



(12) FASCICULE DE BREVET

- (11) N° de publication : **MA 37726 A1** (51) Cl. internationale : **G06F 21/00; G06F 15/16**
- (43) Date de publication : **29.07.2016**

-
- (21) N° Dépôt : **37726**
- (22) Date de Dépôt : **31.12.2014**
- (71) Demandeur(s) : **UNIVERSITÉ MOHAMMED V DE RABAT, Angle avenue Allal El Fassi et Mfadel Cherkaoui, Alirfane 8007.N.U, Rabat Rabat-Chellah (MA)**
- (72) Inventeur(s) : **MOHAMED ESSAIDI ; AHMED BENDAHMANE**
- (74) Mandataire : **FATIMA ZAOUI**

(54) Titre : **TECHNIQUE POUR LA SECURITE DES GRILLES DE CALCUL**

- (57) Abrégé : Dans cet article, nous proposons une nouvelle approche à base de vote réputation, basé sur la technique de contrôles ponctuels. Cette approche améliore du vote basé la crédibilité pour atteindre un taux d'erreur faible, avec un surcout raisonnable. Dans le vote basé sur la crédibilité, un contrôle ponctuel est utilisé pour vérifier périodiquement les ressources informatiques, par l'envoi d'un travail de repérage dont le résultat correct est connu, afin d'estimer la crédibilité de chaque ressource basée sur le résultat retourné. Cette technique conduit à la dissipation des ressources dans le schéma de vote simple, car il nécessite des calculs supplémentaires pour produire le résultat des travaux de repérage. L'idée de base de notre approche proposée consiste à vérifier les ressources informatiques sans attribuer l'emploi de repérage et d'envisager la suite de la décision de vote que celui des contrôles inopinés pour estimer la crédibilité sans calculs supplémentaires. Cette crédibilité est considérée comme réputation qui est utilisée dans la décision, selon l'algorithme de la figure 1. Dans cet algorithme, le service de courtier de grille commence le calcul par l'envoi d'un certain nombre de a ressources de calcul disponibles à la ligne (2) pour la transformation parallélisée. Après le calcul, les résultats générés seront retournés au courtier (lignes 19 et 20). Tant que toutes les tâches sont terminées avec des résultats acceptés (lignes 4-7), la programmation et les processus de réception pour chaque tâche sont répétés. Supposons que chaque tâche est reproduite n fois et attribuée à plusieurs ressources informatiques C_i , de sorte qu'un courtier peut percevoir des résultats différents $V_j m$, ou $i = 1, 2, \dots, N$ et $j = 1, 2, \dots, M$. Chaque ressource informatique a sa réputation la valeur R_i , qui représentent le comportement global. Cette réputation est recueillie par

un service broker- grille, qui contient la liste de la réputation de toutes les ressources de calcul. La réputation est une valeur dans la plage entre 0 et 1. Selon notre vision, le service de courtier de grille construit la réputation de chaque ressource informatique grâce à sa crédibilité. La crédibilité représente la probabilité d'un objet particulier du système à fonctionner correctement. En général, la crédibilité CR (C_i, k_i) de la ressource informatique C_i est calculée en passant des contrôles sur place le temps de k_i . Puisque nous considérons chaque tâche validée avec succès par le courtier en utilisant la RBV comme une tâche de repérage.

Abrége :

Dans cet article, nous proposons une nouvelle approche à base de vote réputation, basé sur la technique de contrôles ponctuels. Cette approche améliore du vote basé la crédibilité pour atteindre un taux d'erreur faible, avec un surcoût raisonnable.

Dans le vote basé sur la crédibilité, un contrôle ponctuel est utilisé pour vérifier périodiquement les ressources informatiques, par l'envoi d'un travail de repérage dont le résultat correct est connu, afin d'estimer la crédibilité de chaque ressource basée sur le résultat retourné. Cette technique conduit à la dissipation des ressources dans le schéma de vote simple, car il nécessite des calculs supplémentaires pour produire le résultat des travaux de repérage. L'idée de base de notre approche proposée consiste à vérifier les ressources informatiques sans attribuer l'emploi de repérage et d'envisager la suite de la décision de vote que celui des contrôles inopinés pour estimer la crédibilité sans calculs supplémentaires. Cette crédibilité est considérée comme réputation qui est utilisée dans la décision, selon l'algorithme de la figure 1. Dans cet algorithme, le service de courtier de grille commence le calcul par l'envoi d'un certain nombre de ressources de calcul disponibles à la ligne (2) pour la transformation parallélisée. Après le calcul, les résultats générés seront retournés au courtier (lignes 19 et 20). Tant que toutes les tâches sont terminées avec des résultats acceptés (lignes 4-7), la programmation et les processus de réception pour chaque tâche sont répétés.

Supposons que chaque tâche est reproduite n fois et attribuée à plusieurs ressources informatiques C_i , de sorte qu'un courtier peut percevoir des résultats différents $V_j m$, où $i = 1, 2, \dots, N$ et $j = 1, 2, \dots, M$. Chaque ressource informatique a sa réputation la valeur R_i , qui représentent le comportement global. Cette réputation est recueillie par un service broker-grille, qui contient la liste de la réputation de toutes les ressources de calcul. La réputation est une valeur dans la plage entre 0 et 1.

Selon notre vision, le service de courtier de grille construit la réputation de chaque ressource informatique grâce à sa crédibilité. La crédibilité représente la probabilité d'un objet particulier du système à fonctionner correctement. En général, la crédibilité $CR(C_i, k_i)$ de la ressource informatique C_i est calculée en passant des contrôles sur place le temps de k_i . Puisque nous considérons chaque tâche validée avec succès par le courtier en utilisant la RBV comme une tâche de repérage.

20 JUL 2016

Titre : technique pour la sécurité des grilles de calcul**Description de l'invention**

Les grilles de calcul (grid computing en anglais) à grandes d'échelle permettent de partager les ressources de calcul réparties et interconnectées par le réseau internet sur différents sites administratifs autonomes. Les progrès rapides des systèmes de grilles ouvrent la porte à de nombreuses entreprises à adopter cette technologie pour leur développement. Ce progrès est caractérisé par l'ouverture croissante et la possibilité de partage des ressources entre les organisations dans différents domaines. Dans le contexte de l'entreprise, ces ressources partagées peuvent être utilisés à mauvais escient par certains utilisateurs malveillants qui peuvent abuser des ressources fournies et de les faire se comporter malicieusement pour retourner des résultats erronés et sabotent ainsi l'exécution des tâches de calcul qui lui sont confiées. La technique couramment utilisée par la plupart des systèmes de grille pour faire face à ce problème et pour assurer une bonne authentification des résultats obtenus est basée sur la réplication avec le vote. Néanmoins, ces techniques reposent sur l'hypothèse que les ressources du réseau se comportent de façon indépendante. Ils peuvent être inefficaces quand un certain nombre de ressources collusoires retournent collectivement les mêmes mauvais résultats relatifs à l'exécution de la même tâche. Afin de surmonter cette menace, nous proposons une approche de la « réputation basée sur le vote » qui enquête sur la fiabilité des ressources de la grille à travers un système de vote sur la réputation des ressources, et prend alors une décision sur les résultats globaux obtenus retournés par les différentes ressources interrogées.

Liste des figures et tableaux

Figure 1 : Algorithme de vote de majorité.

Revendications

1. Un algorithme pour l'authentification des résultats des grilles de calcul par un système de vote sur la réputation de ses ressources informatiques.
2. Un algorithme permettant d'améliorer la sécurité des grilles de calcul.
3. Un algorithme selon la revendication 1 caractérisée en ce que l'authentification des résultats est réalisée par l'approche de vote de majorité des ressources de calcul (informatiques) sur la crédibilité et l'authenticité des résultats.
4. Un algorithme selon la revendication 1 caractérisée en ce que l'authentification se fait avec un coût informatique raisonnablement faible..
5. Un algorithme selon l'une des revendications précédentes caractérisée en ce la fiabilité des résultats obtenus est nettement améliorée et est renforcée.
6. Un algorithme selon l'une des revendications précédentes caractérisée en ce il est très rapide.
7. Un algorithme selon l'une des revendications précédentes caractérisé par la possibilité de le généraliser au Cloud.
8. Un algorithme selon l'une des revendications précédentes caractérisée en ce il n'est pas gourmand en mémoire de l'ordinateur.
9. Un algorithme selon l'une des revendications précédentes caractérisée par les applications dans la sécurité informatique.

ANNEXES

Figure 1 : Algorithme de vote de majorité.

```

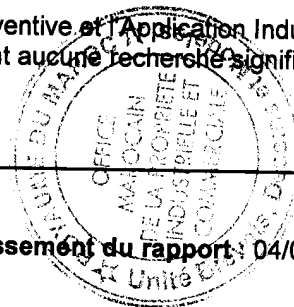
1: LT is the list of tasks to compute
2: LC is the list of computing resources
3:  $R_i = 1 - f$  and  $k_i = 0$  for each  $C_i \in LC$ , according to (2)
4: while ( there is task  $T_k \in LT$  without accepted result ) do
5:     Tasks scheduling ( )
6:     Tasks result receiving and decision for acceptance ( )
7: end while
8: Tasks scheduling ( )
9: while ( there is idle  $C_i \in LC$  )  $\wedge$  ( there is task  $T_k \in LT$  without
    accepted result ) do
10:     $C_i$  = next computing resource in LC
11:    if  $C_i$  is not blacklisted then
12:         $T_r$  = a replica of  $T_k$ 
13:        assign  $T_r$  to  $C_i$ 
14:    end if
15: end while
16: Tasks result receiving and decision for acceptance ( )
17: while ( there is a running task ) do
18: // waiting to receive a result back from a resource  $C_i$ 
19: for each  $T_r$  executed for a task  $T_k$  do
20:    receive a result  $V_j$ 
21:    for  $j = 1$  to  $m$  do
22:        compute  $R(V_j)$  according to (3)
23:        compute  $\max_j(R(V_j))$ 
24:    end for
25:    if a task  $T_k$  has only one replica with one result  $V_j$  then
26:        if  $R(V_j) > R_{min}$  then
27:            accept  $V_j$ 
28:        end if
29:    else
30:        if  $\max_j(R(V_j)) > \lambda \sum_{i=1}^n R_i$  then
31:            accept  $V_j^*$  which represent this maximum
32:            update  $R_i$  of all  $C_i^+$  which generate  $V_j^*$  according to (5) and (2)
33:            add all  $C_i^-$  whose results are different to  $V_j^*$  to the blacklist
34:            backtrack all the results previously returned by  $C_i^-$ 
35:            repeat from line 21 for all  $T_k$  that contain the backtracked results
36:        end if
37:    end if
38: end for
39: end while

```



**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)

Renseignements relatifs à la demande	
N° de la demande : 37726	Date de dépôt : 31/12/2014 ;
Déposant : UNIVERSITE MOHAMMED V DE RABAT	
Intitulé de l'invention : TECHNIQUE POUR LA SECURITE DES GRILLES DE CALCUL	
<p>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.</p> <p>Les documents cités par l'examineur dans la partie rapport de recherche sont joints au présent document.</p>	
<p>Le présent rapport contient des indications relatives aux éléments suivants :</p> <p>Partie 1 : Considérations générales</p> <p><input checked="" type="checkbox"/> Cadre 1 : Base du présent rapport</p> <p><input type="checkbox"/> Cadre 2 : Priorité</p> <p><input type="checkbox"/> Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés</p> <p>Partie 2 : Rapport de recherche</p> <p>Partie 3 : Opinion sur la brevetabilité</p> <p><input checked="" type="checkbox"/> Cadre 4 : Remarques de clarté</p> <p><input checked="" type="checkbox"/> Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle</p> <p><input type="checkbox"/> Cadre 6 : Observations à propos de certaines revendications dont aucune recherche significative n'a pu être effectuée</p> <p><input type="checkbox"/> Cadre 7 : Défaut d'unité d'invention</p>	
Examineur: N KARTIT	
Téléphone: 212 5 22 58 64 14/00	Date d'établissement du rapport: 04/02/2015



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
1 Page
- Revendications
9
- Planches de dessin
1 Page

Partie 2 : Rapport de recherche**Classement de l'objet de la demande :**

CIB : G 06F 15/16, G 06F 21/00

CPC :

Bases de données électroniques consultées au cours de la recherche :

EPOQUE, Orbit

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
X	WO 2009041801 A3 ; MIMOS BERHAD [MY]; NG KANG SIONG [MY] ; 2009-04-02. Abrégé	1-9
X	JP 2009187415 A; NEC CORP ; 2009-08-20. Abrégé	1-9
X	JP 2005056408 A; SEMICONDUCTOR ENERGY LAB; 2005-03-03. Abrégé	1-9
X	CN 101242263 B; UNIV NANJING POSTS & TELECOM;13/08/2008. Abrégé	1-9

***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 clarté*

4.1) La demande ne satisfait pas aux exigences de l'art.35 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, la revendication 1 n'étant pas claire :

- La formulation « système de vote sur la réputation de ressources informatiques » employée dans la revendication est vague et imprécise, et laisse subsister un doute quant à la signification de la caractéristique technique à laquelle elle se rapporte, au point que l'objet de ladite revendication n'est pas clairement défini.

4.2) les revendications 2-9 ne satisfont pas aux exigences de clarté car l'objet de la protection demandée n'est pas défini. Les revendications tentent de définir l'objet par le résultat recherché, En tout état de cause, cette formulation n'est pas acceptable en l'espèce, puisqu'il semble possible de définir l'objet en des termes plus concrets, c'est-à-dire en exposant comment l'effet peut être obtenu.

4.3) Le mot "algorithme" dans les revendications ne définit pas clairement une catégorie selon l'art 11 du Décret d'application de la loi n° 17-97 relative à la protection de la propriété Industrielle .il est interprété comme un procédé.

Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté (N)	Revendications aucune Revendications 1-9	Oui Non
Activité inventive (AI)	Revendications aucune Revendications 1-9	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications 1-9 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 : WO 2009041801 A3;

D2 : JP 2009187415 A;

D3 : JP 2005056408 A;

D4 : CN 101242263 B.

1. Nouveauté (N), Activité inventive (AI):

Nonobstant le manque de clarté mentionné dans le cadre 4, l'objet de la revendication 1 n'est pas nouveau au sens de l'article 26 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

En effet, le document D1 concerne un procédé et un appareil conçus pour sécuriser un traitement informatique exécuté dans un nœud de matériel de calcul d'un système de grille de calcul distribué, par création d'un nœud de confiance virtuel.

Les documents D2-D4 décrivent aussi l'objet de la revendication 1.

Par conséquent, L'objet des revendications 1 tel qu'il a été présenté n'est pas nouveau et donc n'implique pas une activité inventive au sens des articles 26 et 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

Les revendications 2-9 ne contiennent aucune caractéristique qui, combinées avec les caractéristiques de la revendication indépendante, satisfont aux exigences des articles 26 et 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13 en matière de nouveauté et d'activité inventive. Voir D1-D4.

2. Possibilité d'application industrielle (PAI) :

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.