



(43) Date de la publication internationale
12 septembre 2014 (12.09.2014)

WIPO | PCT

(10) Numéro de publication internationale
WO 2014/135683 A1

(51) Classification internationale des brevets :
G06F 21/62 (2013.01)

(21) Numéro de la demande internationale :
PCT/EP2014/054464

(22) Date de dépôt international :
7 mars 2014 (07.03.2014)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
13 00517 7 mars 2013 (07.03.2013) FR

(71) Déposant : THALES [FR/FR]; 45 rue de Villiers, F-92200 Neuilly Sur Seine (FR).

(72) Inventeurs : TOILLON, Patrice Georges Paul; Thales Avionics 18 avenue du Maréchal Juin, F-92362 Meudon La Foret (FR). AGROU, Hicham; Thales Avionics 18 avenue du Maréchal Juin, F-92362 Meudon La Foret (FR).

(74) Mandataires : BLOT, Philippe et al.; Cabinet LAVOIX, 2, place d'Estienne d'Orves, F-75009 Paris (FR).

(81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée :

— avec rapport de recherche internationale (Art. 21(3))

(54) Title : SYSTEM FOR SECURING THE CRITICAL DATA OF AN ON-BOARD AIRPLANE SYSTEM OF AN AIRCRAFT

(54) Titre : SYSTÈME DE SÉCURISATION DE DONNÉES CRITIQUES D'UN SYSTÈME AVIONIQUE EMBARQUÉ À BORD D'UN AÉRONEF

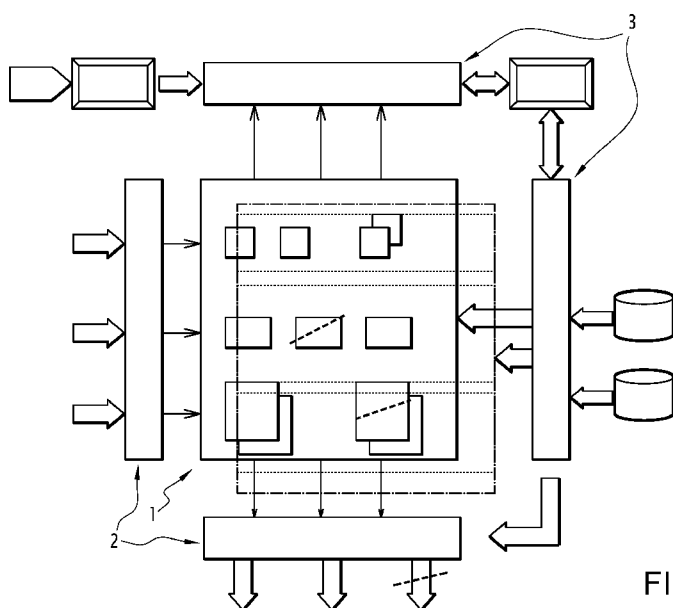


FIG 1

(57) Abstract : The invention relates to a system for securing the critical data of an on-board airplane system of an aircraft that is stored in storage means (1), comprising: means (2, 3) for controlling access, for/by at least one user, to said data such as to validate or invalidate access to said data on the basis of security information thereof, is characterized in that the security information is selected within a group including, *inter alia*: a list of users allowed to access the data; a maximum number of allowed accesses to the data, along with the types of allowed accesses to said data; a time window, having a limited duration, allowed for access to said data; a series/concatenation allowed for access, by different users, to said data; and prioritization of the areas related to the storage means.

(57) Abrégé :

[Suite sur la page suivante]



Ce système de sécurisation de données critiques d'un système avionique embarqué à bord d'un aéronef et stockées dans des moyens de mémorisation (1), comportant des moyens (2, 3) de contrôle des accès pour/par au moins un utilisateur à ces données, pour valider ou non l'accès à ces données en fonction d'informations de sécurité de celles-ci, est caractérisé en ce que les informations de sécurité sont choisies dans un groupe comprenant entre autres : une liste d'utilisateurs autorisés à accéder aux données; un nombre maximum d'accès autorisés à ces données, ainsi que les types d'accès autorisés à ces données; une fenêtre temporelle de durée limitée autorisée d'accès à ces données; une séquence/enchaînement autorisé d'accès par différents utilisateurs à ces données; une hiérarchisation des zones associées aux moyens de mémorisation.

Système de sécurisation de données critiques d'un système avionique embarqué à bord d'un aéronef

La présente invention concerne de façon générale, un système de sécurisation de données.

Plus particulièrement, l'invention se rapporte à un système de sécurisation de données critiques d'un système avionique embarqué à bord d'un aéronef et stockées dans des moyens de mémorisation de ce système.

On sait que les systèmes de ce type comportent des moyens de contrôle des accès pour/par au moins un utilisateur à ces données, pour valider ou non l'accès à ces données en fonction d'informations de sécurité de celles-ci.

En effet, l'accès à ce type de données critiques d'un système avionique doit être maîtrisé et sécurisé au maximum, car ce type de données est extrêmement sensible pour l'aéronef et notamment pour la sécurité de vol de celui-ci.

Le but de l'invention est donc d'améliorer encore la sécurité de ces informations et donc de façon générale la sécurité des aéronefs.

A cet effet, l'invention a pour objet un système de sécurisation de données critiques d'un système avionique embarqué à bord d'un aéronef et stockées dans des moyens de mémorisation, comportant des moyens de contrôle des accès pour/par au moins un utilisateur à ces données, pour valider ou non l'accès à ces données en fonction d'informations de sécurité de celles-ci, caractérisé en ce que les informations de sécurité sont choisies dans un groupe comprenant entre autres :

- une liste d'utilisateurs autorisés à accéder aux données ;
- un nombre maximum d'accès autorisés à ces données, ainsi que les types d'accès autorisés à ces données ;
- une fenêtre temporelle de durée limitée autorisée d'accès à ces données ;
- une séquence/enchaînement autorisé d'accès par différents utilisateurs à ces données ;
- une hiérarchisation des zones associées aux moyens de mémorisation.

Suivant d'autres caractéristiques du système selon l'invention prises seules ou en combinaison :

- les moyens de mémorisation sont organisés :
 - par zone(s) discrète(s) élémentaire(s) associée(s) dont chacune d'elles est associée à un message, ou
 - sous la forme de différentes zones contiguës dont chacune d'elles est associée à une plage d'adresses des moyens de mémorisation,

- les informations de sécurité du groupe et/ou le groupe d'informations de sécurité peut être :

- totalement statique avec une préconfiguration et une préinitialisation, ou
- être modifié dynamiquement suivant les conditions d'accès à chacune des zones permettant ainsi une gestion dynamique adaptée aux détections de non respect de conditions ou de tentatives d'accès non-conformes, ou
- évolutif dans le temps,

- il comporte des moyens d'altération temporaire ou définitive des données en cas de non respect des conditions d'accès ou de tentative d'accès non conforme aux conditions d'accès précitées comprenant entre autres :

- une liste d'utilisateurs autorisés à accéder aux données ;
- un nombre maximum d'accès autorisés à ces données, ainsi que les types d'accès autorisés à ces données ;
- une fenêtre temporelle de durée limitée autorisée d'accès à ces données ;
- une séquence/enchaînement autorisé d'accès par différents utilisateurs à ces données ;
- une hiérarchisation des zones associées aux moyens de mémorisation,

- il comporte des moyens d'effacement temporaire ou définitif des données en cas de non respect des conditions d'accès ou de tentative d'accès non conforme aux conditions d'accès précitées comprenant entre autres :

- une liste d'utilisateurs autorisés à accéder aux données ;
- un nombre maximum d'accès autorisés à ces données, ainsi que les types d'accès autorisés à ces données ;
- une fenêtre temporelle de durée limitée autorisée d'accès à ces données ;
- une séquence/enchaînement autorisé d'accès par différents utilisateurs à ces données ;
- une hiérarchisation des zones associées aux moyens de mémorisation,

- il comporte des moyens de hiérarchisation des utilisateurs, pour valider ou non l'accès à ces données en cas de tentative d'accès simultanés et/ou de tentative de violation de hiérarchie,

- il comporte des moyens de hiérarchisation des utilisateurs, pour bannir un utilisateur en cas de tentative d'accès simultanés et/ou de tentative de violation de hiérarchie,

- il comporte des moyens de bannissement de l'utilisateur pour une durée limitée ou infinie,

- il comporte des moyens de bannissement de l'utilisateur pour une durée configurable,

- la durée de bannissement lorsqu'elle n'est pas infinie, peut évoluer et est caractérisée en ce qu'elle est choisie dans un groupe comprenant entre autres :

- 5 - l'indice d'une fenêtre temporelle,
- l'adresse de la requête émise par l'utilisateur,
- l'identifiant de l'utilisateur,
- le type d'utilisateur,
- la hiérarchie de l'utilisateur ou du groupe d'utilisateurs,
- 10 - le nombre de bannissements temporaires ayant déjà été réalisé et comptabilisé,

- les moyens d'altération et/ou d'effacement temporaire des données sont associés à des moyens de recouvrement de celles-ci,

15 - le fonctionnement des moyens de recouvrement est déclenché à partir d'informations de sécurité choisies dans un groupe comprenant entre autres :

- une liste d'utilisateurs autorisés à accéder aux données ;
- un nombre maximum d'accès autorisés à ces données, ainsi que les types d'accès autorisés à ces données ;
- une fenêtre temporelle de durée limitée autorisée d'accès à ces données;
- 20 - une séquence/enchaînement autorisé d'accès par différents utilisateurs à ces données ;
- une hiérarchisation des zones associées aux moyens de mémorisation,

- les moyens de recouvrement des données comprennent des moyens de rétablissement et/ou de remplacement de toute ou partie de celles-ci.

25 L'invention sera mieux comprise à l'aide de la description qui va suivre, donnée uniquement à titre d'exemple et faite en se référant au dessin annexé qui représente un schéma synoptique illustrant la structure et le fonctionnement général d'un système de sécurisation selon l'invention.

30 On a en effet illustré sur cette figure, la structure générale d'un système de sécurisation de données critiques d'un système avionique embarqué à bord d'un aéronef tel qu'un avion par exemple.

Les données sont stockées dans des moyens de mémorisation désignés par la référence générale 1 sur cette figure.

35 Ce système comporte des moyens formant interface d'accès 2 par au moins un utilisateur à ces données et des moyens de contrôle de ces accès 3 pour ce ou ces

utilisateurs, pour valider ou non l'accès à ces données en fonction d'informations de sécurité de celles-ci.

Les informations de sécurité des données critiques utilisées dans les moyens de contrôle 3 se présentent alors par exemple sous la forme de tables ou des lois...,
5 définissant des conditions notamment d'accès aux données et peuvent être choisies dans un groupe comprenant entre autres :

- une liste d'utilisateurs autorisés à accéder aux données ;
- un nombre maximum d'accès autorisés à ces données, ainsi que les types d'accès autorisés à ces données ;
- 10 - une fenêtre temporelle de durée limitée autorisée d'accès à ces données ;
- une séquence/enchaînement autorisé d'accès par différents utilisateurs à ces données ;
- une hiérarchisation des zones associées aux moyens de mémorisation.

Ceci permet alors de maîtriser les accès à ces données critiques par un ou des
15 utilisateurs.

Les moyens de contrôle 3 sont indépendants des moyens formant interface d'accès 2 et des moyens de mémorisation 1.

Ces différentes tables ou lois peuvent ainsi être matérialisées sous la forme de programmes mis en œuvre au niveau des ces moyens de contrôle.

20 Les moyens de mémorisation 1 peuvent quant à eux être organisés par zone(s) discrète(s) élémentaire(s) associé(s) dont chacune d'elle est associée à un message ou ils peuvent également se présenter sous la forme de différentes zones continues de mémoire dont chacune d'elle est associée à une plage d'adresses des moyens de mémorisation 1.

25 Les informations de sécurité du groupe décrit précédemment et/ou le groupe d'informations de sécurité peuvent être totalement statiques avec une pré configuration et une pré initialisation ou au contraire peuvent être modifiés de façon dynamique suivant les conditions d'accès à chacune des zones.

Ceci permet ainsi une gestion dynamique de celles-ci adaptée aux détections de
30 non respect des conditions ou de tentatives d'accès non-conformes.

On peut également envisager selon une variante, que les informations de sécurité du groupe décrit précédemment et/ou le groupe d'informations de sécurité soient évolutifs dans le temps.

35 Les moyens de contrôle des accès peuvent alors mettre en œuvre des moyens d'altération temporaire ou définitive de tout ou partie de données par des moyens d'effacement temporaire ou définitif de tout ou partie de celles-ci.

Ainsi par exemple, le système peut comporter des moyens d'altération temporaire ou définitive des données en cas de non respect des conditions d'accès ou de tentatives d'accès non conformes aux conditions d'accès précitées et comprenant en outre :

- une liste d'utilisateurs autorisés à accéder aux données,
- un nombre maximum d'accès autorisés à ces données, ainsi que les types d'accès autorisés à ces données ;
- une fenêtre temporelle de durée limitée d'autorisation d'accès à ces données ;
- une séquence/enchaînement autorisé d'accès par différents utilisateurs à ces données, et
- une hiérarchisation des zones associées aux moyens de mémorisation.

Des éléments analogues peuvent également être utilisés par les moyens d'effacement temporaire ou définitif de toute ou partie des données.

Ces moyens peuvent en complément être utilisés avec des moyens de hiérarchisation des utilisateurs pour valider ou non l'accès à ces données en cas de tentatives d'accès simultanées et/ou de tentatives de violation de hiérarchie.

Des moyens de hiérarchisation analogue peuvent également être utilisés pour bannir un utilisateur en cas de tentatives d'accès simultanées et de tentatives de violation de hiérarchie.

Ce bannissement peut alors être un bannissement pour une durée limitée ou un temps infini c'est-à-dire une durée illimitée de cet utilisateur.

Des moyens de bannissement de l'utilisateur pour une durée configurable c'est-à-dire programmable, peuvent également être envisagés.

Cette durée de bannissement lorsqu'elle n'est pas infinie, peut évoluer et est par exemple choisie dans un groupe comprenant en outre :

- l'indice d'une fenêtre temporelle,
- l'adresse de la requête émise par l'utilisateur,
- l'identifiant de l'utilisateur,
- le type d'utilisateur,
- la hiérarchie de l'utilisateur ou du groupe d'utilisateurs, et
- le nombre de bannissements temporaires ayant déjà été réalisés et comptabilisés.

Comme cela a été indiqué précédemment, les moyens d'altération et/ou d'effacement peuvent être temporaires et dans ce cas, ces moyens d'altération et/ou d'effacement peuvent être associés à des moyens de recouvrement des données en tout ou partie.

En fait, le fonctionnement de ces moyens de recouvrement peut être déclenché à partir d'informations de sécurité choisies dans un groupe comprenant entre autres :

- une liste d'utilisateurs autorisés à accéder aux données,
- un nombre maximum d'accès autorisés à ces données, ainsi que les types d'accès autorisés à ces données ;
- une fenêtre temporelle de durée limitée autorisée d'accès à ces données,
- une séquence/enchaînement autorisé d'accès par différents utilisateurs à ces données, et
- une hiérarchisation des zones associées aux moyens de mémorisation.

D'une façon générale, le recouvrement de données peut également être compris comme pouvant englober le rétablissement et/ou le remplacement de toute ou partie de ces données.

On conçoit alors que ceci permet d'améliorer grandement la sécurisation de ces données, ces données étant, comme on l'a indiqué précédemment, des données critiques correspondant aux données relatives au fonctionnement et/ou susceptibles de remettre en cause la sécurité de fonctionnement de l'aéronef.

Ces données critiques ne sont pas à confondre avec les données relatives aux autres fonctions de l'aéronef telles que par exemple les données relatives aux moyens de divertissement mis à la disposition des passagers, etc.

REVENDICATIONS

1.- Système de sécurisation de données critiques d'un système avionique embarqué à bord d'un aéronef et stockées dans des moyens de mémorisation (1),
5 comportant des moyens (2, 3) de contrôle des accès pour/par au moins un utilisateur à ces données, pour valider ou non l'accès à ces données en fonction d'informations de sécurité de celles-ci, caractérisé en ce que les informations de sécurité sont choisies dans un groupe comprenant entre autres :

- une liste d'utilisateurs autorisés à accéder aux données ;
- 10 - un nombre maximum d'accès autorisés à ces données, ainsi que les types d'accès autorisés à ces données ;
- une fenêtre temporelle de durée limitée autorisée d'accès à ces données ;
- une séquence/enchaînement autorisé d'accès par différents utilisateurs à ces données ;
- 15 - une hiérarchisation des zones associées aux moyens de mémorisation,

et en ce qu'il comporte des moyens d'altération temporaire ou définitive des données en cas de non respect des conditions d'accès ou de tentative d'accès non conforme aux conditions d'accès précitées comprenant entre autres :

- une liste d'utilisateurs autorisés à accéder aux données ;
- 20 - un nombre maximum d'accès autorisés à ces données, ainsi que les types d'accès autorisés à ces données ;
- une fenêtre temporelle de durée limitée autorisée d'accès à ces données ;
- une séquence/enchaînement autorisé d'accès par différents utilisateurs à ces données ;
- 25 - une hiérarchisation des zones associées aux moyens de mémorisation.

2- Système de sécurisation de données selon la revendication 1, caractérisé en ce les moyens de mémorisation (1) sont organisés :

- par zone(s) discrète(s) élémentaire(s) associée(s) dont chacune d'elle est associée à un message, ou
- 30 - sous la forme de différentes zones contigües dont chacune d'elles est associée à une plage d'adresses des moyens de mémorisation.

3- Système de sécurisation de données selon la revendication 1 ou 2, caractérisé en ce que les informations de sécurité du groupe et/ou le groupe d'informations de sécurité peut être :

- 35 - totalement statique avec une préconfiguration et une préinitialisation, ou

- être modifié dynamiquement suivant les conditions d'accès à chacune des zones permettant ainsi une gestion dynamique adaptée aux détections de non respect de conditions ou de tentatives d'accès non-conformes, ou

- évolutif dans le temps.

5 4- Système de sécurisation de données selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte des moyens d'effacement temporaire ou définitif des données en cas de non respect des conditions d'accès ou de tentative d'accès non conforme aux conditions d'accès précitées comprenant entre autres :

- 10 - une liste d'utilisateurs autorisés à accéder aux données ;
 - un nombre maximum d'accès autorisés à ces données, ainsi que les types d'accès autorisés à ces données ;
 - une fenêtre temporelle de durée limitée autorisée d'accès à ces données ;
 - une séquence/enchaînement autorisé d'accès par différents utilisateurs à ces
15 données ;
 - une hiérarchisation des zones associées aux moyens de mémorisation.

 5- Système de sécurisation de données selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte des moyens de hiérarchisation des utilisateurs, pour valider ou non l'accès à ces données en cas de tentative d'accès
20 simultanés et/ou de tentative de violation de hiérarchie.

 6- Système de sécurisation de données selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte des moyens de hiérarchisation des utilisateurs, pour bannir un utilisateur en cas de tentative d'accès simultanés et/ou de tentative de violation de hiérarchie.

25 7- Système de sécurisation de données selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte des moyens de bannissement de l'utilisateur pour une durée limitée ou infinie.

 8- Système de sécurisation de données selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte des moyens de bannissement de
30 l'utilisateur pour une durée configurable.

 9- Système de sécurisation de données selon la revendication 7 ou 8, caractérisé en ce que la durée de bannissement lorsqu'elle n'est pas infinie, peut évoluer et est caractérisée en ce qu'elle est choisie dans un groupe comprenant entre autres :

- l'indice d'une fenêtre temporelle,
35 - l'adresse de la requête émise par l'utilisateur,
 - l'identifiant de l'utilisateur,

- le type d'utilisateur,
- la hiérarchie de l'utilisateur ou du groupe d'utilisateurs,
- le nombre de bannissements temporaires ayant déjà été réalisé et comptabilisé.

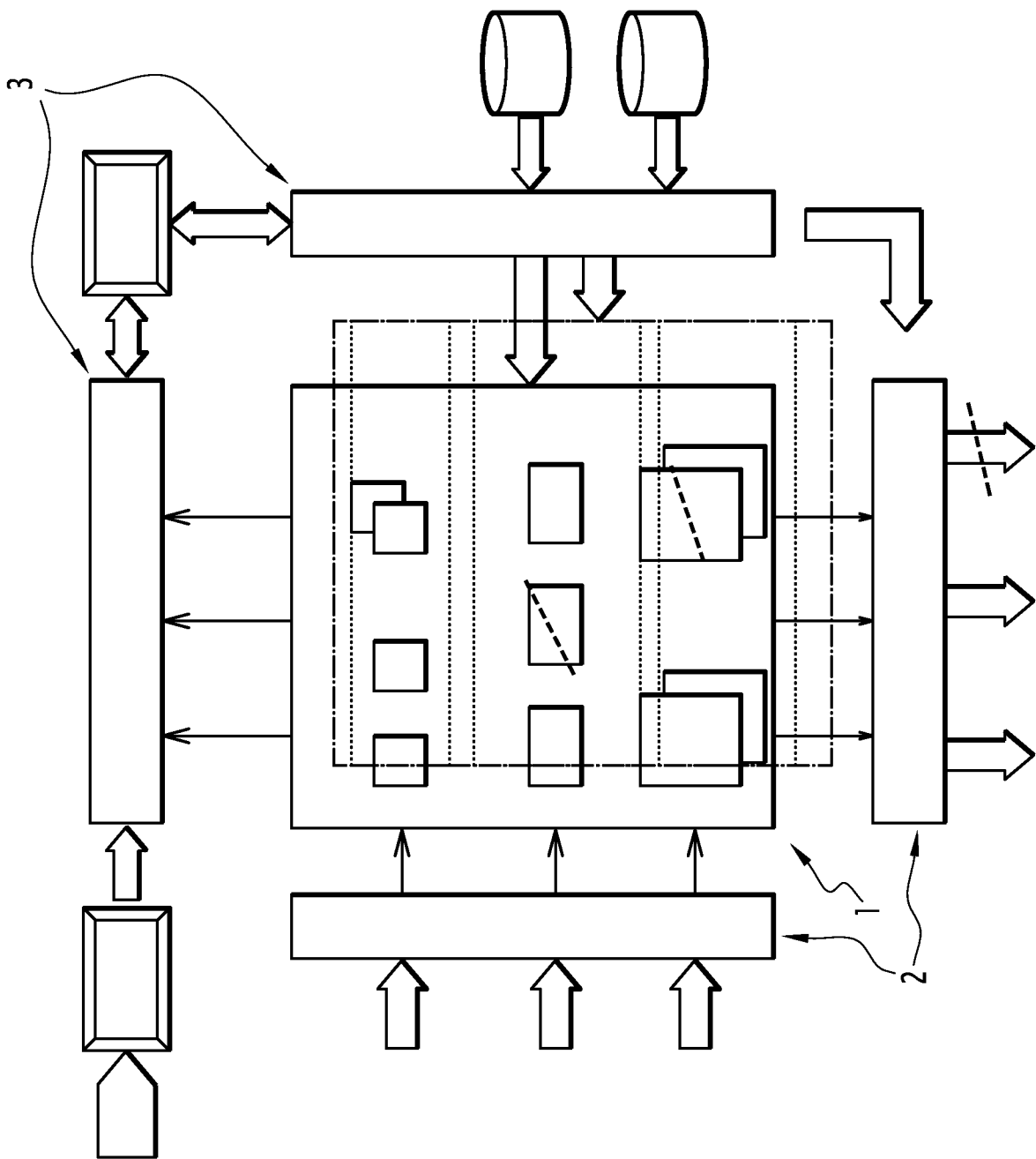
5 10- Système de sécurisation de données selon la revendication 4, caractérisé en ce que les moyens d'altération et/ou d'effacement temporaire des données sont associés à des moyens de recouvrement de celles-ci.

10 11- Système de sécurisation de données selon la revendication 10, caractérisé en ce que le fonctionnement des moyens de recouvrement est déclenché à partir d'informations de sécurité choisies dans un groupe comprenant entre autres :

- une liste d'utilisateurs autorisés à accéder aux données ;
- un nombre maximum d'accès autorisés à ces données, ainsi que les types d'accès autorisés à ces données ;
- une fenêtre temporelle de durée limitée autorisée d'accès à ces données ;
- 15 - une séquence/enchaînement autorisé d'accès par différents utilisateurs à ces données ;
- une hiérarchisation des zones associées aux moyens de mémorisation.

20 12- Système de sécurisation de données selon la revendication 10 ou 11, caractérisé en ce que les moyens de recouvrement des données comprennent des moyens de rétablissement et/ou de remplacement de toute ou partie de celles-ci.

1/1



INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2014/054464

A. CLASSIFICATION OF SUBJECT MATTER
 INV. G06F21/62
 ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2006/069274 A2 (SANDISK CORP [US]; JAGOND-COULOMB FABRICE [US]; HOLTZMAN MICHAEL [US];) 29 June 2006 (2006-06-29) paragraph [0046] - paragraph [0070] paragraph [0101] - paragraph [0115] -----	1-12
A	EP 2 204 753 A2 (FUJITSU LTD [JP]) 7 July 2010 (2010-07-07) paragraph [0162] - paragraph [0172] -----	9-12



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

2 May 2014

Date of mailing of the international search report

12/05/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

Chabot, Pedro

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2014/054464

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006069274	A2	29-06-2006	
		CN 101120353 A	06-02-2008
		CN 101819612 A	01-09-2010
		EP 1836641 A2	26-09-2007
		EP 2284758 A2	16-02-2011
		JP 4857283 B2	18-01-2012
		JP 2008524755 A	10-07-2008
		KR 20070098869 A	05-10-2007
		WO 2006069274 A2	29-06-2006

EP 2204753	A2	07-07-2010	
		EP 2204753 A2	07-07-2010
		JP 5304229 B2	02-10-2013
		JP 2010152750 A	08-07-2010
		US 2010169554 A1	01-07-2010

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/EP2014/054464

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F21/62
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 2006/069274 A2 (SANDISK CORP [US]; JAGOND-COULOMB FABRICE [US]; HOLTZMAN MICHAEL [US];) 29 juin 2006 (2006-06-29) alinéa [0046] - alinéa [0070] alinéa [0101] - alinéa [0115] -----	1-12
A	EP 2 204 753 A2 (FUJITSU LTD [JP]) 7 juillet 2010 (2010-07-07) alinéa [0162] - alinéa [0172] -----	9-12



Voir la suite du cadre C pour la fin de la liste des documents



Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"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

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

2 mai 2014

Date d'expédition du présent rapport de recherche internationale

12/05/2014

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Chabot, Pedro

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/EP2014/054464

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2006069274 A2	29-06-2006	CN 101120353 A	06-02-2008
		CN 101819612 A	01-09-2010
		EP 1836641 A2	26-09-2007
		EP 2284758 A2	16-02-2011
		JP 4857283 B2	18-01-2012
		JP 2008524755 A	10-07-2008
		KR 20070098869 A	05-10-2007
		WO 2006069274 A2	29-06-2006

EP 2204753 A2	07-07-2010	EP 2204753 A2	07-07-2010
		JP 5304229 B2	02-10-2013
		JP 2010152750 A	08-07-2010
		US 2010169554 A1	01-07-2010
