ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) **BREVET D'INVENTION**

(11) N° de publication :
MA 54262 A1

(43) Date de publication :
31.03.2023

(51) Cl. internationale :
G06F 21/60; G06F 21/62; G06N 3/04; H04L 9/00

(21) N° Dépôt :
54262

(22) Date de Dépôt :
27.08.2021

(71) Demandeur(s) :
Université internationale de Rabat, PARC TECNOPOLIS RABAT-SHORE CAMPUS UNIVERSITAIRE UIR ROCADE RABAT-SALE 11100 SALE (MA)

(72) Inventeur(s) :
Boulmalf Mohamed ; KARTIT ALI ; ZKIK KARIM

(74) Mandataire :
Bouya Mohsine

(54) Titre : **Système basé sur le cryptage homomorphe pour sécuriser les images médicales dans le cloud computing.**

(57) Abrégé : La présente invention concerne un système basé sur le cryptage homomorphe pour sécuriser les images médicales stockées dans le cloud computing. Elle a comme objectif de réduire les risques de sécurité associés à la technologie cloud, mais également pour traiter les textes chiffrés. En effet, ce nouveau système est basé sur la fonction MapReduce pour bénéficier du parallélisme lors du traitement des données et le framework Hadoop pour développer et implémenter des applications sécurisées de traitement d'images médicales dans le cloud. Hadoop et MapReduce sont en conjonction avec un système multi-agents pour effectuer un traitement de données distribué. De plus, et pour assurer une gestion efficace de la charge de travail des machines virtuelles (VM) et ainsi garantir l'équilibrage de charge, notre système utilise une méthode basée sur l'algorithme Bat (BA). En fin, ce système qui garantit la confidentialité des données est abordable pour tous les fournisseurs de serveurs basés sur le cloud qui souhaitent protéger leurs bases de données médicales.

MA 54262A1

Titre :

Système basé sur le cryptage homomorphe pour sécuriser les images médicales dans le cloud computing.

ABREGE :

La présente invention concerne un système basé sur le cryptage homomorphe pour sécuriser les images médicales stockées dans le cloud computing. Elle a comme objectif de réduire les risques de sécurité associés à la technologie cloud, mais également pour traiter les textes chiffrés. En effet, ce nouveau système est basé sur la fonction MapReduce pour bénéficier du parallélisme lors du traitement des données et le framework Hadoop pour développer et implémenter des applications sécurisées de traitement d'images médicales dans le cloud. Hadoop et MapReduce sont en conjonction avec un système multi-agents pour effectuer un traitement de données distribué. De plus, et pour assurer une gestion efficace de la charge de travail des machines virtuelles (VM) et ainsi garantir l'équilibrage de charge, notre système utilise une méthode basée sur l'algorithme Bat (BA). En fin, ce système qui garantit la confidentialité des données est abordable pour tous les fournisseurs de serveurs basés sur le cloud qui souhaitent protéger leurs bases de données médicales.

Description :

La présente invention se rapporte à un nouveau système basé sur le cryptage homomorphe pour sécuriser les images médicales dans le cloud computing.

Etat de l'art antérieur

Ces dernières années, il y a eu une demande croissante pour l'adoption du cloud dans les soins de santé pour traiter les données médicales. Malheureusement, ce nouveau paradigme émergent fait face à plusieurs défis, car les données des clients sont stockées sur des serveurs distants plutôt que sur des solutions sur site. Ceci est considéré comme la cause principale des failles de sécurité rencontrées dans les calculs externalisés. En effet, pour résoudre ce problème, plusieurs travaux de recherche sont menés dans ce sens à savoir l'utilisation d'algorithmes cryptographiques classiques tels que RSA (Rivest, Shamir et Adleman), DES (Data Encryption Standard) et AES (Advanced Encryption Standard).

Dans ce sens, le brevet **US20130339722** propose une méthode de protection des données basée sur le chiffrement homomorphe complet dans laquelle le client crypte les données en utilisant un chiffrement entièrement homomorphe et les envoie au serveur. Le serveur du cloud effectue des calculs sans déchiffrer les données et envoie le résultat du calcul chiffré au client. Cependant, cette méthode impose des clés de cryptage très longues et les données chiffrées prennent beaucoup plus de place que les données en clair. Les calculs sur ces données chiffrées volumineuses sont généralement plus lents ce qui nécessite un matériel performant du coté client pour effectuer les opérations de chiffrement et déchiffrement.

Dans le brevet **MA 42881 A1**, les inventeurs ont présenté un système sécurisé de stockage et traitement des données en se basant sur un chiffrement homomorphe. Pour profiter des avantages de chiffrement homomorphe complet sans avoir besoin de ressources informatiques performantes du coté client, ils ont

combinés à la fois le chiffrement additif pour les fonctions utilisant des opérations d'addition et soustraction en faisant recours à l'algorithme de Paillier et le chiffrement multiplicatif pour les fonctions utilisant des opérations de multiplication et de division en faisant recours à l'algorithme RSA.

Malheureusement, aucun de ces deux brevets n'a traité les problèmes liés à la sécurité des images médicales dans le cloud computing. En effet, sécuriser le processus de traitement des images nécessite généralement des techniques plus innovantes pour sécuriser les services cloud. Il existe maintenant une variété de méthodes pour résoudre ce problème, y compris l'architecture orientée services (SOA), les techniques de chiffrement homomorphes, les schémas de partage de secrets Shamir (SSS) et les méthodes de segmentation.

En effet, nous proposons une analyse des cadres actuels pour évaluer leurs limites et faire des recommandations appropriées. Dans ce contexte, les auteurs **Challa, RK, Kakinada, J, Vijaya Kumari, G et Sunny, B** présentent dans leur papier intitulé "**Secure Image Processing using LWE based Homomorphic Encryption**" un nouveau schéma basé sur des méthodes homomorphes pour traiter les images cryptées et empêcher la divulgation malveillante de données. Leur cadre est basé sur la technique d'apprentissage avec erreur (LWE) pour améliorer les schémas homomorphes classiques. Dans ce cas, il est possible d'effectuer des opérations mathématiques de base sur des images cryptées. Idéalement, les clients devraient encoder les enregistrements numériques avant de les télécharger sur le cloud. Dans l'étape suivante, les utilisateurs effectuent des opérations d'addition et de multiplication sur les données stockées dans le cloud computing. Par conséquent, la proposition est une solution adéquate pour résoudre les problèmes de confidentialité dans les services cloud. Cependant, ce modèle ne donne pas toujours des résultats satisfaisants, notamment en termes de performances du système. Dans le papier intitulé "**Ensure Privacy and Security in the Process of Medical Image Analysis**", les auteurs **Gomathisankaran, M,Yuan, X et Kamongi**, s'appuient principalement sur la technique du Residue Number System (RNS) pour faciliter l'évaluation de fonctions mathématiques utiles. Essentiellement, une telle solution permet aux fournisseurs de cloud d'effectuer à distance certaines opérations arithmétiques spécifiques sur des images chiffrées sans avoir la clé privée pour le déchiffrement. En fait, la proposition est considérée comme homomorphe en ce qui concerne les opérations d'addition, de soustraction et de multiplication. Plus important encore, il garantit que les informations médicales ne sont consultées que par les utilisateurs autorisés. Les expérimentations montrent que les techniques proposées permettent aux fournisseurs de cloud d'appliquer le filtre de Sobel aux images chiffrées sans les déchiffrer. Cependant, le principal inconvénient de cette approche est qu'elle prend beaucoup de temps pour analyser les images numériques. Afin de montrer l'utilité de l'approche de chiffrement homomorphe, **Kanithi, SR et Latha** dans leur papier intitulé "**Secure Image Processing using Discrete Wavelet Transform and Paillier Cryptosystem**" développent un outil en ligne pour traiter à distance les images médicales. L'objectif principal de cette solution est de maintenir la confidentialité lors de l'externalisation du traitement des données à des fournisseurs de cloud non fiables. À cet égard, les auteurs utilisent l'algorithme de Paillier avec la transformée en ondelettes discrète (DWT) pour effectuer une analyse de données efficace. En règle générale, le cryptosystème Paillier est utilisé pour effectuer des ajouts aux valeurs cryptées. A la lumière de ce fait, nous pouvons quantifier les coefficients d'approximation puis les traiter. Les résultats de la simulation montrent que cette technique peut effectuer une transformation en ondelettes de Haar (HWT) 2-D dans un domaine crypté. Dans la même ligne, il est possible d'obtenir l'image secrète en utilisant Paillier et IDWT (Inverse Discrete Wavelet Transform). Dans le papier intitulé "**An Efficient Secret**

Key Homomorphic Encryption used in Image Processing Service", les auteurs **Yang et al** étendent le chiffrement homomorphe de Gentry pour prendre en charge les opérations arithmétiques à virgule flottante. Contrairement aux approches conventionnelles, ce cadre utilise le cryptage symétrique au lieu du cryptage à clé publique pour coder les données numériques. Sur la base des résultats de la simulation, la proposition empêche les attaques d'analyse statistique d'atteindre des données sensibles. Compte tenu de ce fait, ce cadre peut être adopté dans le cloud computing pour traiter les données médicales. Bien entendu, les coûts de calcul sont le principal inconvénient de cette solution car elle repose fortement sur des schémas de chiffrement homomorphes classiques. Bien que les techniques homomorphes semblent être une approche prometteuse, il n'y a que quelques implémentations réussies de traitement d'images basées sur le cloud. En réalité, de nombreux problèmes sont encore confrontés à ce nouveau concept qui entrave son adoption dans le traitement des données en cloud computing. Premièrement, les schémas existants ne conviennent pas aux données d'images volumineuses, car ils cryptent, dans la plupart des cas, chaque pixel séparément. Deuxièmement, ces méthodes sont conçues pour effectuer uniquement des opérations mathématiques de base simples, telles que l'addition et la multiplication. Par la suite, le développement d'applications robustes du monde réel à l'aide de ces algorithmes est une tâche difficile. Troisièmement, l'utilisation de cryptosystèmes homomorphes pour crypter les dossiers de santé dans le cloud computing aurait sans aucun doute un impact négatif sur les performances du système selon la publication des auteurs **Farah, S, Javed, MY, Shamim, A et Nawaz, T** intitulée "**An Experimental Study on Performance Evaluation of Asymmetric Encryption Algorithms**".

Description de l'invention :

Notre invention propose un système basé sur le cryptage homomorphe pour sécuriser les images médicales dans le cloud computing. Ce système est composé d'un système multi-agents pour effectuer un traitement de données distribué, de la fonction MapReduce pour bénéficier du parallélisme lors du traitement des données, de système Hadoop pour développer des applications sécurisées de traitement d'images médicales dans le cloud computing et de l'algorithme BA pour améliorer les performances d'équilibrage de charge et ainsi éviter la surcharge des serveurs d'hébergement.

En effet, ce nouveau système vise à sécuriser le traitement des images médicales externalisées via un cryptage homomorphe. Plus précisément, nous avons utilisé la technique de partition avec un système multi-agents pour répondre aux exigences de sécurité et de confidentialité. L'idée clé de cette solution était de diviser l'image d'entrée en plusieurs petites parties avant de les crypter. Dans ce cas, nous avons utilisé le système multi-agents pour prendre en charge le traitement distribué des données. Par conséquent, chaque région générée est analysée par un ensemble d'agents appartenant à un système multi-agents. Pour implémenter cette solution, nous avons proposé le framework Hadoop. Dans ce cas, nous avons utilisé la fonction MapReduce pour diviser chaque tâche en plusieurs petites tâches (sous-tâches) en parallèle pour améliorer les performances du système. De plus, nous avons introduit une méthode basée sur BAT pour assurer une gestion efficace de la charge de travail des machines virtuelles ce qui va garantir l'équilibrage de charge. Par conséquent, notre proposition vise à renforcer l'approche homomorphe dans les services cloud en garantissant à la fois la sécurité et les performances.

Les figures 1, 2, 3, 4 et 5 fournissent une vue synoptique complète de notre système.

Mode de référence de l'invention :

La présente invention sera décrite par l'intermédiaire des figures détaillées du mode de réalisation préféré, en référence aux figures.

FIG.1 : donne un schéma fonctionnel de sécurité des données illustrant le principe du système proposé ;

FIG.2 : donne un schéma illustrant le traitement d'images à l'aide d'un système multi-agents ;

FIG.3 : donne un schéma illustrant le traitement d'image à l'aide de la fonction MapReduce ;

FIG.4 : donne un schéma illustrant le traitement d'image avec le système Hadoop ;

FIG.5 : donne un schéma illustrant la politique d'équilibrage de charge.

Comme tout le monde le connait, le temps d'exécution est le principal aspect négatif du chiffrement homomorphe. Pour résoudre ce problème, nous proposons une méthode de partitionnement visant principalement à améliorer les performances pour gérer de grandes quantités de données. Afin d'augmenter l'efficacité du traitement des données, nous divisons les relevés de santé en petites portions pour prendre en charge un environnement parallèle et une plate-forme distribuée.

L'idée centrale de ce concept est de répartir la charge de travail entre plusieurs serveurs en travaillant en parallèle sur les données. En fait, la gestion des données à grande échelle nécessite un environnement informatique hautes performances et, par conséquent, le centre de données cloud connaît une latence élevée en raison des charges de travail. Fondamentalement, la confiance, la vitesse et la sécurité sont les facteurs les plus influents dans la sélection du bon service cloud. Ainsi, nous appliquons un schéma homomorphe sur chaque partage créé séparément au lieu de l'image entière pour déplacer les charges de travail vers l'environnement le plus approprié. Ce faisant, cette méthode produirait une image cryptée qui nécessite un temps de calcul faible non seulement lors du cryptage des données, mais également lors du traitement. La confidentialité peut être garantie, rendant les enregistrements numériques illisibles à l'aide de cryptosystèmes homomorphes. Le schéma fonctionnel de sécurité des données du système proposé, utilisant la technique d'échantillonnage et le partitionneur, est illustré à la figure 1.

Ensuite, chaque région sera analysée par un agent distinct. Pour atteindre cet objectif, nous introduisons un cadre distribué basé sur un système multi-agents. Ainsi, nous utilisons des agents coopératifs pour effectuer une opération spécifique sur le cloud computing. Par conséquent, une tâche de traitement d'image est généralement mappée sur différents composants d'un système distribué. Dans ce contexte, cette plateforme est essentiellement composée de plusieurs agents opérant sous le contrôle d'un responsable de sous-groupe défini. L'architecture de système multi-agents proposée est divisée en trois modules : Master Manager (MA), Region Manager Agent (RMA) et Agents locaux (LA), comme le montre la figure 2.

Dans un tel concept, MA est responsable de la supervision de l'ensemble du cadre. En particulier, il crée, initialise ou tue les processus RMA. À cet égard, un ensemble d'agents est dédié à une région générée spécifique. Pendant ce temps, chaque composant RMA crée et contrôle tous les agents locaux. De plus, une collaboration efficace entre les agents RMA est nécessaire pour atteindre un objectif spécifique. Enfin, les modules (LA) opèrent au niveau inférieur de l'image pour effectuer un seul traitement d'image médicale. En résumé, l'image secrète est divisée en un certain nombre de segments. En d'autres termes, chaque nœud de la plate-forme cloud n'est pas en mesure de révéler des informations sur l'image secrète.

Dans le même temps, il est également utile d'effectuer un traitement de données distribué. Pour cette raison, nous introduisons un système multi-agents (SMA) de telle sorte que chaque région soit analysée par un certain nombre d'agents. Pour obtenir le résultat final, nous combinons tous les résultats intermédiaires séparés fournis par différents fournisseurs de cloud pour obtenir l'image traitée.

Fondements du cadre proposé. Pour cela, nous utilisons la fonction MapReduce pour bénéficier du parallélisme lors du traitement des données. Dans ce modèle, nous utilisons les fonctions Map et Reduce pour traiter une énorme quantité de données en parallèle. Fonctionnellement, la fonction MapReduce divise souvent l'image d'entrée en portions indépendantes afin d'appliquer la fonction Map de manière complètement parallèle. Dans ce cas, la fonction Reduce combine toutes les valeurs de chaque tâche de mappage pour effectuer une opération spécifique, puis fusionne toutes les sorties dans un seul fichier. Plus précisément, une tâche de réduction utilise une ou plusieurs clés et leurs valeurs d'attribut associées. Par conséquent, le système effectue l'opération de regroupement à l'aide d'une clé dédiée pour une tâche de réduction définie. Dans cette architecture, le nœud maître est implémenté pour gérer les fonctions Map et Reduce. Fondamentalement, le nœud maître fusionne les fichiers de tâches de cartes distinctes qui sont généralement dédiées à une tâche de réduction particulière, comme le montre la figure 3.

Sur la base de ces considérations, nous nous appuyons sur le système Hadoop pour développer des applications sécurisées de traitement d'images médicales dans le cloud computing. Il atteint cet objectif en utilisant le système de fichiers distribué Hadoop (HDFS) pour enregistrer des fichiers sur différents nœuds. Dans ce scénario, les utilisateurs téléchargent leurs données numériques sur HDFS pour traitement. Pour ce faire, nous nous appuyons sur le programme MapReduce pour gérer très efficacement les dossiers de santé d'entrée. Tout d'abord, nous avons divisé l'image médicale secrète en plusieurs parties. Deuxièmement, nous configurons la fonction Map pour crypter des régions séparées à l'aide d'un cryptage homomorphe. Troisièmement, nous traitons chaque petit fichier image. Enfin, nous combinons ces fichiers intermédiaires à l'aide de la fonction Reduce pour obtenir l'image traitée. Le principe du cadre proposé est présenté dans la figure 4.

Pour l'essentiel, Hadoop Image Processing Interface (HIPI) est une bibliothèque de traitement d'images efficace conçue pour être utilisée avec Apache Hadoop MapReduce pour les tâches de programmation parallèle. L'objectif principal de cette solution est de fournir un cadre distribué hautement parallèle. Bien entendu, cela améliorerait les performances du système en répartissant les tâches entre les différents serveurs cloud disponibles. Étant donné que le cloud comprend plusieurs machines virtuelles (VM), nous suggérons d'utiliser des techniques inspirées de la nature pour un équilibrage de charge efficace des tâches sur les machines virtuelles disponibles dans le cloud computing. À cet égard, l'optimisation des essaims de particules (PSO), les algorithmes génétiques (GA) et les algorithmes de colonie d'abeilles artificielles (ABC), l'algorithme BA sont largement utilisés pour améliorer la charge de travail des serveurs d'hébergement. Ces méthodes, en particulier ABC, sont fortement basées sur une politique de machine virtuelle pour améliorer les performances d'équilibrage de charge et éviter la surcharge du serveur. Concrètement, nous nous appuyons sur l'approche basée sur BA pour sélectionner l'instance de VM appropriée pour chaque tâche et affecter un serveur présent dans le cluster optimal. En conséquence, la fonction de fitness g() pour chaque tâche K avec les tailles SZ_k sur la $j^{ème}$ VM est basée sur le temps d'exécution (ET_{kj}) et le coût d'exécution (EC_{kj}), comme le montre l'équation [1].

$$g(k,j) = \alpha\, ET_{kj} + (1-\alpha) EC_{kj} \qquad [1]$$

$$ET_{kj} = \frac{SZ_k}{CP_j}$$

$$EC_{kj} = \frac{ET_{kj}}{\lambda} \times CO_j$$

Où α est un facteur d'équilibre temps-coût dans une plage de [0 1]. CO_j fait référence au coût de l'instance de VM de type j pour une unité de temps (λ).

Techniquement, la solution proposée est composée de trois composants principaux : Clients, Datacenter, Module d'équilibrage de charge intelligent, comme le montre la figure 5.

Fonctionnellement, le module intelligent acquiert des informations à partir des données client et des serveurs actifs. Cette information utile est utilisée pour calculer la fonction de fitness. Par conséquent, le module VMM (Virtual Machine Manager) sélectionne la machine virtuelle appropriée pour chaque tâche. À cette fin, le module VMM est conçu pour surveiller en permanence les modifications de la machine virtuelle active, ainsi que les demandes de tâches. Sur la base de ces mesures, notre proposition peut être utilisée pour résoudre le problème d'exécution dans le chiffrement homomorphe. Cela améliorerait considérablement la qualité de service (QoS) dans les services cloud.

Revendications :

1- Système basé sur le cryptage homomorphe pour sécuriser les images médicales dans le cloud computing composé :
- d'un système multi-agents pour effectuer un traitement de données distribué ;
- d'un système assurant le parallélisme lors du traitement des données utilisant la fonction MapReduce
- de système Hadoop pour développer des applications sécurisées de traitement d'images médicales dans le cloud computing ;
- de l'algorithme BA (Bees Algorithm) pour améliorer les performances d'équilibrage de charge et éviter la surcharge des serveurs d'hébergement.

2- Système basé sur le cryptage homomorphe pour sécuriser les images médicales dans le cloud selon la revendication 1 caractérisé en ce que le système multi-agents est utilisé pour prendre en charge le traitement distribué des données.

3- Système basé sur le cryptage homomorphe pour sécuriser les images médicales dans le cloud selon les revendications 1 et 2 caractérisé en ce que la fonction MapReduce est utilisée pour diviser chaque tâche en plusieurs petites tâches (sous-tâches) en parallèle pour améliorer les performances du système.

4- Système basé sur le cryptage homomorphe pour sécuriser les images médicales dans le cloud selon les revendications 1, 2 et 3 caractérisé en ce que le système Hadoop est employé pour développer et implémenter la solution proposée.

5- Système basé sur le cryptage homomorphe pour sécuriser les images médicales dans le cloud selon les revendications 1, 2, 3 et 4 caractérisé en ce que l'algorithme BA est introduit pour assurer une gestion efficace de la charge de travail des machines virtuelles ce qui va garantir l'équilibrage de charge.

6- Méthode de sécurisation des images par le cryptage homomorphe composée des étapes suivantes :
- Diviser l'image d'entrée en plusieurs petites parties avant de les crypter par un système multi-agents.
- Diviser chaque tâche en plusieurs petites tâches (sous-tâches) en parallèle pour améliorer les performances du système par la fonction MapReduce
- Sécuriser chaque division d'image par une application sécurisée de traitement d'images médicales dans le cloud computing développée par le système Hadoop.
- Améliorer les performances de traitement d'images en termes d'équilibrage de charge et pour éviter la surcharge des serveurs d'hébergement moyennant un algorithme BA.

MA 54262A1

ROYAUME DU MAROC
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE

OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13)

Renseignements relatifs à la demande	
N° de la demande : 54262	Date de dépôt : 27/08/2021
Déposant : Université internationale de Rabat	
Intitulé de l'invention : Système basé sur le cryptage homomorphe pour sécuriser les images médicales dans le cloud computing.	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents brevets cités dans le rapport de recherche sont téléchargeables à partir du site http://worldwide.espacenet.com, et les documents non brevets sont joints au présent document, s'il y en a lieu.

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☐ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☒ Cadre 4 : Remarques de forme et de clarté
- ☐ Cadre 5 : Défaut d'unité d'invention
- ☐ Cadre 6 : Observations à propos de certaines revendications exclues de la brevetabilité
- ☒ Cadre 7 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Examinateur: Sara AGUENDICH	**Date d'établissement du rapport** : 25/05/2022
Téléphone: 212 5 22 58 64 14/00	

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  6 Pages
- Revendications
  6
- Planches de dessin
  0 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04L9/00 ; G06F21/60 ; G06F21/62 ; G06N3/04
CPC : H04L9/008 , G06F21/602 ; G06F21/62 ; G06N3/0454

Plateformes et bases de données électroniques de recherche :

EPOQUENET, WPI, ScienceDirect, IEEE, ORBIT

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
Y	**XP029632607 ; « Security and privacy aspects in MapReduce on clouds: A survey» ; Derbeko Philip; Dolev Shlomi; Gudes Ehud; Sharma Shantan; Elsevier ; 25-05-2016**	1-6
Y	**https://www.mirlabs.net/jnic/secured/Volume4-Issue1/Paper15.pdf ; « Enhanced Bee Colony Algorithm for Efficient Load Balancing and Scheduling in Cloud » ; K. R. Remesh Babu ; Philip Samuel; 15-12-2015**	1-6
A	**XP032491427 ; « The data protection of mapreduce using homomorphic encryption» ; Xu Chen; Qiming Huang ; IEEE ; 23-05-2013**	1-6
A	**https://tis.wu.ac.th/index.php/tis/article/view/3970/225 ; « New Approach Based on Homomorphic Encryption to Secure Medical Images in Cloud Computing» ; Ali Kartit ;TRENDS IN SCIENCES, VOLUME 19, NUMBER 9 ; 01-05-2022**	1-6

***Catégories spéciales de documents cités :**

-« **X** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
-« **Y** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« **P** » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« **E** » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

Partie 3 : Opinion sur la brevetabilité

Cadre 4 : Remarques de forme et de clarté

- Remarques de clarté

- La description de l'invention doit exposer l'invention d'une façon suffisamment claire et complète en divulguant des informations suffisantes permettant à un homme du métier, sans expérimentation excessive, d'exécuter l'invention connue de l'inventeur à la date du dépôt, conformément aux dispositions de l'art.34 de la loi 17-97 telle que modifiée et complétée par la loi 23-13. En effet, ladite demande ne divulgue pas exactement la manière par laquelle le cryptage homomorphe est utilisé sur la fonction MapReduce.
- La revendication 1 ne satisfait pas aux exigences de clarté conformément à l'art. 35 de la loi 17-97 telle que modifiée et complétée par la loi 23-13. En effet, la phrase « un système multi-agents pour effectuer un traitement de données distribué » employée dans la revendication 1 a un sens relatif qui n'est pas bien établi, et elle laisse subsister un doute quant à la signification des caractéristiques techniques auxquelles elle se rapporte, au point que l'objet de ladite revendication n'est pas clairement défini. Le déposant est alors invité à modifier la revendication 1 de sorte à porter plus de clarification à cette phrase.
- Les figures mentionnées dans la description sont manquantes.

Cadre 7 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté	Revendications 1-6 Revendications aucune	Oui Non
Activité inventive	Revendications aucune Revendications 1-6	Oui Non
Application Industrielle	Revendications 1-6 Revendications aucune	Oui Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : XP029632607
D2 : **https://www.mirlabs.net/jnic/secured/Volume4-Issue1/Paper15.pdf**

1. Nouveauté

Aucun des documents cités ci-dessus, considéré isolément, ne divulgue un système basé sur le cryptage homomorphe pour sécuriser les images médicales dans le cloud computing comprenant l'ensemble des caractéristiques techniques des revendications 1 à 6. D'où l'objet desdites revendications est nouveau au sens de l'article 26 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

2. Activité inventive

Le document D1 qui est considéré comme l'état de la technique le plus proche de l'objet de la revendication 1, divulgue un système basé sur le cryptage homomorphe dans le cloud computing composé :

- d'un système assurant le parallélisme lors du traitement des données utilisant la fonction MapReduce.
- d'un système Hadoop pour développer des applications sécurisées dans le cloud computing.

Par conséquent, l'objet de la revendication 1 diffère de D1 en ce que le système de la présente demande est appliqué sur les images médicales et comprend l'algorithme BA (Bees Algorithm).

L'effet technique de ladite différence est celui de sélectionner l'instance de VM (Virtual Machine) appropriée pour chaque tâche et répartir les tâches entre les différents serveurs cloud présents.

Le problème objectif technique que la présente invention se propose de résoudre est considéré comme celui de fournir une solution qui permet d'éviter la surcharge sur les machines virtuelles disponibles dans le cloud computing.

La solution à ce problème, proposée dans la revendication 1 de la présente demande, ne peut pas être considérée comme impliquant une activité inventive puisque le document D2 divulgue un système et une méthode pour optimiser les conditions de surcharge sur les machines virtuelles disponibles dans le cloud computing en utilisant l'algorithme BA (Bees Algorithm). (Voir figures 1-5). En outre, l'utilisation des images médicales ne représente qu'une option de format de données que l'homme du métier sélectionnerait, selon le cas, parmi plusieurs formats de données à grande échelle, afin de résoudre le problème posé, sans faire preuve d'esprit inventif.

Il serait donc évident pour l'homme de métier en partant du système décrit dans D1 et en tenant compte à la fois du problème mentionné ci-dessus et du principe de la solution décrite dans D2, de parvenir au système correspondant à l'objet de la revendication 1 sans faire preuve d'esprit inventif.

Par conséquent, l'objet de la revendication 1 n'implique pas une activité inventive au sens de l'article 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

Les revendications dépendantes 2 à 5 ne semblent pas contenir de caractéristiques supplémentaires qui satisfassent aux exigences de l'activité inventive au sens de l'article 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13 en étant combinées aux caractéristiques de la revendication 1 à laquelle lesdites revendications dépendantes sont liées.

De plus, les mêmes arguments s'appliquent également à la revendication indépendante 6, dont la matière définit les étapes d'une méthode de sécurisation des images par le cryptage homomorphe qui correspondant au système décrit dans la revendication 1. D'où l'objet de la revendication 6 manque également d'activité inventive au sens de l'article 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

3. Application industrielle

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible.