(12) UK Patent Application (19) GB (11) 2555569 (13) A

(43) Date of A Publication 09.05.2018

(21) Application No: 1616788.4

(22) Date of Filing: 03.10.2016

(71) Applicant(s):
Elias Haddad
AppartCity 109, Rue Zenobe Gramme 17, 6700 Arlon, Belgium

(72) Inventor(s):
Elias Haddad

(74) Agent and/or Address for Service:
LOVEN Patents & Trademarks Limited
51 Wragby Road, Sudbrooke, Lincoln, Lincolnshire, LN2 2QU, United Kingdom

(51) INT CL:
G06F 21/62 (2013.01) ***G06F 21/44*** (2013.01)

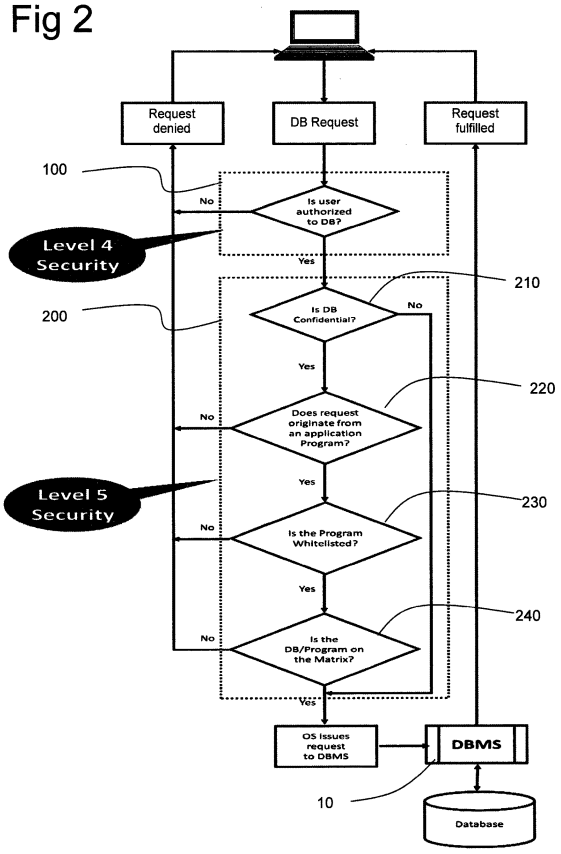
(56) Documents Cited:
EP 2889796 A2 **WO 2001/025870 A2**
US 20120317622 A1

(58) Field of Search:
INT CL **G06F**
Other: **EPODOC, WPI, Patent Full Text**

(54) Title of the Invention: **Enhanced computer objects security**
Abstract Title: **Enhanced computer objects security**

(57) A computer operating system security system and method which provides a layer of information security 200 over and above user authentication 100. The information security system intercepts requests for access to data objects and to check in a look-up table whether the combination of requesting program and location for the requesting program is recorded in the table for a confidential data object. The invention further provides a method of controlling access to data comprising steps of; checking whether a data object is confidential 210, determining which application program requested access 220, checking that program against a register such as a whitelist 230, checking the location of the application program 240, and denying access if any of the checks are failed. The data object can be a database table, or any file to which access is to be restricted, such as a text document, an image file, and an audio file.

Fig 2



GB 2555569 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

Fig 1

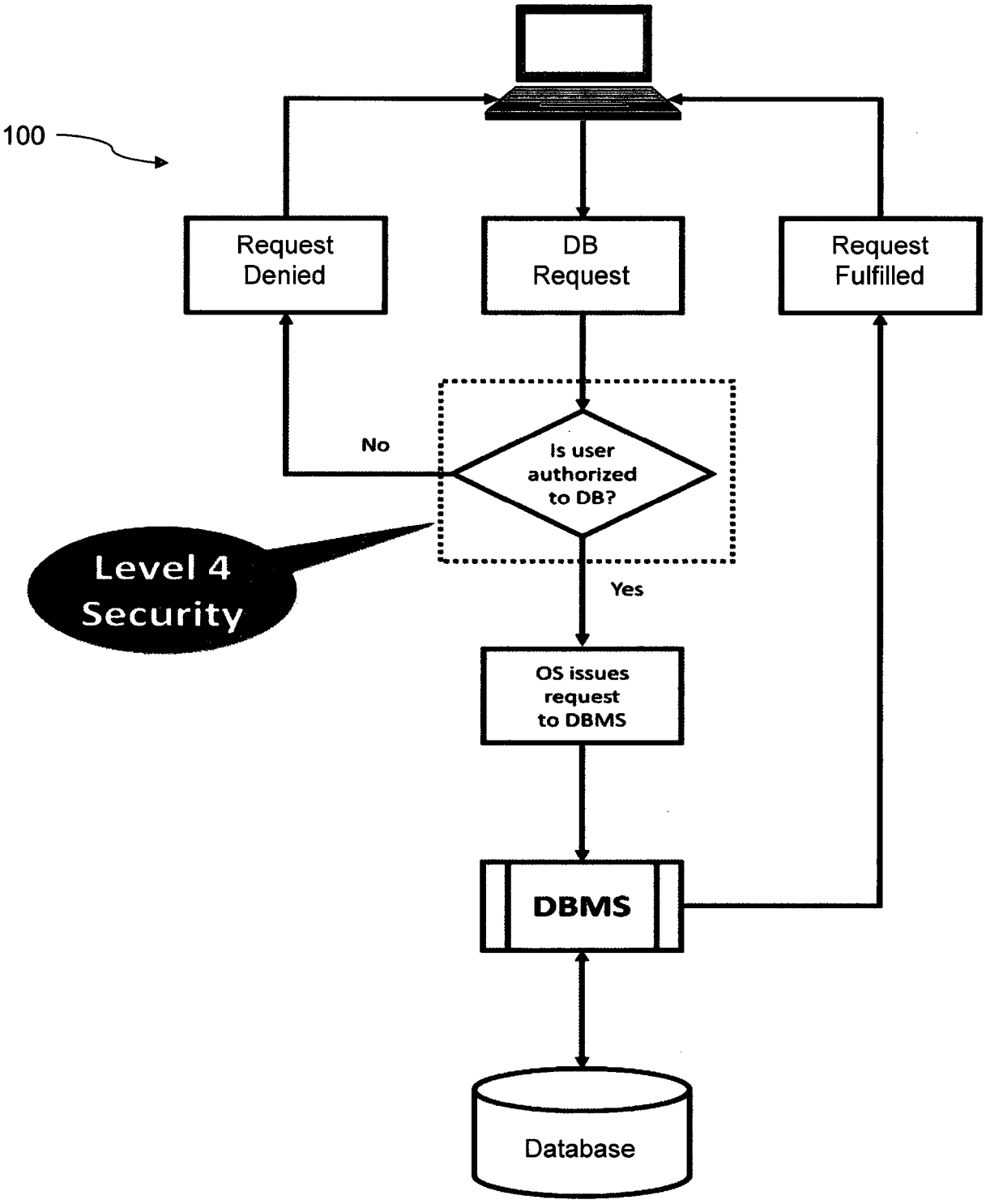

100
Request Denied
DB Request
Request Fulfilled
No
Is user authorized to DB?
Level 4 Security
Yes
OS issues request to DBMS
DBMS
Database

Fig 2

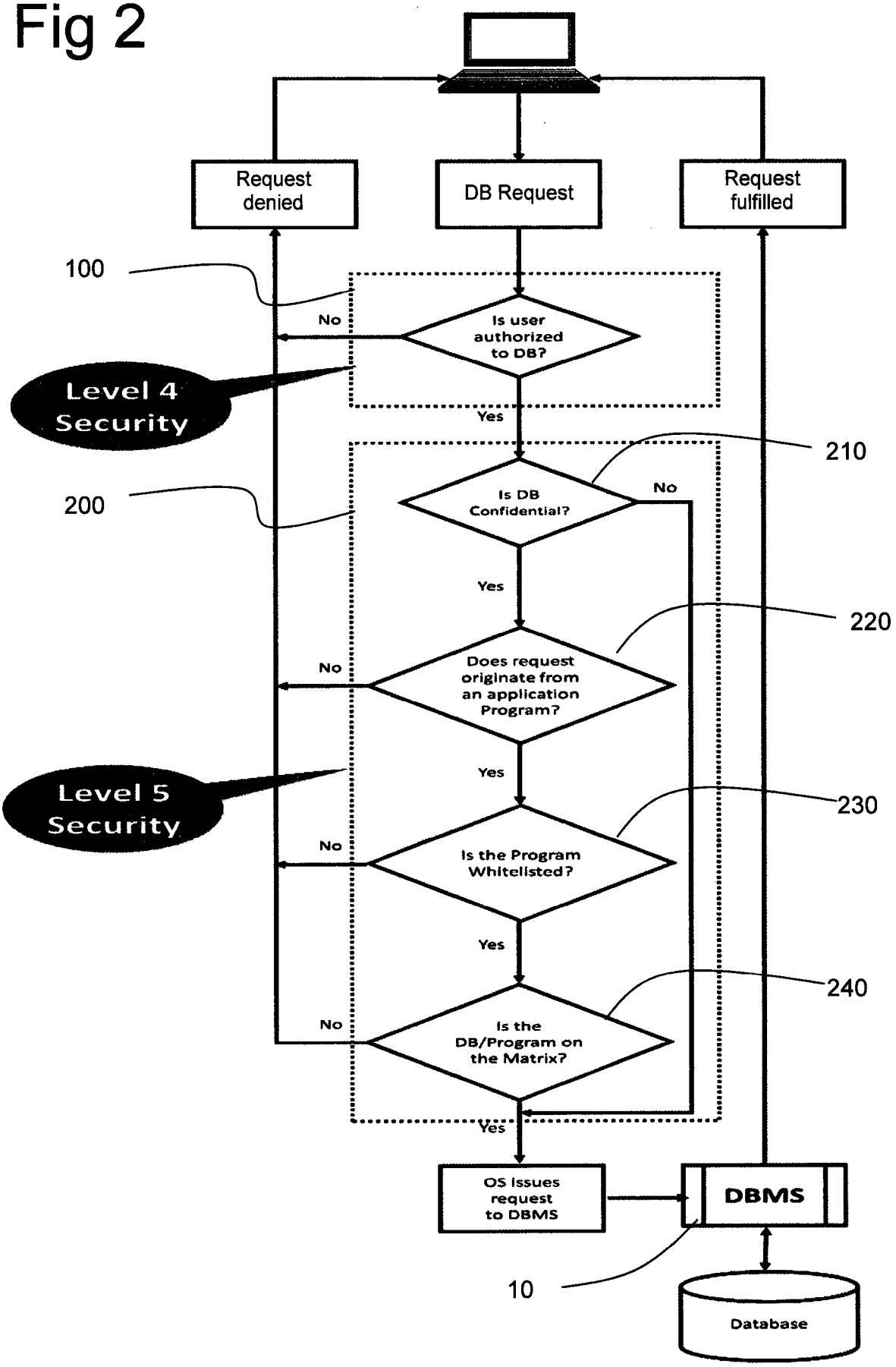

Request denied
DB Request
Request fulfilled
100
No
Is user authorized to DB?
Level 4 Security
Yes
210
200
Is DB Confidential?
No
Yes
220
No
Does request originate from an application Program?
Yes
Level 5 Security
230
No
Is the Program Whitelisted?
Yes
240
No
Is the DB/Program on the Matrix?
Yes
OS Issues request to DBMS
DBMS
10
Database

Fig 3

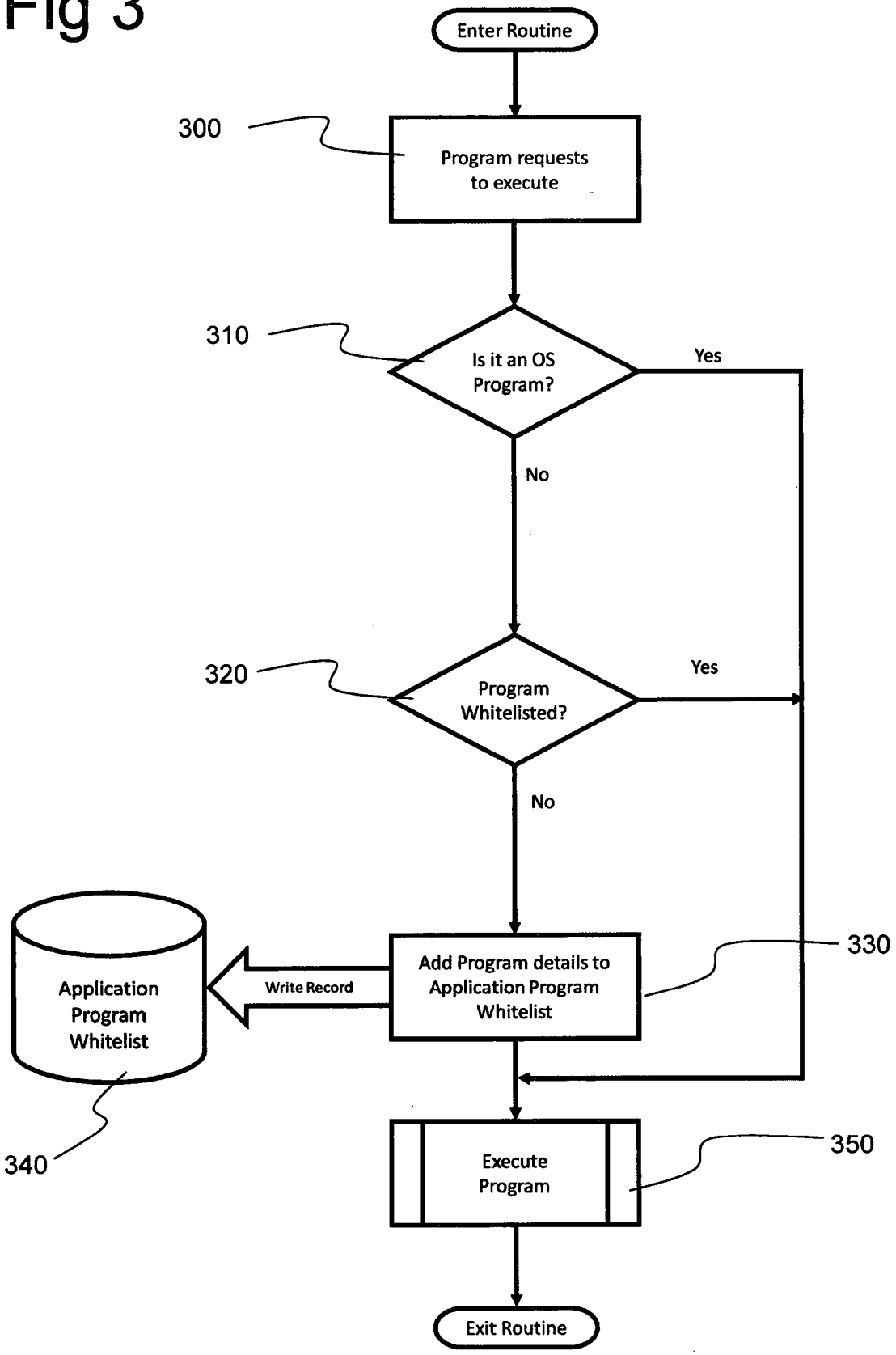
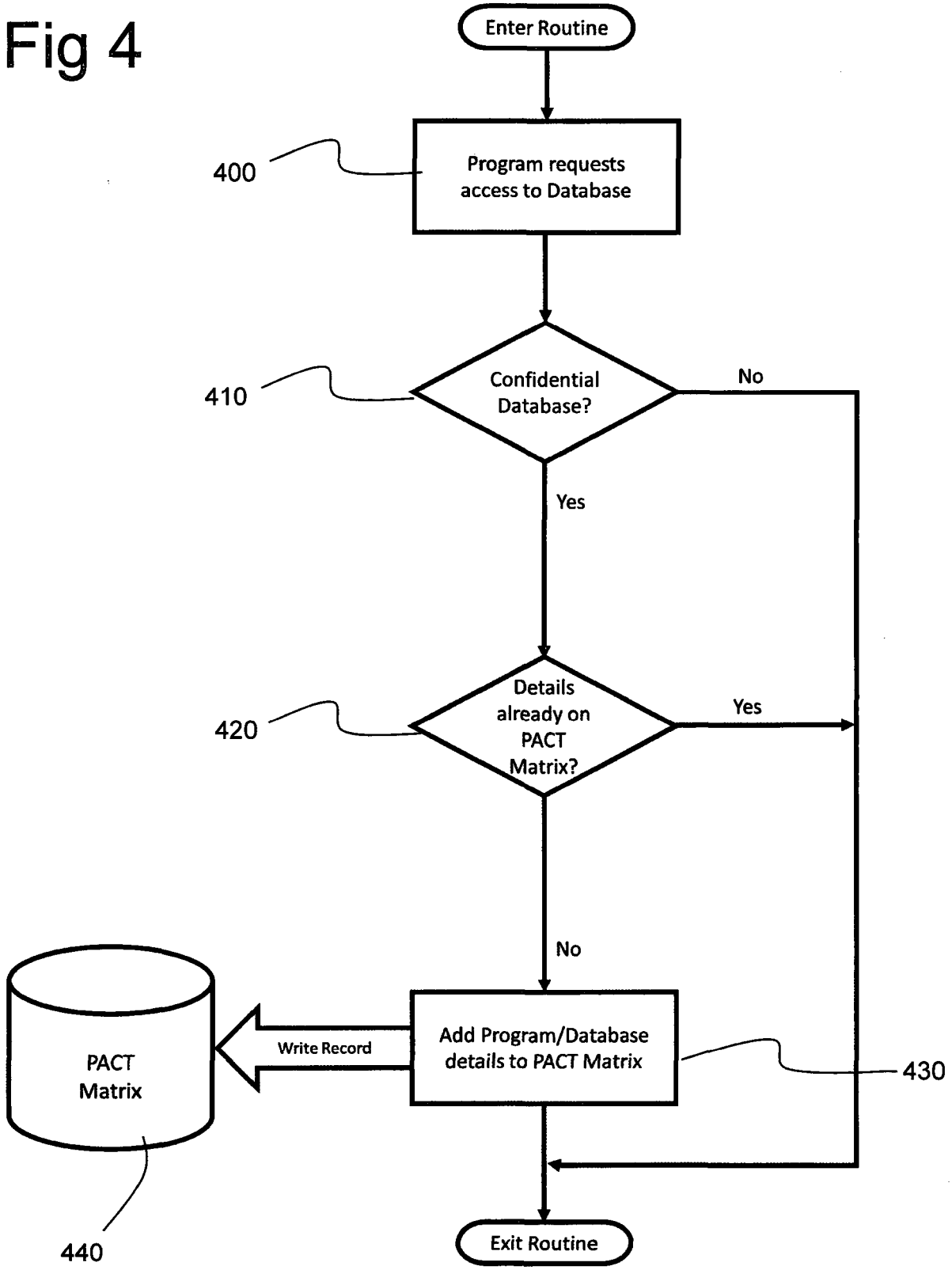

Enter Routine
300
Program requests to execute
310
Is it an OS Program?
Yes
No
320
Program Whitelisted?
Yes
No
Application Program Whitelist
Write Record
Add Program details to Application Program Whitelist
330
340
Execute Program
350
Exit Routine

Fig 4


Enter Routine
400
Program requests access to Database
410
Confidential Database?
No
Yes
420
Details already on PACT Matrix?
Yes
No
PACT Matrix
Write Record
Add Program/Database details to PACT Matrix
430
440
Exit Routine

ENHANCED COMPUTER OBJECTS SECURITY

Field of the Invention

This invention relates to computer operating system security, and in particular to a computer whose operating system includes a data object security system, and to a method of controlling access to confidential data objects.

Background to the Invention

Cyber threats continue to plague governments and businesses around the world. These threats are on the rise as cyber criminals increase their focus and know-how. There is an urgent need for a digital vaccine to inhibit cyber-criminal activity in the case of stealing and/or corrupting our data, yet allows the rest of us to utilize this data without interruption.

Security professionals are relentlessly addressing system vulnerabilities with the latest patches (software fixes), securing the firewall against external threats, deploying antivirus detection and containment/removal, user authentication and best practices thereof, user access controls which regulate application scope, and database authorization to govern users' read, write, update and delete capabilities.

There are four strategic provisions deployed today are as follows:

Level 1: Security Management - the identification of an organization's assets (including information assets), followed by the development, documentation, and implementation of policies and procedures for protecting these assets. An organization uses such security management procedures as information classification, risk assessment, and risk analysis to identify threats, categorize assets, and rate system vulnerabilities so that they can implement effective controls.

Level 2: Network Security - consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, and users are assigned an ID and password or other authenticating information that allows them access to information and programs within their domain.

Level 3: Application Security - intercept and block external threats using either a "blacklist" (antivirus protection) or a "whitelist" strategy to control which program may execute on their system. Application security also encompasses measures taken throughout the development code's life-cycle to prevent gaps in the security policy of an application or the underlying system vulnerabilities through flaws in the design.

Level 4: Database Security - concerns the use of a broad range of controls to protect the data against compromise, including backup and recovery option. The micro management of who can read (including download), write/update/delete (susceptible to corruption) database information are fundamental principles that ensure data integrity.

This strategy has been identified by the inventor as incomplete, because:

a) All bona fide users need varying levels of database access in order to perform their function. This includes the ability to read, write, update and delete data as predetermined by the applications they use; and

b) In most organizations today, it is common practice for users to download a database into an Excel spreadsheet and email the document to themselves or a third party. If bona fide users can do this, so too can cyber criminals.

The basic authority that can be attributed to a database is Read authority, and this satisfies all the cyber criminals' needs. Cyber criminals merely need a user Id and password to log onto a computer system, and that is not hard to obtain judging by the plethora of data breaches occurring today.

Furthermore, cyber criminals have no need to use Application systems; they go directly to all the accessible databases (those with Read authority) and download the data via native languages such as SQL or directly into an Excel spreadsheet as illustrated earlier.

Cyber criminals obtain user Id's and passwords using techniques such as fake wireless access points, infected emails, Trojans, key loggers, cookie thefts, bait and switch, and more. Threats can also originate from within the enterprise.

The scope of the problem therefore is not necessarily to prevent the download of data, but to regulate which data is available for download. Data classified as confidential should certainly never be available for download by anyone - internally or externally.

To appreciate the difference between confidential and non-confidential data, consider the following two examples:

- In a medical establishment, a database containing patients' names, medical records, gender, addresses, dates of birth, credit card details, social security numbers and so on can be classified as confidential data. This brand of information is what cyber criminals hunt for because they can sell the data or exploit it for their own purposes – especially the credit card details.
- In the same medical establishment, a database containing a list of supplies such syringes, bandages, quantities in stock, dates of last orders, suppliers' details and so on may be classified as non-confidential data. It has no value on the black market.

In both these examples, bona fide users have access to the information, both confidential and non-confidential, and as illustrated earlier, so too do cyber criminals.

Summary of the Invention

According to one aspect of the invention there is provided a computer comprising:

one or more hardware processors;

data storage for storing data objects;

a computer operating system in the form of computer-executable instructions which can be executed by one or more of the hardware processors, the operating system comprising:

an object security system for controlling access to objects, the object security system being configured to receive requests for access to data objects stored in the data storage and to determine, upon receipt of a request for access, whether the request is from an authorised user of the object and to block access if the request is not from an authorised user, characterised in that the

security system further comprises a register containing for each data object designated as confidential the or each application program permitted to access the data object and at least one designated location in the computer for the or each application program, the system being further configured to determine from each request if the data object is entered in the register and, if it is, to further determine the application program from which the request originated and to block access if the application program is not present in the register as a permitted application program in a designated location.

Preferably, the operating system further comprises a routine operable to add data objects to the look-up table, the routine being configured:

a) to receive requests for access to data objects stored in the data storage, to determine for each request whether the data object is marked as confidential;

b) to determine, if it is marked as confidential, whether the combination of the object and the requesting program is already in the register; and

c) to create a record in the table if the combination is not already in the register.

The invention further provides a method of controlling access to confidential data objects stored in computer data storage, the method comprising:

a) tagging confidential data objects as confidential;

b) establishing a table recording, for each confidential data object, each application program permitted to open said data object and the designated storage location for the application program;

and then processing each subsequent request for access to a data object in the computer data storage to determine whether the requested data object is confidential and if it is confidential:

c) determining the application program from which the request originated and the location thereof; and

d) blocking access to the data object if the application program is not present in the look-up table as a permitted application program for the data object in a designated location.

In the method step a), tagging confidential data objects preferably comprises entering the data object in a register of confidential data objects.

The designated location may be library, directory or folder, the terms being broadly synonymous, but depending on the type of computer and operating system.

Each of said data objects may comprise digital data representing text, image, audio and/or video information, and metadata describing the content of the object.

In order to facilitate initial compilation of the table, a routine may be run in a set-up phase, under control of an appropriately authorised person, the routine being operable to add data objects to the register, the routine being configured to receive requests for access to data objects stored in the data storage, to determine for each request whether the data object is tagged as confidential, to determine, if it is tagged as confidential, whether the combination of the object and the requesting program is already in the register, and to create a record in the register if the combination is not already in the register.

It will be understood that references herein to “application program” are intended to indicate any user-generated application program specifically designed to access the data objects, rather than to generic programs, for example database programs or text editing programs.

Brief Description of the Drawings

In the drawings, which illustrate one example of a computer system according to the invention:

Figure 1 is a flowchart illustrating the handling of a request for access to a database in the operation of current database security;

Figure 2 is a flowchart illustrating the operation of enhanced security according to one embodiment of the invention;

Figure 3 is a flowchart illustrating the operation of the whitelisting wizard;

Figure 4 is a flowchart illustrating the operation of the automatic matrix maintenance routine.

Detailed Description of the Illustrated Embodiments

Referring first to Figure 1, in a conventional database security system, access to the database depends on whether the request is from a user who is authorised to access the database. This is the Level 4 security as described hereinbefore. As long as the user has a Read authority for the database, then information can be downloaded from the database without restriction. If a cyber-criminal gains access to the computer, he will be regarded as an authorised user.

The present invention imposes a fifth level of security. In the flowchart in Figure 2, the Level 4 security step is illustrated at 100. If the user is authorised, this step passes the request to the Level 5 Information Security (IS) indicated generally as block 200, rather than direct to the database management system 10. In Level 5 Information Security according to the present invention, the first step 210 is to determine whether the database to which access is requested is tagged as confidential. The tagging of user nominated databases as confidential is carried out at Operating System level only by appointed IS Administration officers. The OS manufacturers will retain this confidential-database list as proprietary information and not allow indirect access to it by anyone or any process outside that of appointed IS Administration officers. The tagging of the database as confidential will typically be achieved by inclusion in a table or register of confidential data objects, but it may be possible to effect a modification to the object to indicate confidentiality.

In the next step 220, the system determines whether the request originates from an application program, as opposed to a direct request to access data. If the request is not from an application program it is denied, otherwise it is passed to a whitelist check at step 230, where the presence of the originating application program is checked in a whitelist of permissible programs (this step is not part of the invention, being a known recommended security step, and could be carried out at a lower level). Again, if the program is not in the whitelist, access is denied, otherwise the request is passed to the final stage 240, in which the originating application program and the requested database are checked in a look-up table or matrix identifying the confidential databases and

the application programs which can access them, access only being allowed to the database management system if the application program has been registered in the matrix for the database concerned.

When cyber criminals break into computer systems they are not likely to bring a computer program with them - not unless they were from a certified external software vendor supplying a patch. Even if this patch were the rogue element requiring access to a database, it will come up against the formidable IS defence that the program itself, even if whitelisted, does not satisfy the Matrix criterion - which can only be maintained by IS Administration. If the cyber criminals were to just use SQL or Excel directly, then all they can download is the data from the non-confidential databases – all worthless to them.

Referring to the whitelist described in step 230 above, whitelisting is a computer administration practice used to prevent unauthorized programs from executing. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources. When an application program tries to execute, it is automatically checked against the list and, if found, allowed to run. Building a white list manually is time-consuming, and until the list is completed, there is a risk that an organisation could be struck by a rogue program. Another aspect of the invention provides for the automatic creation of the white list through a routine referred to hereinafter as a whitelisting wizard. When the Whitelisting Wizard is enabled, the OS will intercept every application program execution request and record all essential program details on the Application Program Whitelist. The recorded details should include the program name, address (library/directory/drive/etc.), and all manner of authentication that verifies the program's provenance.

Note: The OS manufacturers (OSMs) such as IBM, Microsoft, Apple and others may already have an Application Program Whitelist table that is maintained manually by IT Security Administration. If this is the case, then the OSMs can easily prepare an interface to load the table automatically if the Whitelisting Wizard feature is enabled.

Figure 3 is the logic flowchart for this special routine. When a program requests to execute at step 300, the routine checks to see if the program is an

OS program and if it is passes the request direct to the Execute Program stage 360, otherwise passing the request to the next stage 320, in which the white list is checked to see whether the program is already whitelisted. If it is, the request is again passed to step 360. Otherwise, the request is passed to step 330, at which the program details are added to the white list 340 before passing the request to step 350.

Figure 4 illustrates a further routine operating alongside the whitelisting wizard to record information for the matrix described hereinbefore. On receipt of a request for a program to access a database at 400, the routine checks at step 410 whether the database is set as a confidential database; if not, the routine is exited. Step 420 checks whether details of the requesting program are already recorded in the matrix with respect to the requested confidential database and exits the routine if they are. Step 430 adds the details to the matrix 440 before exiting the routine.

Three tables are required for the operation of the Level 5 security system described with reference to Figure 2:

The confidential database registry, which is maintained manually by IT Security Administration via a Confidential Database Registry (CDBR) maintenance, for example:

Table 1: Example Confidential Database Registry

Confidential Database	Database Library
Accounts Master	Library.A
Employees Master	Library.B
Patients Master	Library.C

The Application Whitelist: IT Security Administration know exactly how many application programs exist on the system. It is therefore easy to monitor the number of data records added to the Whitelist and gauge when it may be feasible to disable the Wizard. A duration of 7 working days is more than adequate.

Most programs will be repetitively executed on any given business working day, the only exceptions being the month-end and year-end programs. These programs can be manually added to the Whitelist whether the Wizard is enabled or disabled. Any superfluous programs can be subsequently reviewed, and if deemed obsolete, deleted from the system as a precaution.

Table 2: Example Application Program Whitelist

Whitelisted Application Program	Application Program Library
Accounts.Program.1	Library.1
Accounts.Program.2	Library.1
Accounts.Program.3	Library.1
Employees.Program.1	Library.2
Employees.Program.2	Library.2
Employees.Program.3	Library.2
Patients.Program.1	Library.3
Patients.Program.2	Library.3
Patients.Program.3	Library.3

The matrix: The contents of this table will provide the essential information in order to regulate which programs can access which confidential databases.

Table 3: Example Matrix

Confidential Database	Database Library	Whitelisted Application Program	Application Program Library
Accounts Master	Library.A	Accounts.Program.1	Library.1
Accounts Master	Library.A	Accounts.Program.2	Library.1
Accounts Master	Library.A	Accounts.Program.3	Library.1
Employee Master	Library.B	Employees.Program.1	Library.2
Employee Master	Library.B	Employees.Program.2	Library.2
Employee Master	Library.B	Employees.Program.3	Library.2
Patients Master	Library.C	Patients.Program.1	Library.3
Patients Master	Library.C	Patients.Program.2	Library.3
Patients Master	Library.C	Patients.Program.3	Library.3

It will be appreciated that the IS Administration officers' activities relating to this invention must be conducted locally (within the firewall perimeter) on the computer system where these three tables are stored. Furthermore, all the programs listed in the Application Program Whitelist and the Matrix can only be requested to execute locally (within the firewall perimeter) and never from beyond the firewall perimeter.

While the invention has been described with reference to databases, it is applicable to any data object, for example a text document, an image file, or an audio file.

CLAIMS

1. A computer comprising:

one or more hardware processors;

data storage for storing data objects;

a computer operating system in the form of computer-executable instructions which can be executed by one or more of the hardware processors, the operating system comprising:

an object security system for controlling access to objects, the object security system being configured to receive requests for access to data objects stored in the data storage and to determine, upon receipt of a request for access, whether the request is from an authorised user of the object and to block access if the request is not from an authorised user, characterised in that the security system further comprises a register containing for each data object designated as confidential the or each application program permitted to access the data object and at least one designated location in the computer for the or each application program, the system being further configured to determine from each request if the data object is entered in the register and, if it is, to further determine the application program from which the request originated and to block access if the application program is not present in the register as a permitted application program in a designated location.

2. A computer according to Claim 1, wherein each of said data objects comprises digital data representing text, image, audio and/or video information, and metadata describing the content of the object.

3. A computer according to Claim 1 or 2, wherein the operating system further comprises a routine operable to add data objects to the look-up table, the routine being configured:

d) to receive requests for access to data objects stored in the data storage, to determine for each request whether the data object is marked as confidential;

e) to determine, if it is marked as confidential, whether the combination of the object and the requesting program is already in the register; and

f) to create a record in the table if the combination is not already in the register.

4. A computer according to Claim 1, 2 or 3, wherein the security system further comprises a register of confidential objects, objects being designated as confidential by entry in said register.

5. A method of controlling access to confidential data objects stored in computer data storage, the method comprising:

a) tagging confidential data objects as confidential;

b) establishing a table recording, for each confidential data object, each application program permitted to open said data object and the designated storage location for the application program;

and then processing each subsequent request for access to a data object in the computer data storage to determine whether the requested data object is confidential and if it is confidential:

c) determining the application program from which the request originated and the location thereof; and

d) blocking access to the data object if the application program is not present in the look-up table as a permitted application program for the data object and in a designated location.

6. A method according to Claim 5, wherein, in step a), tagging confidential data objects comprises entering the data object in a register of confidential data objects.

7. A method according to Claim 5 or 6, wherein step b) comprises:

i. determining for each request for access to a data object whether the data object is marked as confidential;

ii. determining, if it is marked as confidential, whether the combination of the object and the requesting program is already in the register; and

iii. creating a record in the register if the combination is not already in the register.

Amendments to the claims have been filed as follows

CLAIMS

1. A computer comprising:

one or more hardware processors;

data storage for storing data objects;

a computer operating system in the form of computer-executable instructions which can be executed by one or more of the hardware processors, the operating system comprising:

an object security system for controlling access to objects, the object security system being configured to receive requests for access to data objects stored in the data storage and to determine, upon receipt of a request for access, whether the request is from an authorised user of the object and to block access if the request is not from an authorised user, characterised in that the security system further comprises a register containing for each data object designated as confidential the or each application program permitted to access the data object and at least one designated location in the computer for the or each application program, the system being further configured to determine from each request if the data object is entered in the register and, if it is, to further determine the application program from which the request originated and the location of the application program, and to block access if the application program is not present in the register as a permitted application program in a designated location.

2. A computer according to Claim 1, wherein each of said data objects comprises digital data representing text, image, audio and/or video information, and metadata describing the content of the object.

3. A computer according to Claim 1 or 2, wherein the operating system further comprises a routine operable to add data objects to the register, the routine being configured:

to receive requests for access to data objects stored in the data storage, to determine for each request whether the data object is marked as confidential;

to determine, if it is marked as confidential, whether the combination of the object and the requesting program is already in the register; and

to create a record in the table if the combination is not already in the register.

4. A computer according to Claim 1, 2 or 3, wherein the security system further comprises a register of confidential objects, objects being designated as confidential by entry in said register.

5. A method of controlling access to confidential data objects stored in computer data storage, the method comprising:

a) tagging confidential data objects as confidential;

b) establishing a table recording, for each confidential data object, each application program permitted to open said data object and the designated storage location for the application program;

and then processing each subsequent request for access to a data object in the computer data storage to determine whether the requested data object is confidential and if it is confidential:

c) determining the application program from which the request originated and the location thereof; and

d) blocking access to the data object if the application program is not present in the look-up table as a permitted application program for the data object and in a designated location.

6. A method according to Claim 5, wherein, in step a), tagging confidential data objects comprises entering the data object in a register of confidential data objects.

7. A method according to Claim 5 or 6, wherein step b) comprises:

i. determining for each request for access to a data object whether the data object is marked as confidential;

ii. determining, if it is marked as confidential, whether the combination of the object and the requesting program is already in the register; and

iii. creating a record in the register if the combination is not already in the register.

Application No:	GB1616788.4	**Examiner:**	Mr Matthew Harle
Claims searched:	1-7	**Date of search:**	26 February 2018

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
A	-	US 2012/317622 A1 (HARJANTO) A multi-layer authentication method requiring user authentication and an additional layer of security by challenging a device's digital fingerprint, see Figure 3 and summary.
A	-	WO 2001/25870 A2 (FRIEDMAN) A system for protecting data, where data is stored in a vault and multiple permissions are required to access said data, see Figure 1 and description.
A	-	EP 2889796 A2 (CHOU) A system for safe data access including generation of a digital fingerprint by an authenticated program, see Figure 3 and summary of invention.

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

Worldwide search of patent documents classified in the following areas of the IPC

G06F

The following online and other databases have been used in the preparation of this search report

EPODOC, WPI, Patent Full Text

International Classification:

Subclass	Subgroup	Valid From
G06F	0021/62	01/01/2013
G06F	0021/44	01/01/2013