur le modèle appris pour l'utilisateur correspondant à la session utilisateur est validé.

[0041] Le modèle de référence du comportement d'un utilisateur peut prendre en outre en compte :

- l'origine géographique d'une session utilisateur, et/ou
- la source IP (Internet Protocol) du dispositif utilisateur.

[0042] Dans un mode de réalisation, le module de détection peut comprendre un moteur de calcul de poids d'anomalie 1012 (représenté sur la figure 1) configuré pour calculer un poids pour chaque anomalie détectée.

[0043] Le moteur de calcul de poids d'anomalie 1012 est configuré pour déterminer un indicateur de risque pour chaque modèle de référence de comportement utilisateur

obtenu selon le procédé de la figure 2, en utilisant un ou plusieurs modèles mathématiques.

[0044] Le module d'apprentissage du comportement 1010 peut assimiler de façon automatique et non supervisée des informations relatives aux utilisateurs du système cible 100, ces données étant issues de données historiques et d'analyses statistiques.

[0045] Les modèles de comportement utilisateurs, appelés ci-après UBM, peuvent être ensuite utilisés par le comparateur 1012 pour détecter d'éventuelles fraudes.

[0046] Il est à noter que le système proposé correspond à une modélisation dite «centrée sur l'utilisateur», dans la mesure où les données statistiques utilisées pour la modélisation correspondent à l'utilisateur. Cela permet de capturer le comportement unique de l'utilisateur.

[0047] Les modèles de comportement utilisateurs UBM sont auto-adaptables, c'est-à-dire qu'ils sont mis à jour en fonction des informations nouvelles reçues en temps réel (le comportement d'un même utilisateur pouvant changer avec le temps).

[0048] Dans un mode de réalisation, le module d'apprentissage de comportement 1010 peut s'adapter pour prendre en compte tout type de format de données statistiques (catégories, données numériques, données binaires, texte...).

[0049] Le modèle de comportement utilisateur peut capturer différentes données capable de caractériser une utilisation anormale du système, telles que :

- l'origine IP de l'utilisateur ;
- l'activité de l'utilisateur en termes de séquences d'actions ;
- les informations de l'utilisateur (société, pays, Identifiant de Bureau) ;
- des informations de temps de connexion ;
- des informations relatives au dispositif client de l'utilisateur (par exemple, système d'exploitation, navigateur, etc.) ;
- durée de la session.

[0050] Dans un mode de réalisation, le module d'apprentissage du comportement utilisateur 1010 reçoit en entrée les traces des événements liées à une application donnée du système cible, soit a posteriori pour une analyse dite « post mortem », soit en analyse en temps réel de type *streaming*.

[0051] A partir de ces traces d'événements, le dispositif de détection de fraude 10 extrait des informations (ou caractéristiques) et reconstruit une série de sessions utilisateurs qui traduisent le cheminement des actions des utilisateurs depuis leur authentification dans l'application considérée jusqu'à leur déconnexion de l'application, à partir des informations extraites.

[0052] Pour reconstruire une session utilisateur à partir des traces d'événements fournies par des applications, le dispositif de détection de fraude 10 extrait les informations à partir des traces de façon automatique et ordonnée.

[0053] Par exemple, le dispositif de détection de fraude 10 peut utiliser les informations suivantes pour reconstruire les sessions utilisateur :

- pour une fraude correspondant à une pluralité de différentes actions pouvant comprendre des actions individuellement non frauduleuses en elles-mêmes mais qui effectuées selon un certain ordre peuvent conduire à un détournement du système : le nombre d'actions et la fréquence de ces actions, pour un même utilisateur dans une même application du système ;
- des caractéristiques techniques du logiciel client telles que: l'adresse IP et/ou le pays d'origine dans laquelle sa machine est située ;
- des caractéristiques liées à l'utilisateur telles que l'Identifiant de bureau (Office ID), l'organisation de l'utilisateur, et/ou le type de navigateur utilisé par l'utilisateur ;
- des données relatives aux périodes de connexion telles que: les dates et les heures de connexion / déconnexion, et/ou la durée des sessions.

[0054] Ces informations peuvent être maintenues dans un ou plusieurs registres 31. Pour chacune de ces informations extraites des registres 31, différentes méthodes peuvent être appliquées par le module de modélisation de comportement 1010 pour les interpréter et les modéliser en tenant compte de l'hétérogénéité des données (par exemple, source IP, pays, type de navigateur, durée des sessions...).

[0055] Dans un mode de réalisation, le module de modélisation de comportement 1010 peut appliquer un ensemble de méthodes statistiques de façon simultanée pour modéliser le comportement utilisateur, l'ensemble de méthodes statistiques pouvant comprendre les méthodes statistiques suivantes :

- des distributions statistiques calculées à partir d'un ensemble de valeurs observées extraites de données historiques des registres 31 ;
- des chaînes de Markov pour la modélisation d'un ensemble de séquences de valeurs discrètes, par exemple, pour modéliser des séquences d'actions utilisateur et affecter des probabilités à chaque transition possible d'une action utilisateur à une autre ;
- des modèles de mélanges gaussiens qui utilisent une combinaison de distributions gaussiennes pour modéliser une distribution empirique, comme par exemple une distribution d'horodatage de connexion d'utilisateur ;
- des techniques basées sur la fréquence des modèles, qui calculent la fréquence d'occurrence de toute sous-séquence de longueur k dans une plus longue séquence de longueur n (avec $k << n$) et visent à capturer de courtes séquences récurrentes dans une longue séquence ;
- des techniques basées sur la similarité qui calculent la similarité par paires entre les séquences en utilisant une mesure de comparaison spécifique (par exemple, la distance d'édition, la sous-séquence la plus longue, le n-gramme), puis regroupent toutes les séquences qui ont une similarité par paires dépassant un seuil donné.

[0056] Ainsi, pour chaque type de caractéristique (caractéristique d'entrée) extraite des traces d'événements fournies par les applications, un modèle de comportement utilisateur UBM est obtenu en appliquant une ou plusieurs méthodes statistiques choisies à la caractéristique.

[0057] La table ci-dessous donne des exemples de méthodes statistiques utilisées en fonction des types de catégorie de caractéristiques d'entrée extraites par le dispositif de détection de fraude 10.

[0058] [Tableaux1]

Catégorie	**Caractéristique d'entrée**	**Modèle Statistique**
Origines	Source IP	Distribution Statistiques des fréquences observée
	Pays	
Informations Utilisateur	ID de bureau	
	Organisation	
Information relatives au dispositif client	OS	
	Navigateur	
	Agent Utilisateur	
Activité	Séquence d'actions	Chaines de Markov
Informations temporelles	Temps de connexion	Mélange Gaussien
Durée	Durée de Session	Moyenne Déviation Standard

[0059] Selon certains modes de réalisation, le moteur de calcul de poids d'anomalie 1012 est configuré pour associée un poids d'anomalie à chaque modèle de comportement utilisateur obtenu par application d'une méthode statistique à une caractéristique d'entrée donnée. Lorsque plusieurs sous-modèles sont liés à une même caractéristique d'entrée, les poids d'anomalie fournis par chacun des sous-modèles peuvent être pré-agrégés entre eux, ce qui fournit un poids commun reflétant des anomalies possibles au sein d'une session utilisateur concernant l'aspect spécifique en jeu, représenté par la caractéristique extraite (par exemple, une séquence d'actions), et modélisé par un ensemble de techniques de modélisation différentes.

[0060] Le moteur de calcul de poids d'anomalie 1012 peut être directement basé sur les modèles de comportement utilisateur (UBM) créés pour chaque fonctionnalité (caractéristique d'entrée) extraite des traces d'application.

[0061] Pour calculer le poids associé à un modèle utilisateur, le moteur de calcul de poids d'anomalie 1012 peut appliquer une fonction de calcul de poids d'anomalie associée à chaque méthode statistique. Par exemple :

- pour une méthode statistique de type distribution statistique, le poids d'anomalie peut être obtenu en prenant l'inverse de la fréquence observée, normalisée dans l'intervalle [0,1] ;
- pour une méthode statistique de type Chaînes de Markov, la fonction de calcul de poids d'anomalie peut être fournie par le modèle lui-même, l'anomalie étant un complément de la probabilité de Markov d'une séquence donnée ;
- pour une méthode statistique de type Modèle de Mélanges Gaussiens, le poids d'anomalie peut être obtenu en prenant le complément de la probabilité fournie par le modèle lui-même, normalisé dans l'intervalle [0,1] ;
- pour une méthode statistique de type technique basée sur les fréquences, le poids d'anomalie peut être obtenu en comptant le nombre de sous-séquences peu fréquentes au sein d'une séquence d'essai et en normalisant ce nombre dans l'intervalle [0,1] ;
- pour une méthode statistique de type technique de similarité, le poids d'anomalie d'une séquence d'essai peut être obtenu en calculant sa distance maximale à partir de tous les centroïdes des clusters (groupes) de séquences précédentes et en normalisant cette distance dans l'intervalle [0,1] (la distance la plus éloignée étant associée à la valeur de poids 1, qui est le plus grand poids d'anomalie, et une distance proche de zéro étant associée à un poids d'anomalie égal à 0).

[0062] Au moyen de cet ensemble de fonctions de calcul de poids, le moteur de calcul de poids d'anomalies 1012 peut évaluer des sessions utilisateurs en cours ainsi que les actions de nouveaux utilisateurs par rapport à des modèles précédemment acquis afin de calculer un poids d'anomalie globale, à l'aide de méthodes d'agrégation telles que les méthodes d'analyse de décision multicritères (MCDA).

[0063] Le poids d'anomalie globale ainsi obtenu pour l'ensemble des sessions utilisateurs en cours et nouvelles à partir des modèles de comportement utilisateur UBM forme un indicateur représentatif d'une combinaison d'un nombre quelconque d'anomalies statistiquement pertinentes détectées sur des caractéristiques individuelles. En effet, en agrégeant tous les poids d'anomalies individuelles à l'aide des méthodes d'agrégation telles que les techniques d'analyse de décision multicritères (MCDA), le moteur de calcul des anomalies 1012 peut traiter toutes les combinaisons d'anomalies significatives, même imprévues, et ainsi surmonter certaines des limites des systèmes traditionnels statiques non supervisés.

[0064] Le moteur de calcul de score des anomalies 1012 peut agréger tous les poids d'anomalie individuels fournis par chaque fonction de calcul de poids d'anomalie appliquée à un modèle de comportement utilisateur appris.

[0065] La figure 3 est un organigramme représentant le procédé de détection de fraude selon certains modes de réalisation.

[0066] A l'étape 300, des caractéristiques utilisateurs C_j (e.g. Source IP, Pays, ID de bureau,

Organisation, OS, Navigateur, Agent Utilisateur, Séquence d'actions, Temps de connexion, Durée de Session, etc.) sont extraites des traces d'événements reçues d'une ou plusieurs applications s'exécutant sur le système cible 100.

[0067] A l'étape 301, un modèle de comportement utilisateur U_i est généré en appliquant une méthode statistique M_k à chaque caractéristique utilisateur C_j, ce qui fournit une pluralité de modèles de comportement utilisateur $\{U_1, U_2, \ldots, U_n\}$.

[0068] A l'étape 302, une fonction de calcul de poids d'anomalie est appliquée à chaque modèle de comportement U_i pour calculer un poids d'anomalie pour le modèle U_i. La fonction de calcul de poids d'anomalie appliquée à un modèle U_i étant sélectionnée en fonction de la méthode statistique M_{ki} appliquée pour générer le modèle U_i.

[0069] A l'étape 303, si plusieurs modèles Ui sont liés à une même caractéristique d'entrée, les poids d'anomalie calculé pour ces modèles liés sont pré-agrégés entre eux, ce qui fournit un poids commun pour les différents modèles liés.

[0070] Les étapes 302 et 303 fournissent ainsi un ensemble de poids d'anomalie $\{a_1, a_2, \ldots, a_n\}$ associés aux modèles de comportement utilisateur $\{U_1, U_2, \ldots, U_n\}$, le poids a_i correspondant au poids d'anomalie calculé pour le modèle de comportement utilisateur U_2.

[0071] A l'étape 304, une ou plusieurs fonctions d'agrégation sont appliquées aux différents poids d'anomalie a_i pour déterminer un poids d'anomalie global P (encore appelé « poids d'anomalie agrégé »), comme par exemple les fonctions d'agrégation définie par la méthode MCDA.

[0072] A l'étape 305, il est déterminé si la valeur du poids d'anomalie global P satisfait une ou plusieurs conditions (conditions d'anomalie) relatives à au moins une valeur de poids d'anomalie de référence en comparant la valeur du poids d'anomalie global P à ces valeurs de poids d'anomalie de référence. Si les conditions ne sont pas satisfaites, une fraude est détectée. Sinon, les étapes 300 à 305 sont réitérées à réception de nouvelles traces d'événements d'application.

[0073] A l'étape 306, si une fraude est détectée, une action d'intervention est déclenchée. A l'étape 306, l'action d'intervention peut être déterminée en fonction de la valeur du poids d'anomalie global ou de un ou plusieurs autres paramètres.

[0074] Le poids d'anomalie global P peut être calculé à l'étape 304, en appliquant un ensemble de conditions relatives aux poids d'anomalie élémentaires a_i associés aux modèles de comportement Ui. Par exemple, le poids d'anomalie global P peut être déterminé comme étant supérieur à une valeur seuil S si une première condition selon laquelle un nombre R de poids d'anomalies élémentaires a_i (ou « tous les poids a_i » ou « au moins certains poids a_i ») satisfont une condition relative à un seuil S' relatif à la valeur seuil S est satisfaite comme par exemple si «au moins R poids d'anomalie parmi les n poids d'anomalie ont une valeur strictement supérieure au seuil S (e.g. 0,5) ».

[0075] Les conditions appliquées pour déterminer le poids d'anomalie global P peuvent

également prendre en compte des conditions d'importance ou de dépendance entre plusieurs critères relatifs aux poids d'anomalie élémentaires ai ou aux modèles de comportement utilisateur qui leurs sont associés ou aux caractéristiques d'entrée utilisées pour générer les modèles de comportement utilisateur associés. Par exemple, les poids d'anomalies calculés pour certaines caractéristiques peuvent être considérées comme deux fois plus importantes que les poids d'anomalies calculés pour d'autres caractéristiques, le poids d'anomalie global P étant alors déterminé à partir des poids d'anomalies élémentaires a_i en les pondérant préalablement en fonction de cette condition d'importance. Selon un autre exemple, certaines caractéristiques d'entrée utilisées pour calculer les poids d'anomalie individuels a_i peuvent être considérées interdépendantes, le poids d'anomalie global P étant alors déterminé à partir des poids d'anomalies élémentaires a_i en appliquant un calcul préalable aux poids d'anomalie associés à ces caractéristiques interdépendantes pour tenir compte d'une interaction positive (également appelée « synergie » ou « renforcement positif ») ou d'une interaction négative (également appelée « redondance ») entre ces caractéristiques interdépendante.

[0076] Ces conditions appliquées pour déterminer la valeur de poids d'anomalie global P peuvent être implémentées au moyen d'un ensemble de fonctions d'agrégation définies selon une technique d'analyse de décision multicritères. Telle qu'utilisée ici, une fonction d'agrégation est définie comme un opérateur qui prend en entrée un vecteur $z = [a_1, a_2, \ldots, a_n]$ de longueur n, chaque composante du vecteur z étant une valeur normalisée dans l'intervalle [0, 1], la fonction d'agrégation retournant en sortie une valeur également dans l'intervalle [0, 1] qui représente la fusion de toutes les valeurs d'entrée $\{a_i, a_2, \ldots, a_n\}$.

[0077] Des exemples de fonctions d'agrégation appliquées à l'étape 304 peuvent inclure par exemple :

- une moyenne pondérée WA (« Weighted Average ») qui calcule la moyenne de toutes les valeurs d'entrée en utilisant un vecteur de pondération prédéfini qui établit l'importance relative des caractéristique associées aux poids d'anomalie élémentaires ai ;

- une moyenne ordonné pondérée OWA (« Ordered Weighted Averaging ») qui réordonne les valeurs d'entrée ai (par exemple dans l'ordre décroissant) avant de les agréger à l'aide d'un vecteur de pondération donné. Un tel vecteur de pondération est défini en fonction de l'ordre des poids d'anomalie élémentaires ai et peut être utilisé pour accentuer une distribution donnée de valeurs, par exemple pour mettre l'accent sur un certain nombre de valeurs élevées ou accentuer un ensemble de valeurs moyennes gamme. Les opérateurs OWA permettent de pondérer les valeurs partielles en fonction de leur rang lorsque celles-ci sont ordonnées ;

- une moyenne OWA pondérée WOWA (« Weighted Ordered Weighted Averaging »), qui combine les avantages des fonctions WA et OWA. WOWA utilise deux vecteurs de pondération différents : un vecteur w qui met l'accent sur un ordre donné des valeurs (comme dans OWA) et un vecteur p qui définit l'importance relative sur des critères individuels (par exemple caractéristiques d'entrées associés aux poids d'anomalie), comme dans WA. Les deux vecteurs w, p sont alors combinés par une fonction dite génératrice G, de sorte que les deux vecteurs interagissent dans le processus d'agrégation final ;
- des intégrales Floues (« fuzzy integral» en langue anglo-saxonne), telles que l'intégrale de Choquet, qui généralisent tous les opérateurs ci-dessus et tiennent compte de l'interdépendance ou des interactions entre critères (interaction positive ou négative).

[0078] Le poids d'anomalie global P peut donc être normalisé dans l'intervalle [0,1].

[0079] A l'étape 306, le poids d'anomalie global P ainsi obtenu représente un indicateur de risque de fraude qui peut être utilisé par le moteur d'intervention 102 pour déclencher des actions d'intervention (alarmes, action corrective, action préventive, etc.), en fonction du niveau de risque détecté.

[0080] Le module de détection 101 peut comprendre une unité de détection secondaire 1014 (représenté sur la figure 1) configurée pour détecter les fraudes associé à un nouvel utilisateur. Pour un nouvel utilisateur se connectant au système cible, il n'existe pas de modèle de comportement utilisateur préalable. L'unité de détection secondaire 1014 peut néanmoins détecter un comportement frauduleux de la part d'un nouvel utilisateur en comparant des données choisies relatives au comportement de l'utilisateur à un modèle de comportement de référence obtenu en agrégeant des données des utilisateurs du système cible 100 les plus représentatifs pour de telles données.

[0081] Les modes de réalisation de l'invention permettent ainsi de détecter en temps réel des comportements anormaux ou frauduleux dans un système cible selon une approche non supervisée, le procédé et le dispositif de détection étant utilisables par l'ensemble des applications du système. Ils permettent également d'exécuter des actions correctrices appropriées à la fraude détectée lorsque cela est nécessaire.

[0082] Le dispositif et le procédé de détection peuvent avantageusement détecter tout type de fraude comme par exemple une mauvaise utilisation du système cible pouvant impacter les utilisateurs du système ou une utilisation malveillante à des fins de nuisance sur le système.

[0083] Le dispositif et le procédé de détection permettent de mettre en œuvre des actions proportionnées en fonction du type et du niveau de fraude auquel le système cible est confronté, comme par exemple une action de confirmation du mot de passe ou un blocage complet des accès.

[0084] L'homme du métier comprendra que le systèmes ou des sous-système selon les modes de réalisation de l'invention peuvent être mis en œuvre de diverses manières par matériel (« hardware »), logiciel, ou une combinaison de matériel et de logiciels, notamment sous la forme de code de programme pouvant être distribué sous la forme d'un produit de programme, sous diverses formes. En particulier, le code de programme peut être distribué à l'aide de supports lisibles par ordinateur, qui peuvent inclure des supports de stockage lisibles par ordinateur et des supports de communication. Les procédés décrits dans la présente description peuvent être notamment implémentés sous la forme d'instructions de programme d'ordinateur exécutables par un ou plusieurs processeurs dans un dispositif informatique d'ordinateur. Ces instructions de programme d'ordinateur peuvent également être stockées dans un support lisible par ordinateur.

[0085] Il convient en outre de noter que bien que décrites ensemble ci-dessus, certaines caractéristiques de l'invention peuvent présenter des avantages lorsqu'elles sont considérées séparément. En particulier, l'homme du métier comprendra que le procédé de contrôle d'envoi de messages pourraient être mis en œuvre plus généralement dans tout dispositif nécessitant l'envoi de messages de requêtes entre un premier composant du dispositif et un deuxième dispositif, pour d'autres applications que le calcul de disponibilité. De même, le moteur de simulation et le procédé mis en œuvre par le moteur de simulation pour optimiser l'utilisation des serveurs de calcul sur lesquels est mis en œuvre le dispositif peuvent avoir un intérêt dans d'autres types de dispositif configuré pour traiter des requêtes reçues d'applications internes ou externes au système dans lequel est implémenté le dispositif.

[0086] Par ailleurs, l'invention n'est pas limitée aux modes de réalisation décrits ci-avant à titre d'exemple non limitatif. Elle englobe toutes les variantes de réalisation qui pourront être envisagées par l'homme du métier.

Revendications

[Revendication 1] Dispositif de détection de fraude (101) comprenant un module de détection (101) configuré pour détecter une fraude sur un système informatique cible (100) comprenant un ensemble d'applications exécutables, le module de détection comprenant :
- un module de génération de modèle de comportement utilisateur (1010) configuré pour déterminer un modèle de comportement utilisateur pour chaque caractéristique extraite de traces d'événements reçues d'au moins une application exécutée sur le système cible pendant une session d'un utilisateur connecté au système cible via un dispositif client ;
- un moteur de calcul de poids d'anomalie (1012) configuré pour calculer un poids d'anomalie élémentaire pour chaque modèle de comportement utilisateur associé à une caractéristique donnée ;
- au moins une fonction d'agrégation configurée pour calculer un poids d'anomalie globale à partir des poids d'anomalie élémentaires calculés pour les modèles de comportement utilisateur associé aux caractéristiques extraites,
le dispositif de détection (10) étant configuré pour détecter une fraude à partir du poids d'anomalie global calculé,
le module de détection de fraude déterminant la présence d'une fraude de l'utilisateur sur le système cible en fonction du résultat de la comparaison effectuée par le comparateur.

[Revendication 2] Dispositif selon la revendication 1, caractérisé en ce que le module de génération de modèle de comportement utilisateur (1010) est configuré pour appliquer une méthode statistique choisie à chaque caractéristique extraite pour générer le modèle de comportement utilisateur.

[Revendication 3] Dispositif selon l'une des revendications 1 ou 2, caractérisé en ce que le moteur de calcul de poids d'anomalie (1012) est configuré pour appliquer une fonction de calcul de poids choisie en fonction de la méthode statistique appliquée à la caractéristique par le module de génération de modèle de comportement utilisateur (1010).

[Revendication 4] Dispositif selon la revendication 3, caractérisé en ce que le moteur de calcul de poids d'anomalie (1012) est configuré pour agréger les poids d'anomalie élémentaires associés aux modèles de comportement basés sur la même caractéristique d'entrée, ce qui fournit un poids d'anomalie élémentaire commun, et pour affecter le poids d'anomalie élémentaire

auxdits modèles de comportement utilisateur.

[Revendication 5] Dispositif selon l'une des revendications précédentes, caractérisée en ce que les poids d'anomalie élémentaires et le poids d'anomalie globale ont une valeur comprise entre 0 et 1.

[Revendication 6] Dispositif selon l'une des revendications précédentes, caractérisée en ce que les fonctions d'agrégation sont basées sur une technique CDMA.

[Revendication 7] Dispositif selon l'une des revendications précédentes, caractérisée en ce qu'il est configuré pour déterminer si la valeur de poids global satisfait une condition de fraude liée à au moins une valeur de référence, une fraude étant détectée si la condition de fraude n'est pas satisfaire.

[Revendication 8] Dispositif selon l'une des revendications précédentes, caractérisée en ce qu'il comprend en outre un moteur d'intervention (102) configuré pour déclencher une action d'intervention en fonction de la valeur de poids global.

[Revendication 9] Procédé de détection de fraude sur un système informatique cible (100) comprenant un ensemble d'applications exécutables, le procédé de détection comprenant les étapes consistant à :

- déterminer un modèle de comportement utilisateur pour chaque caractéristique extraite de traces d'événements reçues d'au moins une application exécutée sur le système cible pendant une session d'un utilisateur connecté au système cible via un dispositif client ;
- calculer un poids d'anomalie élémentaire pour chaque modèle de comportement utilisateur associé à une caractéristique donnée ;
- appliquer au moins une fonction d'agrégation pour calculer un poids d'anomalie globale à partir des poids d'anomalie élémentaires calculés pour les modèles de comportement utilisateur associé aux caractéristiques extraites,

le procédé de détection (10) détectant une fraude à partir du poids d'anomalie global calculé.

[Fig. 1]

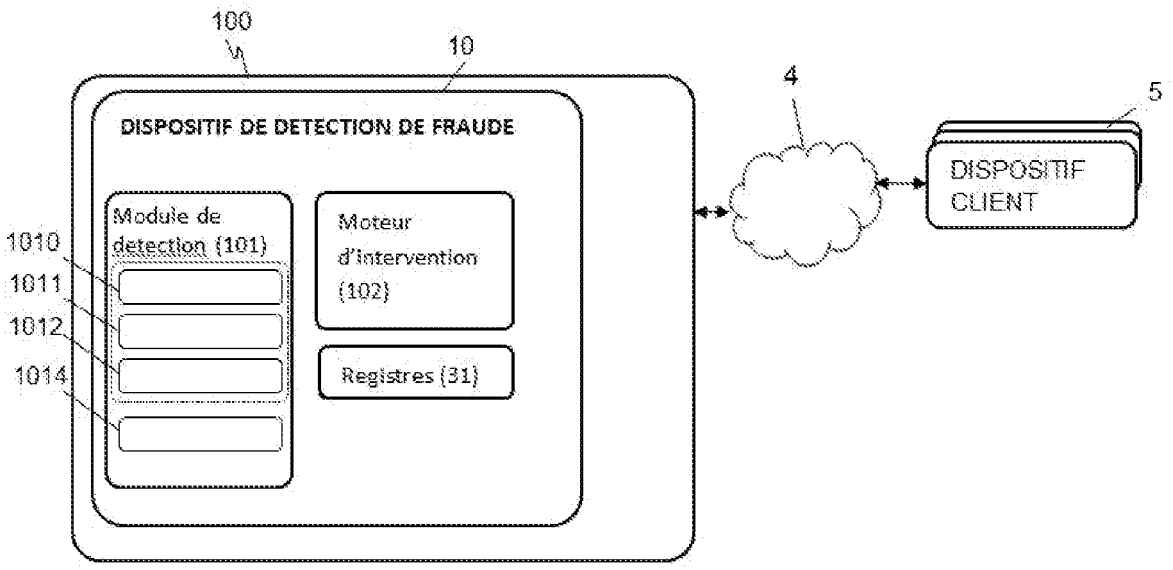


FIGURE 1

[Fig. 2]

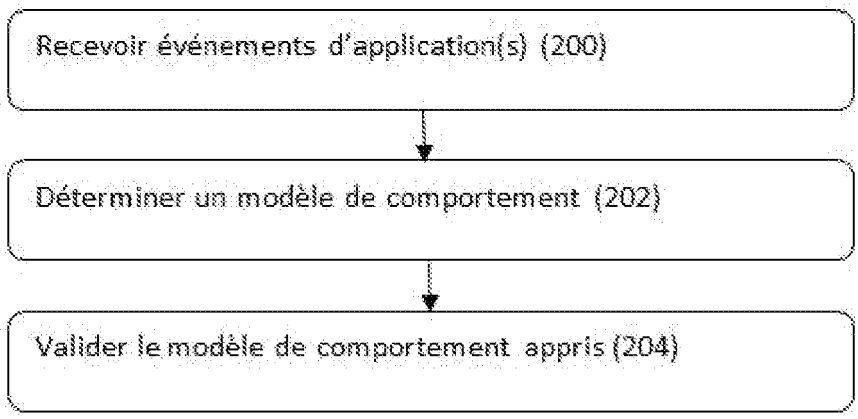


FIGURE 2

[Fig. 3]

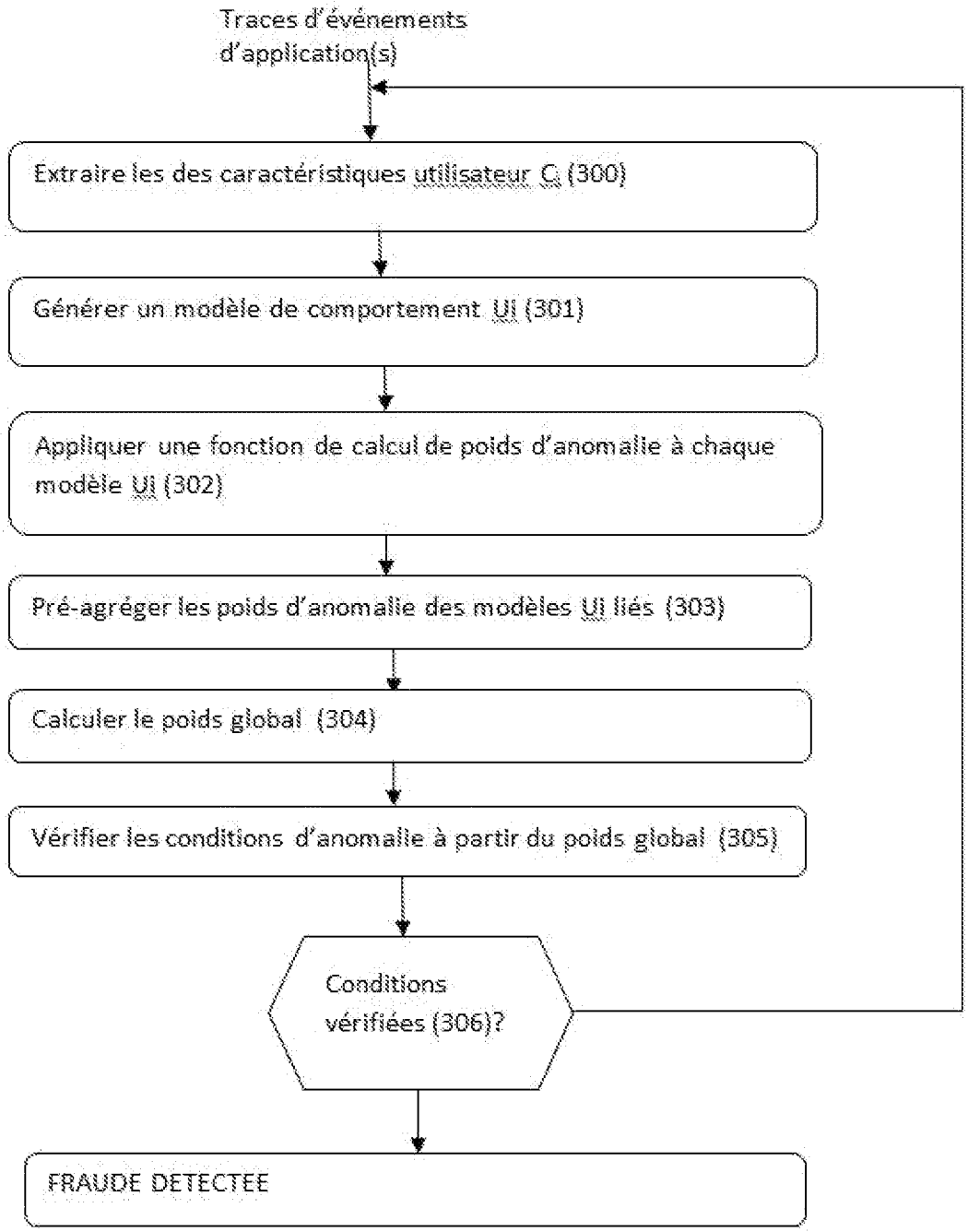


FIGURE 3