ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية
---

(12) FASCICULE DE BREVET

(11) N° de publication :
MA 33308 B1

(43) Date de publication :
01.06.2012

(51) Cl. internationale :
G06F 15/16; G06F 9/455; H04L 29/08

(21) N° Dépôt :
33310

(22) Date de Dépôt :
02.11.2010

(71) Demandeur(s) :
HIJANE MOULAY EL HADI, 87, HAY EL BARAKA, LOTT " EL KSOUR ", ROUTE DE CASABLANCA marrakech (MA)

(72) Inventeur(s) :
HIJANE MOULAY EL HADI

(54) Titre : **SYSTÈME GÉNÉRIQUE DE L'INFORMATION ET DE TRANSACTIONS SÉCURISÉES PAR ÉQUIPEMENT MOBILE SUR DES SOURCES DE DONNÉES DISTRIBUÉES ET HÉTÉROGÈNES.**

(57) Abrégé : SYSTÈME ET PROCÉDÉS PERMETTANT DE PRENDRE EN MAIN UN QUELCONQUE SYSTÈME INFORMATIQUE DÉJÀ EN PLACE ET D'Y INTRODUIRE UNE MUTATION SANS AUCUNE MODIFICATION DE L'EXISTANT, POUR ABOUTIR À UN SYSTÈME PLUS ÉVOLUÉ EN TERMES D'INTÉGRATION DE DONNÉES ET EN TERMES DE TRANSACTIONS CLIENT/SERVEUR PRINCIPALEMENT POUR CLIENT MOBILES ÉQUIPÉS DE JAVA. LE PRÉSENT SYSTÈME CONSTITUE UNE SURCOUCHE À L'EXISTANT, IL PERMET DE PRENDRE EN CHARGE SES DONNÉES DÉJÀ PRÉSENTES, AUPARAVANT MANIPULÉES EXCLUSIVEMENT PAR DES ORDINATEURS ET LES RENDRE ACCESSIBLES VIA DES TERMINAUX MOBILE (PDA, SMARTPHOVES,...) À DES UTILISATEURS PRÈSENTS SUR LE TERRAIN. LA PRÉSENTE INVENTION CONCERNE UN SYSTÈME PERMETTAN D'EFFECTUER DES TRANSACTIONS SÉCURISÉES ENTRE UN UTILISATEUR JOUISSANT D'UN TERMINAL MOBILE(PDA, SMART PHONE,...) ET UNE MULTITUDE DE SOURCES DE DONNÉES DISTRIBUÉES ET HÉTÉROGÈNES. LE SYSTÈME COMPORTE DES PROCÉDÉS PERMETTANT ENTRE AUTRES DE RÉSOUDRE LE PROBLÈME DE L'INTÉGRATION DE PLUSIEURS SOURCES DE DONNÉES HÉTÉROGÈNES À UN SEUL ET MÊME SI(SYSTÈME D'INFOMATION) SANS AUCUNE CONNAISSANCE PRÉABLE DE LEURS STRUCTURE. LEDIT SYSTÈME COMPREND TROIS PARTIES. LE CLIENT QUI EST UNE APPLICATION LOGICIELLE DE TÉLÉPHONE MOBILE INSTALLÉ SUR LE TERMINAL MOBILE DE L'UTILISATEUR DU SYSTÈME LUI PERMETTANT DE S'AUTHENTIFIER, D'ENVOYERDES REQUÊTES ET DE LIRE LES RÉPONSES. LE COEUR DU SYSTÈME EST APPELÉ; CENTRE DE CONTRÔLE, C'EST

UNE PLATEFORME LOGICIEL/MATÉRIEL NÉCESSAIRE AU BON FONCTIONNEMENT DE TOUS LES SERVICES QU'OFFRE LE SYSTÈME. LE CENTRE DE CONTRÔLE JOUE LE RÔLE D'INTERMÉDIARE UNIQUE ET INÉVITABLE ENTRE LE CLIENT ET LE SOURCES DE DONNÉES, IL CONCENTRE TOUT LE TRAFIC, EXÉCUTE LE REQUÊTES DES CLIENTS BIEN AUTHENTIFIÉS ET LEUR LIVRE LE DÉSULTAT. ENFIN, LE SYSTÈME POSSÈDE UN AGENT FOURNISSEUR DE DONNÉES PRÉSENT SUR LE MÊME RÉSEAU LOCAL QUE LA SOURCE DE DONNÉES CIBLÉES. CE DERNIER PERMETTANT DE RÉSOUDRE LE PROPLÈME DE L'INTÉGRATION DES DIVERSES SOURCES DE DONNÉES DISTRIBUÉES ET HÉTÉROGÈNES, DONNAT AINSI L'IMPRESSION À L'UTILISATEUR DU SYSTÈME QU'IL UTILISE UN SYSTÈME NUNIQUE ET HOMOGÈNE. LA SUPERVISION DU SYSTÈME SE FAIT EN INTERNE AU SEIN DU CENTRE DE CONTRÔLE PAR ADMINISTRATEURS AYANTS DES NIVEAUX DE HIÉRARCHIE DIFFÉRENTS. QUAND À L'AGENT FOURNISSEUR DE DONNÉES, IL EST CONTRÔLÉ PAR L'ADMINSTRATEUR DE LA BASE DE DONNÉES À LAQUELLE IL A ACCÉS, CE QUI AUGMENTE LA SÉCURITÉ ET LE NIVEAU DE CONFIANCE ENTRE LES DIFFÉRENTES COMPOSANTES DUDIT SYSTÈME.

Abrégé

Système et procédés permettant de prendre en main un quelconque système informatique déjà en place et d'y introduire une mutation importante sans aucune modification de l'existant, pour aboutir à un système plus évolué en termes d'intégration de données et en termes de transactions client/serveur principalement pour clients mobiles équipés de JAVA.

Le présent système constitue une surcouche à l'existant, il permet de prendre en charge des données déjà présentes, auparavant manipulées exclusivement par des ordinateurs et les rendre accessibles via des terminaux mobiles (PDA, Smartphones,...) à des utilisateurs présents sur le terrain.

La présente invention concerne un système permettant d'effectuer des transactions sécurisées entre un utilisateur jouissant d'un terminal mobile (PDA, smart phone,...) et une multitude de sources de données distribuées et hétérogènes. Le système comporte des procédés permettant entre autres de résoudre le problème de l'intégration de plusieurs sources de données hétérogènes à un seul et même SI (système d'information) sans aucune connaissance préalable de leurs structure.

Ledit système comprend trois parties. Le Client qui est une application logicielle de téléphone mobile installé sur le terminal mobile de l'utilisateur du système lui permettant de s'authentifier, d'envoyer des requêtes et de lire les réponses. Le cœur du système est appelé : centre de contrôle, C'est une plateforme logiciel/matériel nécessaire au bon fonctionnement de tous les services qu'offre le système. Le centre de contrôle joue le rôle d'intermédiaire unique et inévitable entre le client et les sources de données, il concentre tout le trafic, exécute les requêtes des clients bien authentifiés et leur livre le résultat. Enfin, le système possède un agent fournisseur de données présent sur le même réseau local que la source de données ciblées. Ce dernier permettant de résoudre le problème de l'intégration des diverses sources de données distribuées et hétérogènes, donnant ainsi l'impression à l'utilisateur du système qu'il utilise un système unique et homogène.

La supervision du système se fait en interne au sein du centre de contrôle par des administrateurs ayants des niveaux de hiérarchie différents. Quand à l'agent fournisseur de données, il est contrôlé par l'administrateur de la base de données à laquelle il a accès, ce qui augmente la sécurité et le niveau de confiance entre les différentes composantes dudit système.

MA 33308B1

01 JUIN 2012

Système générique d'intégration de l'information et de transactions sécurisées par équipement mobile sur des sources de données distribuées et hétérogènes.

Description

- Titre : Système générique d'intégration de l'information et de transactions sécurisées par équipement mobile sur des sources de données distribuées et hétérogènes.

- Domaine de l'invention :

La présente invention se rapporte au domaine des Technologies de l'Information et de la Communication.

La présente invention se rapporte plus particulièrement à un système informatique, des dispositifs et des procédés permettant la centralisation de transactions sécurisées sur des sources de données distribuées et hétérogènes ainsi que leur manipulation exclusivement via un équipement mobile.

L'invention comporte un protocole (procédé) mis en œuvre pour banaliser le raccordement de tout type de base de données au système sans aucune modification de l'existant ni même connaissance préalable de la structure des données à manipuler.

- Etat de la technique antérieure :

Le système est basé sur le design pattern Modèle Vue Contrôleur (MVC) qui a pour objectif d'organiser la réalisation des applications et de séparer complètement l'interface homme-machine(Vue) des données (Modèle) et de la logique de contrôle (Contrôleur).

Le modèle représente les données de l'application. Il définit aussi l'interaction avec la base de données et le traitement de ces données.
La vue représente l'interface utilisateur, ce avec quoi il interagit. Elle n'effectue aucun traitement, elle se contente simplement d'afficher les données que lui fournit le contrôleur. Il peut tout à fait y avoir plusieurs vues qui présentent les données d'un même modèle.
Le contrôleur gère l'interface entre le modèle et le client. Il va interpréter la requête de ce dernier pour lui envoyer la vue correspondante. Il effectue la synchronisation entre le modèle et les vues.

Le mapping objet-relationnel (ORM) est un procédé permettant de définir au niveau d'une application la correspondance entre les objets manipulés par celle-ci et les de données présentes dans les bases de données relationnelles. Cette tache inévitable est généralement effectuée par le développeur lors de la phase de développement.

Cependant, le problème se pose lors de l'intégration de nouvelles sources données à un système déjà établi. Ajouter de nouvelles sources de données et les rendre accessibles par de nouvelles vues, signifie l'ajout du modèle et du mapping objet-relationnel correspondant pour que celles-ci soient prises en compte par le contrôleur. Ce qui constitue une charge de travail et un coût assez

conséquent pour faire évoluer le projet d'autant plus que la diversité des sources d'information distribuées et leur hétérogénéité sont l'une des principales difficultés rencontrées par les développeurs d'applications évolutives. Cette hétérogénéité peut provenir du format ou de la structure des sources, du mode d'accès et de requête ou de l'hétérogénéité sémantique.

Malgré les facilités que le modèle MVC présente dans le cycle de vie des applications web (Spécification, développement, maintenance...), ce dernier trouve ses limites dans le cas de certaines applications web à besoins particuliers en évolution, ce qui nécessite l'introduction de nouvelles couches ainsi que certains mécanismes.

La présente invention apporte une réponse à ce problème en implémentant le design pattern : «injection de dépendance ». En effet ledit système introduit un agent fournisseur de donnée (4) que nous appelons ici DPA, ayant pour objectif principal de supprimer la dépendance des requêtes vis-à-vis des données ciblées. Nous aboutissons donc à un système possédant un unique contrôleur et des modèles additionnables à la demande, sachant que les vues sont consultées principalement sur appareils mobiles.

- Exposé de l' invention:

La présente invention concerne un système générique à grand niveau d'abstraction inspiré du design pattern MVC, ayant un seul contrôleur, des modèles additionnables à la demande et des vues configurables selon spécifications client.

Le système représente une surcouche à l'existant. Il permet de faire la liaison selon le besoin entre différentes sources de données déjà présentes, manipulées auparavant exclusivement par des ordinateurs et les rendre accessibles via des terminaux portables disposant de la technologie JAVA à des agents sur le terrain.

Comme le système se veut générique, ce dernier a pour vocation de permettre l'accès à autant de nouvelles sources de données (hétérogènes et distribuées) que le besoin le dicte, sans aucune modifications de l'infrastructure déjà existante.

Il faut préciser que toutes les données n'ont pas besoin de l'être, seuls les données pertinentes, critiques et nécessitants un accès en temps réel sans avoir à passer par un intermédiaire humain, à savoir certaines données d'entreprises ou les données gouvernementales. Le besoin découle du gain en temps et en ressources humaines ainsi que le confort de la mobilité et la facilité de la mise en œuvre de la solution. Les cas de figures ne manquent pas, nous en citerons quelques-uns dans le paragraphe : «applications industrielles».

L'architecture du système possède trois composants majeurs :

1. Mobile Client ou MC : Représente l'application cliente J2ME pour terminal mobile disposant de la technologie JAVA.
   En entrant l'url exacte dans le navigateur du terminal, l'utilisateur télécharge une application J2ME, ensuite ce dernier l'installe en deux clics (PS : La procédure d'installation est effectuée une seule fois, lors de la première utilisation).
   Une fois installés ce dernier lance l'application, accepte les conditions d'utilisation et lance une procédure d'authentification forte en remplissant un champ « nom d'utilisateur » et un

autre champ «mot de passe ». Une fois authentifié, l'utilisateur pourra donc interagir librement avec le système.
Aucune donnée relative à l'utilisateur n'est persistante, toutes les données utilisés par le MC sont volatiles (détruites lorsque l'utilisateur quitte l'application).
On ne stocke rien dans le terminal mobile pour des raisons de sécurité, on ne fait qu'envoyer des requêtes et interpréter les pages reçues.
Le dialogue entre le client mobile MC et le serveur (centre de contrôle) passe par un tunnel SSL.

2. Control Center ou CC : Le centre de contrôle est le cœur du système. C'est une plateforme matériel/logiciel qui représente la logique applicative (Contrôleur) et joue le rôle d'interface unique et incontournable entre le terminal mobile et les sources de données.
Toutes les requêtes des différents clients passent obligatoirement par le CC, il n'ya pas de liaisons directes entre les clients et les sources de données.
Le centre de contrôle est une partie, et non la moindre du système. Il assure 90% de la charge de travail (contrôle d'accès, confidentialité, traitement des requêtes, consolidation de données, envoi des réponses, traçabilité, supervision et administration du système ...).
Le CC possède une base de donnée appelée base de contrôle, contenant les informations nécessaires au bon fonctionnement du système : qui fait quoi, où, quand et comment ?
Seuls les administrateurs du système accèdent à la base de contrôle moyennant une interface d'administration et la manipulent en fonction de leurs positions dans la hiérarchie administrative.
Le CC a pour vocation de fournir un service d'authentification performant auprès duquel les utilisateurs son déjà préenregistré et leur permettre d'effectuer des transactions sécurisées de type CRUD (*création, lecture, mise-à-jour, suppression*) sur les SGBD cibles, tout en protégeant ces derniers contre les utilisateurs malveillants.

3. Data Provider Agent ou DPA : Le DPA ou agent fournisseur de donnée représente la couche d'accès aux données (DAO), c'est aussi le dernier maillon de la chaine.
Le DPA est un serveur d'application contenant une couche logicielle qui permet l'adaptation des requêtes reçu de la part du CC, leur transformation en requêtes compréhensible par le SGBD cible, leur exécution et le renvoi du résultat de façon sécurisée (via tunnel SSL).
Il est installé au sein du réseau local (LAN) qui contient les bases de données cible, permettant à ces dernières d'être accessible par le CC (Le dialogue externe du DPA se fait uniquement avec le CC, tandis que son dialogue interne se fait avec les bases de données présentes sur le même réseau local).
L'administrateur du réseau local qui héberge le DPA a toujours la main sur ce dernier, il lui attribue les privilèges nécessaires pour manipuler uniquement les données dont il a besoin, ce qui le rend complètement contrôlable et augmente le niveau de confiance.
Ceci implique que le propriétaire de la base de données cible maîtrise à tout moment le comportement du DPA et les informations auxquelles il a accès.
Enfin, aucune modification ni recompilation de code du DPA n'est indispensable pour brancher une nouvelle source de donnée au système, une seule chose est nécessaire : le bon paramétrage de certains fichiers de configuration (au nombre de trois) au niveau du DPA.

Le Centre de Contrôle agis comme un hub en liaison sécurisée avec plusieurs supports de données qu'il interroge de façon sécurisée et transparente suite à la demande du client. Ces supports de données sont généralement des bases de données distantes ou internes. La communication entre le client et le centre de contrôle passe par un tunnel SSL tout comme celle entre le centre de contrôle et le DPA.

Le système est un mélange de technologies basées essentiellement sur java. Au niveau de l'appareil mobile(1) nous utilisons une application en implémentant la technologie J2ME. Au niveau du centre de contrôle (3) nous implémentons un serveur « Tomcat » sur lequel tourne une application basée sur la technologie J2EE, la sécurité est gérée par la technologie JACC qui définit les permissions correspondantes à chaque rôle. La persistance des donnée de la base de contrôle (5) est gérée par le la technologie « Hibernate ». Le DPA (4) est conteneur EJB3 mis en place sous JBOSS. La sérialisation de donnée est une partie très importante dudit système, pour laquelle nous implémentant l'API « flexjson ».

- Présentation des figures :

La figure 1 représente l'architecture générale du système. Comme représenté, le terminal mobile (1) utilise la technologie GPRS ou 3G (si disponible) pour transmettre et recevoir des paquets en passant par les points d'accès (2) qui gèrent les réseaux GSM.

Le centre de contrôle (3) héberge une base de données appelée base de contrôle (5) qui contient tous les comptes utilisateurs ainsi que leurs autorisations, les comptes administrateurs, les adresses des DPA,... Le CC (3) pioche dans la base de contrôle (5) pour extraire les informations nécessaires pour traiter les requêtes, transfert la requête au DPA (4) correspondant, récupère la réponse du DPA (4), valide le changement d'état du système puis renvois la réponse final au client mobile(1).

A noter que le Centre de contrôle contient au moins un ordinateur dédié à la supervision du système, sous la responsabilité d'au moins un administrateur (6) humain et sur lequel tourne une application dédiée à l'administration du dit système.

La figure 2 représente un cas particulier du système, le cas ou le DPA (4) est présent au sein même du centre de contrôle (3). Ce cas particulier s'explique par le fait que la base de données ciblée par les transactions se trouve au sein du même LAN qui abrite le centre de contrôle. Dans de cas particulier, nous n'avons pas besoin de passer par internet pour récupérer nos données cibles.

La figure 3 représente la façon avec laquelle se fait le dialogue entre les différents composants du système. Les requêtes du client mobile (1) sont ainsi acheminées au centre de control (3) via internet de manière sécurisée en utilisant le protocole HTTPS (nous envoyons nos requêtes http dans des tunnels SSL). Ainsi, il est impossible d'espionner les informations échangées, ni de truquer les informations échangées, ce qui permet une authentification efficace des deux coté. Le protocole HTTPS est implémenté en utilisant des certificats de sécurité délivré par une autorité de certification SSL privée.

Ces certificats SSL sont installés de part et d'autre du système (sur le terminal mobile(1), au centre de contrôle(3) et sur chacun des DPA (4)) pour permettre de bien authentifier tous les protagonistes de ce dialogue.

La figure 4 représente de façon plus concise, le mode de fonctionnement du DPA (4). Comme la figure l'indique, le DPA (4) est monté au sein même du réseau local (D) contenant les bases de données ciblées par les requêtes des utilisateurs. Ici DB1, DB2, DB3, DB4 et DB5 sont des systèmes de gestion de bases de données (SGBD) hébergeant chacun une ou plusieurs bases de données ciblées par les recherches des utilisateurs. Pour rendre ces bases de données accessibles au CC (3), le DPA(4) a besoin de connaitre:

- Le type du SGBD: pour charger le pilote correspondant (SQL Server, MySQL, Oracle, DB2, Informix,...).
- Le chemin vers la base de données.
- Le compte utilisateur : login/mot de passe pour DAP (4) créé par l'administrateur (7) de ce réseau local (D) et attribuant au DPA (4) les privilèges nécessaires et suffisant uniquement sur les tables ciblées par les requêtes.

Ces informations, se trouvent dans les fichiers de configuration du DPA(4).

- Mode de réalisation :

En règle générale, les matières premières du présent système sont les bases de données qui existent déjà et qui ont besoin d'être consultées de manière mobile par des agents présents sur le terrain pour les raisons citées précédemment

La mise en œuvre du système :

1. Nous installons un DPA pour chaque réseaux local contenant des bases de données cible, ce dernier permet de rendre celles-ci accessible au centre de contrôle, il permet aussi de contourner le problème de l'hétérogénéité des donnée en mettant en œuvre le mécanisme d'injection de dépendance.
2. Nous remplissant adéquatement les fichiers de configuration du DPA pour lui permettre de communiquer localement avec la/les base(s) ciblée(s).
3. Nous montons le centre de contrôle sur un site physique choisi par le client, en générale chez le client ou sur un site géré par des tiers.
4. Nous passons à la phase de remplissage de la base de contrôle. Cette base que nous avons introduite précédemment contient toutes les informations nécessaires au bon fonctionnement du système, à savoir : les informations sur les utilisateurs (login, mot de passe,...), les informations sur les DPA, les informations sur les appareils mobiles (numéro IMEI, numéro de licence,...), les informations sur les administrateurs du système (login, mot de passe, hiérarchie,...), etc.
5. Nous créons les vues c.-à-d. les pages qui s'affichent sur le terminal mobile. Ces vues varient suivant spécification client.
6. Nous mettons à disposition des agents mobiles une application mobile (téléchargeable sur nos serveurs)

Le système est maintenant prêt pour l'emploi.

Utilisation du système :

1. A chaque lancement de l'application mobile, l'utilisateur (MC) doit accepter les conditions d'utilisation et s'authentifier avant toute interaction avec le système.
2. L'utilisateur bien authentifié reçoit la page d'accueil sur son terminal et possède désormais une session d'ouverte au centre de contrôle (CC). La page d'accueil comporte une liste de tous les services qu'offre le système pour ce type d'utilisateur.
3. L'utilisateur choisi un service (Exemple : recherche d'article par numéro d'article).
4. Le centre de contrôle lui renvoi la vue correspondante à ce service.
5. Le client reçoit la vue, la remplie et envoi sa requête.
6. Le centre de contrôle reçoit la requête, pioche dans la base de contrôle pour connaitre le DPA qui lui correspond.
7. Le centre de contrôle renvoi la requête au DPA en question
8. Le DPA l'exécute et renvoi sa réponse au centre de contrôle.
9. Le centre de contrôle achemine la réponse au client et sauvegarde l'état du système.
10. On boucle sur l'étape 3 jusqu'à déconnexion de l'utilisateur et destruction de sa session sur le serveur.

- Application industrielle :

Le besoin d'accéder à l'information est un besoin universel qui ne date pas d'hier. Le système trouve son utilité et sa valeur ajoutée dans la manière avec laquelle il permet de banaliser l'accès aux informations critiques et pertinentes.

Les piliers du système sont :

1. La facilité de mise en œuvre (surcouche à l'existant sans modification de ce dernier)
2. Le confort de la mobilité
3. L'absence d'intermédiaire humain
4. Système temps réel
5. La Sécurité des transactions
6. L'intégration de données distribuées et hétérogènes

Suite à cela, on peut donc en déduire deux cas de figure de la manière dont ledit système est susceptible d'application industrielle, à savoir une application orientée entreprises et une application orientée e-gouvernement.

Application pour entreprises :

- Commerciaux
- Logisticiens
- Hôpitaux et cliniques (suivi de malades)
- Solutions sur-mesure
- ...autres

Application gouvernementales :

- Contrôle d'identités

- Contrôle de véhicules (numéros de plaques minéralogique)
- Lutte anti-criminalité (consultation du fichier des personne recherchées, consultation du casier judiciaire)
- Services de douanes (procédure de contrôle import/export)
- Solutions sur-mesure
- ...autres.

Le système permet entre autre de remédier aux situations impliquant un intermédiaire entre l'information et son demandeur, tel que l'obligation de passer par un agent standard téléphonique.

Revendications

1. Système d'intégration de l'information et de transactions sécurisées par équipement mobile sur des sources de données distribuées et hétérogènes, caractérisé par une architecture de type : Modèles, Vues, Contrôleur en ce qu'il comporte une application mobile (1) appelée « Mobile Client » et représentée par le sigle « MC », communicant par GPRS ou 3G avec un serveur central présent au sein de ce que l'on appelle ici « Control Center» (3) et représenté par le sigle « CC », ce dernier communiquant via internet avec des bases de données distribuées et hétérogènes par l'intermédiaire d'un serveur appelé « Data Provider Agent » (4) et représenté par le sigle « DPA ».
2. Système selon la revendication 1, caractérisé en ce que le MC (1) est une application java mobile téléchargée et installé lors de la première utilisation et permettant aux usagers du MC (1) de s'authentifier, envoyer des requêtes au CC (3) et recevoir des réponses sous format XML.
3. Système selon les revendications 1 et 2, caractérisé en ce que le MC (1) comporte l'adresse web (URL) du CC (3) cryptée selon un algorithme propriétaire. L'url est décryptée la première fois lors de l'authentification et gardée en mémoire pour les prochaines requêtes.
4. Procédé selon les revendications 1, 2 et 3, selon lequel la procédure de connexion du MC (1) au Centre de contrôle comporte des étapes bien précises consistant à envoyer le login et mot de passe plus un code généré à partir des deux pour permettre une authentification forte.
5. Système selon la revendication 1, caractérisé en ce que le centre de contrôle (3) qualifié par le terme CC, indique l'ensemble d'une plateforme Matériel/Logiciel montés sur un même réseau local et comportant :
    - Au moins un serveur web sur lequel tourne le contrôleur principal c.-à-d. le cœur du système tout entier.
    - Au moins un serveur de base de données gérant une base de données appelée «base de contrôle » qui contient les données essentielles au fonctionnement du système telles que les login, les mots de passes, les identifiants des appareils mobiles, les informations sur les administrateurs...
    - Au moins un ordinateur dédié à l'administration du système, sous la responsabilité d'un administrateur humain (6) et sur lequel tourne une application propriétaire dédiée à la supervision du dit système.
6. Système selon la revendication 1, caractérisé en ce que le DPA (4) est un conteneur web sur lequel tourne une application qui permet de relier tout type de base de données au CC (3) sans aucune modification sur les données existante et sans aucune connaissance au préalable de la structure des données ciblées.
7. Procédé selon la revendication 1 et 5, caractérisé en ce que le système comporte au niveau du DPA (4), une procédure permettant l'intégration de tout type de base de données au système sans aucune connaissance au préalable de l'architecture de la base de données, en remplissant adéquatement trois fichiers XML de configuration au niveau du DPA (4).
8. Procédé selon les revendications 1, 5 et 6 caractérisé en ce que le DPA (4) comporte un fichier de configuration dans lequel sont décrites toutes les requêtes selon une démarche bien précise.

9. Procédé selon la revendication 8, caractérisé en ce que les requêtes décrites dans les fichiers de configuration du DPA sont divisées en quatre catégories à savoir : les requêtes de lecture de type R (read), les requêtes d'écriture de type W (write), les requêtes de mis-à-jour de type U (update), les requêtes de suppression de type D (delete).
10. Procédé selon la revendication 9, caractérisé en ce que les requêtes décrites dans les fichiers de configuration du DPA et pour les catégories W(write), U(update) on décrit deux champs à savoir : les données à modifier et les nouvelles valeurs.
11. Procédé selon la revendication 9, caractérisé en ce que les requêtes décrites dans les fichiers de configuration du DPA et pour la catégorie R (read), on décrit deux champs à savoir : les données à lire et les valeurs recherchées.
12. Procédé selon la revendication 9, caractérisé en ce que les requêtes décrites dans les fichiers de configuration du DPA et pour les catégories D (delete), on décrit deux champs à savoir : les données à supprimer et les valeurs à supprimer.

Dessins

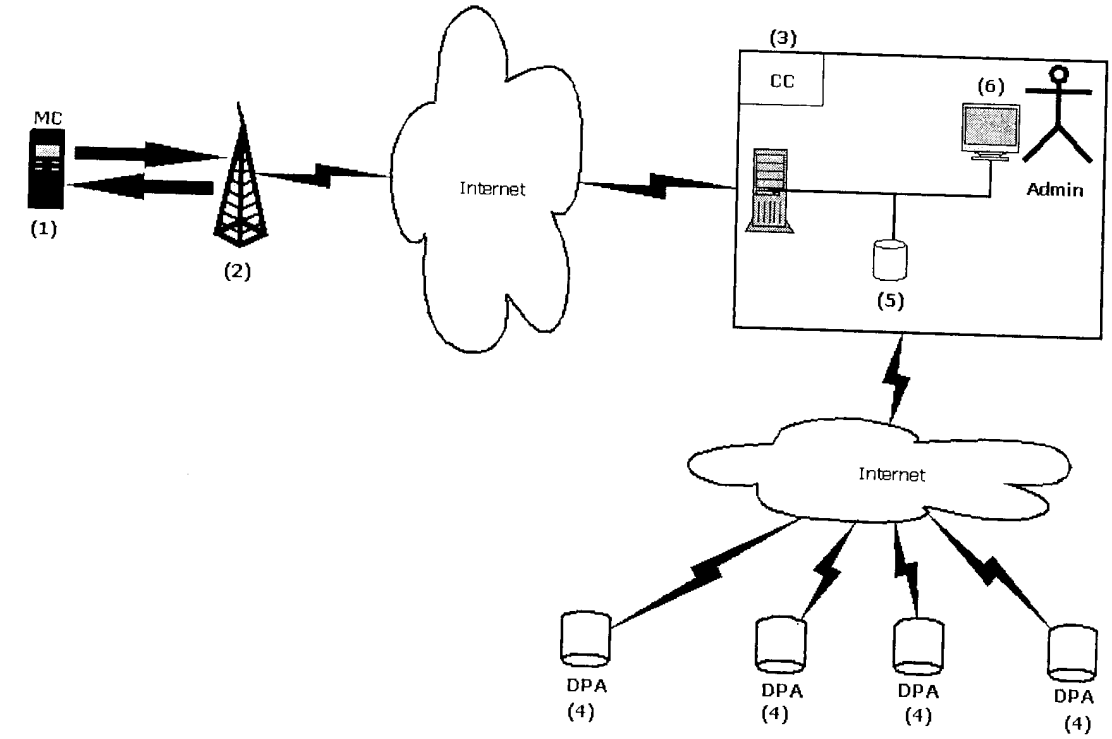

Figure 1

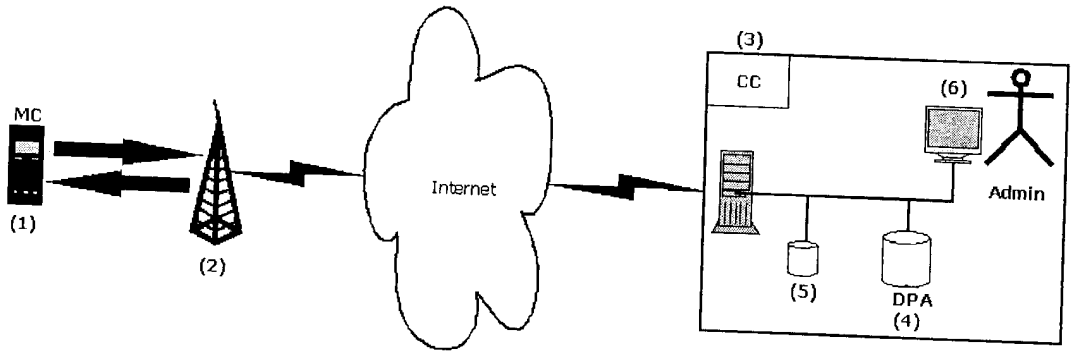

Figure 2

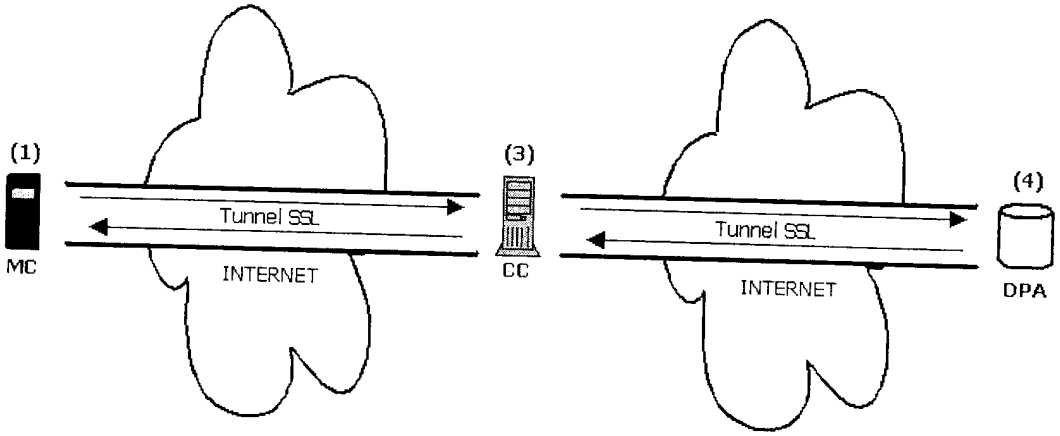

Figure 3

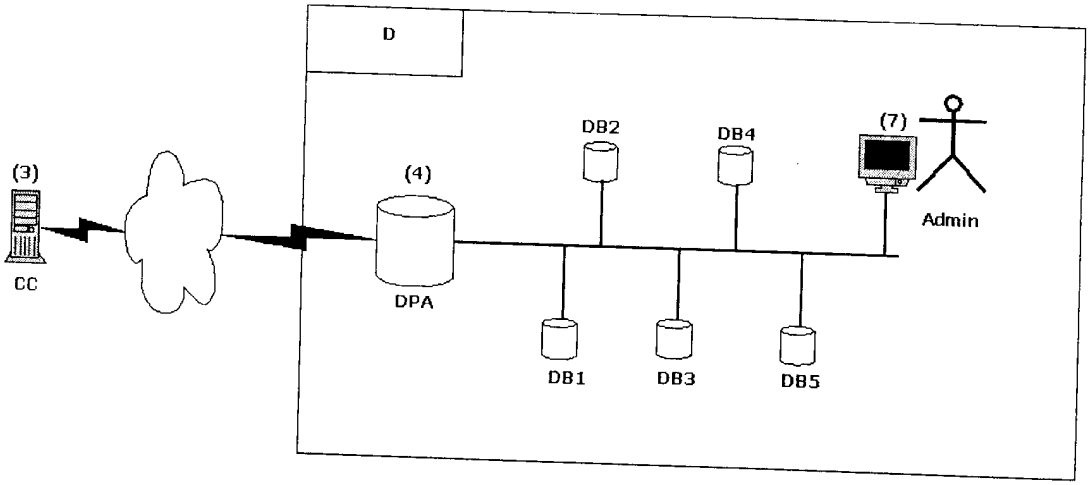

Figure 4