(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 812 422**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **01 09092**

(51) Int Cl[7] : **G 06 F 17/30,** H 04 L 12/22

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 09.07.01.

(30) **Priorité :** 20.07.00 US 09620440.

(43) **Date de mise à la disposition du public de la demande :** 01.02.02 Bulletin 02/05.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

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

(71) **Demandeur(s) :** *GE MEDICAL TECHNOLOGY SERVICES, INC.* — US.

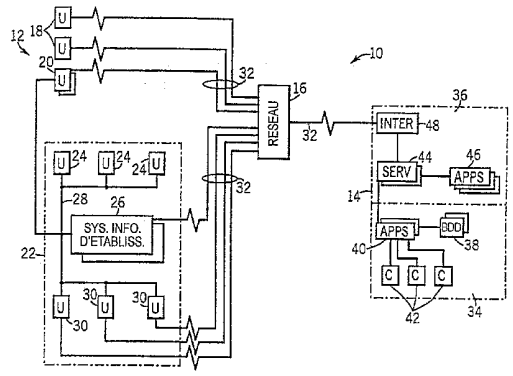
(72) **Inventeur(s) :** KOHLI JAMES FRANCIS.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CASALONGA ET JOSSE.

(54) PREPARATION ET REMISE SECURISEES DE RAPPORTS DE DONNEES.

(57) Il est proposé une technique sécurisée de mémorisation de données d'utilisateur et de génération de rapports utilisateur. Les données d'utilisateur sont saisies manuellement ou automatiquement et sont transmises à un fournisseur de services via un réseau (16). Les données sont mémorisées dans une base de données sécurisée (38) exploitée dans un espace de traitement (34) qui n'est pas directement accessible à l'utilisateur. En se basant sur des modèles de rapport pré-établis, des données d'utilisateur sont extraites de la base de données sécurisée et sont exportées depuis l'espace de traitement sécurisé pour être utilisées dans la génération de rapports utilisateur. Les rapports sont formés dans un second espace de traitement (36), par combinaison du fichier de données avec le modèle de rapport. Le rapport peut ensuite être transmis automatiquement à l'utilisateur, ou l'utilisateur peut y accéder via le réseau (16).



FR 2 812 422 - A1

PREPARATION ET REMISE SECURISEES DE RAPPORTS DE DONNEES

La présente invention concerne globalement le domaine de la collecte et l'analyse de données électroniques. En particulier, l'invention porte sur une technique de conservation sécurisée d'une base de données à des fins d'analyse et de génération de rapports, et sur l'accès sécurisé aux données et la génération sécurisée de rapports basés sur les données obtenues.

Une collecte et une mémorisation sécurisées de données sensibles à des fins de génération de rapports sont requises dans un nombre croissant de domaines. Comme les données sont disponibles sous un nombre croissant de formes et peuvent être collectées par des fonctions d'exploitation de réseau améliorées, les demandes d'une mémorisation de l'information et d'une génération de rapports sécurisées posent des défis croissants. A titre d'exemple, des établissements médicaux peuvent collecter des données médicales portant à la fois sur le fonctionnement de l'établissement et sur les conditions particulières de soins ou physiologiques d'un patient. Des professionnels médicaux peuvent avoir besoin des données pour analyser la santé du patient et pour prodiguer des soins supplémentaires. Toutefois, comme l'information est très sensible, des précautions sont à prendre pour sécuriser sa mémorisation et son accès. Des données relatives à l'utilisation d'équipements au sein d'établissements sont soumises à des exigences de confidentialité similaires. Dans le domaine financier, des enregistrements de transactions financières, telles que des comptes, des virements, des achats et ventes de titres et valeurs et autres, sont soumis aux mêmes exigences. Le chargé de clientèle ou le titulaire d'un compte, tout en exigeant un accès peut-être fréquent et rapide à l'information, souhaite que l'information soit mémorisée d'une manière très sécurisée qui protège à la fois l'identité du titulaire et l'intégrité des données, et qui interdit généralement tout accès non autorisé.

La sécurité de mémorisation des données et de génération de rapports est non seulement liée à la sensibilité des données dans des domaines individuels d'activité, mais est aussi défiée par les approches utilisées pour accéder aux données et transmettre des rapports basés sur elles. Par exemple, des données médicales doivent souvent être accessibles à distance à des médecins traitants ou des établissements, par transfert par des grands réseaux qui, bien qu'ils fournissent certaines mesures de sécurité, peuvent subir des accès non autorisés. D'une manière similaire, dans des transactions financières, les utilisateurs souhaitent de plus en plus pouvoir obtenir des enregistrements et rapports par des grands réseaux et des liaisons configurables similaires, tout en exigeant quand même une mémorisation des données et un accès à elles très sécurisés. Cela est particulièrement vrai dans l'utilisation croissante de l'Internet pour la mémorisation des données et leur accès à distance, en ce qui concerne la réalisation de transactions financières ou autres, la messagerie, etc.

Un secteur d'activité continue à améliorer la sécurité de mémorisation et d'accès aux données. Ces techniques incluent typiquement l'utilisation de mots de passe et d'autres codes

pour limiter l'accès aux personnes autorisées. D'une manière similaire, on a mis au point des techniques de chiffrement pouvant fournir des outils puissants dans le transfert de données, qui requièrent un déchiffrement par divers moyens et, d'une manière inhérente, limitent l'accès aux données ou au moins leur déchiffrement. Bien que ces techniques aient grandement amélioré la sécurité des données, d'autres améliorations sont nécessaires.

Dans de nombreux cas, des techniques complexes de transfert de données ne sont pas adaptées à la protection des données ou des rapports. En particulier dans des applications de l'Internet et d'autres réseaux, les utilisateurs peuvent souhaiter des approches plus directes pour obtenir des rapports basés sur leurs données sécurisées. Globalement, il serait souhaitable de proposer une technique directe qui, bien qu'étant essentiellement transparente pour l'utilisateur, forme une barrière très efficace entre le rapport et son fichier de remise, et le répertoire de la base de données sous-jacentes. En outre, comme des bases de données à grande capacité ou complètes peuvent inclure un large éventail d'informations, les performances du système peuvent être significativement dégradées par des demandes de rapports répétées et non anticipées. Les performances du système pourraient être fortement améliorées par une génération de rapports sécurisée, préprogrammée ou au moins périodique, séparant de nouveau en quelque sorte la fonction de remise de rapport des fonctions de génération de rapport et de mémorisation des données.

Il existe donc un besoin d'une technique améliorée pour la génération sécurisée de rapports basés sur des données sensibles mémorisées dans un répertoire de données. Il existe un besoin particulier d'une technique qui puisse être appliquée dans des cadres tels que des grands réseaux, en particulier l'Internet et sa descendance, pour l'accès sécurisé à des données sensibles et la génération sécurisée de rapports d'une manière qui n'affecte pas sensiblement les performances de la base de données ou de son logiciel d'accès et qui fournit le niveau souhaité de séparation entre la base de données et le logiciel générateur de rapport.

La présente invention propose une technique de génération sécurisée de rapports conçue pour répondre à ces besoins. On peut employer cette technique avec un large éventail de données sensibles incluant des dossiers médicaux, financiers, d'emploi, personnels, juridiques, etc. En outre, on peut employer cette technique dans un large éventail de cadres, mais elle est particulièrement puissante lorsqu'on l'applique à des rapports générés dans un espace de traitement relativement peu sécurisé, tel que par un agent Web pour une remise sur un grand réseau, conjointement avec des données mémorisées dans un espace de traitement plus sensible ou contrôlé. On peut employer ce système avec des techniques existantes de contrôle d'accès telles qu'une protection par mot de passe, un chiffrement, etc., pour fournir un niveau supplémentaire de protection des données et rapports.

Selon des aspects de la présente technique, des données sous-jacentes utilisées pour la génération des rapports sont mémorisées dans un espace de traitement qui est sécurisé et qui n'est généralement pas accessible à une classe d'utilisateurs incluant le correspondant auquel un rapport est destiné. Un modèle de rapport ou un dispositif logiciel similaire définit

les données qui sont requises pour la génération du rapport. Un fichier de données est donc créé dans l'espace de traitement et est mémorisé et exporté vers le premier espace de traitement pour la génération du rapport. Le modèle de rapport peut alors être complété dans le premier espace de traitement et mis à l'un quelconque de divers formats, tels que dans une page HTML. Le rapport peut alors être remis, par exemple par des grands réseaux, des réseaux privés virtuels, ou de n'importe quelle autre manière appropriée sans permettre à l'utilisateur d'accéder à l'espace de traitement plus contrôlé.

L'invention sera mieux comprise à l'étude de la description détaillée de quelques formes de réalisation, illustrée par les dessins annexés sur lesquels:

la figure 1 est une représentation schématique d'un système de collecte de données et de génération de rapports incorporant des aspects de la présente technique;

la figure 2 est une représentation schématique de composants fonctionnels du système de la figure 1 conçu pour la collecte de données d'utilisateur, leur mémorisation sécurisée et la génération sécurisée de rapports;

la figure 3 est un organigramme de données illustrant les sources de données utilisées dans la génération sécurisée de rapports réalisée par le système de la figure 2; et

la figure 4 est un schéma synoptique illustrant un exemple de logique de commande pour la collecte des données, leur mémorisation et la génération de rapports sécurisées selon des aspects de la présente technique.

A propos maintenant des dessins, et tout d'abord de la figure 1, un système 10 de collecte d'information et de génération de rapports est représenté schématiquement et est apte à recevoir des données d'utilisateur, à traiter et mémoriser les données d'utilisateur, et à générer des rapports basés sur les données d'utilisateur. Le système peut être employé dans un large éventail de cadres utilisant une mémorisation et une génération de rapports sécurisées de données relatives à un utilisateur, ou de données dérivées de données collectées. A titre d'exemple, des données collectées et rapportées dans le système 10 peuvent inclure des données médicales, des données financières, des dossiers personnels, des dossiers commerciaux, des documents confidentiels, des dossiers juridiques ou judiciaires, etc. Globalement, le système est particulièrement bien adapté à des applications dans lesquelles un ou des utilisateurs introduisent des données et exigent une exploitation confidentielle des données, et ont besoin d'obtenir périodiquement ou à la demande une sortie ou un rapport des mêmes données ou de données connexes. Tel que décrit plus bas, ces rapports peuvent être générés à la demande d'un utilisateur, ou selon des horaires pré-établis. De plus, le système est particulièrement bien adapté à des applications dans lesquelles des données d'utilisateur sont transmises par un réseau configurable, tel que l'Internet. Par conséquent, même si la mémorisation des données et la génération de rapports s'effectuent d'une manière qui protège le répertoire dans lequel les données sont mémorisées, des données et rapports concrets peuvent être transmis par un moyen quelque peu moins sécurisé. En outre, le système 10 est bien adapté à des applications dans lesquelles une base de données sécurisée n'est accessible qu'à une population limitée

d'utilisateurs ou d'applications logicielles spécifiques, pour améliorer ainsi sensiblement la sécurité de la base de données et réduire le nombre de consultations individuelles de la base de données, et améliorer les performances du système.

Tel que représenté sur la figure 1, le système 10 inclut diverses sources de données, globalement repérées 12, qui communiquent avec un fournisseur de services 14 par l'intermédiaire d'un réseau 16, tel que l'Internet. On remarquera cependant qu'on peut employer d'autres réseaux dans la présente technique, incluant des réseaux internes, des réseaux spécialisés, des réseaux privés virtuels, etc. Parmi les sources de données, des utilisateurs individuels 18 peuvent directement contacter ou être contactés par le fournisseur de services 14. De plus, des utilisateurs consultants 20, qui peuvent être en liaison permanente ou intermittente avec des établissements 22, peuvent aussi constituer des sources de données tel que décrit plus bas. Ces consultants peuvent inclure des consultants financiers, des techniciens, des ingénieurs services, etc.

Lorsque des établissements 22 sont inclus dans le système, ils peuvent inclure en leur sein divers utilisateurs et systèmes d'utilisateurs qui peuvent aussi constituer des sources de données. Par exemple, des utilisateurs individuels 24 peuvent être reliés à un système informatique 26 d'un établissement, par exemple via un intranet 28, par exemple à topographie Ethernet. D'une manière similaire, d'autres utilisateurs 30 peuvent être présents dans l'établissement et être aussi reliés au système informatique de l'établissement. Les utilisateurs à l'intérieur de l'établissement peuvent former différentes classes ou groupes, par exemple dans lesquels les utilisateurs 24 ne peuvent accéder à des sources d'information éloignées, telles que le fournisseur de services 14, que par l'intermédiaire du système informatique de l'établissement ou d'autres circuits de transfert de données. Les autres utilisateurs 30 peuvent être munis de circuits et logiciels d'interface de télécommunication individuels, spécialisés ou autres particuliers pour accéder directement aux sources d'information éloignées.

Les utilisateurs 18, 20, 24 et 30, ainsi que des services informatiques 26 de l'établissement, peuvent être reliés au réseau 16 par n'importe quel circuit approprié. A titre d'exemple, les utilisateurs peuvent être raccordés à l'Internet par des modems conventionnels, des modems câble, des modems sans fil, des banques de modem, des serveurs, ou n'importe quel autre dispositif de télécommunication. En outre, bien que des liaisons réseau 32 soient représentées pour chacun des utilisateurs, celles-ci peuvent, en pratique, constituer n'importe quel moyen approprié, employant divers protocoles de télécommunication tels que TCP/IP. Le fournisseur de services 14 est aussi relié au réseau 16 par une liaison réseau 32, qui est compatible avec le réseau et les liaisons réseau employées par les utilisateurs.

Le fournisseur de services 14 est généralement utilisé ou contacté par les utilisateurs pour une mémorisation et un accès à des données et rapports. Le fournisseur de services peut donc constituer un simple fournisseur de données, ou peut offrir d'autres services aux utilisateurs, tels que des services financiers, médicaux, techniques, etc. Pour une

mémorisation et un traitement sécurisés des données des utilisateurs, le fournisseur de services 14 inclut des capacités de traitement divisées en un premier espace de traitement sécurisé 34, et un second espace de traitement 36 auquel les utilisateurs peuvent globalement accéder pour introduire des données et recevoir des rapports.

A l'intérieur de l'espace de traitement sécurisé 34, le fournisseur de services 14 inclut une ou plusieurs bases de données 38 qui ne sont pas globalement accessibles aux utilisateurs. On remarquera que la base de données 38 peut inclure un éventail de bases de données connexes ou étroitement reliées et peut être mémorisée dans un ou plusieurs dispositifs de mémorisation en un ou plusieurs emplacements, en particulier pour les plus grandes bases de données, et dans un but de redondance et de sauvegarde. Plusieurs applications 40 sont exploitées à l'intérieur de l'espace de traitement sécurisé 34, par exemple pour l'enregistrement d'informations dans la base de données 34, l'accès à des données de la base de données, etc. On remarquera qu'on peut employer n'importe quelle configuration matérielle appropriée pour exploiter les applications 40, incluant des ordinateurs personnels, des postes de travail, des macro-ordinateurs, etc. Si on le souhaite, le fournisseur de services 14 peut inclure une série de postes clients 42 reliés via les applications 40 à la base de données, et aux utilisateurs, de manière à permettre une maintenance de la base de données et des applications, et de coordonner la circulation des données à l'intérieur du système informatique du fournisseur de services.

A l'intérieur du second espace de traitement 36, le fournisseur de services 14 peut inclure un ou plusieurs serveurs 44 qui mémorisent et dirigent des données entre les utilisateurs et l'espace de traitement sécurisé 34. Plusieurs applications 46 sont accessibles aux serveurs 44, par exemple pour le formatage et la remise de rapports, et pour la réception de données d'utilisateur, tel que décrit plus bas. Un circuit d'interface 48 est prévu pour envoyer et recevoir des données via un réseau 16.

On remarquera que, si on le souhaite, le fournisseur de services 14 peut inclure d'autres circuits et systèmes de traitement des données et de communication avec les utilisateurs. A titre d'exemple, un établissement médical ou une installation de services médicaux peut inclure un large éventail d'outils analytiques aptes à traiter et analyser les données d'utilisateur pour évaluer un niveau d'équipement, des performances financières d'un établissement, etc. De même, un fournisseur de services financiers peut inclure des dossiers relatifs aux comptes, aux historiques des utilisateurs, etc. En outre, le fournisseur de services 14 peut inclure d'autres composants fonctionnels pour transmettre et recevoir des informations à et depuis des utilisateurs, par exemple par l'intermédiaire de sites Web, d'applications et logiciels spécialisés, et équivalents.

La figure 2 représente certains de composants fonctionnels du système de la figure 1, spécifiquement aptes à transmettre et recevoir des données, mémoriser les données d'une manière sécurisée, et générer des rapports sur les données d'une manière sécurisée. Tel que représenté sur la figure 2, le système est particulièrement bien adapté à un raccordement aux utilisateurs 18, 20, 24, 26 et 30 via des applications réseau conventionnelles telles qu'un

navigateur 50 de client. Si on le souhaite, on peut employer n'importe quelle autre application d'interface réseau, et le navigateur 50 peut être exploité sur n'importe quel système informatique approprié, tel qu'un ordinateur personnel ou un poste de travail conventionnels. D'autres applications 52 complètent le navigateur 50, par exemple pour la mémorisation de données d'utilisateur ou l'exécution de calculs sur les données d'utilisateur. Le navigateur 50, et toutes les éventuelles applications d'interface réseau requises, communiquent avec un serveur, tel qu'un serveur Web 44 du fournisseur de services par l'intermédiaire d'au moins un dispositif 54 d'isolation et de protection tel qu'un coupe-feu. Le serveur Web 44, qui est apte à exploiter des applications logicielles d'interface avec le navigateur du client, est complété par les matériels et logiciels 46 exploités à l'intérieur de l'espace de traitement 36 du fournisseur de services. En particulier, un module d'interface 56 coopère avec le serveur Web pour recevoir des données des utilisateurs et les introduire dans l'espace de traitement sécurisé 34. Le module d'interface 56 coopère donc avec un module d'interface 56 similaire exploité à l'intérieur de l'espace de traitement sécurisé 34 par l'intermédiaire d'un autre dispositif 58 d'isolation et de protection, tel qu'un coupe-feu interne du système informatique du fournisseur de services. Le module d'interface 56 et le coupe-feu 58 servent à transmettre des données d'utilisateur à la base de données sécurisée 38, et à isoler la base de données d'un accès direct aux utilisateurs. A l'intérieur de l'espace de traitement sécurisé 34, le fournisseur de services inclut un module 60 générateur de rapport qui est conçu pour extraire des données désirées de la base de données sécurisée 38 en vue de générer des rapports utilisateur.

A l'intérieur de l'espace de traitement 36 du fournisseur de services, une ou plusieurs applications et un ou plusieurs fichiers sont mémorisés pour la génération, le formatage, la mémorisation et la transmission de rapports d'utilisateur basés sur les données extraites par le module 60 générateur de rapport. Dans la forme de réalisation représentée sur la figure 2, un contenu Web 62 est mémorisé dans l'espace de traitement 36 et inclut des instructions pour le formatage de rapports pouvant être remis par le réseau. Une application, telle qu'un agent Web 64, accède au contenu Web 62 pour générer des rapports basés sur des modèles de rapport prédéfinis. En général, le modèle de rapport définit les données spécifiques de la base de données sécurisée 38 qui sont requises pour générer un rapport d'utilisateur. Tel que décrit plus bas, grâce au modèle de rapport prédéfini et mémorisé dans le second espace de traitement 36, le générateur de rapport 60 est apte à extraire les données requises de la base de données sécurisée 38 et à générer un fichier de données 66. Le fichier de données 66, qui est de préférence spécifique à l'utilisateur et au rapport, peut inclure des données brutes de la base de données sécurisée, ainsi que des données traitées telles que des données combinées à, comparées à ou autrement analysées avec des données provenant de la base de données sécurisée ou d'autres sources pour générer le fichier de données. Le fichier de données 66 est ensuite exporté de l'espace de traitement sécurisé 34 au second espace de traitement 36 via le coupe-feu 58.

L'agent Web 64, conjointement avec n'importe quel contenu Web 62 mémorisé dans l'espace de traitement 36, formate un rapport d'utilisateur pour générer un fichier de rapport 68 basé sur le fichier de données et sur le contenu Web. Tel que mentionné plus haut, le contenu Web inclut généralement un modèle de rapport et des instructions pour le formatage du rapport. Dans une configuration présentement préférée, l'agent Web formate le fichier de rapport 68 pour générer un rapport présentable à l'utilisateur sous la forme d'une série de pages HTML. Si on le souhaite, on peut employer d'autres langages et formats de rapport. Le fichier de rapport 68 est mémorisé dans l'espace de traitement 36, depuis lequel il est remis à l'utilisateur par le serveur Web 44.

Les diverses entrées considérées pour la création des rapports générés par le générateur de rapport 60, conjointement avec l'agent Web 64 et le serveur 44, peuvent inclure à titre d'exemple celles illustrées sur la figure 3. En général, les rapports peuvent inclure à la fois des données d'utilisateur provenant de la source de données sécurisée 38 et des données formant le modèle de rapport, repéré 70 sur la figure 3. Tel que mentionné plus haut, le fichier de modèle de rapport est mémorisé dans l'espace de traitement 36 et est employé dans la définition du fichier de données généré par le générateur de rapport 60, et dans la compilation du rapport basé sur le fichier de données en vue d'une transmission à l'utilisateur. En outre, le générateur de rapport utilise des données de sources qui incluent les utilisateurs eux-mêmes tel que représenté sur la figure 3. Tel que mentionné plus haut, comme l'espace de traitement sécurisé 34 n'est globalement pas directement accessible à l'utilisateur, ces données d'utilisateur vont typiquement être dirigées à travers des modules d'interface 56, tel que représenté sur la figure 2. D'autres sources de données pour les rapports incluent des systèmes informatiques 26 d'établissements, qui peuvent générer des données dérivées de données d'utilisateurs particuliers. D'autres bases de données peuvent aussi servir de base pour les rapports. Tel que représenté sur la figure 3, d'autres bases de données 72 peuvent inclure des bases de données publiques, des bases de données à abonnement, des bases de données spéciales contenues ou compilées par le fournisseur de services, etc. A titre d'exemple, lorsqu'une information d'évaluation ou de comparaison est incluse dans les rapports, la base de données utilisée pour ces comparaisons peut être compilée par le fournisseur de services, par exemple en se basant sur une population connue d'utilisateurs comparables à l'utilisateur pour lequel le rapport est généré. Des bases de données historisées 74 peuvent aussi être employées pour la génération du rapport. Ces bases de données historisées peuvent inclure des données historisées relatives à l'utilisateur, telles que des données de transactions, de services exécutés pour l'utilisateur, d'achats de l'utilisateur, d'inventaires de l'utilisateur, de comptes de l'utilisateur, etc.

En se basant sur ces entrées, le générateur de rapport 60 crée le fichier de données tel que décrit plus haut et exporte le fichier de données vers l'agent Web 64. La flèche tracée en trait interrompu sur la figure 3 indique que l'agent Web 64 peut aussi employer certaines des sources utilisées par le générateur de rapport. Par conséquent, certaines des données utilisées pour générer le rapport final peuvent être mémorisées dans ou accessibles depuis le

second espace de traitement 36. Une fois que le fichier de rapport a été généré par l'agent Web 64 et mémorisé dans l'espace de traitement 36, le serveur 44 est utilisé pour la remise du rapport tel que décrit plus bas.

La figure 4 illustre des étapes exemplaires d'une logique de commande pour la mémorisation de données d'utilisateur et la génération de rapports sécurisées et avec une intervention minimale dans le fonctionnement de la base de données sécurisée. La logique de commande exemplaire de la figure 4 peut être divisée en une séquence 78 de collecte de données et une séquence 80 de rapport. La séquence 78 de collecte de données commence par une saisie de données d'utilisateur. Cette saisie peut inclure n'importe quelle séquence d'étapes appropriée, et peut en général inclure une saisie de données hors ligne, repérée 82. Cette saisie hors ligne peut être réalisée pendant que des services sont fournis à un utilisateur, ou pendant que l'utilisateur exécute des fonctions ou demande des services ou des transactions au fournisseur de services. La saisie de données peut aussi se produire en ligne, tel que repéré 84, par exemple durant la fourniture de services. En outre, la saisie de données peut inclure des séquences automatiques d'acquisition de données, telles que des séquences dans lesquelles le serveur du fournisseur de services accède à et télécharge des informations automatiquement depuis des postes d'utilisateur, un équipement à abonnement, etc.

Après l'introduction initiale des données, une connexion est établie entre l'utilisateur et le fournisseur de services à une étape 88. Tel que mentionné plus haut, la connexion réseau entre l'utilisateur et le fournisseur de services peut être indirecte, par exemple pour des utilisateurs connectés au réseau d'un établissement. A une étape 90, les données sont transmises de l'utilisateur au fournisseur de services, et à une étape 92 les données sont synchronisées avec les données de la base de données. L'opération de synchronisation exécutée à l'étape 92 est conçue pour garantir une mémorisation des données d'utilisateur les plus récentes dans la base de données sécurisée. Si on le souhaite, l'introduction des données, incluant la saisie originale des données et/ou la synchronisation des données avec la base de données sécurisée, peut être limitée à des utilisateurs ou postes spécifiques, avec utilisation d'une protection par mot de passe, d'un chiffrement, ou de n'importe quelle autre technique appropriée pour limiter ou restreindre la saisie de données et pour assurer l'intégrité des données d'utilisateur dans la base de données sécurisée.

Une fois que les données d'utilisateur sont mémorisées dans la base de données sécurisée, des rapports peuvent être générés, comme l'indique la séquence 80 de rapport. En général, ces rapports sont de préférence créés conformément à un modèle qui est créé à une étape 94. Tel que mentionné plus haut, le modèle est de préférence mémorisé dans le second espace de traitement 36 conservé par le fournisseur de services. Les données requises pour compléter ou remplir le rapport sont donc définies à une étape 96 en se basant sur le modèle de rapport. On remarquera que des rapports très divers peuvent être créés à l'étape 94, les données correspondantes étant définies à l'étape 96. Les rapports peuvent inclure des rapports spécifiques à un utilisateur ou une transaction, ainsi qu'une série de "rapports

virtuels" comprenant, par exemple, des pages présentables à l'utilisateur et sur lesquelles l'utilisateur peut naviguer à l'aide d'un navigateur Web conventionnel. A une étape 98, le modèle de rapport est mémorisé en vue d'une utilisation dans la compilation et le formatage du rapport.

Des rapports peuvent être générés à la demande des utilisateurs, comme l'indique une étape 100 sur la figure 4, ou conformément à un horaire régulier, comme l'indique une étape 102. Dans une forme de réalisation préférée, la programmation des rapports est préférée lorsque l'utilisation de la base de données (par exemple, le nombre d'accès à la base de données pour extraire des données d'utilisateur) peut ralentir ou autrement paralyser les performances du système. En fonction des données d'utilisateur, et du cycle des rapports, ces rapports peuvent être programmés régulièrement pour être générés d'une manière mensuelle, hebdomadaire, quotidienne, ou autre.

Une fois que la génération d'un rapport a été déclenchée soit par une demande soit par un horaire régulier, le fichier de données sécurisé décrit plus haut est créé à une étape 104. Tel que mentionné plus haut, le fichier est créé par extraction de données d'utilisateur de la base de données sécurisée, conformément aux données définies par le modèle de rapport. A une étape 106 le fichier de données est exporté de l'espace de traitement sécurisé 34 à l'espace de traitement 36. A l'intérieur de l'espace de traitement 36, le fichier de données est combiné au modèle de rapport pour créer le rapport, comme l'indique une étape 108. Le rapport terminé est ensuite transmis à l'utilisateur, comme l'indique une étape 110. On remarquera que, si on le souhaite, le rapport peut être mémorisé après sa création et peut être conservé pendant une période de temps prédéterminée, pour permettre de nouveau à l'utilisateur d'accéder à, de transmettre, de revoir, et de manipuler autrement le rapport à distance. Dans ce cas, un simple avis peut être transmis à l'utilisateur à l'étape 110 à la première occasion, l'utilisateur accédant au rapport à un instant ultérieur qui lui convient via le serveur du fournisseur de services et la connexion réseau.

Bien que l'invention soit susceptible de diverses modifications et variantes, des formes de réalisation spécifiques ont été représentées à titre d'exemple sur les dessins et décrites en détail dans la présente. On comprendra toutefois que l'invention ne se limite pas aux formes particulières décrites. L'invention englobe plutôt toutes les modifications, équivalents et variantes tombant dans l'esprit et la portée de l'invention telle qu'elle est définie par les revendications annexées qui suivent.

REVENDICATIONS

1. Procédé de génération sécurisée de rapports en vue d'une transmission par un réseau configurable, caractérisé par les étapes de:

mémorisation (82, 84, 86) de données d'un utilisateur (18, 20) dans un répertoire de données sécurisé (38) exploité dans un premier espace de traitement (34) inaccessible à l'utilisateur;

accès (104) à des données du répertoire pour créer un fichier de données sécurisé (66) dans le premier espace de traitement;

transmission du fichier de données sécurisé (66) à un second espace de traitement (36) séparé du premier espace de traitement par un dispositif de sécurité (58); et

génération (108) du rapport (68) dans le second espace de traitement en se basant sur le fichier de données sécurisé, en vue d'une transmission à l'utilisateur via le réseau configurable (16).

2. Procédé selon la revendication 1, caractérisé en outre par une génération d'un modèle de rapport (70) définissant des données de rapport à présenter dans le rapport, le fichier de données sécurisé (66) étant généré en se basant sur les données de rapport.

3. Procédé selon la revendication 2, caractérisé en outre par une mémorisation (94) du modèle de rapport (70) dans le second espace de traitement (36).

4. Procédé selon la revendication 3, caractérisé en ce que le rapport (68) est généré dans le second espace de traitement (36) en se basant sur le modèle de rapport (70) et le fichier de données sécurisé (66).

5. Procédé selon la revendication 1, caractérisé en outre par un formatage du rapport dans le second espace de traitement (36) en vue d'une transmission à l'utilisateur via le réseau configurable (16).

6. Procédé selon la revendication 5, caractérisé en ce que le rapport (68) est formaté comme au moins une page présentable à l'utilisateur dans un langage de balisage.

7. Procédé selon la revendication 5, caractérisé en ce que le réseau configurable (16) inclut l'Internet.

8. Procédé selon la revendication 1, caractérisé en ce que le second espace de traitement (36) est séparé du réseau configurable (16) par un second dispositif de sécurité (54).

9. Procédé selon la revendication 1, caractérisé en ce que l'accès (104) aux données est réalisé conformément à un horaire prédéterminé de rapport.

10. Procédé selon la revendication 1, caractérisé en ce que l'accès (104) aux données est réalisé en réponse à une invite de l'utilisateur pour la génération de rapport.

11. Procédé selon la revendication 1, caractérisé en ce que le dispositif de sécurité (58) inclut un coupe-feu.

12. Procédé selon la revendication 1, caractérisé en outre par une génération automatique (110) d'un message d'avertissement indicatif de la disponibilité du rapport (68), et une transmission du message d'avertissement à l'utilisateur via le réseau configurable.

13. Procédé selon la revendication 12, caractérisé en ce que le rapport (68) est conservé dans le second espace de traitement (36) au moins jusqu'à ce que l'utilisateur accède au rapport via le réseau configurable (16).

14. Procédé de génération sécurisée de rapports de données associées à un utilisateur, caractérisé par les étapes de:

mémorisation (82, 84, 86) de données d'utilisateur associées à l'utilisateur dans un premier répertoire de données;

transmission d'au moins une partie des données d'utilisateur du premier répertoire de données à un second répertoire de données (38) exploité dans un premier espace de traitement (34) inaccessible à l'utilisateur;

définition (94) d'un modèle de rapport, le modèle de rapport identifiant les données à présenter dans un rapport (68);

génération d'un fichier de données sécurisé (66) dans le premier espace de traitement (34) comprenant des données identifiées dans le modèle de rapport;

exportation (106) du fichier de données sécurisé (66) vers un second espace de traitement (36) séparé du premier espace de traitement et inaccessible à l'utilisateur; et

génération (108) du rapport (68) dans le second espace de traitement (36) en se basant sur le modèle (94) et le fichier de données (66).

15. Procédé selon la revendication 14, caractérisé en ce que les données d'utilisateur sont mémorisées dans le premier répertoire de données et sont synchronisées (92) avec des données mémorisées dans le second répertoire de données (38).

16. Procédé selon la revendication 14, caractérisé en ce que le premier espace de traitement (34) est séparé du second espace de traitement (36) par un coupe-feu (58).

17. Procédé selon la revendication 14, caractérisé en ce que les données d'utilisateur sont transmises du premier répertoire de données au second répertoire de données (38) durant une séquence (86) de collecte de données automatisée.

18. Procédé selon la revendication 14, caractérisé en ce que le fichier de données sécurisé (66) est généré conformément à un horaire prédéterminé de génération de rapport.

19. Procédé selon la revendication 14, caractérisé en ce que le rapport (68) est mémorisé dans le second espace de traitement (36) au moins jusqu'à ce que l'utilisateur y accède.

20. Système pour la génération de rapports de données d'utilisateur, caractérisé par:

un répertoire de données sécurisé (38) exploité dans un premier espace de traitement (34) pour mémoriser des données d'utilisateur introduites via un réseau configurable, le premier espace de traitement étant inaccessible à l'utilisateur (18, 20) via le réseau (16);

un module (40) de programme d'accès aux données, exploité dans le premier espace de traitement (34) pour extraire des données de rapport (66) du répertoire de données sécurisé (38);

un second répertoire de données (44) exploité dans un second espace de traitement (36) séparé d'une manière sécurisée du premier espace de traitement (34) pour mémoriser les données de rapport extraites par le module de programme d'accès aux données;

un modèle de rapport (70) mémorisé dans le second espace de traitement (36); et

un module (60) de programme générateur de rapport, exploité dans le second espace de traitement (36) pour la génération d'un rapport (68) en se basant sur les données de rapport (66) et le modèle de rapport (70).

21. Système selon la revendication 20, caractérisé en ce que le module (40) de programme d'accès aux données est configuré pour extraire les données désirées conformément à un horaire prédéterminé.

22. Système selon la revendication 20, caractérisé en ce que le second répertoire de données (44) est configuré pour mémoriser le rapport (68).

23. Système selon la revendication 20, caractérisé en ce que le second répertoire de données (44) est accessible à l'utilisateur via le réseau (16).

24. Système selon la revendication 20, caractérisé par un serveur couplé au second répertoire de données (44) pour transmettre le rapport (68) à l'utilisateur.

25. Système selon la revendication 24, caractérisé en ce que le serveur est configuré pour être connecté à un grand réseau (16), et pour transmettre le rapport (68) à l'établissement médical (22) via le grand réseau (16).

26. Système selon la revendication 20, caractérisé en ce que les premier et second espaces de traitement (34, 36) sont séparés par un coupe-feu (58).

27. Système pour la génération sécurisée de rapports en vue d'une transmission par un réseau configurable, caractérisé par:

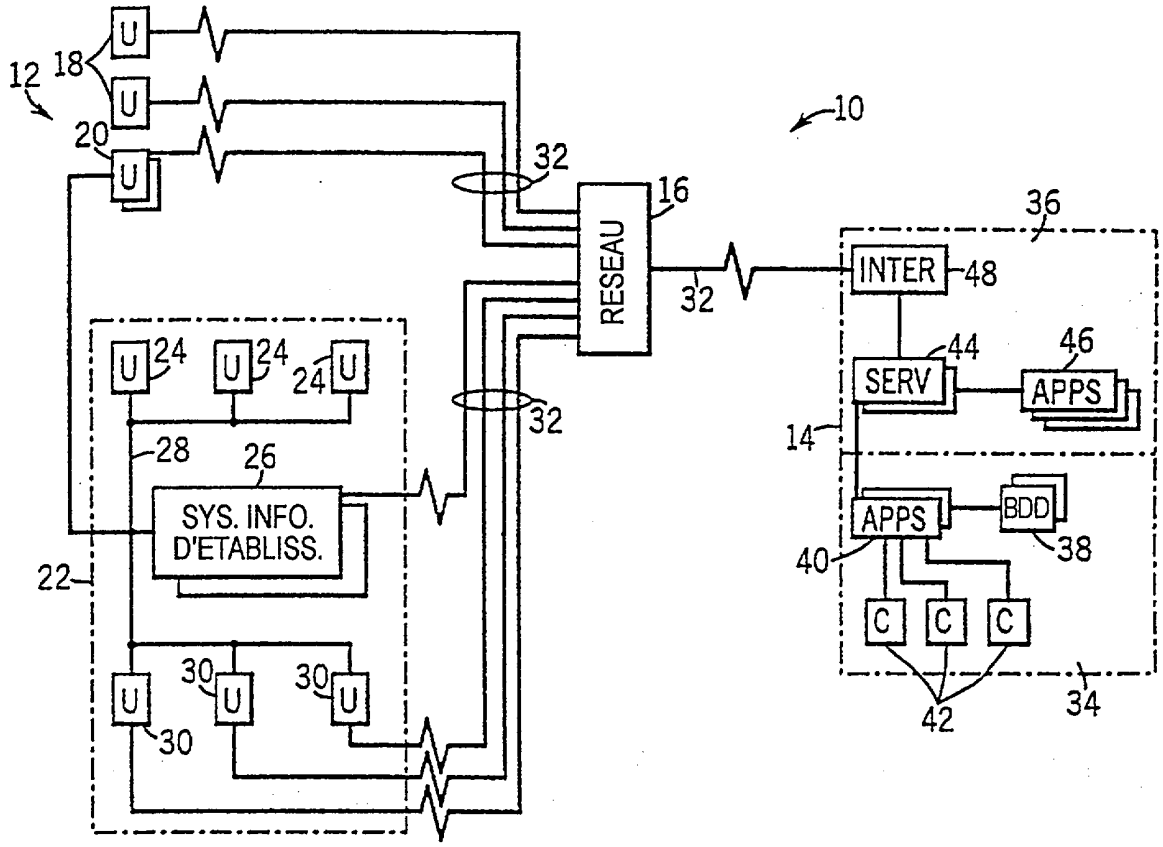
un moyen (38) pour mémoriser des données d'un utilisateur (18, 20) dans un répertoire de données sécurisé (38) exploité dans un premier espace de traitement (34) inaccessible à l'utilisateur;

un moyen (60) pour accéder aux données du répertoire afin de créer un fichier de données sécurisé (66) dans le premier espace de traitement;

un moyen (60, 64) pour transmettre le fichier de données sécurisé à un second espace de traitement (36) séparé du premier espace de traitement par un dispositif de sécurité (58); et

un moyen (60) pour générer le rapport (68) dans le second espace de traitement (36) en se basant sur le fichier de données sécurisé (66) en vue d'une transmission à l'utilisateur via le réseau configurable (16).

FIG. 1


12
18
20
U
10
32
16
RESEAU
36
INTER
48
44
SERV
46
APPS
14
24
28
26
SYS. INFO.
D'ETABLISS.
22
30
BDD
38
40
C
42
34

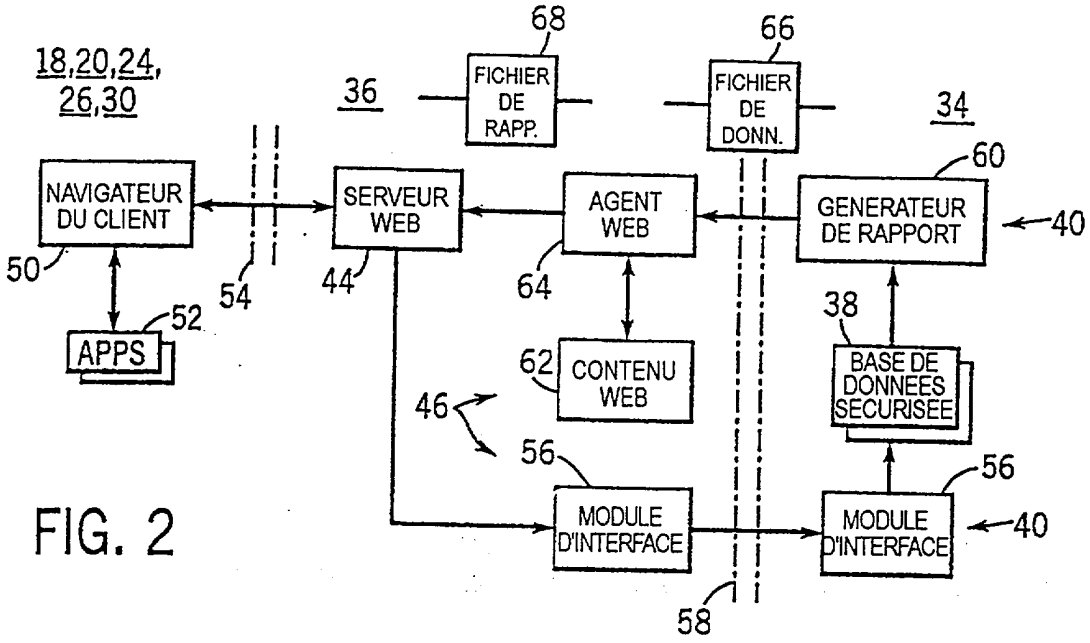

18,20,24,
26,30
36
68
FICHIER DE RAPP.
66
FICHIER DE DONN.
34
NAVIGATEUR DU CLIENT
SERVEUR WEB
AGENT WEB
GENERATEUR DE RAPPORT
60
40
50
54
44
64
52
APPS
38
62
CONTENU WEB
BASE DE DONNEES SECURISEE
46
56
56
MODULE D'INTERFACE
MODULE D'INTERFACE
40
58

FIG. 2

FIG. 3

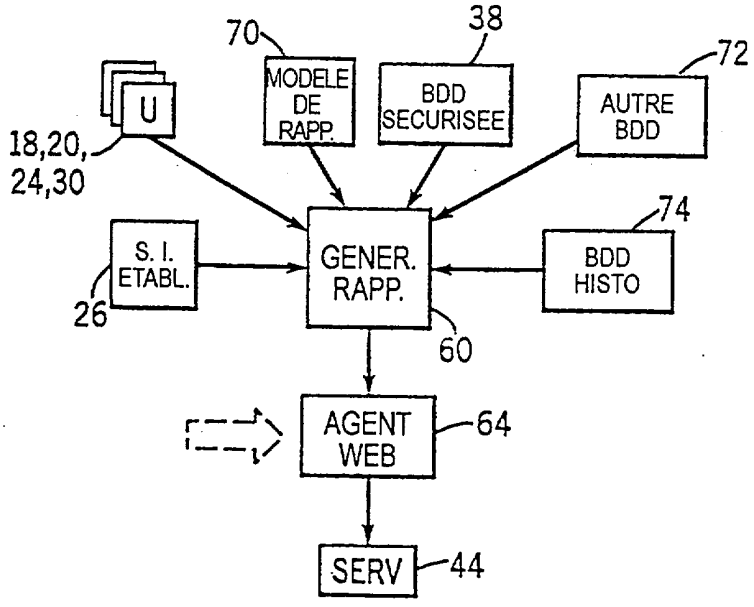
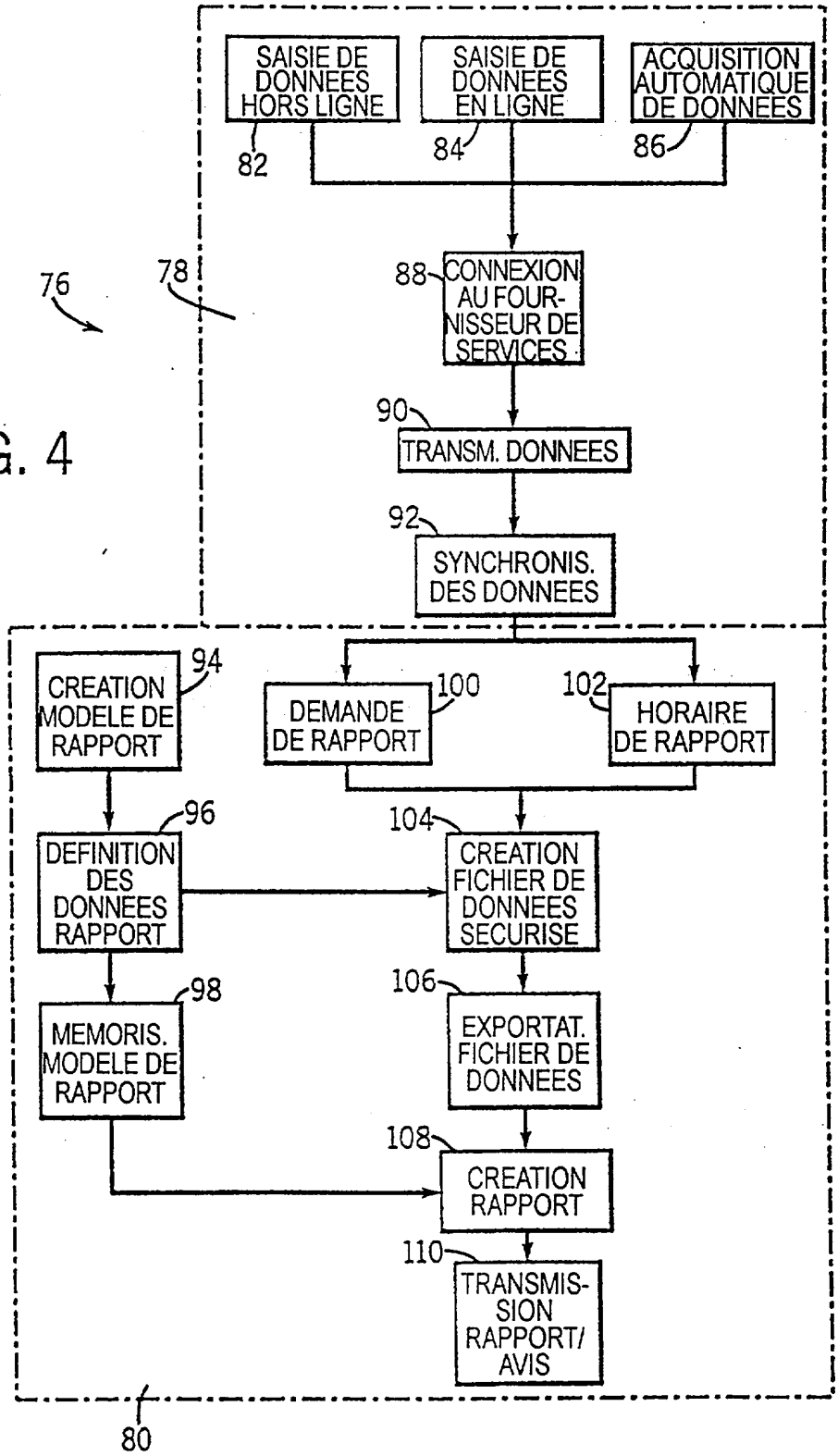

70
38
72
U
MODELE DE RAPP.
BDD SECURISEE
AUTRE BDD
18,20,
24,30
74
S. I. ETABL.
GENER. RAPP.
BDD HISTO
26
60
AGENT WEB
64
SERV
44

FIG. 4


SAISIE DE DONNEES HORS LIGNE
82
SAISIE DE DONNEES EN LIGNE
84
ACQUISITION AUTOMATIQUE DE DONNEES
86
76
78
88
CONNEXION AU FOURNISSEUR DE SERVICES
90
TRANSM. DONNEES
92
SYNCHRONIS. DES DONNEES
CREATION MODELE DE RAPPORT
94
DEMANDE DE RAPPORT
100
102
HORAIRE DE RAPPORT
DEFINITION DES DONNEES RAPPORT
96
104
CREATION FICHIER DE DONNEES SECURISE
MEMORIS. MODELE DE RAPPORT
98
106
EXPORTAT. FICHIER DE DONNEES
108
CREATION RAPPORT
110
TRANSMISSION RAPPORT/ AVIS
80