(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 065 555**

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

(21) **N° d'enregistrement national :** **17 53497**

(51) Int Cl[8] : ***G 06 F 21/62*** *(2017.01), G 06 F 15/173*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 21.04.17.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 26.10.18 Bulletin 18/43.

(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) :** *ORANGE Société anonyme* — FR.

(72) **Inventeur(s) :** HE RUAN et HAN XIAO.

(73) **Titulaire(s) :** ORANGE Société anonyme.

(74) **Mandataire(s) :** CABINET BEAU DE LOMENIE.

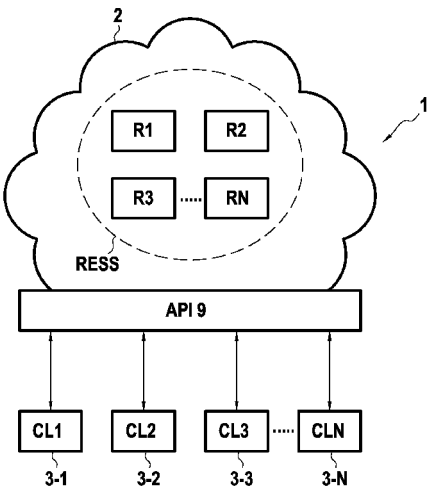
(54) PROCEDE DE GESTION D'UN SYSTEME INFORMATIQUE A ALLOCATION DYNAMIQUE DE RESSOURCES.

(57) L'invention concerne un procédé de gestion d'un système informatique en nuage (2), apte à allouer dynamiquement à une pluralité de clients (CL1,...,CLN) des ressources informatiques et réseaux (RESS), chaque client (CLn) étant associé à au moins un utilisateur susceptible d'accéder aux ressources informatiques et réseaux allouées au client par le système informatique. Ce procédé comprend, pour au moins un client du système informatique:

une étape de réception (E40), en provenance dudit client, d'un modèle primaire de contrôle d'accès et d'une politique primaire de contrôle d'accès basée sur ce modèle primaire de contrôle d'accès;

une étape de réception (E45), en provenance dudit client, d'un modèle secondaire de contrôle d'accès et d'une politique secondaire de contrôle d'accès basée sur ce modèle secondaire de contrôle d'accès, ladite politique secondaire pouvant être mise en oeuvre par ladite politique primaire de contrôle d'accès; et

une étape d'application (E50) desdites politiques primaire et secondaire de contrôle d'accès à au moins une requête d'accès émise par ledit client pour contrôler un accès d'un utilisateur du client à au moins une ressource allouée au client par le système.



FR 3 065 555 - A1

Arrière-plan de l'invention

L'invention se rapporte au domaine général du contrôle de l'accès, par un terminal ou client, à des ressources gérées dynamiquement par un système informatique.

Un enjeu majeur du contrôle d'accès d'un tel système est de garantir la protection et la sécurisation de l'accès à des ressources informatiques et réseaux mises à la disposition d'un client par un système, ces ressources pouvant éventuellement être partagées par plusieurs clients distincts, voire hétérogènes.

L'invention s'applique en conséquence notamment, mais de façon non limitative, aux systèmes informatiques dits « en nuage », connus également sous le nom de systèmes de « cloud computing »aux systèmes de cloud computing multi-entités ou « multi-tenant » en anglais.

Dans le contexte du cloud computing, par entité cliente ou client du système de cloud computing, on entend ici un système d'information (ex. système informatique d'une organisation ou d'une entreprise, application, etc.), locataire des ressources mises à disposition par le système de cloud computing (aussi appelé « tenant » en anglais).

Selon la définition donnée par le National Institute of Standards and Technology (NIST), l'informatique en nuage ou « cloud computing » est un modèle permettant à des utilisateurs, ou plus généralement à des clients, d'accéder via un réseau, à la demande et en libre-service, à des ressources informatiques et réseaux telles que par exemple un espace de stockage, de la puissance de calcul, des applications, un accès réseau, des logiciels ou encore des services, qui sont virtualisées (i.e. rendues virtuelles) et mutualisées entre ces clients. Autrement dit, les ressources informatiques ne se trouvent plus sur un serveur local ou sur un poste d'utilisateur, mais sont, conformément au concept de cloud computing, dématérialisées dans un nuage composé de plusieurs serveurs physiquement distants interconnectés entre eux, et accessibles par les clients et leurs utilisateurs via par exemple une application réseau. Les clients et plus particulièrement leurs utilisateurs peuvent ainsi accéder de manière évolutive à ces ressources, sans avoir à gérer l'infrastructure sous-jacente de gestion de ces ressources qui est souvent complexe.

Le concept de « cloud computing » est décrit plus en détail dans le document édité par l'ITU (International Telecommunication Union) intitulé « FG Cloud TR, version 1.0 – Part 1 : Introduction to the cloud ecosystem : définitions, taxonomies, use cases and high-level requirements », février 2012.

De façon connue, le « cloud computing » bénéficie de nombreux avantages :

— flexibilité et diversité des ressources qui sont mutualisées et quasiment illimitées,

— évolutivité possible des ressources, fournies à la demande,
— administration simple et automatisée des infrastructures informatiques et réseaux des entreprises, et réduction des coûts d'administration,
— etc.

Pour garantir la sécurité d'un système informatique dans lequel les ressources allouées aux clients sont gérées allouées dynamiquement, par exemple un système informatique en nuage, il est nécessaire de définir, pour chaque client du système informatique, un modèle de contrôle d'accès et une politique de contrôle d'accès s'appuyant sur ce modèle pour ses utilisateurs et pour les ressources qui lui sont allouées dynamiquement et éventuellement virtuellement. Une politique de contrôle d'accès est un ensemble de règles qui permet de réguler l'accès des utilisateurs aux ressources du client. Par exemple, une telle politique de contrôle d'accès spécifie via un ensemble de règles les droits des utilisateurs pour accéder à différents fichiers du client stockés sur un disque ; ces règles peuvent indiquer à titre illustratif que l'utilisateur Bob a des droits en lecture sur un fichier F1.h et que l'utilisateur Alice a des droits en écriture sur un fichier F2.c. Cette politique de contrôle d'accès s'appuie sur un modèle de contrôle d'accès qui définit la façon dont la décision d'autoriser ou non l'accès à la ressource est prise.

Il existe dans l'état de la technique, de nombreux modèles de contrôle d'accès qui permettent d'encadrer l'usage des ressources d'un client : ces modèles sont généralement conçus pour vérifier si une entité active (aussi désigné par sujet) telle un utilisateur via un terminal, peut accéder à une entité passive (aussi désignée par objet) telle une ressource informatique et réseau, en effectuant une opération donnée (aussi désignée par action), et le cas échéant, autoriser l'accès à l'entité passive par l'entité active via ladite opération. Des modèles de contrôle d'accès connus plus ou moins complexes sont par exemple les modèles RBAC (Role-Based Access Control), OrBAC (Organization-Based Access Control), ou encore MLS (MultiLevel Security).

Ces modèles ont été conçus à la base pour gérer le contrôle d'accès dans un système informatique associé à une même entité. Les systèmes informatiques en nuage s'appuient aujourd'hui sur ces modèles, mais en sélectionnent un unique qu'ils imposent de manière uniforme à chacun de leurs clients. En d'autres mots, tous les clients d'un système informatique définissent leurs politiques de contrôle d'accès en s'appuyant sur le même modèle de contrôle d'accès choisi par l'opérateur du système informatique, comme par exemple sur le modèle OrBAC ou sur le modèle RBAC.

Une configuration aussi rigide n'est de toute évidence pas bien adaptée au paysage actuel des systèmes d'information et des télécommunications qui promeut l'avènement de multiples acteurs et applications amenés à partager des ressources informatiques et réseaux via des systèmes informatiques, ces acteurs et applications multiples ayant des besoins distincts en matière de politiques de sécurité et plus particulièrement de politiques de contrôle d'accès.

Objet et résumé de l'invention

L'invention permet de remédier notamment à cet inconvénient en proposant un procédé de gestion d'un système informatique apte à allouer dynamiquement à une pluralité de clients des ressources informatiques et réseaux, chaque client étant associé à au moins un utilisateur susceptible d'accéder aux ressources informatiques et réseaux allouées au client par le système informatique . Ce procédé comprend, pour au moins un client du système informatique :

— une étape de réception, en provenance du client, d'un modèle primaire de contrôle d'accès et d'une politique primaire de contrôle d'accès basée sur ce modèle primaire de contrôle d'accès ;

— une étape de réception, en provenance du client, d'un modèle secondaire de contrôle d'accès et d'une politique secondaire de contrôle d'accès basée sur ce modèle secondaire de contrôle d'accès, cette politique secondaire pouvant être mise en œuvre par ladite politique primaire de contrôle d'accès ; et

— une étape d'application des politiques primaire et secondaire de contrôle d'accès à au moins une requête d'accès émise par ledit client pour contrôler un accès d'un utilisateur du client à au moins une ressource allouée au client par le système informatique .

Corrélativement, l'invention vise aussi un système informatique apte à allouer dynamiquement à une pluralité de clients des ressources informatiques et réseaux, chaque client étant associé à au moins un utilisateur susceptible d'accéder aux ressources informatiques et réseaux allouées au client par le système informatique. Ce système comprend :

— un module de réception, apte à recevoir, en provenance du client, un modèle primaire de contrôle d'accès et une politique primaire de contrôle d'accès basée sur ce modèle primaire de contrôle d'accès, ce module de réception étant en outre apte à recevoir en provenance dudit client, au moins un modèle secondaire de contrôle d'accès et une politique secondaire de contrôle d'accès basée sur ce modèle secondaire de contrôle d'accès, cette politique secondaire pouvant être mise en œuvre par ladite politique primaire de contrôle d'accès ; et

— un module de sécurité configuré pour appliquer lesdites politiques primaire et secondaire de contrôle d'accès à au moins une requête d'accès émise par ledit client pour contrôler un accès d'un utilisateur du client à au moins une ressource allouée au client par le système informatique .

L'invention ne pose aucune limite quant aux types des politiques primaire et secondaire(s) de contrôle d'accès. Une politique de sécurité est dite « primaire » lorsqu'elle met en œuvre une autre politique, à savoir une politique dite « secondaire » et une politique est dite « secondaire », lorsqu'elle est mise en œuvre par une autre politique, à savoir une politique dite « primaire ».

En particulier, une politique peut être à la fois qualifiée de politique primaire et de politique secondaire, si elle peut d'une part mettre en œuvre une autre politique et d'autre part être mise en œuvre par une autre politique.

De façon équivalente, on peut dire que les politiques primaire et secondaire au sens de l'invention sont chaînées.

L'invention propose ainsi un procédé et un système permettant de définir des modèles et des politiques d'accès simples et de les chaîner. Elle évite ainsi aux utilisateurs d'avoir à concevoir des politiques d'accès autonomes, sans relation entre elles, et donc plus complexes à définir et à maintenir.

Au sens de l'invention, la politique primaire de contrôle d'accès et plusieurs politiques secondaires de contrôle d'accès peuvent être chaînées en cascade. Une politique secondaire de contrôle d'accès peut elle-même être chaînée avec la politique primaire de contrôle d'accès ou avec une autre politique secondaire de contrôle d'accès qui la précède dans la chaîne.

La chaîne de politiques de contrôle d'accès ainsi définie peut avoir une topologie quelconque. Elle peut en particulier être linéaire, présenter une forme ramifiée (lorsqu'une politique primaire ou secondaire est chaînée avec plus d'une politique), et éventuellement contenir une ou plusieurs boucles.

L'invention s'applique en particulier dans le contexte d'un système informatique dans lequel les ressources sont allouées dynamiquement, mais aussi virtuellement, par exemple dans un système informatique en nuage.

Dans un mode particulier de réalisation, le procédé de gestion d'un système informatique selon l'invention est remarquable en ce qu'il comporte :

- une étape de fourniture, au client, d'un méta-modèle comprenant une pluralité d'éléments permettant de définir un modèle de contrôle d'accès et une politique de contrôle d'accès pour le client basée sur ce modèle ; en ce que
- ledit modèle primaire de contrôle d'accès et ladite politique primaire de contrôle d'accès sont définis par une première instance dudit méta-modèle ; et en ce que
- ledit au moins un modèle secondaire de contrôle d'accès et ladite politique secondaire de contrôle d'accès basée sur ce modèle sont définis par une deuxième instance dudit méta-modèle.

Dans ce mode de réalisation, l'invention propose donc, qu'au lieu d'imposer un même modèle de contrôle d'accès à tous ses clients, le système informatique leur fournisse un méta-modèle prédéfini permettant à chacun des clients du système informatique de créer ses propres modèles de contrôle d'accès et de baser ses politiques de contrôle d'accès sur les modèles ainsi créés.

Ce nouveau paradigme en matière de contrôle d'accès dans un contexte de cloud computing est particulièrement flexible et permet à chaque client de définir avec plus de liberté des politiques de contrôle d'accès qui lui sont propres et s'adapte à ses spécificités et à ses besoins en matière de sécurité.

Cette définition est faite à la volée (autrement dit de manière dynamique) par le client à partir du méta-modèle fourni par le système informatique : le méta-modèle définit de manière

générique un certain nombre d'éléments permettant de créer un modèle de contrôle d'accès et de spécifier des politiques de contrôle d'accès s'appuyant sur ce modèle, que le client vient instancier auprès du système informatique (autrement dit, il vient renseigner les éléments du méta-modèle pour créer les modèles primaire et secondaire de contrôle d'accès sur lequel il souhaite baser ses politiques de contrôle d'accès.

Ainsi, au lieu de protéger le système informatique comme un tout via un unique modèle de contrôle d'accès, l'invention permet de limiter et d'adapter l'étendue de la protection à chaque client. Chaque client peut avoir un contrôle personnalisé de l'accès aux ressources qui lui sont allouées dynamiquement et virtuellement par le système informatique.

On note que cette façon de gérer le contrôle de l'accès aux ressources au niveau du système informatique est particulièrement bien adaptée au caractère évolutif des ressources et des clients au sein d'un système informatique. De même qu'un modèle et une politique de contrôle d'accès peuvent être créés à la volée pour un client du système informatique, ceux-ci peuvent être supprimés à la volée dès lors que ce client n'est plus servi par le système informatique.

Le nouveau paradigme proposé par l'invention est donc flexible, dynamique, adaptatif et évolutif.

Si ce mode de réalisation de l'invention permet de définir une pluralité de modèles et de politiques de contrôle d'accès distincts pour chacun des clients du système informatique , il s'appuie néanmoins sur un méta-modèle unique commun à tous les clients, et un contrôle d'accès aux ressources réalisé de façon centralisée par le système informatique . Ceci permet d'assurer la consistance du contrôle d'accès aux ressources fournies par le système informatique mis en œuvre et renforce son efficacité.

Il convient de noter que les clients d'un système informatique peuvent, via le méta-modèle fourni par le système informatique , baser leur politique de contrôle d'accès sur un modèle de contrôle d'accès connu. Ainsi, dans un mode particulier de réalisation de l'invention, l'instance du méta-modèle fournie par le client définit un modèle de contrôle d'accès de type RBAC, OrBAC, ACL, DTE (Domain Type Enforcement), ABAC (« Attribute Based Access Control ») ou MLS.

L'invention permet également de créer de nouveaux modèles de contrôle d'accès, ou d'adapter les modèles de contrôle d'accès existants en introduisant de nouvelles caractéristiques dans ces modèles (ex. ajout de nouvelles entités aux modèles, définition de nouvelles catégories d'attributs associées à ces entités, introduction de notions dans les modèles de contrôle d'accès connus telles que la notion de session, de délégation, de hiérarchie, de contrôle d'usage, etc.), permettant d'intégrer des fonctionnalité avancées et inédites dans le contrôle d'accès réalisé. Pour plus de renseignements sur les notions de session et de délégation notamment, l'homme du métier peut se reporter au document « D.F Ferraiolo, R. Sandhu, S. Gavrila D.R.Kuhn R.Chandramouli. Proposed nist standard for role-based access control. ACM Transactions on Information and System Security, 2001 ».

A cet effet, comme mentionné précédemment, le méta-modèle proposé par le système informatique à ses clients dans ce mode de réalisation de l'invention comprend avantageusement une pluralité d'éléments permettant de définir le modèle de contrôle d'accès adopté par le client pour sa politique de contrôle d'accès. Dans un mode particulier de réalisation, la pluralité d'éléments du méta-modèle comprend :

— un périmètre du modèle de contrôle d'accès définissant une pluralité d'entités impliquées dans la politique de contrôle d'accès du client. Par exemple, la pluralité d'entités impliquées comprend au moins un sujet, et/ou un objet et/ou une action ;

— des métadonnées définissant pour chaque entité au moins une catégorie d'attributs associée à cette entité ;

— des données définissant des valeurs possibles pour chaque catégorie d'attributs définie par les métadonnées ;

— au moins une métarègle identifiant au moins une catégorie d'attributs définie par les métadonnées et utilisée pour fournir au moins une instruction conforme à la politique de contrôle d'accès du client ;

— au moins une règle de contrôle d'accès basée sur ladite au moins une métarègle et fournissant une instruction conforme à la politique de contrôle d'accès du client ; et

— un ensemble de valeurs assignées par le client à chaque entité définie pour ce client dans le périmètre du modèle de contrôle d'accès, pour chaque catégorie d'attributs associée à cette entité et comprise dans une métarègle, lesdites valeurs assignées étant choisies parmi les données,

— ladite instruction comprenant :

— une autorisation ou un refus d'un accès à une ressource déterminée allouée au client par le système informatique ; ou

— une mise à jour d'au moins un attribut de ladite requête d'accès et de redirection de ladite requête d'accès mise à jour vers une politique de contrôle d'accès.

Ces différents éléments forment un méta-modèle générique offrant un cadre flexible permettant de créer des modèles de contrôle d'accès et de définir des politiques de contrôle d'accès très diversifiés. En particulier, les instructions de redirection permettent de chaîner les politiques de sécurité.

Ainsi selon un autre aspect, l'invention vise également un fichier informatique comprenant des instructions décrivant un méta-modèle comprenant une pluralité d'éléments permettant de définir un modèle de contrôle d'accès et une politique de contrôle d'accès pour un client d'un système informatique apte à allouer dynamiquement à une pluralité de clients des ressources informatiques et réseaux, ladite pluralité d'éléments du méta-modèle comprenant :

— un périmètre du modèle de contrôle d'accès définissant une pluralité d'entités impliquées dans la politique de contrôle d'accès du client ;

— des métadonnées définissant pour chaque entité au moins une catégorie d'attributs associée à cette entité ;

— des données définissant des valeurs possibles pour chaque catégorie d'attributs définie par les métadonnées ;

— au moins une métarègle identifiant au moins une catégorie d'attributs définie par les métadonnées et utilisée pour fournir au moins une instruction conforme à la politique de contrôle d'accès du client ;

— au moins une règle de contrôle d'accès basée sur ladite au moins une métarègle et fournissant une instruction conforme à la politique de contrôle d'accès du client ; et

— un ensemble de valeurs assignées par le client à chaque entité définie pour ce client dans le périmètre du modèle de contrôle d'accès, pour chaque catégorie d'attributs associée à cette entité et comprise dans une métarègle, lesdites valeurs assignées étant choisies parmi les données,

— ladite instruction comprenant :

— une autorisation ou un refus d'un accès à une ressource déterminée allouée au client par le système informatique ; ou

— une mise à jour d'au moins un paramètre d'une requête d'accès émises par ledit client pour accéder à une ressource déterminée allouée au client par le système informatique et de redirection de ladite requête mise à jour vers une politique de contrôle d'accès..

On note que le méta-modèle proposé par l'invention s'appuie dans ce mode particulier de réalisation sur une spécification basée sur la notion d'attributs. La pertinence de cette approche pour décrire de nombreux modèles de contrôle d'accès a été démontrée, les différentes propriétés des entités (sujet, objet ou action) en matière de sécurité pouvant être considérées comme des attributs associés à ces entités.

Ainsi, dans un mode particulier de réalisation, au moins une catégorie d'attributs définie pour une entité est choisie parmi :

— un niveau de sécurité (exemple : niveau de sécurité d'un sujet ou d'un objet) ;

— un rôle (exemple : rôle d'un sujet) ;

— un type (exemple : type d'objet) ;

— un domaine (exemple : domaine auquel a accès un sujet).

Ainsi, ce mode de réalisation de l'invention, par l'intermédiaire du méta-modèle proposé au client, permet à celui-ci de définir une politique de contrôle d'accès classique au moyen de règles autorisant ou refusant l'accès à une ressource en fonction des valeurs des attributs associés à une ou plusieurs entités

Dans un mode particulier de réalisation, l'instance du méta-modèle est fournie par le client via une interface de configuration du système informatique commune à la pluralité de clients du système informatique.

Le méta-modèle proposé par le système informatique étant commun à tous les clients du système informatique, il peut avantageusement être instancié via une interface de contrôle unifiée pour tous les clients.

Selon un autre aspect, l'invention vise aussi un procédé mis en œuvre par un client pour définir des politiques de contrôle d'accès dans un système informatique apte à allouer dynamiquement à une pluralité de clients des ressources informatiques et réseaux, chaque client étant associé à au moins un utilisateur susceptible d'accéder aux ressources informatiques et réseaux allouées au client par le système informatique. Ce procédé comprend :

— une étape de définition d'un modèle primaire de contrôle d'accès et d'une politique primaire de contrôle d'accès basée sur ce modèle de contrôle d'accès pour ledit client ;

— une étape de définition d'au moins un modèle secondaire de contrôle d'accès et d'au moins une politique secondaire de contrôle d'accès basée sur ce modèle secondaire de contrôle d'accès pour ledit client, ladite politique secondaire de contrôle d'accès pouvant être mise en œuvre par ladite politique primaire de contrôle d'accès ; et

— une étape de fourniture desdits modèles primaire et secondaire de contrôle d'accès et desdites politiques primaire et secondaire de de contrôle d'accès audit système informatique , lesdites politiques étant destinées à être appliquées aux requêtes d'accès émises par ledit client pour contrôler un accès d'un utilisateur dudit client à au moins une desdites ressources.

Dans un mode de réalisation, ce procédé de définition de politiques de contrôle d'accès est remarquable en ce qu'il comporte :

· une étape d'obtention d'un méta-modèle fourni par le système informatique et comprenant une pluralité d'éléments permettant de définir un modèle de contrôle d'accès et une politique de contrôle d'accès pour le client ; et en ce que

· ledit modèle primaire de contrôle d'accès et ladite politique primaire de contrôle d'accès sont définis par une première instance dudit méta-modèle ; et en ce que

· ledit au moins un modèle secondaire de contrôle d'accès et ladite politique secondaire de contrôle d'accès basée sur ce modèle sont définis par une deuxième instance dudit méta-modèle.

Corrélativement, l'invention concerne un dispositif d'un client d'un système informatique apte à allouer dynamiquement à une pluralité de clients des ressources informatiques et réseaux, chaque client étant associé à au moins un utilisateur susceptible d'accéder aux ressources informatiques et réseaux allouées au client par le système informatique . Ce dispositif comprend :

— un module de définition d'un modèle primaire de contrôle d'accès et d'une politique primaire de contrôle d'accès basée sur ce modèle de contrôle d'accès,

— au moins un module de définition d'au moins un modèle secondaire de contrôle d'accès et d'une politique secondaire de contrôle d'accès basée sur ce modèle de contrôle d'accès ; et

— un module de fourniture, configuré pour fournir lesdits modèles primaire et secondaire de contrôle d'accès et lesdites politiques primaire et secondaire de contrôle d'accès audit système informatique , lesdites politiques étant destinées à être appliquées aux requêtes d'accès émises par ledit client pour contrôler un accès d'un utilisateur dudit client à au moins une desdites ressources.

Dans un mode particulier de réalisation, ce dispositif est caractérisé en ce qu'il comporte :

- un module d'obtention configuré pour obtenir un méta-modèle fourni par le système informatique et comprenant une pluralité d'éléments permettant de définir un modèle de contrôle d'accès et une politique de contrôle d'accès pour le client ; et en ce que

· ledit modèle primaire de contrôle d'accès et ladite politique primaire de contrôle d'accès sont définis par une première instance dudit méta-modèle ; et en ce que

· ledit au moins un modèle secondaire de contrôle d'accès et ladite politique secondaire de contrôle d'accès basée sur ce modèle sont définis par une deuxième instance dudit méta-modèle.

Le procédé de définition de politiques de contrôle d'accès et le dispositif du client du système informatique bénéficient des mêmes avantages cités précédemment que le procédé de gestion et le système informatique.

Dans un mode particulier de réalisation, les différentes étapes du procédé de gestion et/ou du procédé de définition de politiques de contrôle d'accès sont déterminées par des instructions de programmes d'ordinateurs.

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans un système informatique ou plus généralement dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de gestion tel que décrit ci-dessus. L'invention vise également un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans un dispositif d'un client d'un système informatique ou plus généralement dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de définition de politiques de contrôle d'accès tel que décrit ci-dessus.

Chacun de ces programmes peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

L'invention vise aussi un support d'informations ou d'enregistrement lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

Le support d'informations ou d'enregistrement peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

D'autre part, le support d'informations ou d'enregistrement peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

Alternativement, le support d'informations ou d'enregistrement peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

L'invention vise également un système comprenant :

— un système informatique selon l'invention, apte à allouer à une pluralité de clients des ressources informatiques et réseaux, chaque client étant associé à au moins un utilisateur susceptible d'accéder aux ressources informatiques et réseaux allouées au client par le système informatique ; et
— une pluralité de dispositifs des clients du système informatique conformes à l'invention.

On peut également envisager, dans d'autres modes de réalisation, que le procédé de gestion, le procédé de définition de politiques de contrôle d'accès, le système informatique, le dispositif d'un client du système informatique et le système selon l'invention présentent en combinaison tout ou partie des caractéristiques précitées.

Brève description des dessins

D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent un exemple de réalisation dépourvu de tout caractère limitatif. Sur les figures :

— la figure 1 représente, de façon schématique, un système selon l'invention comprenant un système informatique et des dispositifs clients du système informatique, conformes à l'invention ;
— la figure 2A représente l'architecture matérielle sur laquelle s'appuie le système informatique de la figure 1 ;
— la figure 2B représente différents éléments fonctionnels du système informatique de la figure 1 configurés pour mettre en œuvre le procédé de gestion selon l'invention ;
— la figure 3A représente l'architecture matérielle des dispositifs clients de la figure 1 ;

— la figure 3B représente différents éléments fonctionnels des dispositifs clients de la figure 1 configurés pour mettre en œuvre le procédé de définition de politiques d'accès selon l'invention ;

— la figure 4 illustre schématiquement les principaux modules logiciels définis par le standard de référence XACML pour réaliser le contrôle d'accès et mis en œuvre par le système informatique en nuage de la figure 1 ;

— la figure 5 illustre les principales étapes d'un procédé de gestion selon l'invention tel qu'il est mis en œuvre par le système informatique en nuage de la figure 1, et les principales étapes d'un procédé de définition de politiques d'accès selon l'invention tel qu'il est mis en œuvre par chaque dispositif client de la figure 1 ; et

— la figure 6 illustre le mécanisme de chaînage des politiques de sécurité dans un mode particulier de réalisation de l'invention.

Description détaillée de l'invention

La **figure 1** représente, dans son environnement, un système 1 conforme à l'invention, dans un mode particulier de réalisation.

Dans ce mode de réalisation, le système 1 comprend :

— un système informatique en nuage 2, conforme à l'invention, et apte à allouer à une pluralité de clients CL1, CL2, ..., CLN, N désignant un entier supérieur à 1, des ressources informatiques et réseaux RESS. Aucune limitation n'est attachée à la nature des ressources informatiques et réseaux RESS ; il peut s'agir par exemple d'espace de stockage, de puissance de calcul, d'applications, de connexions réseaux, de logiciels ou encore de services, qui sont virtualisés et mutualisés entre les clients CL1, CL2,..., CLN du système informatique en nuage 2 ; et

— une pluralité de dispositifs 3-1, 3-2, ..., 3-N, associés respectivement à chacun des clients CL1, CL2, ..., CLN du système informatique en nuage 2 et conformes à l'invention. Ces dispositifs communiquent avec le système informatique en nuage 2 via un ou plusieurs réseaux de télécommunications (non représentés) tels que par exemple un réseau WiFI, WLAN, mobile (3G, 4G, 5G, etc.), le réseau public Internet, etc.

Au sens de l'invention, un client CLn, n=1,...,N du système informatique en nuage désigne tout type de système d'information, locataire de ressources Rn mises à disposition dynamiquement et virtuellement par le système informatique en nuage. Un tel client est également appelé « tenant » en anglais. Il peut s'agir par exemple d'un système informatique (IT) d'une organisation ou d'une entreprise, d'une application logicielle, etc. Ce client CLn dispose, de façon connue en soi, pour accéder aux ressources informatiques et réseaux qui lui sont allouées par le système informatique en nuage 2, d'un compte client enregistré auprès du système informatique en nuage. Ce compte client est protégé par un ou plusieurs paramètres d'authentification (ex. Identifiant, mot de passe, etc.) permettant au système informatique en nuage 2 d'identifier le client CLn.

Aucune limitation n'est attachée à la nature des clients du système informatique en nuage 2. Chacun de ces clients comprend un ou plusieurs utilisateurs susceptibles d'accéder, via tout type de dispositifs (ex. via un serveur, un terminal tel qu'un ordinateur, un téléphone intelligent (smartphone) ou une tablette numérique, etc.) aux ressources informatiques et réseaux allouées aux clients par le système informatique en nuage 2.

Conformément à l'invention, le contrôle d'accès aux ressources allouées par le système informatique en nuage 2 aux clients CL1, CL2, ..., CLN est assuré par le système informatique en nuage 2. A cet effet, le système informatique en nuage 2 a l'architecture matérielle d'un ordinateur, telle que représentée à la **figure 2A**. Il comprend notamment un processeur 4, une mémoire morte 5, une mémoire vive 6, une mémoire non volatile 7, ainsi que des moyens de communication 8 avec notamment les dispositifs 3-1, 3-2,...,3-N. Ces moyens de communication 8 intègrent par exemple ici une carte réseau, connue en soi et non détaillée ici, ou tout autre moyen permettant de communiquer sur un réseau de télécommunications. On note que les éléments matériels 4-8 du système informatique en nuage 2 peuvent être localisés sur un unique serveur du système informatique en nuage 2 ou être dispatchés sur plusieurs équipements (par exemple plusieurs ordinateurs) du système informatique en nuage 2 communiquant entre eux et ayant chacun l'architecture matérielle illustrée à la figure 2A. Dans le mode de réalisation décrit ici, on suppose que ces éléments matériels sont colocalisés sur un même serveur.

La mémoire morte 5 du système informatique en nuage 2 constitue un support d'enregistrement conforme à l'invention, lisible par le processeur 4 et sur lequel est enregistré un programme d'ordinateur PROG1 conforme à l'invention, comportant des instructions pour l'exécution des étapes d'un procédé de gestion conforme à l'invention, décrites ultérieurement en référence à la figure 5 dans un mode particulier de réalisation.

Ce programme d'ordinateur définit, de façon équivalente, des modules fonctionnels du système informatique en nuage 2 qui s'appuient ou commandent les éléments matériels 4-8 du système informatique en nuage 2, et qui comprennent plus précisément, en référence à la **figure 2B** :

- un module de fourniture 2A, configuré pour fournir aux clients CL1, ..., CLN du système informatique en nuage 2 un méta-modèle META comprenant une pluralité d'éléments permettant à chaque client CLn, n=1,...,N de définir au moins un modèle de contrôle d'accès ACMn et au moins une politique de contrôle d'accès ACPn pour ce client. Le méta-modèle META est décrit sous forme d'instructions dans un fichier informatique FILE stocké ici dans la mémoire non volatile 7 du système informatique en nuage 2 ;
- un module de réception 2B, apte à recevoir de chaque client CLn, n=1,...,N une première instance du méta-modèle META fournie par le client CLn, cette première instance définissant un modèle primaire de contrôle d'accès ACMPn et une politique primaire de contrôle d'accès ACPPn basée sur ce modèle primaire de contrôle d'accès définies par le client CLn et au moins une deuxième instance du méta-modèle META fournie par le client CLn, cette deuxième

instance définissant un modèle secondaire de contrôle d'accès ACMSn et une politique secondaire de contrôle d'accès ACSPn basée sur ce modèle secondaire de contrôle ; et

— un module de sécurité 2C configuré pour appliquer, pour chaque client CLn, les politiques primaire ACPPn et secondaire(s) ACPSn de contrôle d'accès définies par celui-ci pour contrôler un accès d'un utilisateur de ce client à au moins une ressource parmi les ressources Rn qui lui ont été allouées par le système informatique en nuage 2. On note que le module de sécurité 2C peut être dispatché sur un ou plusieurs équipements (par exemple dans un centre de données) du système informatique en nuage 2 selon que les ressources Rn allouées au client sont hébergées par un seul ou plusieurs équipements dans le système informatique en nuage 2.

Les modules de fourniture 2A et de réception 2B s'appuient sur une interface dite interface unifiée de contrôle 9 du système informatique en nuage 2, que celui-ci met à disposition de ses clients pour accéder au méta-modèle META et l'instancier. Une telle interface peut être par exemple une interface de programmation applicative de type API (Application Programming Interface), connue en soi et non décrite en détail ici, qui permet aux clients CLn de manipuler les différents éléments du méta-modèle META fourni par le système informatique 2 et de l'instancier (c'est-à-dire de le renseigner ou encore de le paramétrer ou de le configurer pour créer un modèle de contrôle d'accès et une politique de contrôle d'accès s'appuyant sur ce modèle).

Les fonctions des modules 2A, 2B et 2C sont décrits plus en détail ultérieurement, lors de la description des étapes du procédé de gestion selon l'invention.

Dans le mode de réalisation décrit ici, chaque dispositif 3-n associé à chaque client CLn (aussi appelé dans la description « dispositif client 3-n »), n=1,...,N a également l'architecture matérielle d'un ordinateur, telle que représentée à la **figure 3A**. Il comprend notamment un processeur 10, une mémoire morte 11, une mémoire vive 12, une mémoire non volatile 13, ainsi que des moyens de communication 14 avec notamment le système informatique en nuage 2. Ces moyens de communication 14 intègrent par exemple ici une carte réseau, connue en soi et non détaillée ici, ou tout autre moyen permettant de communiquer sur un réseau de télécommunications.

La mémoire morte 11 du dispositif 3-n constitue un support d'enregistrement conforme à l'invention, lisible par le processeur 10 et sur lequel est enregistré un programme d'ordinateur PROG2 conforme à l'invention, comportant des instructions pour l'exécution des étapes d'un procédé de définition de politiques de contrôle d'accès conforme à l'invention, décrites ultérieurement en référence à la figure 5 dans un mode particulier de réalisation.

Ce programme d'ordinateur définit, de façon équivalente, des modules fonctionnels du dispositif client 3-n qui s'appuient ou commandent les éléments matériels 10-14 du dispositif 3-n, et qui comprennent plus précisément, en référence à la **figure 3B** :

— un module d'obtention 3A, configuré pour obtenir (c'est-à-dire ici accéder via l'interface unifiée de contrôle 9) le méta-modèle META fourni par le système informatique en nuage 2 ;

— un module de définition 3B, configuré pour instancier (générer ou encore construire) le méta-modèle META de manière à créer :
  - une première instance du méta-modèle définissant un modèle primaire de contrôle d'accès ACMPn et une politique primaire de contrôle d'accès ACPPn basée sur ce modèle de contrôle d'accès sélectionnés par le client CLn et ;
  - au moins une deuxième instance du méta-modèle définissant un modèle secondaire de contrôle d'accès ACMSn et une politique secondaire de contrôle d'accès ACPSn basée sur ce modèle de contrôle d'accès; et
— un module de fourniture 3C, configuré pour fournir ces instances (autrement dit pour fournir le modèle primaire de contrôle d'accès ACMPn, la politique primaire de contrôle d'accès ACPPn, le ou les modèles secondaires de contrôle d'accès ASMSn et la ou les politiques secondaires de contrôle d'accès ACPSn) au système informatique en nuage 2, via ici l'interface de contrôle 9 du système informatique en nuage 2.

Les fonctions des modules 3A, 3B et 3C sont décrits plus en détail ultérieurement, lors de la description des étapes du procédé de définition de politiques de contrôle d'accès selon l'invention.

Dans le mode de réalisation décrit ici, le système informatique en nuage 2 s'appuie, pour réaliser le contrôle de l'accès aux ressources qu'il met à disposition de ses clients, sur l'architecture de référence XACML (eXtensible Access Control Markup Language) définie par le standard IETF, illustrée schématiquement à la **figure 4**.

De façon connue, cette architecture propose un standard pour le déploiement des modules logiciels nécessaires à la mise en œuvre d'un contrôle d'accès dans une infrastructure telle que par exemple le système informatique en nuage 2. Les modules logiciels définis par le standard XACML comprennent notamment un module PDP (pour « Policy Decision Point ») de prise de décision qui applique la politique de contrôle d'accès envisagée aux requêtes d'accès des utilisateurs reçues via un ou plusieurs modules PEP (pour « Policy Enforcement Point) d'exécution. Le module PDP renvoie ici une décision d'autoriser ou non les accès requis (instruction conforme à la politique de contrôle d'accès définie au sens de l'invention) . Le module de prise de décision PDP peut à cet effet interroger un module PIP (pour « Policy Information Point ») d'information pour obtenir des informations complémentaires sur les utilisateurs à l'origine de ces requêtes ou toutes autres informations nécessaires à la prise de décision ne figurant pas dans les requêtes. Le standard XACML prévoit également un module logiciel PAP (pour « Policy Administration Point ») d'administration permettant de gérer les politiques de contrôle d'accès et un répertoire PR (pour « Policy Repository ») dans lequel sont stockées les politiques de contrôle d'accès à appliquer.

Ces modules logiciels étant définis par le standard XACML, ils ne sont pas décrits en détail ici. Dans le mode de réalisation décrit ici, ces différents modules logiciels sont mis en œuvre

par le système informatique en nuage 2. Ils intègrent, pour certains, les modules fonctionnels 2A à 2C du système informatique en nuage 2 décrits précédemment.

Plus particulièrement, les modules fonctionnels 2A et 2B du système informatique en nuage 2 permettant la définition pour chaque client CLn du système informatique en nuage 2 d'un modèle primaire de contrôle d'accès ACMPn, d'une politique primaire associée ACPPn, d'au moins un modèle secondaire de contrôle d'accès ACMSn et d'une politique secondaire associée ACPPn sont intégrés dans le module PAP. On note que dans le mode de réalisation décrit ici, les catégories d'attributs définies pour chaque modèle de contrôle d'accès ACMPn, ACMSn et chaque client CLn sont stockées dans le module PIP, tandis que les règles définissant les politiques de contrôle d'accès APCPn et APCSn du client CLn sont stockées dans le répertoire PR.

Le module fonctionnel de sécurité 2C qui est configuré pour appliquer aux requêtes issues d'utilisateurs d'un client CLn les politiques de contrôle d'accès ACPPn, ACPSn et les modèles de contrôle d'accès ACMPn et ACMSn définis pour ce client est intégré dans le module PDP.

Dans le mode de réalisation décrit ici, le système informatique en nuage 2 s'appuie, pour assurer le contrôle d'accès aux ressources RESS qu'il met à disposition de ses clients CL1,...,CLN, sur un méta-modèle META qu'il fournit via l'API 9 aux clients CL1,...,CLN pour configurer et créer leurs politiques primaire et secondaire(s) de contrôle d'accès et les modèles primaire et secondaire(s) de contrôle d'accès sur lesquels ils souhaitent baser ces politiques. Ce méta-modèle META comprend à cet effet une pluralité d'éléments permettant à chaque client CLn, via l'instanciation du méta-modèle par l'intermédiaire de l'API 9, de définir ses modèles de contrôle d'accès ACMPn, ACMSn et ses politiques de contrôle d'accès ACPPn, ACPSn. Les modèles de contrôle d'accès sont par exemple conformes à des modèles existants tels que RBAC, ORBAC, MLS, etc.

Plus précisément, dans le mode de réalisation décrit ici, le méta-modèle META comprend les éléments suivants :

— le périmètre du modèle de contrôle d'accès : ce périmètre est destiné à définir les différentes entités impliquées dans la politique de contrôle d'accès spécifiée par le client. Ces entités sont typiquement des sujets (ex. utilisateurs), des objets (ex. ressources) et/ou des actions (ex. opérations réalisées par les sujets sur les objets). Souvent en effet, une politique de contrôle d'accès ne peut pas protéger toutes les entités associées à un client, mais se concentre sur un sous-ensemble limité d'entités, spécifié par le client en instanciant le périmètre du modèle de contrôle d'accès ;

— des métadonnées : ces métadonnées sont destinées à définir pour chaque entité identifiée dans le périmètre du modèle de contrôle d'accès une ou plusieurs catégories d'attributs associées à cette entité. Aucune limitation n'est attachée à la nature des catégories d'attributs pouvant être spécifiées dans les métadonnées par un client. Il peut s'agir par exemple d'un niveau de sécurité pour une entité telle un sujet ou une action, d'une action sur un objet, d'un rôle pour un sujet, d'un type pour un objet, etc. ;

— des données : ces données définissent des valeurs possibles pour chaque catégorie ou type d'attributs défini(e) par les métadonnées. Par exemple, pour un niveau de sécurité d'une action, ces données peuvent inclure les niveaux « bas », « moyen », « élevé » ;

— une ou plusieurs métarègles : chaque métarègle est une sorte d'algorithme logique identifiant une ou plusieurs catégories d'attributs définies par les métadonnées et utilisées pour fournir au moins une instruction conforme à la politique de contrôle d'accès souhaitée par le client. Une métarègle vise à définir la ou les catégories d'attributs utilisées pour construire la politique de contrôle d'accès du client et décrit comment ces catégories sont utilisées (c'est-à-dire liées entre elles) pour fournir au moins une instruction conforme à la politique de contrôle d'accès du client (par exemple pour prendre une décision d'autoriser ou non un accès conformément à la politique de contrôle d'accès du client) ;

— une ou plusieurs règles de contrôle d'accès : chaque règle est basée sur (i.e. associée à) une métarègle et décrit un algorithme impliquant les entités identifiées par cette métarègle et reprenant la politique de contrôle d'accès du client. En d'autres mots, l'ensemble des règles de contrôle d'accès définit la politique de contrôle d'accès du client. Chaque règle est définie de sorte à fournir au moins une instruction élaborée en fonction de la politique de contrôle d'accès du client. Chaque règle fournit une instruction conforme à la politique de contrôle d'accès du client ; et un ensemble de valeurs destinées à être assignées par le client à chaque entité définie pour ce client dans le périmètre du modèle de contrôle d'accès, pour chaque catégorie d'attributs associée à cette entité et comprise dans une métarègle, ces valeurs assignées étant choisies parmi les données.

Conformément à l'invention, une instruction issue d'une règle ou d'une métarègle comprend :

— suite à une requête d'accès, une autorisation ou un refus d'un accès à une ressource déterminée allouée au client par le système informatique ; ou

— une mise à jour d'au moins un attribut de ladite requête d'accès et de redirection de ladite requête d'accès mise à jour vers une politique de contrôle d'accès pour permettre le chaînage des politiques.

L'instanciation des métadonnées et des métarègles permet de créer les modèles primaire ACMPn et secondaire(s) ACMSn de contrôle d'accès. L'instanciation des données, des règles, du périmètre et de l'ensemble de valeurs permet de définir les politiques primaire ACPPn et secondaires ACPSn de contrôle d'accès qui s'appuient sur ces modèles de contrôle d'accès ACMPn et ACMSn.

Dans le mode de réalisation décrit ici, le méta-modèle META est décrit sous forme d'instructions dans un fichier informatique FILE conforme à l'invention stocké dans la mémoire non volatile 7 du système informatique en nuage 2. Aucune limitation n'est attachée au langage informatique utilisé pour décrire le méta-modèle META dans le fichier FILE. Il peut être décrit par

exemple en utilisant les langages connus JSON (JavaScript Object Notation), XML (eXtensible Markup Language) ou encore YAML (Yet Another Markup Language).

On note que le méta-modèle META, par son caractère générique, permet d'instancier, autrement dit de créer, des modèles primaires ou secondaires de contrôle d'accès très divers. Il peut être utilisé notamment pour instancier des modèles de contrôle d'accès connus comme par exemple un modèle de contrôle d'accès de type RBAC, OrBAC, ACL, DTE, ABAC, MLS, session ou délégation comme illustré ultérieurement. Le méta-modèle META peut également être utilisé facilement pour instancier d'autres modèles de contrôle d'accès, ou des variantes de modèles de contrôle d'accès connus s'appuyant sur des caractéristiques avancées comme par exemple les notions de session, de délégation, etc.

Nous allons maintenant décrire en référence à la **figure 5** comment ce méta-modèle META est utilisé par le système 1 dans ce mode de réalisation de l'invention pour assurer le contrôle d'accès aux ressources RESS mises à disposition de ses clients CL1,...,CLN par le système informatique en nuage 2 tout en permettant à chaque client CLn, n=1,...,N de spécifier ses propres modèles de contrôle d'accès, de définir et de chaîner ses propres politiques de contrôle d'accès et pour réaliser le contrôle de l'accès aux ressources Rn parmi les ressources RESS qui lui sont allouées. Plus précisément, la figure 5 représente les principales étapes du procédé de gestion mis en œuvre par le système informatique en nuage 2 pour gérer l'accès à ses ressources RESS par les utilisateurs associés à ses clients CL1,...,CLN, et les principales étapes du procédé de définition des politiques de contrôle d'accès mis en œuvre par chaque dispositif client 3-n de chaque client CLn pour spécifier auprès du système informatique en nuage 2, via l'instanciation du méta-modèle META décrit précédemment, ses politiques primaire ACPPn et secondaire(s) ACPSn de contrôle d'accès et les modèles primaire ACMPn et secondaire(s) ACMSn de contrôle d'accès ACMn sur lesquels se basent ces politiques.

Plus précisément, on suppose que suite par exemple à l'enregistrement du client CLn auprès du système informatique en nuage 2, ce dernier lui alloue dynamiquement et virtuellement des ressources Rn parmi ses ressources RESS (étape E10) et l'invite à définir les politiques de contrôle d'accès qu'il souhaite appliquer pour contrôler l'accès aux ressources Rn par ses utilisateurs.

A cet effet, le système informatique en nuage 2 fournit au dispositif 3-n du client CLn, via son interface 9 et son module de fourniture 2A (intégrés dans le module XACML PAP du système informatique en nuage 2) le méta-modèle META (étape E20).

Le client CLn, via le module de définition 3B du dispositif 3-n et l'interface 9 mise à disposition par le système informatique en nuage 2, instancie le méta-modèle META obtenu de sorte à créer le modèle primaire de contrôle d'accès ACMPn et la politique primaire ACPPn de contrôle d'accès ACPn basée sur ce modèle qu'il souhaite appliquer aux ressources Rn qui lui sont allouées (étape E30). Puis, le client CLn, via le module de définition 3B, instancie le méta-modèle

META de sorte à créer un ou plusieurs modèles secondaires de contrôle d'accès ACMSn, et la ou les politique(s) secondaire(s) ACPSn de contrôle d'accès ACPn basées sur ces modèles (étape E35).

A cet effet, le client CLn renseigne (i.e. paramètre ou encore configure), via le module de définition 3B, pour chaque modèle primaire ou secondaire les différents éléments du méta-modèle META dans l'interface 9.

Trois exemples sont donnés ci-après à titre illustratif pour montrer comment le client CLn via le module de définition 3B peut configurer les éléments du méta-modèle META pour créer un modèle primaire de contrôle d'accès de type RBAC et deux modèles secondaires de contrôle d'accès de type session et délégation.

On considère tout d'abord que le client CLn instancie le méta-modèle META de la façon suivante pour créer un modèle de contrôle d'accès primaire de type RBAC :

— il définit comme périmètre du modèle ACMn les entités suivantes :
  - pour les sujets, deux utilisateurs « user0 » et « user1 » ;
  - pour les objets, une machine virtuelle « vm0 » parmi les ressources Rn ;
  - pour les actions, une action de démarrage de la machine virtuelle « start » et une action d'arrêt de la machine virtuelle « stop » ;
— il définit comme métadonnées les catégories d'attributs suivantes :
  - pour les sujets, une catégorie « role » regroupant des attributs de type rôle ;
  - pour les objets, une catégorie « id » regroupant des attributs de type identifiants ;
  - pour les actions, une catégorie « action-type » regroupant des attributs de types d'actions ;
— il définit comme données, c'est-à-dire comme valeurs possibles des catégories d'attributs spécifiées par les métadonnées :
  - pour la catégorie « role », les valeurs « admin » (administrateur) et « employee » (employé) ;
  - pour la catégorie « id », la valeur « vm0 »
  - pour la catégorie « action-type», la valeur « vm-action »
— il définit comme métarègle, une métarègle identifiant les catégories d'attributs « role », « id » et « action-type » ;
— il définit comme règle de contrôle d'accès pour prendre une décision d'autoriser ou de refuser un accès, la règle suivante : « si la catégorie « role » est « admin », la ressource requise est identifiée par « vm0 » et la catégorie « action-type » est « vm-action » alors l'instruction est « accès accepté » ». Cette règle fournit une instruction d'autorisation de l'accès ;
— enfin, il assigne les valeurs suivantes à chaque entité définie dans le périmètre du modèle de contrôle d'accès :
  - à l'utilisateur user0, la valeur « admin » de la catégorie « role » ;
  - à l'utilisateur user1, la valeur « employee » de la catégorie « role » ;
  - à l'objet vm0, la valeur « vm0 » de la catégorie « id » ;

- à l'action start, la valeur « vm-action » de la catégorie « action-type » ; et
- à l'action stop, la valeur « vm-action » de la catégorie « action-type ».

Ainsi, dans ce modèle RBAC et la politique de contrôle d'accès créés par le client CLn à partir du méta-modèle META, seul l'utilisateur user0 qui a le rôle d'administrateur peut démarrer ou arrêter la machine virtuelle vm0. L'utilisateur user1 qui a le rôle d'employé ne peut pas accéder à la machine virtuelle vm0.

On considère ensuite que le client CLn instancie le méta-modèle META de la façon suivante pour créer un premier modèle de contrôle d'accès secondaire « Session » de type session :

— il définit comme périmètre du modèle Session les entités suivantes :
  - pour les sujets, deux utilisateurs « user0 » et « user1 » ;
  - pour les objets, deux rôles « admin » (administrateur) et « employee » (employé) ;
  - pour les actions, une action « activate » d'activation de rôle et une action « desactivate » de désactivation de rôle. ;
— il définit comme métadonnées les catégories d'attributs suivantes :
  - pour les sujets, une catégorie « subjectid» regroupant des attributs de type sujet ;
  - pour les objets, une catégorie « rôle » regroupant des attributs de type rôle;
  - pour les actions, une catégorie « session-action » regroupant des attributs de type action ;
— il définit comme données, c'est-à-dire comme valeurs possibles des catégories d'attributs spécifiées par les métadonnées :
  - pour la catégorie « subjectid», les valeurs user0 et user1 ;
  - pour la catégorie « rôle », les valeurs « admin » (administrateur) et « employee » (employé) ;
  - pour la catégorie « session-action », les valeurs « activate » et « desactivate »
— il définit comme métarègle, une métarègle identifiant les catégories d'attributs « subjectid », « role » et « session-action » ;
— il définit une première règle suivante : « si la catégorie « subjectid » est « user0», le rôle est « admin » (administrateur) et la catégorie « session-action» est « activate» alors l'instruction est d'ajouter le rôle pour l'utilisateur dans la requête et d'envoyer la requête à la politique primaire RBAC. Cette règle fournit une instruction de mise à jour d'au moins un attribut de la requête de contrôle d'accès et une instruction de redirection d'une requête de contrôle d'accès vers la politique primaire RBAC ;
— il définit une deuxième règle suivante : « si la catégorie « subjectid » est « user1», le rôle est « employee » (employé) et la catégorie « session-action» est « desactivate» alors l'instruction est de retirer le rôle pour l'utilisateur dans la requête et d'envoyer la requête à la politique primaire RBAC. Cette règle fournit une instruction de mise à jour d'au moins un attribut de la

requête de contrôle d'accès et une instruction de redirection d'une requête de contrôle d'accès vers la politique primaire RBAC ;

— enfin, il assigne les valeurs suivantes à chaque entité définie dans le périmètre du modèle de contrôle d'accès :

  - à l'utilisateur user0, la valeur user0 de la catégorie SubjectID ;
  - à l'utilisateur user1, la valeur user1 de la catégorie SubjectID ;
  - à l'objet admin, la valeur « admin» de la catégorie « rôle » ;
  - à l'objet employee, la valeur « employee» de la catégorie « rôle » ;
  - à l'action activate, la valeur « activate» de la catégorie « session-action » ; et
  - à l'action desactivate, la valeur « desactivate» de la catégorie « session-action ».

Ainsi, ce modèle Session et la politique de contrôle d'accès créés par le client CLn à partir du méta-modèle META permettent d'activer et de désactiver temporairement le rôle de l'utilisateur.

On considère enfin que le client CLn instancie le méta-modèle META de la façon suivante pour créer un deuxième modèle de contrôle d'accès secondaire « Delegation » de type délégation:

— il définit comme périmètre du modèle Session les entités suivantes :

  - pour les sujets, l'utilisateur « user0 » ;
  - pour les objets, le rôle « user1 » ;
  - pour les actions, une action « delegate» de délégation de rôle ;

— il définit comme métadonnées les catégories d'attributs suivantes :

  - pour les sujets, une catégorie « subjectid» regroupant des attributs de type sujet ;
  - pour les objets, une catégorie « delegated » regroupant des attributs de type rôle;
  - pour les actions, une catégorie « delegation-action » regroupant des attributs de type action ;

— il définit comme données, c'est-à-dire comme valeurs possibles des catégories d'attributs spécifiées par les métadonnées :

  - pour la catégorie « subjectid», la valeur user0 ;
  - pour la catégorie « delegated », la valeur « user1 » ;
  - pour la catégorie « delegation-action », la valeur « delegate » ;

— il définit comme métarègle, une métarègle identifiant les catégories d'attributs « subjectid », « delegated » et « delegated-action » ;

— il définit une règle suivante : « si la catégorie « subjectid » est « user0», la catégorie « delegated » est « user1 » et la catégorie « delegation-action» est « delegate» alors l'instruction est d'ajouter le rôle de user0 pour l'utilisateur user1 dans la requête et d'envoyer la requête à la politique primaire RBAC. Cette règle fournit une instruction de mise à jour des paramètres de la requête de contrôle d'accès et une instruction de redirection d'une requête de contrôle d'accès vers la politique primaire RBAC ;

— enfin, il assigne les valeurs suivantes à chaque entité définie dans le périmètre du modèle de contrôle d'accès :

- à l'utilisateur user0, la valeur user0 de la catégorie SubjectID ;
- à l'utilisateur user1, la valeur user1 de la catégorie SubjectID ;
- à l'action delegate, la valeur delegate de la catégorie « delegation-action».

Ainsi, ce modèle Delegation et la politique de contrôle d'accès créés par le client CLn à partir du méta-modèle META permettent d'établir temporairement une relation de confiance entre deux utilisateurs, le premier utilisateur délégant temporairement son rôle au deuxième utilisateur.

Bien entendu, ces exemples ne sont donnés qu'à titre illustratif et d'autres modèles de contrôle d'accès peuvent être créés par le client CLn à partir du méta-modèle META comme mentionné précédemment.

Le modèle primaire de contrôle d'accès ACMPn et la politique primaire de contrôle d'accès ACPPn définis par le module de définition 3B du dispositif 3-n constituent une instance du méta-modèle META au sens de l'invention. De même, chaque modèle secondaire de contrôle d'accès ACMSn et la politique secondaire de contrôle d'accès ACPSn associée définis par le module de définition 3B du dispositif 3-n constituent une instance du méta-modèle META au sens de l'invention. Ils sont fournis par le module de fourniture 3C du dispositif 3-n via l'interface 9 au système informatique en nuage 2 (étape E40). Ils sont reçus par son module de réception 2B (intégré dans le module XACML PAP du système informatique en nuage 2) et stockés dans sa mémoire non volatile 7 par exemple (dans les modules PIP et PR définis par l'architecture XACML décrits précédemment).

Dès lors, le système informatique en nuage 2 est apte à appliquer, par l'intermédiaire de son module de sécurité 2C (intégré dans son module XACML PDP), les politiques primaire et secondaire(s) de contrôle d'accès ACPPn, ACPSn définies par le client CLn à toute requête provenant d'un utilisateur du client CLn visant à accéder à une ressource choisie parmi les ressources Rn allouées au client CLn (étape E50). Le module de sécurité 2C s'appuie à cet effet sur les modules logiciels PIP et PR décrits précédemment de l'architecture XACML.

Le système informatique en nuage 2 procède de la même façon préférentiellement pour chacun de ses clients CLn, n=1,...,N. De cette sorte il peut appliquer pour chacun de ses clients une politique de contrôle d'accès spécifiée par celui-ci et propre à celui-ci.

En référence à la figure 6, nous allons maintenant décrire plus un exemple de mise en œuvre d'un chaînage de politiques de sécurité. Dans cet exemple, on considère que le PDP définit la politique primaire de contrôle d'accès de type RBAC et les deux politiques secondaires de contrôle d'accès de type Session et de type Delegation décrites précédemment.

On considère dans cet exemple que le PEP envoie au PDP, au cours d'une étape F1, une requête par laquelle l'utilisateur user1 de type « employee » demande à démarrer une ressource virtuelle vm0.

La politique primaire de contrôle d'accès de type RBAC reçoit la requête du PEP et y insère les attributs {sujet, objet, action} :

- pour le sujet, le rôle de user1 à savoir « employee » ;
- pour l'objet, l'identifiant vm0 de le ressource virtuelle concernée ;
- pour l'action, la valeur « start ».

La politique primaire RBAC vérifie alors (étape F2) sur la base de ses propres règles si l'utilisateur user1 a l'autorisation de démarrer la ressource virtuelle vm0. Si cette action était autorisée, le PDB renverrait une réponse positive au PEP (étape F3).

Mais dans cet exemple, la politique de contrôle d'accès RBAC refuse le démarrage de la machine virtuelle vm0 par l'utilisateur user1 car pour user1, la valeur « employee » a été assignée dans le périmètre du modèle de contrôle d'accès et conformément à la règle de contrôle d'accès définie, l'instruction est « accès accepté » uniquement si la catégorie « role » est « admin ». La requête est par conséquent transférée (étape F4) à la première politique secondaire, à savoir, la politique Session.

La politique Session vérifie (étape F5) si le rôle « admin » a été activé pour l'utilisateur user1. Si c'est le cas, par application des règles de cette politique, la requête est modifiée en y retirant le rôle « employee » et en y ajoutant le rôle « admin » (étape F6), puis redirigée (étape F7) vers la politique primaire de contrôle d'accès de type RBAC.

La politique primaire de contrôle d'accès RBAC vérifie (étape F8) sur la base de la requête d'accès modifiée si l'autorisation peut maintenant être donnée à l'utilisateur user1 de démarrer la machine virtuelle vm0. Conformément à la règle de cette politique, si l'action de délégation a été activée, la requête est modifiée (étape F10) pour remplacer la valeur de l'attribut « user1 » par « user0 » de sorte à ce que user0 délègue temporairement ses droits à user1. La requête mise à jour est redirigée (étape F11) vers la politique primaire RBAC qui peut finalement autoriser ou non le démarrage de la machine virtuelle vm0 par user1 selon les droits attribués à user0.

Dans le mode de réalisation décrit précédemment, les modèles primaire et secondaire(s) de contrôle d'accès et les politiques primaire et secondaire(s) de contrôle d'accès sont obtenus par instanciations d'un même meta-modèle.

L'invention n'est cependant pas limitée à cette caractéristique, les modèles primaire et secondaire(s) de contrôle d'accès et les politiques primaire et secondaire(s) de contrôle d'accès peuvent être obtenus ou définis indépendamment les uns des autres, par instanciations de meta-modèles différents, ou directement, sans passer par un méta-modèle.

Dans le mode de réalisation décrit précédemment, la politique primaire de contrôle d'accès est de type RBAC et les politiques secondaires de contrôle d'accès sont de type Session et Delegation à savoir des caractéristiques avancées au sens de RBAC.

Il ne s'agit que d'un exemple, car comme dit précédemment l'invention ne pose aucune limite quant aux types des politiques primaire et secondaire(s) de contrôle d'accès. La

politique primaire de contrôle d'accès peut aussi être une caractéristique avancée au sens de RBAC par exemple de type session ou délégation et la ou les politiques secondaires de sécurité peuvent être de type RBAC, OrBAC, ACL, DTE, ABAC, MLS.

REVENDICATIONS

1. Procédé de gestion d'un système informatique (2), apte à allouer dynamiquement à une pluralité de clients (CL1,...,CLN) des ressources informatiques et réseaux (RESS), chaque client (CLn) étant associé à au moins un utilisateur susceptible d'accéder aux ressources informatiques et réseaux allouées au client par le système informatique, ledit procédé comprenant, pour au moins un client du système informatique :

— une étape de réception (E40), en provenance dudit client, d'un modèle primaire de contrôle d'accès et d'une politique primaire de contrôle d'accès basée sur ce modèle primaire de contrôle d'accès ;

— une étape de réception (E45), en provenance dudit client, d'au moins un modèle secondaire de contrôle d'accès et d'une politique secondaire de contrôle d'accès basée sur ce modèle secondaire de contrôle d'accès, ladite politique secondaire pouvant être mise en œuvre par ladite politique primaire de contrôle d'accès ; et

— une étape d'application (E50) desdites politiques primaire et secondaire de contrôle d'accès à au moins une requête d'accès émise par ledit client pour contrôler un accès d'un utilisateur du client à au moins une ressource allouée au client par le système informatique .

2. Procédé de gestion d'un système informatique (2) selon la revendication 1, ledit procédé étant caractérisé en ce qu'il comporte :

— une étape de fourniture (E20), audit client, d'un méta-modèle (META) comprenant une pluralité d'éléments permettant de définir un modèle de contrôle d'accès et une politique de contrôle d'accès pour le client basée sur ce modèle ; en ce que

— ledit modèle primaire de contrôle d'accès et ladite politique primaire de contrôle d'accès sont définis par une première instance dudit méta-modèle ; et en ce que

— ledit au moins un modèle secondaire de contrôle d'accès et ladite politique secondaire de contrôle d'accès basée sur ce modèle sont définis par une deuxième instance dudit méta-modèle.

3. Procédé de gestion selon la revendication 2 dans lequel la pluralité d'éléments du méta-modèle comprend :

— un périmètre du modèle de contrôle d'accès définissant une pluralité d'entités impliquées dans la politique de contrôle d'accès du client ;

— des métadonnées définissant pour chaque entité au moins une catégorie d'attributs associée à cette entité ;

— des données définissant des valeurs possibles pour chaque catégorie d'attributs définie par les métadonnées ;

— au moins une métarègle identifiant une ou plusieurs catégories d'attributs définies par les métadonnées et utilisées pour fournir au moins une instruction conforme à la politique de contrôle d'accès du client ;

— au moins une règle de contrôle d'accès basée sur ladite au moins une métarègle et fournissant une instruction conforme à la politique de contrôle d'accès du client ; et

— un ensemble de valeurs assignées par le client à chaque entité définie pour ce client dans le périmètre du modèle de contrôle d'accès, pour chaque catégorie d'attributs associée à cette entité et comprise dans une métarègle, lesdites valeurs assignées étant choisies parmi les données,

— ladite instruction comprenant :

— une autorisation ou un refus d'un accès à une ressource déterminée allouée au client par le système informatique ; ou

— une mise à jour d'au moins un attribut de ladite requête d'accès et de redirection de ladite requête d'accès mise à jour vers une politique de contrôle d'accès.

4. Procédé selon la revendication 3 dans lequel ladite pluralité d'entités comprend au moins un sujet, et/ou au moins un objet, et/ou au moins une action.

5 Procédé selon la revendication 3 ou 4 dans lequel au moins une catégorie d'attributs définie pour une entité est choisie parmi :

— un niveau de sécurité ;

— un rôle ;

— un type ; et

— un domaine.

6. Procédé mis en œuvre par un client pour définir des politiques de contrôle d'accès (CL1,...,CLN) dans un système informatique (2) apte à allouer dynamiquement à une pluralité de clients (CL1,...,CLN) des ressources informatiques et réseaux (RESS), chaque client étant associé à au moins un utilisateur susceptible d'accéder aux ressources informatiques et réseaux allouées au client par le système informatique , ledit procédé comprenant :

— une étape (E30) de définition d'un modèle primaire de contrôle d'accès et d'une politique primaire de contrôle d'accès basée sur ce modèle de contrôle d'accès pour ledit client ;

— une étape (E35) de définition d'au moins un modèle secondaire de contrôle d'accès et d'au moins une politique secondaire de contrôle d'accès basée sur ce modèle secondaire de contrôle d'accès pour ledit client, ladite politique secondaire de contrôle d'accès pouvant être mise en œuvre par ladite politique primaire de contrôle d'accès ; et

— une étape de fourniture (E40) desdits modèles primaire et secondaire de contrôle d'accès et desdites politiques primaire et secondaire de de contrôle d'accès audit système informatique,

lesdites politiques étant destinées à être appliquées aux requêtes d'accès émises par ledit client pour contrôler un accès d'un utilisateur dudit client à au moins une desdites ressources.

7. Procédé de définition de politiques de contrôle d'accès selon la revendication 6, ledit procédé étant caractérisé en ce qu'il comporte :

— une étape d'obtention (E20) d'un méta-modèle (META) fourni par le système informatique et comprenant une pluralité d'éléments permettant de définir un modèle de contrôle d'accès et une politique de contrôle d'accès pour le client ; et en ce que

— ledit modèle primaire de contrôle d'accès et ladite politique primaire de contrôle d'accès sont définis par une première instance dudit méta-modèle ; et en ce que

— ledit au moins un modèle secondaire de contrôle d'accès et ladite politique secondaire de contrôle d'accès basée sur ce modèle sont définis par une deuxième instance dudit méta-modèle.

8. Procédé de définition de politiques de contrôle d'accès selon la revendication 7 dans lequel la pluralité d'éléments du méta-modèle comprend :

— un périmètre du modèle de contrôle d'accès définissant une pluralité d'entités impliquées dans la politique de contrôle d'accès du client ;

— des métadonnées définissant pour chaque entité au moins une catégorie d'attributs associée à cette entité ;

— des données définissant des valeurs possibles pour chaque catégorie d'attributs définie par les métadonnées ;

— au moins une métarègle identifiant au moins une catégorie d'attributs définie par les métadonnées et utilisée pour fournir au moins une instruction conforme à la politique de contrôle d'accès du client ;

— au moins une règle de contrôle d'accès définissant ladite au moins une métarègle et fournissant une instruction conforme à la politique de contrôle d'accès du client ; et

— un ensemble de valeurs assignées par le client à chaque entité définie pour ce client dans le périmètre du modèle de contrôle d'accès, pour chaque catégorie d'attributs associée à cette entité et comprise dans une métarègle, lesdites valeurs assignées étant choisies parmi les données,

— ladite instruction comprenant :

— une autorisation ou un refus d'un accès à une ressource déterminée allouée au client par le système informatique ; ou

— une mise à jour d'au moins un attribut de ladite requête d'accès et de redirection de ladite requête d'accès mise à jour vers une politique de contrôle d'accès.

9. Programme d'ordinateur (PROG1,PROG2) comportant des instructions pour l'exécution des étapes du procédé de gestion selon l'une quelconque des revendications 1 à 5 ou du procédé de définition de politiques de contrôle d'accès selon l'une quelconque des revendications 6 à 8 lorsque ledit programme est exécuté par un ordinateur.

10. Système informatique (2) apte à allouer dynamiquement à une pluralité de clients (CL1,...,CLN) des ressources informatiques et réseaux (RESS), chaque client (CLn) étant associé à au moins un utilisateur susceptible d'accéder aux ressources informatiques et réseaux allouées au client par le système informatique , ledit système comprenant :

— un module de réception (2B), apte à recevoir, en provenance dudit client, un modèle primaire de contrôle d'accès et une politique primaire de contrôle d'accès basée sur ce modèle primaire de contrôle d'accès, ledit module de réception étant en outre apte à recevoir en provenance dudit client, au moins un modèle secondaire de contrôle d'accès et une politique secondaire de contrôle d'accès basée sur ce modèle secondaire de contrôle d'accès, ladite politique secondaire pouvant être mise en œuvre par ladite politique primaire de contrôle d'accès ; et

un module de sécurité (2C) configuré pour appliquer lesdites politiques primaire et secondaire de contrôle d'accès à au moins une requête d'accès émise par ledit client pour contrôler un accès d'un utilisateur du client à au moins une ressource allouée au client par le système informatique.

11. Système informatique (2) selon la revendication 10, caractérisé en ce qu'il comporte:

- un module de fourniture (2A), configuré pour fournir audit client, un méta-modèle (META) comprenant une pluralité d'éléments permettant de définir un modèle de contrôle d'accès et une politique de contrôle d'accès pour le client ; en ce que

· ledit modèle primaire de contrôle d'accès et ladite politique primaire de contrôle d'accès sont définis par une première instance dudit méta-modèle ; et en ce que

· ledit au moins un modèle secondaire de contrôle d'accès et ladite politique secondaire de contrôle d'accès basée sur ce modèle sont définis par une deuxième instance dudit méta-modèle.

12. Dispositif (3-1,...,3-N) d'un client (CL1,...,CLN) d'un système informatique (2) apte à allouer dynamiquement à une pluralité de clients des ressources informatiques et réseaux (RESS), chaque client étant associé à au moins un utilisateur susceptible d'accéder aux ressources informatiques et réseaux allouées au client par le système informatique, ledit dispositif comprenant :

— un module de définition (3B) d'un modèle primaire de contrôle d'accès et d'une politique primaire de contrôle d'accès basée sur ce modèle de contrôle d'accès,

— au moins un module de définition (3B) d'au moins un modèle secondaire de contrôle d'accès et d'une politique secondaire de contrôle d'accès basée sur ce modèle de contrôle d'accès ; et

— un module de fourniture (3C), configuré pour fournir lesdits modèles primaire et secondaire de contrôle d'accès et lesdites politiques primaire et secondaire de contrôle d'accès audit système informatique, lesdites politiques étant destinées à être appliquées aux requêtes d'accès émises par ledit client pour contrôler un accès d'un utilisateur dudit client à au moins une desdites ressources.

13. Dispositif selon la revendication 12, ledit dispositif étant caractérisé en ce qu'il comporte :

- un module d'obtention (3A) configuré pour obtenir un méta-modèle (META) fourni par le système informatique et comprenant une pluralité d'éléments permettant de définir un modèle de contrôle d'accès et une politique de contrôle d'accès pour le client ; et en ce que

· ledit modèle primaire de contrôle d'accès et ladite politique primaire de contrôle d'accès sont définis par une première instance dudit méta-modèle ; et en ce que

· ledit au moins un modèle secondaire de contrôle d'accès et ladite politique secondaire de contrôle d'accès basée sur ce modèle sont définis par une deuxième instance dudit méta-modèle.

14. Système (1) comprenant :

— un système informatique (2) selon la revendication 10 ou 11, apte à allouer dynamiquement à une pluralité de clients des ressources informatiques et réseaux, chaque client étant associé à au moins un utilisateur susceptible d'accéder aux ressources informatiques et réseaux allouées au client par le système informatique ; et

— une pluralité de dispositifs des clients (3-1,...,3-N) du système informatique conformes à la revendication 12 ou 13.

15. Fichier informatique (FILE) comprenant des instructions décrivant un méta-modèle comprenant une pluralité d'éléments permettant de définir un modèle de contrôle d'accès et une politique de contrôle d'accès pour un client d'un système informatique apte à allouer dynamiquement à une pluralité de clients des ressources informatiques et réseaux, ladite pluralité d'éléments du méta-modèle comprenant :

— un périmètre du modèle de contrôle d'accès définissant une pluralité d'entités impliquées dans la politique de contrôle d'accès du client ;

— des métadonnées définissant pour chaque entité au moins une catégorie d'attributs associée à cette entité ;

— des données définissant des valeurs possibles pour chaque catégorie d'attributs définie par les métadonnées ;

— au moins une métarègle identifiant au moins une catégorie d'attributs définie par les métadonnées et utilisée pour fournir prendre une instruction conforme à la politique de contrôle d'accès du client ;

— au moins une règle de contrôle d'accès basé sur ladite au moins une métarègle et fournissant une instruction conforme à la politique de contrôle d'accès du client ; et

— un ensemble de valeurs assignées par le client à chaque entité définie pour ce client dans le périmètre du modèle de contrôle d'accès, pour chaque catégorie d'attributs associée à cette entité et comprise dans une métarègle, lesdites valeurs assignées étant choisies parmi les données,

— ladite instruction comprenant :

— une autorisation ou un refus d'un accès à une ressource déterminée allouée au client par le système informatique ; ou

— une mise à jour d'au moins un paramètre d'une requête d'accès émises par ledit client pour accéder à une ressource déterminée allouée au client par le système informatique de redirection de ladite requête mise à jour vers une politique de contrôle d'accès.

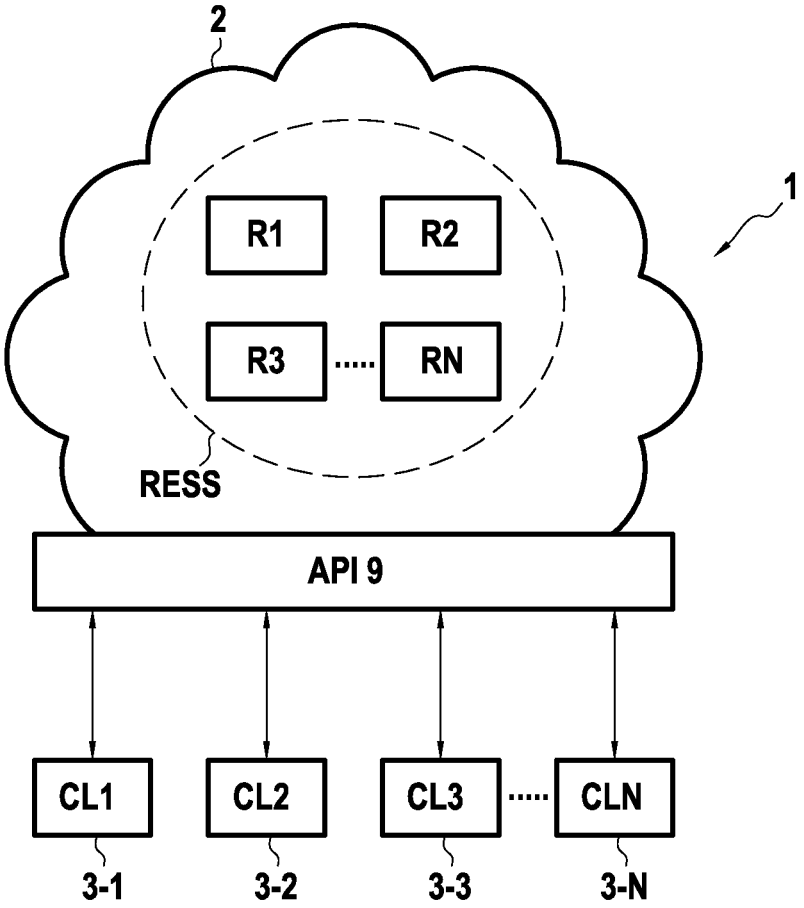


FIG.1

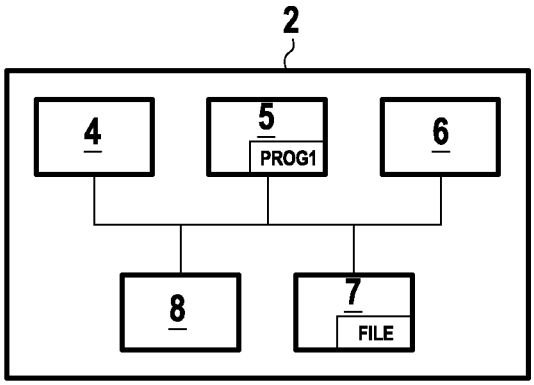


FIG.2A

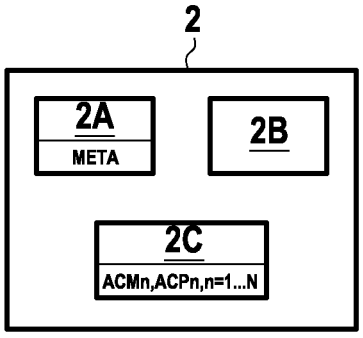


FIG.2B

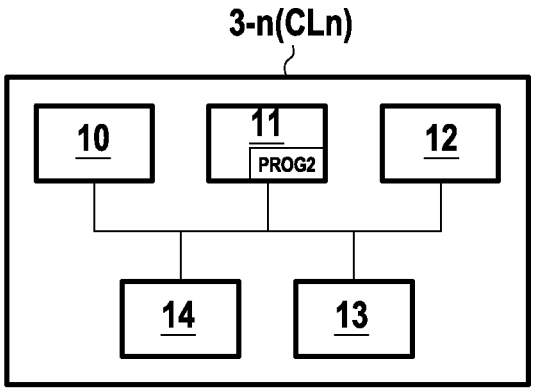


FIG.3A

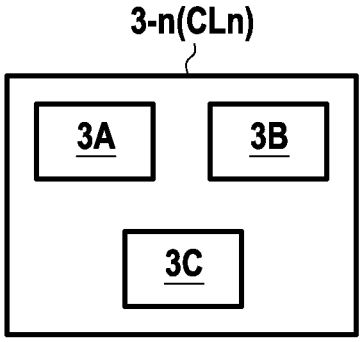


FIG.3B

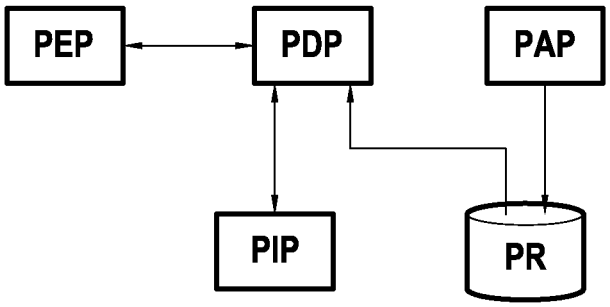


FIG.4

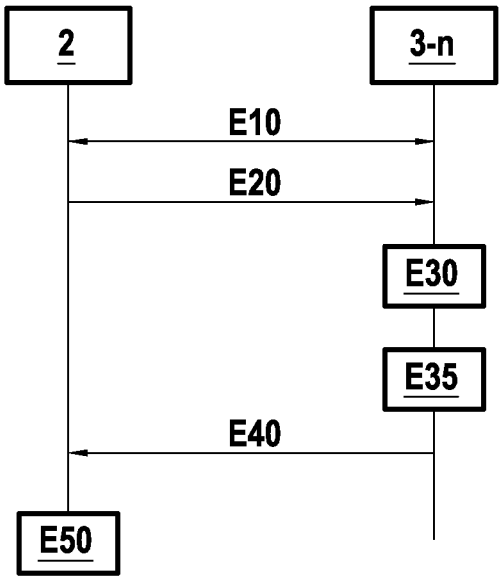


FIG.5

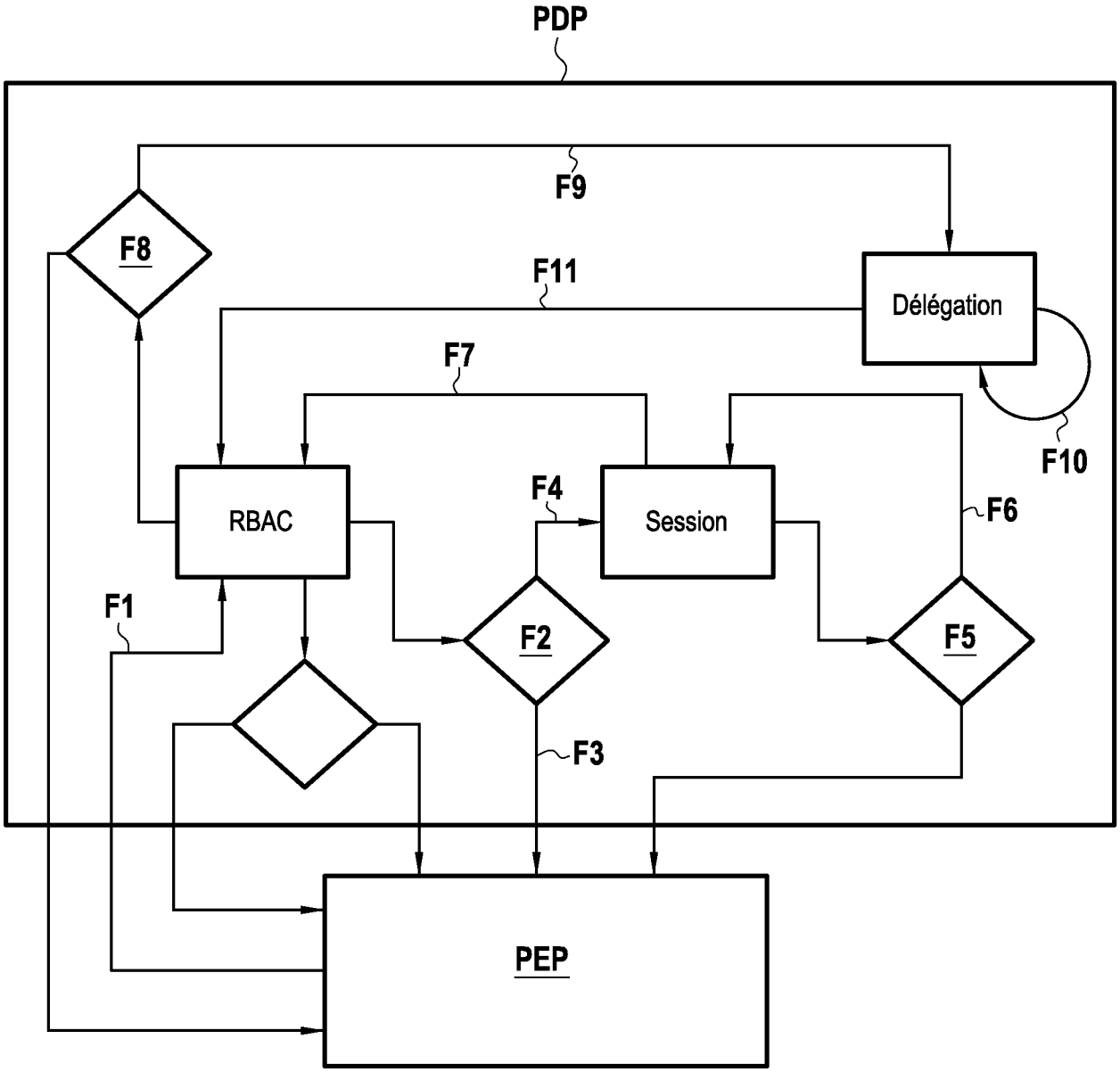

PDP
F9
F8
F11
Délégation
F7
F10
F4
RBAC
Session
F6
F1
F2
F5
F3
PEP

FIG.6

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 840026
FR 1753497

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	US 8 813 174 B1 (KOETEN ROBERT [US] ET AL) 19 août 2014 (2014-08-19) * colonne 7, ligne 7 - colonne 14, ligne 37 * * figure 1 *	1-15	G06F21/62 G06F15/173

X	EP 2 819 052 A1 (ORANGE [FR]) 31 décembre 2014 (2014-12-31)	15	
A	* alinéas [0018], [0019], [0045] * * alinéas [0080] - [0090] * * figure 1 *	1-14	

A	SALIM KHAMADJA ET AL: "Designing flexible access control models for the cloud", SECURITY OF INFORMATION AND NETWORKS, ACM, 2 PENN PLAZA, SUITE 701 NEW YORK NY 10121-0701 USA, 26 novembre 2013 (2013-11-26), pages 225-232, XP058036026, DOI: 10.1145/2523514.2527005 ISBN: 978-1-4503-2498-4 * abrégé * * pages 226-232 *	1-15	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

G06F
H04L

Date d'achèvement de la recherche	Examinateur
13 décembre 2017	Segura, Gustavo

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 1753497 FA 840026

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 13-12-2017
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 8813174 B1	19-08-2014	US 8813174 B1	19-08-2014
		US 8819768 B1	26-08-2014
		US 9087189 B1	21-07-2015
		US 9450945 B1	20-09-2016
		US 9749331 B1	29-08-2017
EP 2819052 A1	31-12-2014	EP 2819052 A1	31-12-2014
		FR 3007551 A1	26-12-2014
		US 2014380048 A1	25-12-2014

EPO FORM P0465