(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
4 octobre 2007 (04.10.2007)

PCT

(10) Numéro de publication internationale
WO 2007/110545 A2

(51) Classification internationale des brevets :
G06F 21/20 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2007/051016

(22) Date de dépôt international : 26 mars 2007 (26.03.2007)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
06 51072 28 mars 2006 (28.03.2006) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6 Place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BOURON, Thierry** [FR/FR]; 2, Route de Gourdon, F-06620 Le Bar Sur Loup (FR). **ANTOINE, Gilles** [FR/FR]; 3, Rue des Bergeronnettes, F-91220 Bretigny-sur-orge (FR).

(74) Mandataire : **FRANCE TELECOM/FTR & D/PIV/Brevets**; Catherine CASPAR, 38-40 Rue du Général Leclerc, F-92794 Issy Les Moulineaux Cedex 9 (FR).

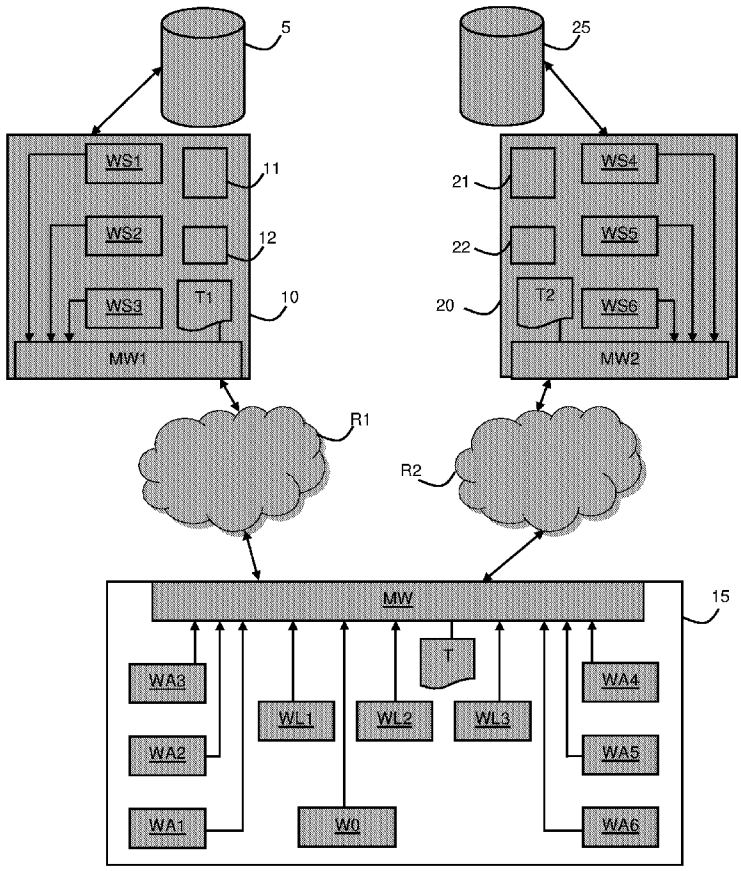
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS,

[Suite sur la page suivante]

WO 2007/110545 A2

(54) Title: METHOD AND SYSTEM FOR CONTROLLING ACCESS TO THE DATA IN A DATABASE

(54) Titre : PROCEDE ET SYSTEME DE CONTROLE D'ACCES AUX DONNEES D'UNE BASE DE DONNEES



traitement (WS1 -WS6)

(57) Abstract: The system comprises a program intended to execute a predefined processing operation, the program (WO) being able to trigger, when said operation is executed, the retransmission of at least one request to activate at least one processing module (WS1 - WS6) designed to execute at least one processing operation on at least one part of said data. The system also comprises control means intended to determine whether the program (WO) originating the activation request is authorized to activate said processing module (WS1 - WS6) and intended to provoke, in case of authorization, the execution of said at least one processing operation.

(57) Abrégé : Le système comprend un programme destiné à exécuter un processus prédéfini de traitement, le programme (WO) étant apte à déclencher lors de l'exécution dudit processus rémission d'au moins une requête d'activation d'au moins un module de traitement (WS1 - WS6) conçu pour exécuter au moins une opération de traitement sur au moins une partie desdites données. Le système comprend en outre des moyens de contrôle destinés à déterminer si le programme (WO) à l'origine de la requête d'activation est autorisé à activer ledit module de

[Suite sur la page suivante]

LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* **:** ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

et destinés à provoquer, en cas d'autorisation, l'exécution de ladite au moins une opération de traitement.

Procédé et système de contrôle d'accès aux données d'une base de données

L'invention concerne un procédé et un système de traitement des données d'une base de données, permettant le contrôle d'accès aux données de la base de données.

Dans le domaine des bases de données, il est connu d'utiliser des serveurs de traitement de données qui sont capables d'exécuter un processus de traitement sur tout ou partie des données de la base de données après interrogation de cette base.

Dans les systèmes de gestion de bases de données actuels, les règles définissant les droits d'accès aux données d'un système d'information donnent des droits en lecture et/ou écriture à des entités données (entreprises, utilisateurs, etc…) en fonction de niveaux d'autorisation et de profils associés à ces niveaux. Il en résulte une limitation forte des possibilités d'accès aux données du système d'information, une entité n'ayant accès qu'à la partie des données pour laquelle elle possède un droit de lecture ou d'écriture.

Par exemple, lorsqu'une entité n'est pas intéressée par obtenir les données confidentielles telles que stockées dans la base de données, mais par une information plus globale par rapport à ces données, comme par exemple la moyenne ou l'écart type d'une liste de valeurs stockées dans la base de données, information qui elle n'est pas forcément confidentielle, il peut être utile de disposer d'un système qui soit capable de contrôler les droits d'accès aux données en fonction des opérations de traitements effectuées sur ces données.

Les systèmes actuels de gestion de base de données ne sont pas capables de mettre en œuvre un tel contrôle. Il est donc nécessaire de compléter le système de gestion de base de données par le développement d'une application spécifique qui soit apte à mettre en œuvre un tel contrôle. Une telle application spécifique doit, d'une part, s'adapter aux besoins et aux moyens d'informatiques des entités interrogeant la base de données, et d'autre part, être capable de s'interfacer avec le système de gestion de bases de données existant. Un tel développement peut en outre s'avérer coûteux. En outre, il n'est pas simple de vérifier que cette application spécifique exécute bel et bien, et uniquement, un processus particulier autorisé. En effet une telle vérification doit s'effectuer sur le code source de l'application, et par un processus manuel de comparaison entre le code source et les spécifications fonctionnelles de l'application.

Il existe donc un besoin pour un dispositif de traitement des données d'une ou plusieurs bases de données, permettant de garantir simplement et à moindre coût que l'accès aux données du système d'information se fait dans le cadre d'un processus de traitement prédéfini. L'invention vient répondre à ce besoin.

L'invention a pour objet un système de traitement de données comprenant un serveur de médiation entre une première entité dite entité cliente et une deuxième entité dite entité fournisseur,

ledit serveur comprenant des moyens d'exécution de programme pour exécuter, sur requête en provenance de l'entité cliente, un programme mettant en œuvre un processus prédéfini de traitement,

ledit programme étant apte à déclencher, lors de l'exécution dudit processus, une émission à travers une liaison de communication d'au moins une requête d'activation d'au moins un module de traitement d'un serveur de l'entité fournisseur afin d'exécuter au moins une opération de traitement sur au moins une partie des données d'au moins une base de données accessible via le serveur de l'entité fournisseur,

le système comprenant des moyens de contrôle conçus pour, en cas d'authentification dudit programme, déterminer si ledit programme est autorisé à activer ledit module de traitement et pour, en cas d'absence autorisation, inhiber l'exécution de ladite au moins une opération de traitement.

Le dispositif selon l'invention permet d'autoriser l'accès à des données d'une base de données dans un cadre limité à un processus de traitement prédéfini, qui est celui mis en œuvre par le programme de traitement autorisé, et de contrôler l'exécution du processus lors de l'activation des modules de traitement.

Le dispositif permet ainsi d'offrir à une entité une visibilité sélective des données d'une base de données. L'autorisation d'accès aux données de la base est accordée pour un usage donné, c'est-à-dire pour l'exécution d'un processus de traitement donné. Seul ce processus est considéré pour la détermination de l'autorisation d'accès et pas seulement la nature des données. De la sorte, seule importe l'utilisation qui est faite des données, et non pas les données utilisées.

Selon un mode de réalisation particulier, le système selon l'invention comprend des moyens d'authentification dudit programme, lesdits moyens de contrôle étant destinés à n'être activés qu'en cas d'authentification.

La sécurité du système est renforcée du fait que seul un programme préalablement authentifié est susceptible d'être autorisé à invoquer un module de traitement.

Selon un mode de réalisation particulier, le serveur de médiation comprend des moyens de génération logicielle aptes à générer ledit programme à partir d'une description en langage formel dudit processus, ladite description étant définie par référence à au moins un module choisi parmi une pluralité de modules de traitement du serveur de l'entité fournisseur activables indépendamment les uns des autres.

La description formelle permet, par référence aux modules de traitement, de définir les opérations de traitement sur les entités, ainsi que les données sur lesquelles ces opérations vont être effectuées et les données en résultant. Elle détermine la manière dont deux entités vont pouvoir échanger des données résultant des traitements ou des accès effectués sur les données de leurs bases de données.

Ainsi le contexte d'usage dans lequel une entité est autorisée à accéder à des données, est entièrement déterminé par la description d'un processus de traitement de données,

description utilisant un langage formel de description de processus.

Le dispositif est ainsi facilement adaptable à l'évolution des besoins des entités interrogeant le système d'information, par modification de la description du processus et génération automatique du module logiciel mettant en œuvre le processus décrit.

Selon un mode de réalisation particulier, le système selon l'invention comprend des moyens de détection d'une occurrence d'au moins un événement prédéfini, occurrence à laquelle est subordonnée l'exécution dudit processus.

Il est ainsi possible de programmer très précisément le moment du déclenchement de l'exécution du processus. Cela permet d'automatiser complètement un processus de coopération entre deux entités, notamment lorsqu'il s'agit d'un processus itératif, ou à exécuter de manière périodique. Le programme est dans ce cas préférentiellement réinitialisé après chaque exécution, afin d'entrer dans la phase de détection déterminant l'exécution suivante.

Le module de traitement mettant en œuvre l'opération de traitement est choisi parmi une pluralité de modules de traitement activables indépendamment les uns des autres. Par la présence de modules logiciels autonomes, activables indépendamment les uns des autres, il est ainsi possible de définir, opération par opération ou groupe d'opérations par groupe d'opérations, les conditions d'accès aux données de la base.

De préférence, le serveur de médiation comprend des moyens pour vérifier si une entité est autorisée à invoquer l'exécution dudit programme. De cette manière, le serveur de médiation jour le rôle de tiers de confiance entre l'entité cliente et l'entité fournisseur.

L'ensemble du processus de coopération entre ces deux entités est contrôlé au niveau du serveur de médiation, notamment à travers l'emploi d'un programme authentifiable, issu d'une description validée par les entités coopérant. Le serveur de médiation joue le rôle de médiateur en ce que l'exécution du processus de coopération nécessite l'intervention du serveur de médiation, et en ce que, d'une part il reçoit les requêtes en provenance de l'entité cliente, d'autre part active, par requête émise à destination du serveur de l'entité fournisseur, les différents modules de traitements permettant l'accès aux données d'une base de l'entité fournisseur.

L'invention a également pour objet un serveur de médiation entre une entité cliente et une entité fournisseur,

ledit serveur de médiation comprenant des moyens d'exécution de programme pour exécuter, sur requête en provenance de l'entité cliente, un programme mettant en œuvre un processus prédéfini de traitement,

ledit programme étant apte à déclencher, lors de l'exécution dudit processus, une émission à travers une liaison de communication d'au moins une requête d'activation d'au moins un module de traitement du serveur de l'entité fournisseur afin d'exécuter au moins une opération de traitement sur au moins une partie des données d'au moins une base de

données accessible via le serveur de l'entité fournisseur,

ledit serveur de médiation comprenant des moyens de contrôle conçus pour, en cas d'authentification dudit programme, déterminer si ledit programme est autorisé à activer ledit module de traitement et pour, en cas d'absence autorisation, inhiber l'exécution de ladite au moins une opération de traitement.

L'invention a également pour objet un serveur de traitement de données accédant à au moins une base de données,

ledit serveur de traitement étant apte à communiquer à travers une liaison de communication avec un serveur de médiation entre une entité cliente et une entité fournisseur,

ledit serveur de traitement comprenant au moins un module de traitement, conçu pour exécuter au moins une opération de traitement sur au moins une partie desdites données de ladite base de données et activable par requête à partir du serveur de médiation au moyen d'un programme mettant en œuvre un processus prédéfini de traitement,

ledit serveur de traitement comprenant des moyens de contrôle pour, suite à l'émission par ledit programme d'une requête d'activation d'un module de traitement, vérifier si ledit programme est autorisé à activer ledit module de traitement et pour, en cas d'absence autorisation, inhiber l'exécution de ladite au moins une opération de traitement.

Corrélativement au système selon l'invention, l'invention a pour objet un procédé de traitement de données incluses dans d'au moins une base de données, ledit procédé comprenant au moins,

- une étape d'exécution par un serveur de médiation d'un programme mettant en œuvre un processus prédéfini de traitement, ladite étape d'exécution étant destinée à être exécutée suite à la réception par le serveur de médiation d'une requête en provenance d'une entité cliente,
- une étape de déclenchement par ledit programme, lors de l'exécution dudit processus, de l'émission à travers une liaison de communication d'au moins une requête d'activation d'au moins un module de traitement du serveur de traitement afin d'exécuter au moins une opération de traitement sur au moins une partie desdites données,
- une étape de contrôle pour déterminer si le programme à l'origine de la requête d'activation est autorisé à activer ledit module de traitement,
- une étape de déclenchement de l'exécution de ladite au moins une opération de traitement, ladite étape de déclenchement n'étant exécutée qu'en cas d'autorisation.

Ce procédé comprend de préférence une étape d'authentification du programme à l'origine de la requête d'activation, ladite étape de contrôle n'étant exécutée qu'en cas d'authentification.

D'autres buts, caractéristiques et avantages de l'invention apparaîtront à travers la description qui va suivre, donnée uniquement à titre d'exemple non limitatif, et faite par référence aux dessins annexés sur lesquels:

- la figure 1 est une représentation schématique d'un système incorporant le dispositif selon l'invention,

- la figure 2 est un exemple de description de processus mis en œuvre par le dispositif selon l'invention,

- la figure 3 est un organigramme simplifié du procédé selon l'invention.

Le fonctionnement du dispositif selon l'invention est décrit dans un contexte industriel où deux entités E1 et E2 (deux entreprises) sont amenées à coopérer.

L'entité E1 est un fournisseur de composants de base pour la fabrication de produits manufacturés. L'entité E2 est un client de l'entité E1 et s'approvisionne en composants auprès de l'entité E1. L'entité E2 assure la fabrication de produits manufacturés et la distribution des produits manufacturés qu'elle produit.

Le système représenté à la figure 1 comprend:

- une base de données 5,

- un serveur 10, représentant le système d'information 10 de l'entité E1, accédant à la base de données 5,

- une base de données 25,

- un serveur 20, représentant le système d'information 20 de l'entité E2, accédant à la base de données 25,

- un serveur 15 mettant en œuvre le dispositif selon l'invention et apte à communiquer avec le serveur 10 via un réseau R1 de communication et avec le serveur 20 via un réseau R2 de communication, les deux réseaux R1 et R2 pouvant être confondus.

Le serveur 10 comprend un module logiciel 12 de gestion de la base de données 5 ainsi qu'un module logiciel 11 dédié à une activité de l'entité E1, par exemple un logiciel de régulation de la production.

De manière symétrique, le serveur 20 comprend un module logiciel 22 de gestion de la base de données 25 ainsi qu'un module logiciel 21 dédié à une activité de l'entité E2, par exemple un logiciel d'établissement de commandes de produits.

Dans la base de données 5 sont stockées notamment des informations sur les quantités de composants disponibles dans les stocks de l'entité E1. Dans la base de données 25 sont stockées notamment des informations sur les quantités de composants et de produits manufacturés disponibles dans ses stocks et des informations sur les quantités de produits commandés à l'entité E2.

Le serveur 15 représenté à la figure 1 comprend des moyens d'exécution de programme ainsi qu'un ensemble de modules logiciels WA1 à WA6, WL1 à WL3, et W0. Le système d'information 10 met en œuvre les modules logiciels WS1 à WS3, et

symétriquement, le système d'information 20 met en œuvre les modules logiciels WS4 à WS6. Ces différents modules logiciels coopèrent et communiquent entre eux grâce à un middleware MW, MW1, MW2 qui est mis en œuvre de manière répartie entre le serveur 15 (partie MW du middleware), le système d'information 10 (partie MW1 du middleware) et système d'information 20 (partie MW2 du middleware).

Les modules logiciels WA1, WA2, WA3 sont des modules d'accès aux données du système d'information 10, mettant en œuvre une interface permettant au serveur 15 d'interroger le système d'information 10 et sa base de données 5. Chacun des modules WA1, WA2, WA3 constitue en fait une interface de type API (Application Program Interface) vis-à-vis respectivement des modules logiciels WS1, WS2, WS3, correspondant mis en œuvre dans le système d'information 10. Les modules WS1, WS2, WS3 accèdent à la base de données 5 via le module 12 de gestion de la base de données. En outre ils mettent en œuvre une ou plusieurs fonctions de traitement sur les données auxquelles ils accèdent.

De manière symétrique, les modules logiciels WA4, WA5, WA6 sont des modules d'accès aux données du système d'information 20, mettant en œuvre une interface permettant au serveur 15 d'interroger le système d'information 20 et sa base de données 25. Chacun des modules WA4, WA5, WA6 constitue en fait une interface de type API (Application Program Interface) vis-à-vis respectivement des modules logiciels WS4, WS5, WS6, correspondant mis en œuvre dans le système d'information 20. Les modules WS4, WS5, WS6 accèdent à la base de données 25 via le module 22 de gestion de la base de données. En outre ils mettent en œuvre une ou plusieurs fonctions de traitement sur les données auxquelles ils accèdent.

Le module logiciel W0 est un module de pilotage mettant en œuvre un processus automatisé de traitement de données, processus correspondant à une manière pour les entités E1 et E2 de coopérer à travers leurs systèmes d'informations. Le serveur 15 est susceptible d'exécuter simultanément plusieurs tels module logiciels W0', W0", etc. Cependant pour des raisons de clarté un seul module logiciel W0 a été représenté à la figure 1.

Les modules logiciels WL1, WL2, WL3 sont des modules de traitement de données de base, susceptibles d'être invoqués par le module W0, disponibles par exemple via une librairie de composants logiciels de traitement.

Les différents modules logiciels précités W0, WA1 à WA6, WS1 à WS6, WL0 à WL3, sont des composants logiciels autonomes, activables indépendamment les uns des autres. Ils sont de préférence réalisée sous la forme de composants invocables via un réseau de communication tel Internet, par exemple des services Web (ou "Web Service" selon la dénomination anglo-saxonne). Une description et spécification détaillée de tels composants peuvent être trouvées sur le site Internet http://www.w3.org. Ces composants sont invocables au moyen de requêtes conformes au protocole HTTP (Hypertext Transfert Protocol).

Le middleware MW, MW1, MW2 est mis en œuvre en utilisant un protocole de communication approprié à la communication entre de tels composants, par exemple le

protocole SOAP (Simple Object Access Protocol). Un tel protocole permet l'envoi de messages SOAP entre les composants. Le middleware comprend de préférence des fonctions de sécurité, permettant la mise en œuvre de procédure d'authentification et de contrôle d'accès lors des communications entres les composants, notamment lors de l'invocation d'un composant.

Les messages SOAP pouvant être transportés par le protocole HTTP, les différents modules logiciels précités W0, WA1 à WA6, WS1 à WS6, WL0 à WL3 qui sont exécutés par le serveur 15 ou par un des systèmes d'information 10 ou 20, sont susceptibles être invoqués par message SOAP à partir de n'importe quel terminal ou système disposant d'un logiciel disposant d'une interface d'accès au Web (par exemple un navigateur Web) et accédant via le réseau R1 ou R2 au serveur 15 ou à un des systèmes d'information 10 ou 20.

Le système d'information 20 de l'entité E2 transmet au serveur 15 des requêtes ou messages en vue de l'exécution d'opérations prédéfinies sur les données du système d'information 10 de l'entité E1. Ces opérations peuvent être des traitements mathématiques, et logiques ou de simples interrogations des données du système d'information 10 de l'entité E1. Réciproquement, le système d'information 10 de l'entité E1 peut transmettre au serveur 15 des requêtes ou messages en vue de l'exécution d'opérations prédéfinies sur les données du système d'information 20 de l'entité E2.

La figure 1 montre que le système est bidirectionnel dans la mesure où le serveur 15 peut être utilisé simultanément, d'une part pour l'exécution d'un processus lorsque l'entité E1 envoie au serveur une requête au serveur 15 pour accéder à des données du système d'information de l'entité E2, et d'autre part, pour l'exécution d'un processus lorsque l'entité E2 envoie au serveur une requête au serveur 15 pour accéder à des données du système d'information de l'entité E1.

Les modalités selon lesquelles l'entité E2 est autorisée à accéder aux données du système d'information 10 de l'entité E1 (ou vice versa) sont formalisées au moyen d'une description d'un processus de traitement.

Un tel processus décrit les modalités de coopération entre les systèmes d'information des entités E1 et E2, c'est-à-dire la manière dont le serveur 15 traite de manière automatique les requêtes qu'il reçoit de l'un des systèmes d'information.

Un tel processus comprend:

- une ou plusieurs opérations de traitement sur les données d'un des systèmes d'information 10 ou 20,

- le cas échéant, une ou plusieurs opérations de contrôle nécessaires au contrôle de l'exécution du processus, notamment des opérations de vérification de conditions ou des opérations d'attente d'un événement particulier tel que: réception d'un email, d'un document, d'un SMS, d'un appel téléphonique, etc.

Les conditions à vérifier lors du processus sont par exemple:

- des conditions relatives à des données extraites d'un des systèmes d'information 10 ou 20,

- des conditions relatives à des données résultant d'une opération de traitement précédente,

- des conditions relatives à d'autres données, par exemple la date ou l'heure courante, l'identité de l'émetteur de la requête, ou toute autre donnée accessible par le serveur 15,

- plus généralement, des conditions relatives à un algorithme définissant l'enchaînement des opérations et les conditions dans lesquelles elles s'enchaînent.

Des opérations de vérification de conditions sont par exemple exécutées avant ou après l'exécution d'une opération de traitement. Il en est de même pour les autres opérations d'attente. Une opération d'attente d'un événement prédéfini peut en outre être exécutée au début du processus, de manière à conditionner le début de l'exécution du processus par l'occurrence de cet événement.

Le processus comporte par exemple:

- une première opération O1 de détermination du nombre de produits à commander à l'entité E1 en fonction du nombre de produits dans les stocks de l'entité E1 et du nombre de commandes reçues par l'entité E2,

- une deuxième opération O2 de détermination du nombre produits à commander à d'autres fournisseurs, cette deuxième opération étant exécutée consécutivement à la première opération lorsque deux conditions sont remplies, la première condition étant que le nombre de produits dans les stocks de l'entité E1 est inférieur à un seuil donné, la deuxième condition étant que le nombre de produits dans les stocks de l'entité E1 déterminé lors de la première opération O1 ne permet pas de répondre à toutes les commandes reçues par l'entité E2.

La description formelle de ce processus est réalisée en utilisant un langage formel approprié pour la description de processus, par exemple le langage graphique BPMN (Business Process Management Notation).

Un outil d'édition capable d'éditer une description en langage BPMN est utilisé pour générer la description et ainsi formaliser le processus. Un tel langage permet de définir la manière d'exécuter et d'enchaîner les opérations de traitement mises en œuvre par les composants fournis par la librairie, de définir les flux de données, de définir de nouvelles opérations de traitement.

Un exemple de telle description graphique est présenté à la figure 2, dans le cas d'exemple d'un processus élémentaire d'inventaire de stocks court terme et moyen terme de produits utilisés sous certaines conditions dans un processus d'approvisionnement.

Dans la notation graphique utilisée, le rond avec trait fin désigne l'état initial du processus. Les rectangles avec des bords arrondis désignent des opérations exécutées par

un service Web. Les autres opérations de traitement sont représentées par des rectangles. Les opérations de test sont représentées par des losanges.

Dans l'exemple de processus PROC illustré à la figure 2, la description du processus comprend les éléments suivants:

- une étape S200 correspondant à l'étape d'initialisation du processus;
- une étape S210 de traitement, correspondant à la détermination, par interrogation de la base de données 25 de l'entité E2, du nombre X de composants d'un type T donné qui sont disponibles dans les stocks de l'entité E2;
- une étape S215 de traitement, correspondant à la détermination, par interrogation de la base de données 25 de l'entité E2, du nombre Y de produits manufacturés incorporant le composant du type T qui sont à produire par l'entité E2;
- une étape S220 de traitement, correspondant à la comparaison des résultats obtenus aux étapes S210 et S215 et à la détermination de la quantité Z de composants de type T à commander correspondant à la différence Z=Y-X;
- une étape S225 de vérification d'une condition lors de laquelle on vérifie si la quantité Z de composants calculée à l'étape S220 est non nulle; dans l'affirmative le processus se poursuit à l'étape S230, sinon à l'étape S260;
- une étape S230 de traitement, correspondant à la détermination, par interrogation de la base de données 5 de l'entité E1, du nombre Z1 de composants de type T qui sont disponibles dans les stocks de l'entité E1;
- une étape S240 de vérification d'une condition, lors de laquelle on vérifie si la quantité Z1 est supérieure à un seuil; dans l'affirmative le processus se poursuit à l'étape S250, sinon à l'étape S260;
- une étape S250 lors de laquelle une commande de composants est envoyée à l'entité E1;
- une étape S260 correspondant à la fin du processus et à la libération des ressources logicielles et matérielles utilisées par le processus.

L'étape initiale S200 comprend optionnellement une opération de vérification d'une condition prédéfinie ou de détection de l'occurence d'au moins un événement prédéfini. Cette opération conditionne l'exécution des étapes S210 à S260 suivantes. Cet événement est par exemple la réception d'une requête ou d'un message en provenance d'une entité donnée, par exemple de l'entité E2 ou E1, ou d'une toute autre entité, la réception d'un document, la réception d'un SMS, la réception d'un appel téléphonique, l'occurrence d'une date ou d'une heure donnée, etc.

La description en langage BPMN du processus PROC est interprétée par un moteur de génération automatique capable de générer du code source en langage BPEL4WS (Business Process Execution Language for Web Service) qui permet de générer des composants de type service Web et d'invoquer des services Web existant. De tels outils bien connus des experts du domaine de la gestion de processus. Avec ce type d'outils, un processus peut être

défini à partir de composants types prédéfinis ou de gabarits, notamment comme une coopération et un ordonnancement particulier de ces composants types. Des composants de type service Web WS1 à WS6 sont alors utilisés lors de la mise en œuvre du processus, chaque service Web correspondant à une instanciation d'un gabarit ayant servi à la définition du processus.

L'exécution par le composant W0 du processus PROC de la figure 2 fait appel, dans l'exemple décrit ici, aux composants WA3 à WA5, WS3 à WS5 et WL1 à WL3.

Chacun des modules logiciels WL1 à WL3 est apte à mettre en œuvre une ou plusieurs opérations élémentaires de traitement prédéfinies. Dans le processus PROC d'exemple illustré à la figure 2, l'étape S220, (respectivement S225, S240) est mise en œuvre par le module logiciel WL1 (respectivement WL2, WL3). Les modules logiciels WL1 à WL3 peuvent eux-mêmes être issus d'une génération automatique à partir d'une description en langage formel.

L'étape S210 du processus PROC décrit à la figure 2 est mise en œuvre par le module logiciel WS4 en coopération avec le module WA4, constituant l'API côté serveur 15 du module logiciel WS4. De même, l'étape S215 (respectivement S230) du processus PROC décrit à la figure 2 est mise en œuvre par le module logiciel WS5 (respectivement WS3) en coopération avec le module WA5 (respectivement WA3), constituant l'API côté serveur 15 du module logiciel WS5 (respectivement WS3).

Les modules logiciels WS1 à WS6 peuvent eux-mêmes être issus d'une génération automatique à partir d'une description en langage formel.

Le processus PROC est lui-même mis en œuvre par un composant de type services Web, qui dans l'exemple décrit est le module logiciel W0. Une interface en langage WSDL (Web Service Description Language) permet d'invoquer l'exécution du processus PROC au même titre que celle d'un autre service Web. Le processus PROC mis en œuvre par le module logiciel W0 correspond ainsi au processus décrivant les modalités de coopération entre les systèmes d'information des entités E1 et E2.

A partir d'une description en langage formel d'un processus peuvent être générés automatiquement un ou plusieurs composants logiciels (W0) aptes à mettre en œuvre le processus défini par cette description formelle.

Dans un mode de réalisation de l'invention, les entités E1 et E2 concernées par le processus de coopération, génèrent puis valident la description du processus. Le serveur 15 comprend de préférence des moyens d'édition, de validation et d'enregistrement de la description du processus. L'édition et la validation du processus s'effectue à partir d'un terminal en liaison de communication avec le serveur 15.

De préférence, le serveur 15 comprend des moyens pour vérifier si une entité est autorisée à éditer ou valider ladite description. Dans ce cas des données d'identification et/ou d'authentification de l'entité concernée sont transmises au serveur 15 qui identifie et/ou

authentifie l'entité avant de lui donner accès à la description validée.

En complément, la description validée est encryptée et/ou signée numériquement, de manière à ce qu'elle ne puisse être modifiée sans l'accord des entités qui l'ont approuvée ou uniquement par une entité autorisée. Dans ce cas, le serveur 15 vérifie la signature de ladite description avant de procéder à la génération des composants logiciels aptes à mettre en œuvre le processus défini par cette description formelle.

Le serveur 15 joue ainsi le rôle de tiers de médiation et de confiance. Il est le dépositaire de la description validée et met en œuvre le processus tel que validé. En outre, comme décrit plus en détail plus loin, il comprend des moyens de contrôle et de sécurité garantissant que l'accès aux données d'un des systèmes d'information 10 ou 20, se fait exclusivement via les composants correspondant au processus tel que validé. De cette manière, l'accès par une autre entité à des données du système d'information d'une entité n'est autorisé que dans un cadre limité à un processus validé et approuvé par ces entités. En d'autres termes, les services Web WS1 à WS3 (respectivement WS4 à WS6) ne peuvent être invoqués que par un processus de traitement autorisé par l'entité E1 (respectivement l'entité E2).

Le serveur 15 comprend en outre un moteur de génération automatique capable de générer automatiquement le composant logiciel W0 à partir de la description validée qu'il reçoit. Dès lors le serveur 15 est apte à traiter des requêtes pour l'exécution du processus correspondant.

Le serveur 15 après génération du module logiciel W0 transmet une donnée d'identification et/ou d'authentification de ce module aux systèmes d'information 10 et 20 qui est stockée respectivement dans des tables T1 et T2. Les tables T1 et T2 définissent quels sont les programmes autorisés à invoquer les différents services Web mis en œuvre respectivement dans les systèmes d'information 10 et 20. Dans un mode de réalisation, ces tables associent à chaque identifiant de service Web les identifiants des programmes autorisés à invoquer le service Web. La table T1 (respectivement T2) est stockée dans le système d'information 10 (respectivement 20), de préférence au niveau d'une extension du middleware MW1 (respectivement MW2).

L'activation du module W0 est soit libre, soit réservée à une entité donnée. Dans ce deuxième cas, une identification de l'entité invoquant le module W0 est transmise lors de cette activation.

Chaque requête émise par l'un des systèmes d'information 10 ou 20 et reçue par le serveur 15 déclenche l'exécution d'un processus particulier associé à la requête. En variante, un seul processus global est défini, capable de traiter toutes les requêtes et mettant en œuvre un sous-processus associé à la requête. Dans cette variante, le processus global comprend des conditions et des opérations de traitement relatives à la requête reçue: analyse de la requête reçue, obtention d'une identification du sous-processus pour lequel la requête a été émise, puis exécution du sous-processus correspondant.

Le procédé selon l'invention est décrit plus détail par référence à la figure 3. Il correspond au traitement par le serveur 15 d'une requête émise par l'un des systèmes d'information 10 ou 20, en l'occurrence par le système d'information 20.

A l'étape S100 une requête est émise par le système d'information 20 de l'entité E2, en vue d'exécuter le processus PROC sur les données du système d'information 10 de l'entité E1. Cette requête est transmise au module logiciel W0. Des données d'identification et/ou d'authentification (par exemple, login avec mot de passe) de l'entité E2 émettrice de la requête sont envoyées avec la requête.

A l'étape S110, le module logiciel W0 reçoit la requête, vérifie l'identité de l'entité émettrice à partir des données d'authentification transmises, et, si l'entité émettrice E2 est autorisée à demander l'exécution du programme PROC, déclenche l'exécution du processus PROC. Dans le cas contraire, l'exécution du processus PROC n'est pas déclenchée et un message d'avertissement est envoyé à l'entité émettrice E2 .

A l'étape S120, le module logiciel W0 exécute l'étape d'initialisation du processus PROC. Lors de la première exécution de l'étape S120, c'est l'étape S200 du processus PROC qui est exécutée. Comme décrit plus haut, cette étape S200 peut comporter l'attente d'un événement particulier conditionnant l'exécution de la suite du processus PROC.

A l'étape S125, le processus PROC mis en œuvre par le composant logiciel W0 se poursuit. Si l'exécution du processus PROC est terminé, le procédé selon l'invention se poursuit à l'étape S160 finale. Sinon, le composant W0 détermine s'il doit invoquer un composant logiciel WS1 à WS6 de traitement. Dans l'affirmative, le procédé selon l'invention se poursuit à l'étape S130. En l'occurrence dans l'exemple donné, l'étape suivante du processus PROC étant l'étape S210, nécessitant l'activation du composant logiciel WS1, le procédé se poursuit à l'étape S130.

A l'étape S130, par exemple lors de l'exécution de l'étape S210 du processus PROC, le composant logiciel W0 invoque le composant logiciel WS4 de traitement mettant en œuvre une opération de traitement ou de consultation des données du système d'information 10 de l'entité E1.

Le module logiciel W0 émet une requête d'activation à destination du composant WS4, via son interface WA4. Cette requête est transmise sous forme de message conforme au protocole SOAP au module logiciel destinataire via les parties MW et MW1 du middleware. Cette requête comprend des données d'identification et/ou d'authentification du composant logiciel W0. Ces données peuvent être des jetons de sécurité, par exemple des certificats ou clefs d'infrastructure de sécurité.

La transmission des requêtes entre composants s'effectue de préférence dans un environnement sécurisé. Un mécanisme de sécurité utilisant une combinaison de clé publique et clé privée conformément à la norme X509 peut être utilisé pour crypter la requête au moyen d'une clé privée avant sa transmission via le middleware ou le réseau, la clé publique de

décryptage étant connue de l'environnement d'exécution des composants de manière à ce que la requête puisse être décryptée au moyen de cette clé publique avant traitement par le composant destinataire.

A l'étape S135, suite à l'émission de la requête d'activation, le composant WS4 recevant le message, identifie et authentifie le module logiciel W0 émetteur de la requête à partir des données d'identification et/ou d'authentification reçues. En cas d'authentification du module logiciel émetteur de la requête, le composant WS4 détermine, à partir de la table de données T1 de référence gérée par le système d'information 10, si le composant W0 authentifié est autorisé à invoquer le module WS4.

Des technologies connues adaptées aux services Web peuvent être utilisées pour l'authentification du composant W0, par exemple l'architecture Web Service Security (WS-Security) utilisant divers mécanismes de sécurité: couple identifiant/mot de passe, méthode du jeton de sécurité et celle des certificats notamment. Cette technologie permet d'authentifier l'émetteur du message SOAP à partir des données du message. Plus précisément, elle définit les données à insérer dans un message SOAP permettant la vérification des droits d'accès correspondant à ces différents mécanismes de sécurité.

Par ailleurs il est possible d'obtenir l'adresse de l'émetteur d'un message SOAP des données de la couche transport HTTP via laquelle ce message a été transporté. Une telle adresse peut être utilisée pour effectuer les opérations d'authentification en combinaison avec les données du message.

L'authentification peut aussi être réalisée au niveau du middleware véhiculant le message ou de préférence au niveau de l'environnement d'exécution des services Web (par exemple Axis). Dans un tel environnement, il est possible de définir des traitements à effectuer sur un message SOAP avant l'exécution du service Web destinataire du message.

En alternative, l'authentification et l'autorisation d'accès est effectuée non pas par les composants WS1 à WS6 mis en œuvre dans le système d'information 10 ou 20, mais par les composants WA1 à WA6, mis en œuvre dans le serveur 15 et servant d'interface respectivement aux composants WS1 à WS6. Dans ce cas, le serveur 15 comprend une table T stockant les informations des tables T1 et T2, table qui est stockée au niveau du middleware MW du serveur 15. Cette alternative suppose que le serveur fournisse un accès sécurisé aux données de ces tables de manière à garantir l'intégrité des données qui y sont stockées.

En cas d'autorisation, le procédé selon l'invention se poursuit à l'étape S140. Dans le cas contraire, un message d'erreur est retourné au composant W0 qui à son tour transmet un message d'erreur au système d'information 20 de l'entité E2 émettrice de la requête de demande de traitement. Le procédé se termine à l'étape S160.

L'exécution et l'activation du composant W0 de pilotage du processus se fait exclusivement à partir du serveur 15. C'est grâce à ce module, généré à partir de la description validée, que le serveur est en mesure d'assurer l'usage exclusif des données dans

le contexte d'un processus de traitement donné, en garantissant que l'accès aux données se fait uniquement pour des opérations de traitement faisant partie d'un processus correspondant à la description validée.

A l'étape S140, le module logiciel WS4 invoqué émet une requête d'interrogation du système d'information 10 et de la base de données 5 à travers le réseau R1, afin d'obtenir les données requises pour l'exécution de l'opération de traitement qui lui est associée.

A l'étape S150, le module logiciel WS4 exécute l'opération de traitement qui lui est associée à partir des données obtenues puis retourne au module W0 les données résultant de l'exécution de cette opération.

A l'étape S160 le module logiciel W0 termine l'exécution du processus PROC et retourne au système d'information 20 de l'entité E2 les données résultant de l'exécution du processus PROC.

Les étapes S130 à S150 sont à nouveau exécutées à chaque fois que le composant logiciel W0 invoque un nouveau module logiciel WS1 à WS6 de traitement et d'accès aux données, notamment lors de l'exécution de l'étape S210, S215, S230 du processus PROC.

Le dispositif ou le procédé, selon l'invention permet l'automatisation de l'exécution de processus de coopération entre plusieurs entreprises partenaires dans des contextes particulièrement dynamiques nécessitant des échanges d'information rapides, voire temps réel.

Son intérêt devrait s'accroître avec le déploiement de solution technologiques facilitant la mise à jour en temps réel de données d'un système d'information, notamment dans le cas de la gestion de stocks au moyen d'étiquettes RFID.

L'invention a été décrite dans le contexte d'entreprise dans le domaine des produits manufacturés. Les secteurs d'application de l'invention peuvent cependant être très variés.

Le secteur pharmaceutique donne un exemple de d'entité E2 (les pharmacies) distribuant des produits fournis par des entités E1 (les laboratoires/industries) avec des gestions de stocks internes à E1 et E2 et des connaissances sur le marché distribuées au niveau des entités E2. Les secteurs High-tech ou de l'industrie automobile sont d'autres exemples de secteurs travaillant de plus en plus en flux tendu avec des stocks réduits au niveau de E2.

Selon une implémentation préférée, les différentes étapes du procédé selon l'invention sont exécutées au moyen d'instructions de programmes d'ordinateurs.

Ces étapes sont ainsi de préférence mises en œuvre par le ou les processeurs du serveur 15 et des serveurs 10 ou 20, processeur(s) faisant appel à des programmes ou sous-programmes conçus pour l'exécution des différentes étapes de ce procédé.

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 ordinateur ou par un processeur de données, ce programme comportant des instructions adaptées à la

mise en œuvre d'un procédé de traitement de donné selon l'invention.

Ce programme 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 lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

Le support d'informations 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 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 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.

REVENDICATIONS

1. Système de traitement de données comprenant un serveur (15) de médiation entre une première entité dite entité cliente (E2) et une deuxième entité dite entité fournisseur (E1),
ledit serveur comprenant des moyens d'exécution de programme pour exécuter, sur requête en provenance de l'entité cliente, un programme (W0) mettant en œuvre un processus (PROC) prédéfini de traitement,
ledit programme (W0) étant apte à déclencher, lors de l'exécution dudit processus, une émission à travers une liaison de communication d'au moins une requête d'activation d'au moins un module de traitement (WS1-WS6) d'un serveur de l'entité fournisseur afin d'exécuter au moins une opération de traitement sur au moins une partie des données d'au moins une base de données (5) accessible via le serveur de l'entité fournisseur,
le système comprenant des moyens (T1, T2) de contrôle conçus pour, en cas d'authentification dudit programme, déterminer si ledit programme (W0) est autorisé à activer ledit module de traitement (WS1-WS6) et pour, en cas d'absence autorisation, inhiber l'exécution de ladite au moins une opération de traitement.

2. Système selon la revendication 1, ledit serveur de médiation comprenant des moyens de génération logicielle aptes à générer ledit programme à partir d'une description en langage formel dudit processus, ladite description étant définie par référence à au moins un module choisi parmi une pluralité de modules de traitement du serveur de l'entité fournisseur activables indépendamment les uns des autres.

3. Système selon la revendication 2, ledit serveur de médiation comprenant des moyens permettant l'édition et la validation de ladite description à partir d'un terminal en communication avec ledit serveur.

4. Système selon la revendication 3, ledit serveur de médiation comprenant des moyens pour vérifier si une entité est autorisée à éditer ou valider ladite description.

5. Système selon l'une quelconque des revendications précédentes, ledit serveur de médiation comprenant des moyens pour vérifier si une entité est autorisée à invoquer l'exécution dudit programme.

6. Serveur (15) de médiation entre une entité cliente (E2) et une entité fournisseur (E1),
ledit serveur de médiation comprenant des moyens d'exécution de programme pour exécuter, sur requête en provenance de l'entité cliente, un programme (W0) mettant en œuvre un processus (PROC) prédéfini de traitement,
ledit programme (W0) étant apte à déclencher, lors de l'exécution dudit processus, une

émission à travers une liaison de communication d'au moins une requête d'activation d'au moins un module de traitement (WS1-WS6) d'un serveur de l'entité fournisseur afin d'exécuter au moins une opération de traitement sur au moins une partie des données d'au moins une base de données (5) accessible via le serveur de l'entité fournisseur,
ledit serveur de médiation comprenant des moyens (T1, T2) de contrôle conçus pour, en cas d'authentification dudit programme, déterminer si ledit programme (W0) est autorisé à activer ledit module de traitement (WS1-WS6) et pour, en cas d'absence autorisation, inhiber l'exécution de ladite au moins une opération de traitement.

7. Serveur (10, 20) de traitement de données accédant à au moins une base (5, 25) de données,
ledit serveur de traitement étant apte à communiquer à travers une liaison de communication avec un serveur (15) de médiation entre une entité cliente (E2) et une entité fournisseur (E1),
ledit serveur de traitement comprenant au moins un module de traitement (WS1-WS6), conçu pour exécuter au moins une opération de traitement sur au moins une partie desdites données de ladite base de données et activable par requête à partir du serveur (15) de médiation au moyen d'un programme (W0) mettant en œuvre un processus (PROC) prédéfini de traitement,
ledit serveur de traitement comprenant des moyens (T1, T2) de contrôle pour, suite à l'émission par ledit programme d'une requête d'activation d'un module de traitement, vérifier si ledit programme est autorisé à activer ledit module de traitement (WS1-WS6) et pour, en cas d'absence autorisation, inhiber l'exécution de ladite au moins une opération de traitement.

8. Procédé de traitement de données incluses dans au moins une base de données accessible via un serveur (10, 20) de traitement de données, ledit procédé comprenant au moins,
- une étape d'exécution par un serveur de médiation d'un programme (W0) mettant en œuvre un processus prédéfini de traitement, ladite étape d'exécution étant destinée à être exécutée suite à la réception par le serveur de médiation d'une requête en provenance d'une entité cliente,
- une étape de déclenchement par ledit programme (W0), lors de l'exécution dudit processus, de l'émission à travers une liaison de communication d'au moins une requête d'activation d'au moins un module de traitement (WS1-WS6) du serveur de traitement afin d'exécuter au moins une opération de traitement sur au moins une partie desdites données,
- une étape de contrôle pour déterminer si le programme (W0) à l'origine de la requête d'activation est autorisé à activer ledit module de traitement (WS1-WS6),

- une étape de déclenchement de l'exécution de ladite au moins une opération de traitement, ladite étape de déclenchement n'étant exécutée qu'en cas d'autorisation.

9. Procédé selon la revendication 8 comprenant une étape d'authentification du programme à l'origine de la requête d'activation, ladite étape de contrôle n'étant exécutée qu'en cas d'authentification.

10. Support de données sur lequel a été mémorisée au moins une série d'instructions de code de programme pour l'exécution d'au moins une étape du procédé conforme à l'une des revendications 8 à 9.

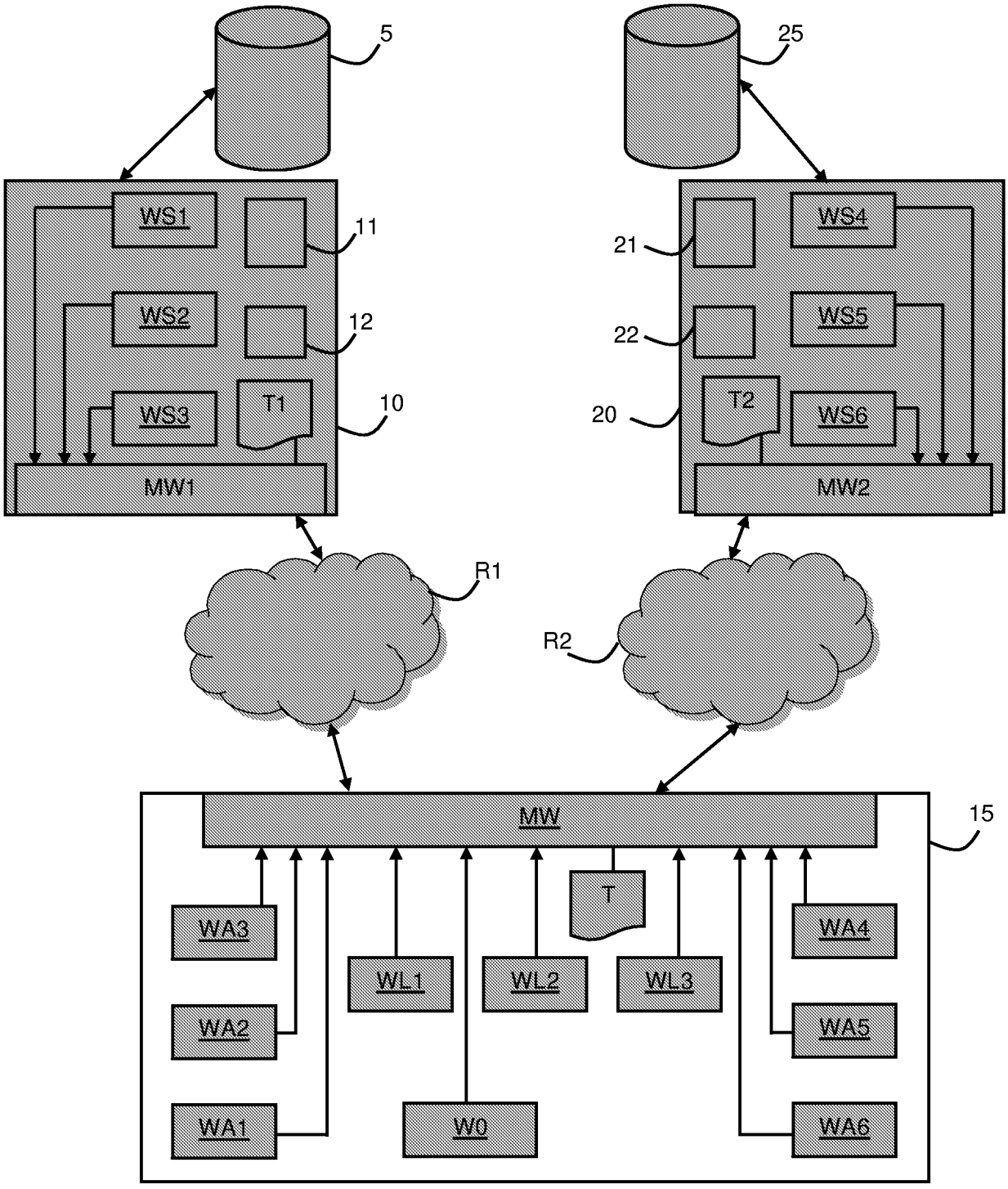

5
25
WS1
11
WS2
12
WS3
T1
10
MW1
21
WS4
22
WS5
20
T2
WS6
MW2
R1
R2
MW
15
T
WA3
WA4
WL1
WL2
WL3
WA2
WA5
WA1
W0
WA6

Fig. 1

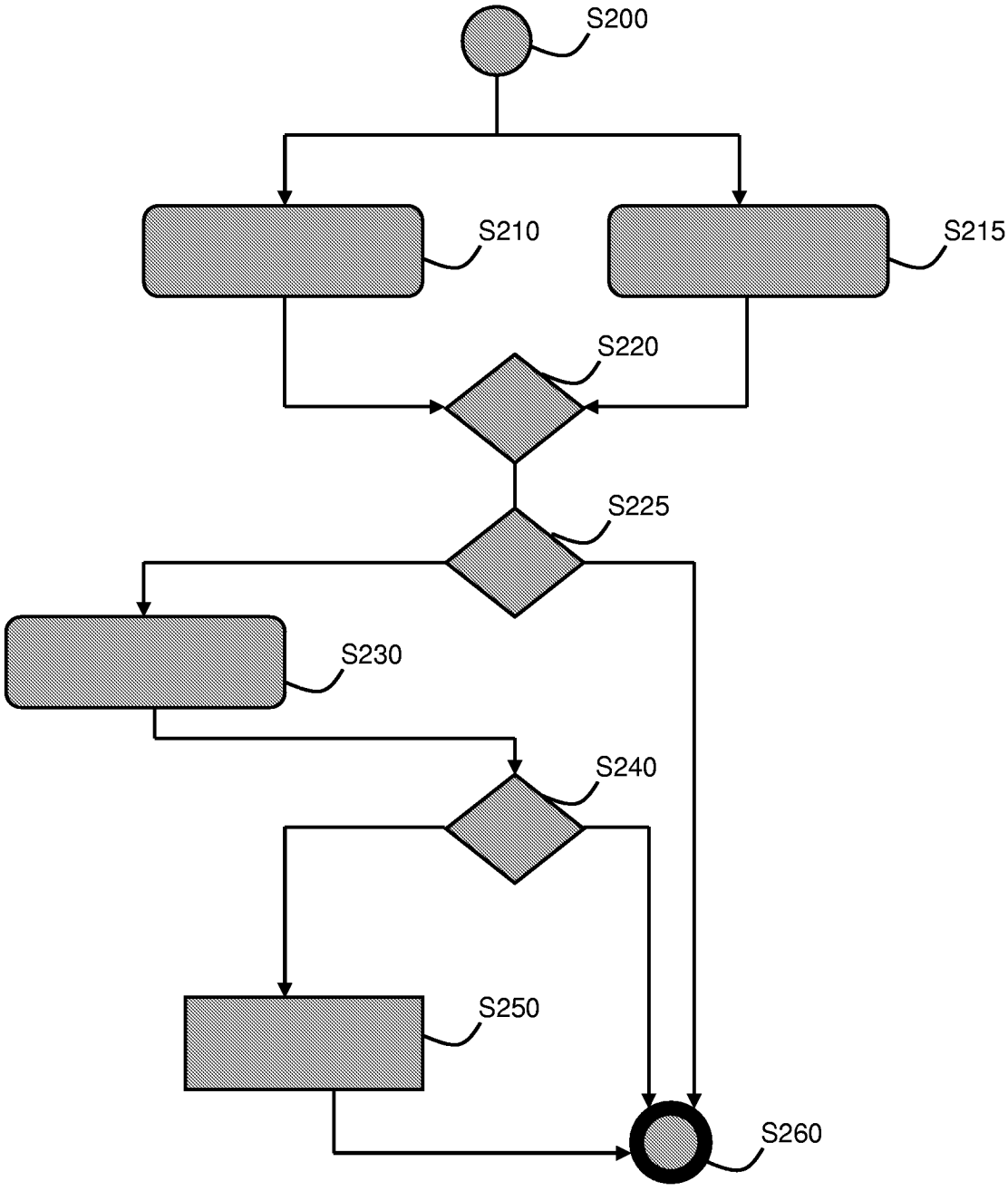


Fig. 2

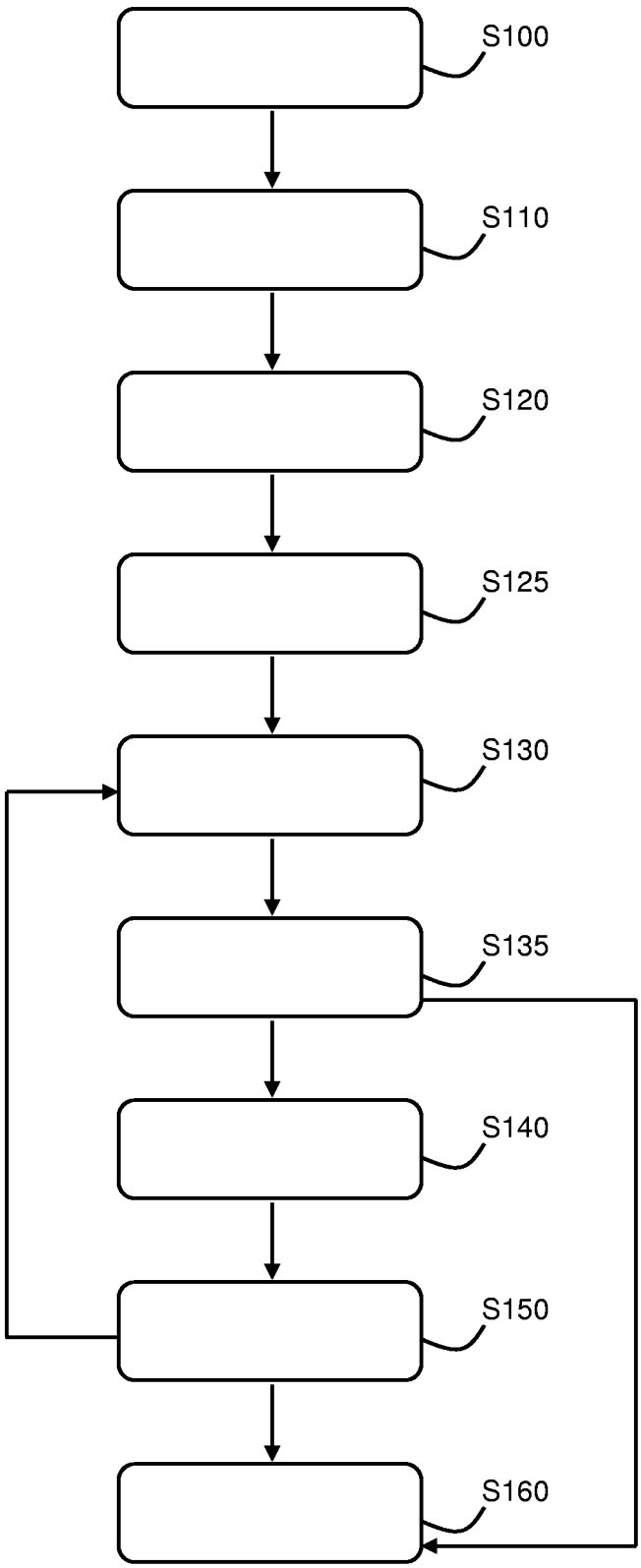


Fig. 3