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 42881 A1

(51) Cl. internationale :
H04L 9/28

(43) Date de publication :
31.01.2020

(21) N° Dépôt :
42881

(22) Date de Dépôt :
24.07.2018

(71) Demandeur(s) :
Université Mohammed V RABAT, Avenue des Nations Unies, Agdal, bp 8007 NU, Rabat, 10000, Maroc (MA)

(72) Inventeur(s) :
DERFOUF Mostapha ; ELEULDJ Mohcine

(74) Mandataire :
KARTIT ZAID

(54) Titre : **Système sécurisé de stockage et traitement des données dans le Cloud à base du cryptage homomorphe**

(57) Abrégé : La présente invention présente un système sécurisé de stockage et traitement des données basé sur le chiffrement homomorphe dans les environnements de Cloud Computing. Dans ce système une combinaison à la fois, de chiffrement homomorphe additif pour les fonctions utilisant des opérations d'addition et soustraction, de chiffrement homomorphe multiplicatif pour les fonctions utilisant des opérations de multiplication et de division. Ce système nécessite moins de ressources informatiques du côté client, en plus la taille des données chiffrées n'est pas volumineuse, ce qui ne pénalise pas la bande passante contrairement au chiffrement homomorphe complet.

Titre : Système sécurisé de stockage et traitement des données dans le Cloud à base du cryptage homomorphe

Description

Domaine technique :

La présente invention a trait à un système sécurisé de stockage et traitement des données en se basant sur un chiffrement homomorphe. Il s'agit exactement d'un système capable d'exécuter des opérations sur des données cryptées au niveau du fournisseur du Cloud sans les décrypter, ce qui donnera les mêmes résultats après les calculs comme si nous avions travaillé directement sur les données en clair.

Pour illustrer l'intérêt de cette invention nous supposons que le client veut réaliser un traitement sur des données confidentielles, l'exemple le plus simple est la somme ou la multiplication de deux nombres. Le client ne souhaite pas que le fournisseur du Cloud sache ces nombres, donc si X1 et X2 sont deux nombres, E(X1) et E(X2) représentent le cryptage de ces nombres avec une clé secrète du client, le service du Cloud serait en mesure de calculer E(X1) + E(X2) ou E(X1) * E(X2) sans savoir la clé secrète.

Etat Antérieur :

Dans les techniques de chiffrement traditionnelles, les données sur le Cloud doivent être déchiffrées à chaque fois que le client veut effectuer un calcul ou un traitement sur les données ce qui demande plus de temps et de ressources. Dans le brevet US20130339722 l'inventeur 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 renvoie le résultat du calcul chiffré au client. La solution proposée dans le brevet US20130339722 repose sur un chiffrement homomorphe complet qui impose des clés de cryptage très longues (plus de 2 Gigabits) et les données chiffrées prennent beaucoup plus de place que les données en clair, en plus les algorithmes de traitement de données sont encore très couteux en termes de ressources, les exigences en matière de communication augmentent généralement. Les calculs sur ces données chiffrées volumineuses sont généralement plus lents, ce type de chiffrement homomorphe nécessite un matériel performant du côté client pour pouvoir effectuer l'opération de chiffrement/déchiffrement homomorphe complet.

Brève description des figures :

La figure 1 : Présente le diagramme d'état-transition expliquant le fonctionnement de l'interface pour une requête contenant une seule opération (somme ou multiplication)de fonctionnement de l'interface du système pour une requête contenant une seule opération (somme ou multiplication)

La figure 2 : Le principe général du système

La figure 3 : Le principe du système proposé pour le cas de la somme

La figure 4 : Le principe du système proposé pour le cas du produit

La figure 5 : Le Système de stockage et traitement sécurisé des données en se basant sur un chiffrement homomorphe dans le cas de SQL

La table 1 : Données en clair dans la base de données du Cloud

La table 2 : Exemple réel des données chiffrées (Chiffrement de Paillier et RSA) dans la base de données du Cloud. Le chiffrement est appliqué également sur les noms de colonnes.

Description détaillé :

Dans le Cloud Computing les utilisateurs se connectent aux applications hébergées dans l'espace du Cloud. Ces applications utilisent généralement une base de données pour le stockage des données des utilisateurs qui peuvent être récupérées via des requêtes, il est également possible d'effectuer des traitements et des calculs sur ces données en utilisant les fonctions disponible dans les langages de requêtes des bases de données.

Dans la présente invention nous combinons à la fois le chiffrement additif pour les fonctions utilisant des opérations d'addition et soustraction en faisant recours au chiffrement de Paillier (chiffrement asymétrique) et le chiffrement multiplicatif pour les fonctions utilisant des opérations de multiplication et de division en faisant recours à l'algorithme RSA. Ceci permet de profiter des avantages du chiffrement homomorphe complet et sans avoir besoin de ressources informatiques performantes du côté client, en plus la taille des données chiffrées n'est pas volumineuse ce qui ne pose pas de problème de stockage et de traitement (les algorithmes Paillier et RSA utilisés dans notre invention sont plus rapides et moins complexes que ceux du chiffrement homomorphe complet) côté client et ne pénalise pas la bande passante contrairement au chiffrement homomorphe complet.

Nous allons d'abord exposer les fonctions usuelles de calcul dans les langages d'interrogation des bases de données et ensuite les présenter sous format mathématique pour ensuite procéder au chiffrement homomorphe additif en utilisant le cryptage de Paillier pour les opérations d'addition et au chiffrement homomorphe multiplicatif en utilisant RSA pour les opérations de multiplication afin de garantir les avantages du chiffrement homomorphe complet.

Les fonctions d'agrégation dans les différents langages de requêtes tels que SQL, XQUERY, XSL… permettent d'effectuer des opérations de récupération et de calcul sur un ensemble d'enregistrements. Étant données que ces fonctions s'appliquent à plusieurs lignes en même temps, elles permettent de réaliser des opérations qui servent à récupérer l'enregistrement le plus petit, le plus grand ou bien encore de déterminer la valeur moyenne sur une colonne. Les principales fonctions sont les suivantes :

a. AVG() : pour calculer la moyenne sur une colonne. La formule mathématique formelle pour la moyenne est :

b. $$A = \frac{1}{n} * \sum_{i=1}^{n} x_i$$

c. A = average (Moyenne)
d. n = le nombre de termes (par exemple, le nombre d'éléments)
e. xi = la valeur de chaque élément individuel dans la liste des nombres

f. MAX() : pour récupérer la valeur maximale d'une colonne sur un ensemble de lignes.

g. MAX(a, b) = 1/2 (a+b+ |a - b|)

h. MIN() : pour récupérer la valeur minimale de la même manière que MAX()

i. MIN(a, b) = (a + b - | a - b |)/2

j. SUM() : pour calculer la somme sur un ensemble d'enregistrements. La formule est la suivante :

k. $$\textbf{SUM(ai)} = \sum_{i=m}^{n} a_i = a_m + a_{m+1} + a_{m+2} + \cdots + a_{n-1} + a_n$$

l. On suppose que **m** est inférieur ou égal à **n**.

L'utilisation la plus générale en SQL consiste à utiliser la syntaxe suivante :

m. SELECT fonction(colonne) FROM table.

n. Au niveau de la base de données du Cloud, chaque champ sera chiffré 2 fois, une fois en utilisant le chiffrement homomorphe additif en appliquant le cryptage de Paillier et une autre fois en utilisant le chiffrement homomorphe multiplicatif à base de RSA. C'est à dire que chaque information ou donnée sera représentée sur 2 colonnes une chiffrée avec l'algorithme de Paillier et l'autre avec RSA (table 2). Pour garantir un haut niveau de sécurité et empêcher le fournisseur du Cloud de comprendre la signification des données stockées nous procédons également au chiffrement des noms de colonnes ainsi que les noms des tables en utilisant à la fois RSA et Paillier (table 2).

Le système proposé consiste à doter le client du Cloud d'une interface (figure1). Le rôle de l'interface du système consiste d'abord à analyser le type d'opération de calcul

(addition ou multiplication) choisie par l'utilisateur et la transforme en une expression mathématique en fonction des opérateurs + et *. Selon le type de l'opération de calcul (addition ou multiplication) l'interface choisit le chiffrement homomorphe à effectuer (Paillier pour l'addition ou RSA pour la multiplication) ainsi que les colonnes concernées (chiffrées avec l'algorithme de Paillier ou avec RSA) au niveau de la base de données du Cloud. Si l'utilisateur utilise les opérateurs + et * au lieu des fonctions de calcul l'interface peut également choisir le type de chiffrement en fonction des opérateurs spécifiés (Paillier pour l'addition « + » ou RSA pour la multiplication « * »). Pour l'implémentation de cette interface l'algorithme proposé doit être alimenté avec les différents noms de fonctions de calcul des différents langages de programmation. Le diagramme de fonctionnement de l'interface se présente comme montré dans la figure 1.On on considère que la requête du client ne contient qu'une seule opération de calcul (somme ou multiplication), l'interface récupère d'abord la requête du client (1), puis effectue un test sur la fonction de calcul (2) et (3) (somme ou multiplication) et sur l'opérateur('+' ou '*' s'ils sont spécifiés), en fonction de ce test l'interface choisit le type du chiffrement à effectuer, s'il s'agit d'une opération de somme l'interface crypte le paramètres en utilisant l'algorithme de Paillier (4), s'il s'agit d'une opération de multiplication l'interface crypte le paramètres en utilisant l'algorithme RSA (4), ensuite l'interface remplace la fonction par la formule mathématique convenable et envoi la requête chiffrée au Cloud (5).

La figure 2 illustre le principe général du fonctionnement du système dans lequel le client envoie une requête de calcul (somme ou produit), cette requête passe par l'interface du protocole qui se charge de transformer la requête en une expression mathématique adéquate selon le type d'opération spécifié par le client et en chiffrant les paramètres (chiffrement additif ou multiplicatif) en se basant sur ce type d'opération. La requête transformée est envoyée au Cloud pour le traitement et le résultat chiffré sera ensuite déchiffré par l'interface du système qui retourne le résultat en clair au client. Pour simplification nous utilisons l'abréviation **PA** pour le chiffrement homomorphe additif à base de Paillier et **RSA** pour chiffrement homomorphe multiplicatif à base de RSA.

Comme montré dans la **figure 3** l'utilisateur demande la somme de 3 nombres, il envoie la requête à l'interface du système qui se charge de la lire et de l'analyser. L'interface commence d'abord par détecter le type d'opération qui est dans ce cas la somme puis transforme la requête en une expression mathématique, dans ce cas **somme (a,b,c)** devient **a+b+c.** Vu qu'il s'agit d'une addition l'interface applique le chiffrement homomorphe additif et procède à la sélection des champs chiffrés à base de l'algorithme Paillier, la requête sera transformée en :

PA (a) + PA (b) + PA (c)

Cette requête sera envoyée au Cloud pour faire les traitements (la somme) sur les données chiffrées de la table. Le résultat chiffré sera ensuite déchiffré par l'interface du système et le résultat en clair sera envoyé au Client.

La **figure 4** illustre le cas d'un utilisateur demandant le produit de 3 nombres, il envoie la requête à l'interface du système qui se charge de lire la requête et l'analyser. L'interface

Revendications :

1. Un système sécurisé de stockage et traitement des données basé sur le chiffrement homomorphe dans le Cloud Computing caractérisé en ce que 'il utilise une combinaison à la fois, de chiffrement homomorphe additif pour les fonctions utilisant des opérations d'addition et soustraction, de chiffrement homomorphe multiplicatif pour les fonctions utilisant des opérations de multiplication et de division ; dans ledit système le client est doté d'une interface capable d'analyser le type d'opération de calcul choisie par l'utilisateur et la transforme en une expression mathématique en fonction des opérateurs + et *.

2. Le système selon la revendication 1 caractérisé en ce que ledit système est une interface à installer au niveau de poste client ; ladite interface utilise le chiffrement de paillier pour une opération d'addition et le chiffrement RSA pour une opération de multiplication.

3. L'Interface selon les revendications 1 et 2 caractérisé en ce que dans la base de données Au niveau du Cloud, les données sont stockées dans deux colonnes ,une première colonnes contient des données chiffrées avec RSA et une seconde colonnes chiffrés avec la méthode de paillier .

4. L'Interface selon les revendications 1 et 2 caractérisé en ce que les noms des colonnes ainsi que les noms des tables au niveau du Cloud sont chiffrées en utilisant à la fois RSA et Paillier.

5. L'Interface selon les revendications précédentes caractérisé en ce qu'elle utilise moins de ressources informatiques pour produire un volume réduit de données chiffrées toute en optimisant la bande passante entre le client et le fournisseur.

6. L'Interface selon l'une quelconque des revendications précédentes caractérisée en ce qu'elle Procède comme suit :

a. Récupération de la requête du client

b. Lecture de l'opération et les paramètres

c. Test sur la fonction de calcul à effectuer

d. Choix du type du chiffrement à effectuer selon le résultat dudit test.

e. Remplacement de la fonction par la formule mathématique convenable

f. Envoie la requête chiffrée au Cloud.

commence d'abord par détecter le type d'opération qui est dans ce cas le produit puis transforme la requête en une expression mathématique**, power (a,b,c)** devient donc **a*b*c**. Vu qu'il s'agit d'une multiplication l'interface applique le chiffrement homomorphe multiplicatif et procède à la sélection des champs chiffrées sur la base de RSA, la requête sera transformée en :

RSA(a) * RSA (b) * RSA (c)

Cette requête sera envoyée au Cloud pour faire les traitements (calcul du produit) sur les données chiffrées de la table et envoyer le résultat chiffré à l'interface du système qui se charge de le déchiffrer et de transférer le résultat en clair au client initial.

Comme montré dans la table 2, la première ligne correspond aux noms des colonnes qui sont chiffrées en utilisant Paillier et RSA.

par exemple le nom de colonne ayant le nom 'montant' est chiffré 2 fois, une fois avec Paillier (chiffrement homomorphe additif) ce qui donne '**247406971455444437902533367534335689769584610979586559163910462333017922112 42**' comme nom de colonne qui va contenir les différentes valeurs du montant chiffrées avec l'algorithme Paillier, de même le nom de la colonne 'montant' et chiffré également une deuxième fois avec RSA (chiffrement homomorphe multiplicatif) pour obtenir le nom de colonne'**cN+hwKSmMjsKnlisfN97KGrsHzpiLplnffRk6N92BMgY2pf+INw0kamA9MvaAWZ+1oGVs/X4Rtay3nVbHW9HlTQvdAzGIGnUo+oLSAfnJcXWjY7WrngzMxZV1S7B7VmkO8DtRI2HQ51lbX6XrwN/jMjA9eHEcvy0Pc21tsMw9jc=**', ceci garantit un masquage des données et empêche le fournisseur du Cloud de comprendre la signification réélle des données. La même procédure est faite pour la colonne ayant le nom 'Année' qui est chiffrée avec Paillier pour donner un nom de colonne '**1830455646895263123443025568362170767471500981298568909096854663230785427756 2**', de même le nom de colonne 'Année est également chiffré avec RSA pour donner le nom de colonne'**K1AQlaUwMgUBWcFfRiC0DCCPz4cYd86Fc3zqBX+dJUBBChgEm0/T2dG6m1I6V+XHB441Ve/pPfEZSmTcT3MNDSJawLKfP9GvqH2F9HEr/JRtBaoMHPm4SNY/FDwXeXT8oPdJb6BjDiJkXImr4vGJq9hAI5McfDSG4bVz4RpYgPk=**'. (table2)

Dans le cas de calcul de la somme et du produit en SQL on suppose que le client veut calculer la somme des montants multiplié par 4. Le client envoie la requête : **SELECT SUM(montant) * 3 FROM ventes** à l'interface, cette dernière traduit d'abord la fonction en une expression mathématique comme suit :

SELECT (montant1 + montant2 + montant3) * 3

L'interface détecte qui 'il s'agit d'une addition suivie d'une multiplication et applique le chiffrement Paillier pour l'addition et celui du RSA pour la multiplication on obtient alors :

(Chiffrement additif(montant1) + Chiffrement additif(montant2) + Chiffrement additif(montant3))

La première partie de la requête est envoyé au Cloud qui retourne le résultat :

- **Chiffrement additif(montant1) + Chiffrement additif(montant2) + Chiffrement additif(montant3) = X**
- L'interface déchiffre d'abord **X** pour trouver le résultat réel de la somme des montant qu'on suppose **Y** ensuite la requête devient : **Y * 3**
- Dans ce cas l'interface grâce à son algorithme détecte qu'il s'agit d'une multiplication et procède à l'application du chiffrement RSA pour obtenir la requête suivante :

CHIFFREMENT MULTIPLICATIF(Y) * CHIFFREMENT MULTIPLICATIF(3)

Cette requête est envoyée au Cloud qui se charge d'effectuer le calcul sur des valeurs chiffrées et envoie le résultat à l'interface, cette dernière déchiffre le résultat en utilisant RSA et envoie la valeur en clair au client.

MA 42881A1

Abrégé : La présente invention présente un système sécurisé de stockage et traitement des données basé sur le chiffrement homomorphe dans les environnements de Cloud Computing. Dans ce système une combinaison à la fois, de chiffrement homomorphe additif pour les fonctions utilisant des opérations d'addition et soustraction, de chiffrement homomorphe multiplicatif pour les fonctions utilisant des opérations de multiplication et de division. Ce système nécessite moins de ressources informatiques du côté client, en plus la taille des données chiffrées n'est pas volumineuse, ce qui ne pénalise pas la bande passante contrairement au chiffrement homomorphe complet.

Dessins

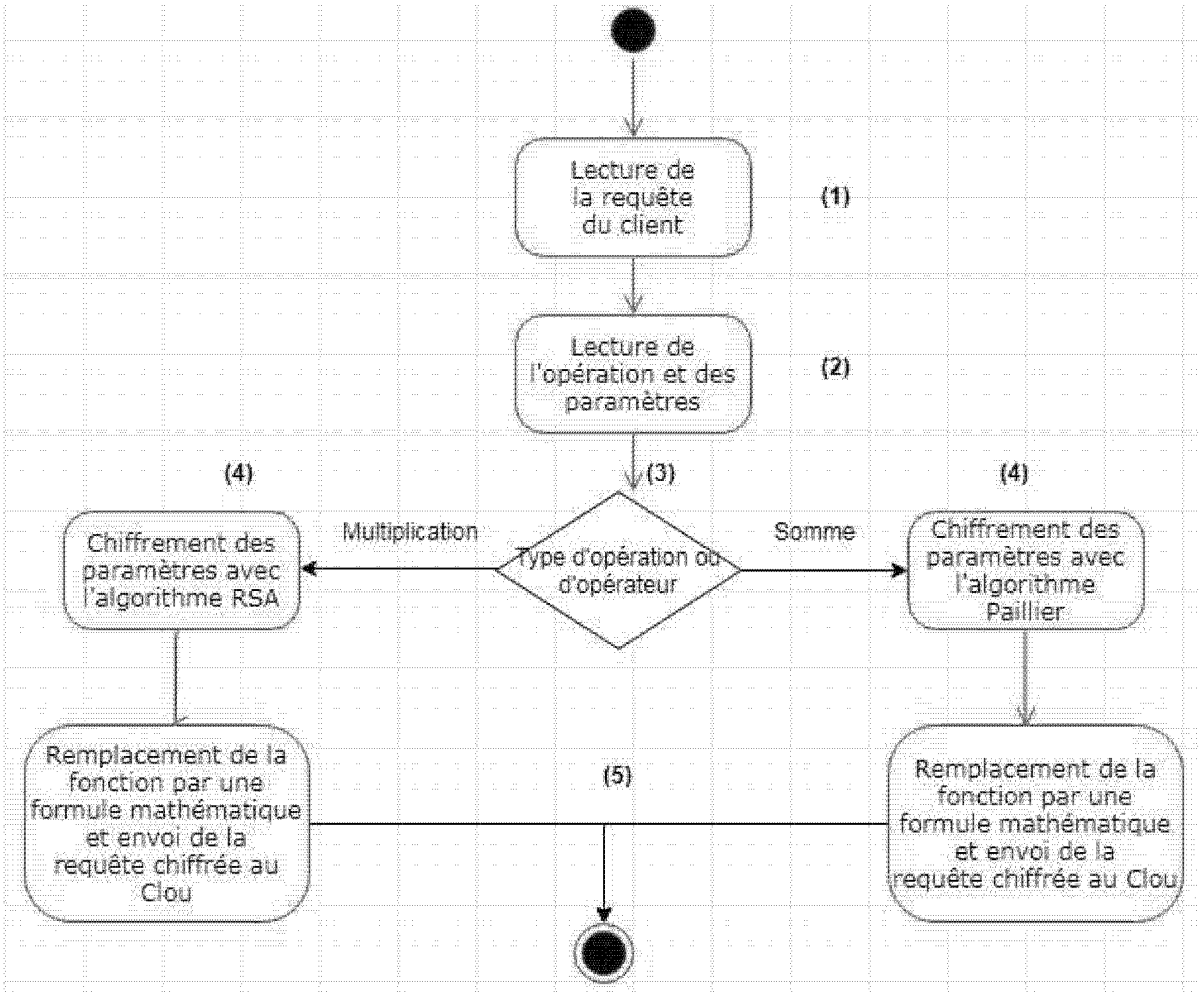

Figure 1.

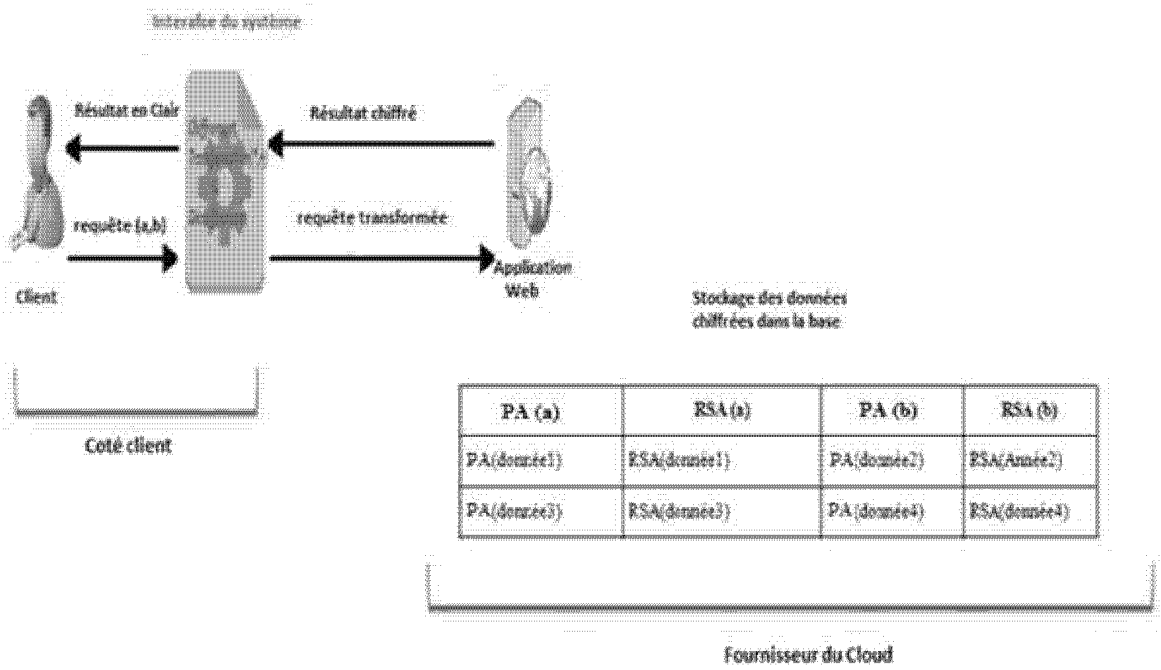

Figure 2.

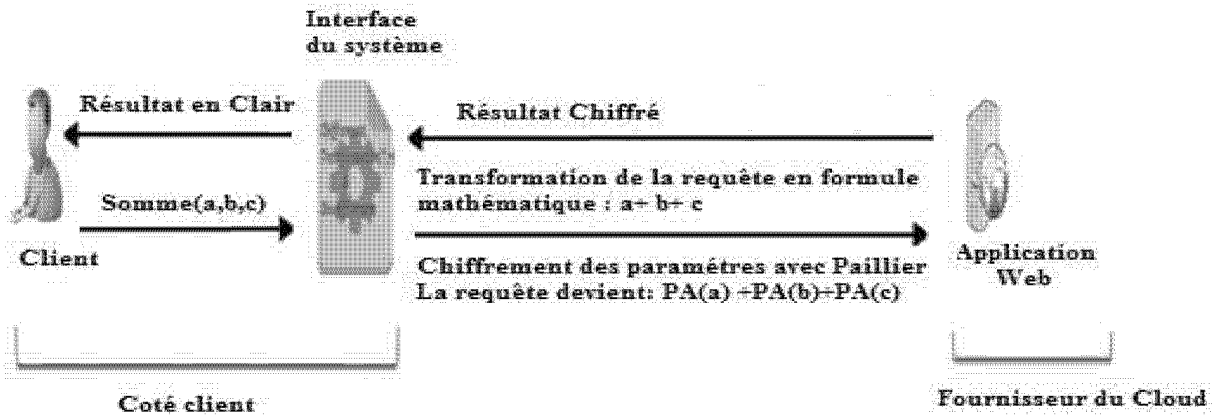

Figure 3.

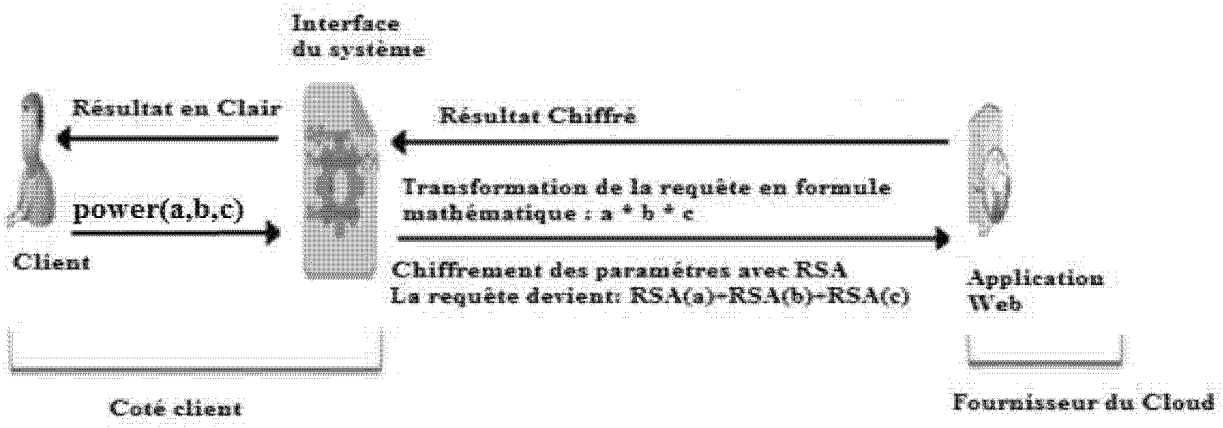

Figure 4.

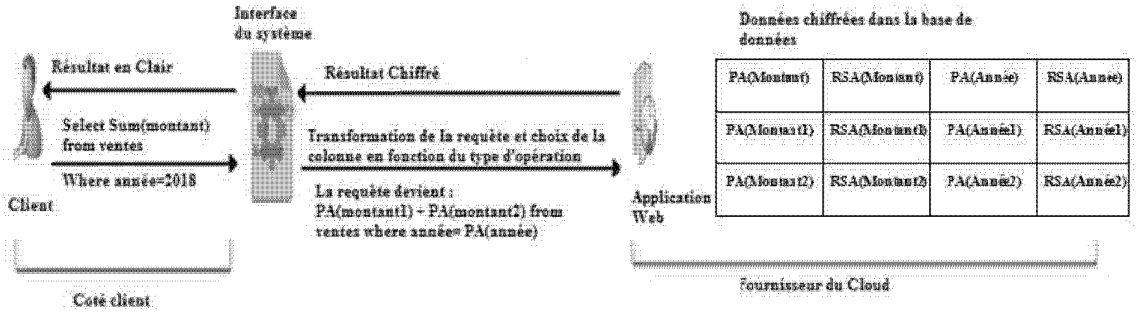

Figure 5

2. Montant	**3. Année**
4. 2301	5. 2017
6. 120	7. 2015
8. 548	9. 2014

Table 1

10. Première colonne 11. Chiffrée avec Paillier	12. Deuxième colonne 13. Chiffrée avec RSA	14. Troisième colonne 15. Chiffrée avec Paillier	16. Quatrième colonne 17. Chiffrée avec RSA	18.
19. 2474069714554444379025333675343356897695846109795865591639104623330179221124 2	**20. cN+hwKSmMjsKnlisfN97KGrsHzpiLplnffRk6N92BMgY2pf+INw0kamA9MvaAWZ+1oGVs/X4Rtay3nVbHW9HlTQvdAzGIGnUo+oLSAfnJcXWjY7WrngzMxZV1S7B7VmkO8DtRI2HQ51lbX6XrwN/jMjA9eHEcvy0Pc21tsMw9jc=**	**21. 1830455646895263123443025568362170767471500981298568909096854663230785427756 2**	**22. K1AQlaUwMgUBWcFfRiC0DCCPz4cYd86Fc3zqBX+dJUBBChgEm0/T2dG6m1I6V+XHB441Ve/pPfEZSmTcT3MNDSJawLKfP9GvqH2F9HEr/JRtBaoMHPm4SNY/FDwXeXT8oPdJb6BjDiJkXImr4vGJq9hAI5McfDSG4bVz4RpYgPk=**	**23.**
24. 1242288709027805555712780451976645988259036034763014022755037127611608929627 8	25. BXdpisUn3mJTAuYw0huh4HPisDP2TxuZit2+K5dNHdFgQD5nWGl89RL82TCYZIE64xFwfDDjcseEeaA3hrQxbuU++QRP/W1jpSHaXn0xQ+ickgptQDTN22jGdUoo948aaRVBHGCBYY/ldvfLnnoyS3Xc+xnB1rEYZqXxumudLl0=	26. 2819813458625362938778174342924850335347031192774292749146950953066833619 4751	27. ReEm7lIbARxUT8WMqIrNgZmooXI/Zl33rJGN3QSkVWXOGMdaWYKPh6LGuQCjsVFisycuiOIq6IJzouw0sxob2HW0kSFjelj7pXHOcBsyVj+r2/BklRlEdDnoLIrRc7xAGbyjTwKZHUxpTMU0xkcQMFx37Jl9qoBr1bDVfVTSz9Q=	28. 29. Premier enregistrement
30. 5186470782383679785320943439082252296468743997191102345586671586077774444648	31. AwVTpQOAj1QjIe4kbMwUHuAHAzNSVm04MK/8wLj9fR6aKFSUziARVqILXiGrbTqgYrNu10qgQz+VQvvegoaW7WoW8nANxDY8tSBTBkcPB3wu8Ldy0p7bPpitqXV8ZsqHHjjYdDR2Dje6g6w1iBrMCTUbKoG98gEFofxS0EjcF+U=	32. 1273339999769582562197347407069220367386389958509487729570296396758006249752 1	33. E9b6gUjfVqpWd+6YRdznIIaYU+3MjpawXNR/Vmc2ozc1pC4lMLfqWAZl8qYZ2tVVS0Q9Vy05ANGjeW4XSuj+47TstSByeQU5RFB5i9hx3KQ1iMfQQQEARkn62rzC074gEIHyd7zOQAsie6kkuk0MNW4PdiEspgOqU5DsfLXCwcI=	34. 35. Deuxième enregistrement

36. 5814216421594 4342705263921 4311753850457 9178941261129 1888873323110 27944593151	37. OiQtTM8vGqvo 9TBcHs2+5WSu KDTyOr3uM82h kwQVEdNVHN Cj8EuFGO3C//K EA2xaM67E7p3 s9hFT+e8MUezj k/NA5djlBeDsge iLfeQLuItXx3JI RNstOHOrw+el np18w7uBsNC WdJxx6K0uFxU PUUaq1JQ1zGE 2h9JHVHEbJUw =	38. 14278349 46532985 38454733 14972692 11199262 89113224 32967868 29877787 46050932 14745	39. bkv3n7irx/liBe8Hir POPjlc8dQlGNBu WA/DME7FpEKH Le+WEtrheW3d3m kN1tmqVU6cjv3pZ mAFr5FN9yqwvT7 Nlla3dn1ftNh1+JTu IZnf3W+Xk3kgZejs lVr8Tc/5KyH1BOE aloj1hKuvJXP0lJsE k5hQwV50tgWLpA lJ8PE=	40. 41. Troisième enregistrement

Table 2.

ROYAUME DU MAROC
****
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
****

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 : 42881	Date de dépôt : 24/07/2018
Déposant : Université Mohammed V RABAT	
Intitulé de l'invention : Système sécurisé de stockage et traitement des données dans le Cloud à base du cryptage homomorphe	

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: BAMI MOHAMMED	**Date d'établissement du rapport** : 15/01/2019
Téléphone: 212 5 22 58 64 14/00	ROYAUME DU MAROC OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE CASABLANCA

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
  1-6
- Planches de dessin
  4 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04L9/28

Plateformes et bases de données électroniques de recherche :

EPOQUENET, WPI, ScienceDirect, ORBIT

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
X	JP2014126865A ; Fujitsu Ltd ; 07/07/2014	1-6
A	US9083526B2 ; International Business Machines Corp ; 07/14/2015	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 forme

Le préambule des revendications dépendantes 2-6 n'est pas le même que la revendication indépendante 1. En effet la revendication 1 porte sur un système, alors que les revendications 2-6 portent sur une interface.

- Remarques de clarté

La revendication 1 de catégorie système n'est pas rédigée de sorte à préciser les composants du

système de chiffrement.

L'objet des revendications 1-6 manque donc de clarté au sens de l'article 35 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

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 : JP2014126865A

1. Nouveauté

Aucun document ne divulgue l'objet des revendications 1-6 qui est donc 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 est considéré comme l'état de la technique le plus proche de l'objet de la revendication 1 et divulgue : Un système sécurisé de traitement de données basé sur le chiffrement homomorphe caractérisé en ce qu'il utilise une combinaison à la fois de chiffrement homomorphe additif pour le fonctions d'addition, et un chiffrement homomorphe multiplicatif pour les fonctions de multiplication (voir description de D1).

L'objet de la revendication 1 diffère de D1 en ce que le système comprend une interface capable d'analyser le type d'opération de calcul choisie par l'utilisateur et la transforme en une expression mathématique en fonction des opérateurs + et *.

Aucun problème ne semble être résolu par ladite différence.

L'objet de la revendication 1 manque donc d'activité inventive au sens de l'article 28 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

L'objet des revendications 2-6 ne contient aucune caractéristique technique qui, en combinaison avec l'une quelconque des revendications à laquelle elle se réfère, implique une 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.