



- (51) International Patent Classification:
G06F 17/30 (2006.01)
- (21) International Application Number:
PCT/SG2015/000141
- (22) International Filing Date:
17 November 2015 (17.11.2015)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
10201408352X 15 December 2014 (15.12.2014) SG
- (71) Applicant: IIA TECHNOLOGIES PTE LTD [SG/SG];
17, Tukang Innovation Drive, Singapore 618300 (SG).
- (72) Inventor: MEHTA, Vishal, Jatin; c/o 65, OCBC Centre,
Chulia Street, # 38-02, Singapore 049513 (SG).
- (81) Designated States (unless otherwise indicated, for every
kind of national protection available): 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, 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.

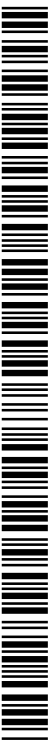
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, 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).

Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

— with international search report (Art. 21(3))



(54) Title: A SYSTEM OF MONITORING AND CONTROLLING THE OPERATION OF MULTIPLE MACHINES FOR PRODUCING DIAMONDS AND A METHOD THEREOF

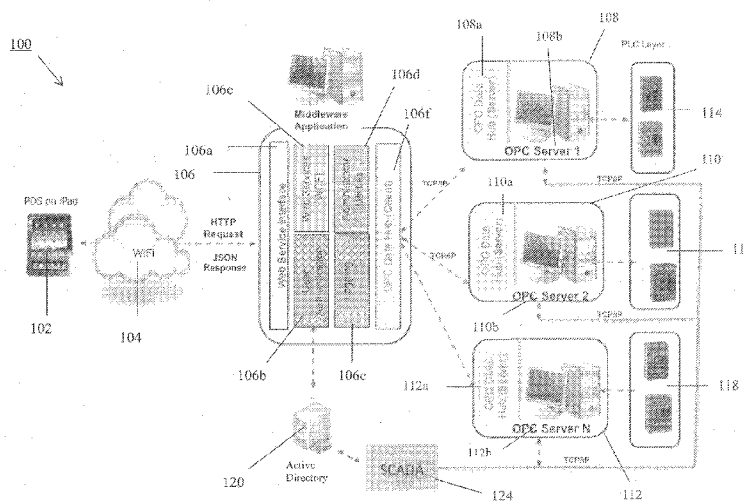


Figure 1

(57) Abstract: A system of monitoring and controlling an operation, comprising: an input means, the input means is adapted for user to input user-defined parameters, a middleware application in connection with the input means via a network, the middleware application is in communication with a directory database and also a relational database management system via communication means, a data management system being installed as a slave program in the middleware application and as a slave program in one more external server or external device, the middleware application is in communication with the external servers or device via communication means, whereby the master-slave relation allows exchange of data between the middleware application and the server architecture.

A SYSTEM OF MONITORING AND CONTROLLING THE OPERATION OF MULTIPLE MACHINES FOR PRODUCING DIAMONDS AND A METHOD THEREOF

Field of the invention

The invention relates to a system and method of monitoring and controlling the operation of multiple machines adapted for producing diamonds from a remote location.

Background

Large-scale production of diamond has long been an objective of both research and industry. Diamond, in addition to its gem properties, is the hardest known material, has the highest known thermal conductivity, and is transparent to a wide variety of electromagnetic radiation. It is valuable because of its wide range of applications in a number of industries, in addition to its value as a gemstone. However, a diamond can have low fracture toughness that will make it unsuitable for many applications, such as high impact machine tools.

There exist many systems and methods with the objective of producing diamonds at a large scale. More specifically, an example of such a system and method of producing diamonds at a large scale is described as follows.

A machine is adapted to produce diamonds. To cope with the demand of the diamonds, the production rate of the diamonds has to be increased. The existing method makes use of multiple machines to increase the production rate of the diamonds. Each machine is provided with a Human Machine Interface (HMI) mounted thereto to allow user to control the operation of the production of diamonds therein.

A drawn back of the above described example is that the HMI is mounted onto each machine. The HMI is not portable. In addition, the HMI is costly too. In order to operate the multiple machines, the user has to go to each of the individual machines to operate the production of the diamonds via the HMI on the machine at every regular time interval. The user has to manually record the parametric values on a data sheet for every machine at the same time interval. It is submitted that the present method is tedious, error-prone, unproductive, inefficient and time consuming. In addition, manpower and labour cost goes up

if there is a need to deploy more users to operate multiple machines for producing diamonds.

It is an objective of the present invention to provide a method and system of controlling the operation of the production of diamonds in multiple machines by using an input means from a remote location. The manpower and labour cost goes down as it is possible to have only one user to control the entire operation.

In addition, the security of operation of production of diamonds in multiple machines is also improved as only approved personnel can access the system. The system is also more user-friendly and thus facilitating new user to learn how to use the system faster and easier. In addition, the paperwork is significantly reduced as most of the work is now done electronically by the system. Furthermore, the system also allows the addition of new machines if the production rate needs to grow in view of increasing demand. The user's experience with the system is thus significantly enhanced since the user can have a better control of the system. It is submitted that the system improves the overall productivity and efficiency of the production of diamonds.

Other objects and advantages of the present invention will become apparent from the following description, taken in connection with the accompanying drawings, wherein, by way of illustration and example, an embodiment of the present invention is disclosed.

Summary of Invention

In accordance with a first aspect of the present invention, there is provided a system of monitoring and controlling an operation, comprising:

- an input means, the input means is adapted for user to input user-defined parameters,

- a middleware application in connection with the input means via a network, the middleware application is in communication with a directory database and also a relational database management system via communication means,

- a data management system being installed as a slave program in the middleware application and as a slave program in one more external server or external device, the middleware application is in communication with the external servers or device via communication means, whereby the master-slave relation allows exchange of data between the middleware application and the server

architecture.

In accordance with a second aspect of the present invention, there is provided a system of monitoring and controlling the operation of multiple machines, comprising:

an input means, the input means is adapted for user to input user-defined parameters,

a middleware application in connection with the input means via a network, the middleware application is in communication with a directory database and also a relational database management system via communication means,

one or more server architectures, the middleware application is in communication with each of the server architectures via communication means, each of the server architecture is further in communication with multiple machines via communication means,

a data management system being installed as a slave program in the middleware application and as a slave program in one more server architectures, the middleware application is in communication with the server architectures via communication means, whereby the master-slave relation allows exchange of data between the middleware application and the server architecture.

In accordance with a third aspect of the present invention, there is provided a method of controlling the operation of multiple machines for producing diamonds at a normal access level, comprising:

logging in into the system according to claims 1 to 19,

verifying the authentication of the user's credential,

gaining access to the system if the authentication result is positive,

starting the system,

keying in user-defined parameters on the input device to control the operation of the machines,

transmitting the parameters from the input device to the middleware application,

transmitting the parameters from the middleware application to the server architecture via a slave-master relation established from the slave program installed in the middleware and the master program installed in the server architecture,

transmitting the parameters from the master program to the OPC (Open Process Control) server in the server architecture,

transmitting the parameters from the server architecture to the machine.

In accordance with a fourth aspect of the present invention, there is provided a method of gaining special access to the system, comprising:

- logging in into the system according to claims 1 to 19 via a third computing device,
- verifying the authentication of the user's credential,
- gaining access to the system if the authentication result is positive,
- starting the system,
- keying in user-defined parameters on the SCADA client,
- transmitting the parameters from the SCADA client to the third party computing device and then to the machines via the OPC (Open Process Control) server in the server architecture,
- transmitting the data from the machine to the third party device via the OPC (Open Process Control) server.

In accordance with a fifth aspect of the present invention, there is provided a method of enhancing the security of the system according to claims 1 to 19, comprising:

- launching the application software on the input device,
- launching the login screen by the application software,
- entering the log in details of the user,
- saving the log in details of the user if the log in is successful,
- accessing the application software by the user,
- launching the control panel,
- keying in user-defined parameters to on the input device to control the operation of the machines,
- locking the screen if the user is not actively using the application software,
- prompting the user to re-enter the password up to 3 attempts,
- launching the control panel if successful and relaunching the login in screen if unsuccessful.

In accordance with a sixth aspect of the present invention, there is provided a method of enhancing the security of the system according to claims 1 to 19, comprising:

- launching the application software on the input device,
- launching the login screen by the application software,

entering the log in details of the user,
saving the log in details of the user if the log in is successful,
accessing the application software by the user,
launching the control panel,
keying in user-defined parameters to on the input device to control the
operation of the machines,
locking the screen if the user is not actively using the application software,
prompting the user to re-enter the log in details,
launching the control panel if successful.

Brief description of drawings

This then generally describes the invention but to assist with understanding reference will now be made to the accompanying drawings which show preferred embodiments of the invention.

Figure 1 shows the system of controlling the operation of multiple machines adapted for producing diamonds using a tablet computer from a remote location according to a preferred embodiment of the present invention.

Figure 2 shows the components within the middleware application and how they co-operate with other components according to a preferred embodiment of the present invention.

Figure 3 shows the flow chart of controlling the operation of multiple machines adapted for producing diamonds using a tablet computer from a remote location according to a preferred embodiment of the present invention.

Figure 4 shows the security of the system in accordance to a preferred embodiment of the present invention.

DETAILED DESCRIPTION

The Figures are diagrammatic and not drawn to scale. In the Figures, elements which correspond to elements already described have the same reference numerals.

According to a first aspect of the present invention, there is provided a system of monitoring and controlling an operation using an input means, the input means is adapted for user to input user-defined parameters. The system comprises of an input means for allowing user to input user-defined parameters. Furthermore, the system also comprises a middleware application which is in connection with the input means via a network. A data management system is also provided to be installed as a slave program in the middleware application and as a master program in one or more external servers or external devices. The master-slave relation allows exchange of data between the middleware application and the external server(s) or external device(s). Beside in connection with the input means and in communication with one or more external servers or external devices, the middleware application is in further communication with a directory database and also a relational database management system.

In a preferred embodiment of the present invention as shown in Figure 1, there is provided a system 100 of monitoring and controlling an operation using an input means 102 from a remote location, the input means is adapted for user to input user-defined parameters. The input means includes a input device 102 provided with an user interface and a suitable platform is installed therein in order for the input device 102 to be functional.

The system 100 comprises a middleware application 106 which is in connection with the input device 102 via a network 104.

The input device 102 may be in the form of tablet computer having a suitable platform installed therein in order for the input device 102 to be functional. The tablet computer may be an Apple iPad or other suitable type of tablet computers. In other embodiment, the input means may be in the form of website.

The input device 102 can transmit commands signals to the service-oriented architecture 106e in the form of web service (WCF) via a network by means of JavaScript Object Notation (JSON) sent over Hypertext Transfer Protocol (http) and is also able to process the response sent by the web service (WCF) 106e. The network 104 is either a wired network or a wireless

network. Wireless network may be a WI-FI in a preferred embodiment of the present invention.

The middleware application 106 is also provided with a web service interface 106a adapted to provide contact point between the service-oriented architecture 106e and the input device 102.

The middleware application 106 comprises of a storage medium for storing administrative utilities information 106d and a service-oriented architecture 106e in the form of WCF service (Windows Communication Foundation)

The service-oriented architecture 106e is adapted to support distributed computing where services have remote consumers. For instance, the WCF service 106e processes user authentication 106b and also logging 106c. In addition, the WCF service 106e also facilitates data communication between the input device 102 and the external server(s) or external device(s). The WCF service 106e also retrieves special permission or messages from the Windows AppFabric Cache 106h (see Figure 2) and transmits it to the input device 102. The WCF service 106e also provides information to the administrative utilities portal 106d.

An administration portal or also known as administrative utilities portal 106d is provided for administration purpose. For instance, the administration portal 106d enables an administrator to terminate a user session. The administrator has the power to assign access right to those operating the system 100. Other administration tasks include setting up temporary access right, setting up message for user of input device application. The administration portal 106d may be a web based portal so that the administrator can access the portal as long as there is a network connection.

The data management system is installed as a slave program 106f (also known as OPC Datahub (client) or just simply client) in the middleware application 106 and as a master program (108a, 110a, 112a) (also known as OPC Datahub (server) or just simply server) in an external server or external device. The master-slave relation allows exchange of data between the middleware application 106 and the external server(s) or external device(s). Data management system may be created by Cogent Datahub or some other suitable manufacturer.

In this system, in order to establish the slave-master connection, the tunnelling means in the form of a socket based Transmission Control Protocol (TCP/IP) is established between OPC Data Hub (server) (also known as master program) (108a, 110a, 112a) and the OPC Data Hub (client) (also known as slave program) 106f which replicates any data change occurring at one end immediately at the other end.

In this system, there can be only one slave program per service instance but there can be multiple master programs. Each master program facilitates the data communication between the OPC datahub server to which it is connected and the slave program 106f. The slave program 106f connects only to the master program (108a, 110a, 112a) and propagates this information to the user via the input device 102.

According to a second aspect of the present invention as shown in Figure 1, there is provided a system of monitoring and controlling an operation of one or more machines using an input means from a remote location, the input means is adapted for user to input user-defined parameters. The system comprises of an input means for allowing user to input user-defined parameters. Furthermore, the system also comprises a middleware application which is in connection with the input means via a network. The system also comprises one or more server architectures adapted for transmitting parameters to the machines. The middleware application is in communication with each of the server architectures via communication means. Each of the server architectures are in communication with the machines via communication means. A data management system is also provided to be installed as a slave program in the middleware application and as a master program in each of the server architectures. The master-slave relation allows exchange of data between the middleware application and the server architectures. Beside in connection with the input means and in communication with one or more server architectures, the middleware application is in further communication with a directory database and a relational database management system.

In the preferred embodiment of the present invention as shown in Figure 1, the system 100 of operating one or more machines (114, 116, 118) using an input means from a remote location, the input means is adapted for user to input user-defined parameters. Each machine (114, 116, 118) may be adapted to produce diamonds therein. The input means includes input device 102 provided with an user interface and a suitable platform is installed therein in order for the input device 102 to be functional.

The system 100 comprises a middleware application 106 which is in connection with the input device 102 via a network 104.

The input device 102 may be in the form of tablet computer having a suitable platform installed therein in order for the input device 102 to be functional. The tablet computer may be an Apple iPad or other suitable type of tablet computers. In other embodiments, the input means may be in the form of website.

The input device 102 can transmit commands signals to the service-oriented architecture 106e in the form of web service (WCF) via a network by means of JavaScript Object Notation (JSON) sent over Hypertext Transfer Protocol (http) and is also able to process the response sent by the web service (WCF) 106e. The network 104 is either a wired network or a wireless network. Wireless network may be a WI-FI in a preferred embodiment of the present invention.

The middleware application 106 is also provided with a web service interface 106a adapted to provide contact point between the service-oriented architecture 106e and the input device 102.

The middleware application 106 comprises of a storage medium for storing administrative utilities information 106d and a service-oriented architecture 106e in the form of WCF service (Windows Communication Foundation).

The service-oriented architecture 106e is adapted to support distributed computing where services have remote consumers. For instance, the WCF service 106e processes user authentication 106b and also logging 106c. In addition, the WCF service 106e also facilitates data communication between the input device 102 and the OPC servers (108b, 110b, 112b). The WCF service 106e also retrieves special permission or messages from the Windows AppFabric Cache 106h (see Figure 2) and transmits it to the input device 102. The WCF service 106e also provides information to the administrative utilities portal 106d.

An administration portal or also known as administrative utilities portal 106d is provided for administration purpose. For instance, the administration portal enables an administrator to terminate a user session. The administrator has the power to assign access right to those operating the system 100. Other administration tasks include setting up temporary access

right, setting up message for user of input device application. The administration portal 106d may be a web based portal so that the administrator can access the portal as long as there is a network connection.

The data management system is installed as a slave program 106f (also known as OPC Datahub client or just simply client) in the middleware application 106 and as a master program (108a, 110a, 112a) (also known as OPC Datahub server or just simply server) in the server architecture (108, 110, 112). The master-slave relation allows exchange of data between the middleware application 106 and the server architecture (108, 110, 112). Data management system may be created by Cogent Datahub or some other suitable manufacturer.

In this system, in order to establish the slave-master connection, the tunnelling means in the form of a socket based Transmission Control Protocol (TCP/IP) is established between OPC Data Hub (server) (also known as master program) (108a, 110a, 112a) and OPC Data Hub (client) (also known as slave program) 106f which replicates any data change occurring at one end immediately at the other end.

In this system, there can be only one slave program per service instance but there can be multiple master programs. Each master program facilitates the data communication between the OPC datahub server to which it is connected and the slave program 106f. The slave program 106f connects only to the master program (108a, 110a, 112a) and propagates this information to the user via the first input means 102.

The system 100 is provided with one or more server architectures (108, 110, 112) adapted for transmitting parameters to the machines (114, 116, 118). The middleware application 106 is in communication with each of the server architectures (108, 110, 112) via communication means. Each of the server architectures (108, 110, 112) are in communication with the machines (114, 116, 118) via communication means. The communication means may be in the form of TCP/IP.

The server architectures (108, 110, 112) comprise of OPC (Open Process Control) server (108b, 110b, 112b) and also master program (108a, 110a, 112a). Each of the server architectures (108, 110, 112) is installed within a computing device and also is in communication with one or more machines (114, 116, 118) via a communication means. The

communication means may be in the form of TCP/IP. The OPC server is known as OLE (object linking and embedding) for process control. It is submitted that the number of machines per server architecture may be 36 or 72 for optimum performance.

The system 100 also provided with a special access. As shown in Figure 1, the third party computing device 124 is installed with industrial control system in the form of SCADA application (supervisory control and data acquisition). Industrial control systems are program logic controlled (PLC) systems that monitor and control industrial processes that exist in the physical world.

The SCADA application installed in the third party computing device 124 is able to process user authentication and also logging. The SCADA application is adapted to verify if the user who log in into the SCADA application is in the active directory's list 120 and if so, the user will be identified to be an approved personnel. If the user is identified to be an approved personnel, the SCADA application will be accessible by the user. In addition, the SCADA application is able to perform data monitoring, data logging, data control and visualization. In a special access, the user will key in user-defined parameters on the SCADA client. The parameters will be transmitted from the SCADA client to the third party computing device 124 and then to the machine (114, 116, 118) via the OPC server (108b, 110b, 112b). At the same time, the user can also monitor the status of the machine (114, 116, 118) when the data from the machines (114, 116, 118) is transmitted back to the third party computing device 124 via the OPC server (108b, 110b, 112b).

The third party computing device 124 is in direct communication with both of the OPC servers (108b, 110b, 112b) and the active directory 124 via a communication means. The communication means may be in the form of TCP/IP.

Unlike the normal access (see Figure 3), the special access enables direct data communication between the third party computing device 124 and the OPC server (108b, 110b, 112b).

Figure 2 shows the components within the middleware application 106 according to a preferred embodiment of the present invention.

As shown in Figure 2, the service-oriented architecture in the form of web services (WCF)

106e and the administrator portal 106d (also known as administrator utilities in Figure 1) may be hosted in a hosting platform, such as Internet Information System (IIS) 7.0 running on a Microsoft Windows 2008 R2. The middleware application 106 is further installed with a caching provider and a monitoring service 106h, a data management system (DMS) 106f and a software framework 106g.

The caching provider and the monitoring service 106h is in the form of Windows Server AppFabric adapted to build, scale and manage web and composite applications that run on Internet Information System (IIS). It is an extension to the middleware application 106 role of the Windows Server, and any application is free to use its parts separately or together.

In this system 100, Windows Server AppFabric 106h improve the performance by providing a distributed caching mechanism to store frequently used data. Furthermore, Windows Server AppFabric 106h is also used as a temporary repository to store special permissions and messages. These special permissions and messages will then be transmitted from the SQL Server database 122 to the Windows Server AppFabric 106h when time elapses so that the tablet computer application can pick up this information when it polls the WCF service 106e every second. If the cache is not there, then it requires a database to hit every second to retrieve this information.

The data management system is installed as a slave program 106f (also known as OPC Datahub (client) or just simply client) in the middleware application 106 and as a master program (108a, 110a, 112a) (also known as OPC Datahub (server) or just simply server) in the server architecture (108, 110, 112). The master-slave relation allows exchange of data between the middleware application 106 and the server architecture (108, 110, 112). Data management system may be created by Cogent Datahub or some other suitable manufacturer.

In this system, in order to establish the slave-master connection, the tunnelling means in the form of a socket based Transmission Control Protocol (TCP/IP) is established between OPC Data Hub (server) (also known as master program) (108a, 110a, 112a) and OPC Data Hub (client) (also known as slave program) 106f which replicates any data change occurring at one end immediately at the other end.

In this system, there can be only one slave program per service instance but there can be

multiple master programs. Each master program facilitates the data communication between the OPC server to which it is connected and the slave program 106f. The slave program 106f connects only to the master program (108a, 110a, 112a) and propagates this information to the user via the input device 102.

The software framework 106g is in the form of Microsoft .NET Framework 4.0. It includes a large library and provides language interoperability (each language can use code written in other languages) across several programming languages. Programs written for the .NET Framework execute in a software environment (as contrasted to hardware environment), known as the Common Language Runtime (CLR), an application virtual machine that provides services such as security, memory management, and exception handling. The class library and the CLR together constitute the .NET Framework. The .NET Framework's Base Class Library provides user interface, data access, database connectivity, cryptography, web application development, numeric algorithms, and network communications. Programmers produce software by combining their own source code with the .NET Framework and other libraries. The .NET Framework is intended to be used by most new applications created for the Windows platform. Microsoft also produces an integrated development environment largely for .NET software called Visual Studio.

As shown in Figure 2, middleware application 106 is in communication with a directory database 120 and a relational database management system 122 according to an aspect of the present invention. The directory database 120 is also known as active directory adapted to store the information relating to the credential of approved personnel (both supervisor and operator).

The middleware application 106 is able to verify if the user who log in into the system 100 is an approved personnel by tallying with the records in the active directory 120. If the user is identified to be an approved personnel, the system 100 will be accessible by the user.

The relational database management system is in the form of Microsoft SQL server 122 adapted to store data such as logs, special permissions, messages and various configurations. As a database, it is a software product whose primary function is to store and retrieve data as requested by other software applications, be it those on the same computer or those running on another computer across a network (including the Internet). There are at least a dozen different editions of Microsoft SQL Server aimed at different audiences and for

different workloads (ranging from small applications that store and retrieve data on the same computer, to millions of users and computers that access huge amounts of data from the Internet at the same time). Its primary query languages are T-SQL and ANSI SQL.

The system 100 has additional features such as messaging and temporary permission which can be set up using a web based administration portal 106d. This information is saved in the SQL database 122. A windows service running in the background will pick up the new permission/messages and will place them in the AppFabric Cache 106h from where these will be picked up by the web services (WCF) 106e and then passed on to the input device 102 based on the user who is logged in.

Figure 3 shows the flow chart 300 of controlling the operation of the machines according to a preferred embodiment of the present invention.

According to a third aspect of the present invention, to start operating the system, the user first log in into the system 100 using the input device at step 302.

At step 304a, the service oriented architecture in the form of web service (WCF) 106e will process the authentication of the user's credential. The authentication is done by cross-checking the user credential against the active directory 120.

If the authentication result is negative, the user is denied access into the system 100.

If the authentication result is positive, the user gains access into the system 100 at step 308a to start the operation. Every successful log in attempt and user activity will be recorded in a storage medium in the middleware application 106. Every user session will be terminated after a pre-configured duration of usage for security reasons. This is to prevent any unauthorised use of the system if the user forgets to log out of the system. In case if the session is terminated under such circumstances, the user is notified immediately so that the user can log into the system again. The security of the system will be described more in detail in Figure 4.

In a normal access 310, the operation starts at step 316a. In order to operate the machines (114, 116, 118), the user will key-in user-defined parameters onto the interface of the input device 102 at step 320a. At the same time, the user can also monitor the status of the machine (114, 116, 118) when the data from the machines (114, 116, 118) is transmitted back

to the input device 102.

At step 322, the parameters are transmitted from the input device 102 to the middleware application 106.

The slave program 106f installed in the middleware application 106 and the master program (108a, 110a, 112a) installed in the server architecture (108, 110, 112) establishes a slave-master relation which enables the parameters to be transmitted from the middleware application 106 to the OPC server (108b, 110b, 112b) at step 328a via steps 324 and 326 consecutively.

The parameters are then transmitted to the machine (114, 116, 118) at step 330a so as to operate the machine (114, 116, 118) according the configuration defined by the user-defined parameters.

According to another embodiment of the present invention, a special access to the system 100 is provided for the user. As shown in Figure 1, the third party computing device 124 at step 311 is installed with industrial control system in the form of SCADA application (supervisory control and data acquisition). Industrial control systems are program logic controlled (PLC) systems that monitor and control industrial processes that exist in the physical world.

The SCADA application installed in the third party computing device 124 is able to process user authentication and also logging. The SCADA application is adapted to verify if the user who log in into the SCADA application is in the active directory's list 120 at step 304b and if so, the user will be identified to be an approved personnel. If the user is identified to be an approved personnel, the SCADA application will be accessible by the user at step 308b and 312, after which the operation will start at step 316b. In addition, the SCADA application is able to perform data monitoring, data logging, data control and visualization. In a special access, the user will key in user-defined parameters on the SCADA client at step 320b. The parameters will be transmitted from the SCADA client to the third party computing device 124 and then to the machine (114, 116, 118) via the OPC server (108b, 110b, 112b) at steps 328b and 330b. At the same time, the user can also monitor the status of the machine (114, 116, 118) when the data from the machines (114, 116, 118) is transmitted back to the third party computing device 124 via the OPC server (108b, 110b, 112b).

The third party computing device 124 is in direct communication with both of the OPC servers (108b, 110b, 112b) and the active directory 120 via a communication means. The communication means may be in the form of TCP/IP.

Unlike the normal access, the special access enables direct data communication between the third party computing device 124 and the OPC server (108b, 110b, 112b) from step 320b to step 328b.

Figure 4 shows the security of the system 400 in accordance to a preferred embodiment of the present invention.

In accordance with a fourth aspect of the present invention, an application software in the form of iGem App which is pre-installed in an input device is launched at step 402 when the user switch on the input device.

At step 404, the application software will launch a login screen for the user to enter the log in details.

If the log in is successful, the details of the log in details of the user is saved at step 406.

At step 408, the application software is run and accessible by the user.

The control panel in the form of iSO multi task application background panel will be launched at step 410 whereby the user can key in parameters to control the operation of the machine. The steps of controlling the operation of the machine have been earlier described in Figure 3.

When the user is not actively using the iSO multi task application background panel, the screen will be automatically locked for security purpose.

At step 412, a screen showing the entry of password will be shown to prompt the user to re-enter the password to re-log into the system. If the password is correct, the application software is relaunched at step 408. If the password is incorrect at step 414, the system will prompt the user to re-enter the password up to 3 attempts at step 416. If the user is still unsuccessful after 3 attempts, the login screen will be relaunched at step 404 whereby the user is required to re-enter the entire log in details again.

The system can also be configured such that if when the user is not actively using the ISO multi task application background panel, the screen will be automatically locked for security purpose. The log in screen will be relaunched again at step 404 whereby the user is required to re-enter the entire log in details again.

It is apparent to a person skilled in the art that many modifications, alternatives and variations may be made to the preferred embodiment of the present invention as described above without departing from the spirit and scope of the present invention. Accordingly, it is intended to embrace all such modifications, alternatives and variations that fall within the scope of the included claims.

CLAIMS:

1. A system of monitoring and controlling an operation, comprising:
 - an input means, the input means is adapted for user to input user-defined parameters,
 - a middleware application in connection with the input means via a network, the middleware application is in communication with a directory database and also a relational database management system via communication means,
 - a data management system being installed as a slave program in the middleware application and as a slave program in one more external server or external device, the middleware application is in communication with the external servers or device via communication means, whereby the master-slave relation allows exchange of data between the middleware application and the server architecture.

2. A system of monitoring and controlling the operation of multiple machines, comprising:
 - an input means, the input means is adapted for user to input user-defined parameters,
 - a middleware application in connection with the input means via a network, the middleware application is in communication with a directory database and also a relational database management system via communication means,
 - one or more server architectures, the middleware application is in communication with each of the server architectures via communication means, each of the server architecture is further in communication with multiple machines via communication means,
 - a data management system being installed as a slave program in the middleware application and as a slave program in one more server architectures, the middleware application is in communication with the server architectures via communication means, whereby the master-slave relation allows exchange of data between the middleware application and the server architecture.

3. The system according to any one of the preceding claims, wherein the input means includes an input device provided with an user interface and a suitable platform installed therein in order for the input device to be functional.

3. The system according to claim 3, wherein the input device is the form of tablet computer having a suitable platform installed therein in order of the input device to be functional.
4. The system according to any one of the preceding claims, wherein the middleware application comprises of a storage medium for storing administrative utilities and a service-oriented architecture, the administrative utilities is adapted for administration purpose and the service-oriented architecture is adapted to support distributed computing where services have remote consumers.
5. The system according to claim 4, wherein the service-oriented architecture and the administrative utilities may be hosted in a hosting platform in the form of Internet Information System.
6. The system according to claims 4 or 5, wherein the service-oriented architecture may be in the form of WCF services (Windows Communication Foundation).
7. The system according to any one of the preceding claims, wherein the middleware application further comprises of a caching and a monitoring service and a software framework.
8. The system according to claim 7, wherein the caching and monitoring service is in the form of Windows Server AppFabric adapted to build, scale and manage web and composite applications that run on Internet Information System.
9. The system according to claim 7, wherein the software framework is in the form of Microsoft .NET Framework.
10. The system according to any one of claims 2 to 9, wherein the server architecture comprise of OPC (Open Process Control) server and a data management in the form of master program.
11. The system according to any one of the preceding claims, wherein the network may be a wireless network.

12. The system according to claim 11, wherein the wireless network is a WI-FI.
13. The system according to any one of the preceding claims, wherein the communication means is the form of TCP/IP.
14. The system according to any one of the preceding claims, further comprise of additional features such as messaging and temporary permission which can be set up using the web based administration portal.
16. The system according to any one of the preceding claims, whereby the machine is adapted to produce diamonds.
17. The system according to any one of the preceding claims, wherein the relational database management is in the form of Microsoft SQL server adapted to store data such as logs, special permissions, messages and various configurations.
18. The system according to any one of the preceding claims, wherein the middleware application is provided with a web service interface adapted to provide contact point between the service-oriented architecture and the input device.
19. The system according to any one of claims 2 to 18, wherein the server architecture is installed with a computing device.
20. A third party computing device installed with industrial control system in the form of SCADA (supervisory control and data acquisition) application is provided to be in communication with the system according to claims 1 to 19.
21. A method of controlling the operation of multiple machines for producing diamonds at a normal access level, comprising:
 - logging in into the system according to claims 1 to 19,
 - verifying the authentication of the user's credential,
 - gaining access to the system if the authentication result is positive,
 - starting the system,
 - keying in user-defined parameters on the input device to control the operation of the machines,

transmitting the parameters from the input device to the middleware application,

transmitting the parameters from the middleware application to the server architecture via a slave-master relation established from the slave program installed in the middleware and the master program installed in the server architecture,

transmitting the parameters from the master program to the OPC (Open Process Control) server in the server architecture,

transmitting the parameters from the server architecture to the machine.

22. A method of gaining special access to the system, comprising:

logging in into the system according to claims 1 to 19 via a third computing device,

verifying the authentication of the user's credential,

gaining access to the system if the authentication result is positive,

starting the system,

keying in user-defined parameters on the SCADA client,

transmitting the parameters from the SCADA client to the third party computing device and then to the machines via the OPC (Open Process Control) server in the server architecture,

transmitting the data from the machine to the third party device via the OPC (Open Process Control) server.

23. A method of enhancing the security of the system according to claims 1 to 19, comprising:

launching the application software on the input device,

launching the login screen by the application software,

entering the log in details of the user,

saving the log in details of the user if the log in is successful,

accessing the application software by the user,

launching the control panel,

keying in user-defined parameters to on the input device to control the operation of the machines,

locking the screen if the user is not actively using the application software,

prompting the user to re-enter the password up to 3 attempts,

launching the control panel if successful and relaunching the login in screen if

unsuccessful.

24. A method of enhancing the security of the system according to claims 1 to 19, comprising:

- launching the application software on the input device,
- launching the login screen by the application software,
- entering the log in details of the user,
- saving the log in details of the user if the log in is successful,
- accessing the application software by the user,
- launching the control panel,
- keying in user-defined parameters to on the input device to control the operation of the machines,
- locking the screen if the user is not actively using the application software,
- prompting the user to re-enter the log in details,
- launching the control panel if successful.

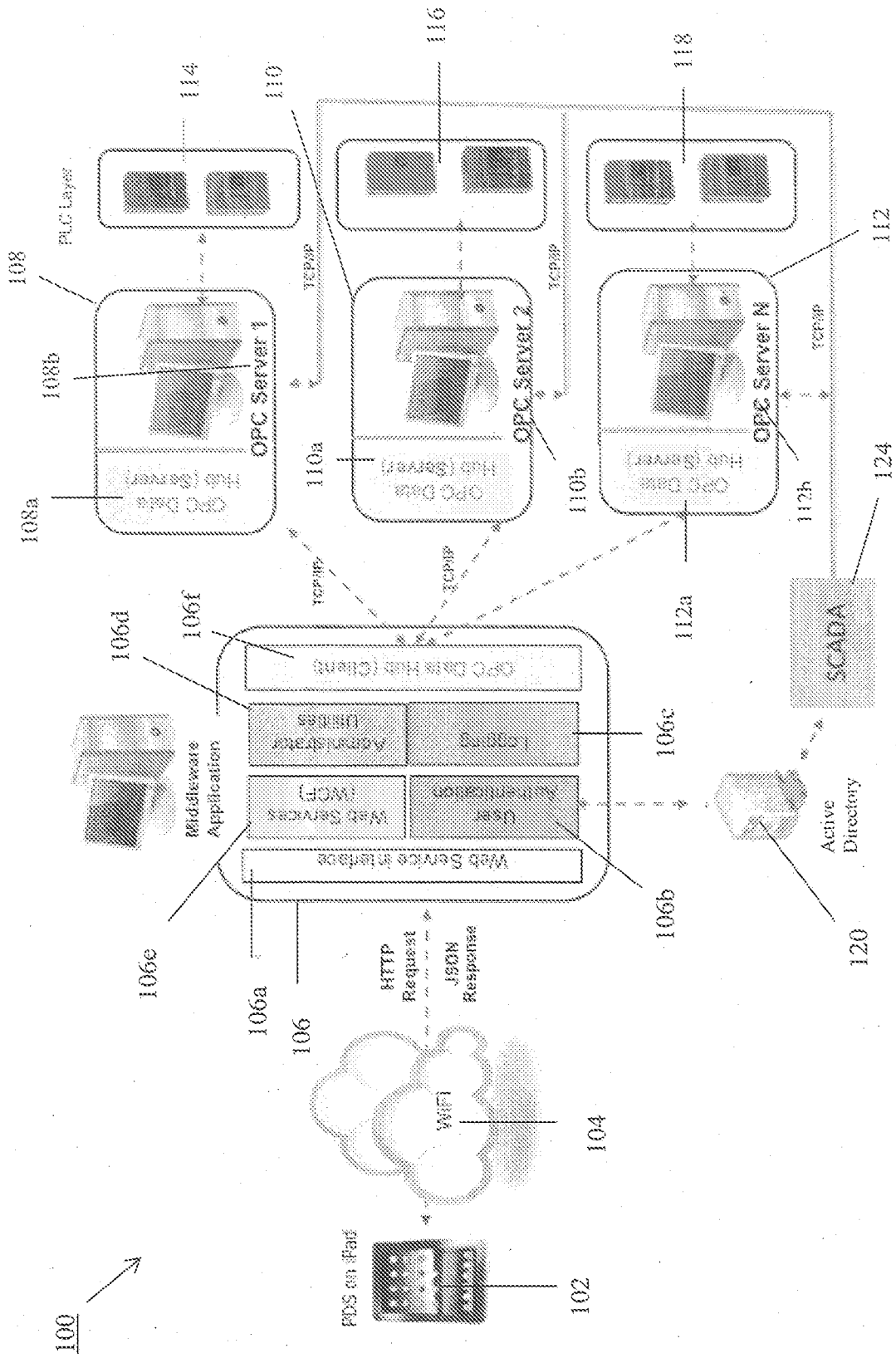


Figure 1

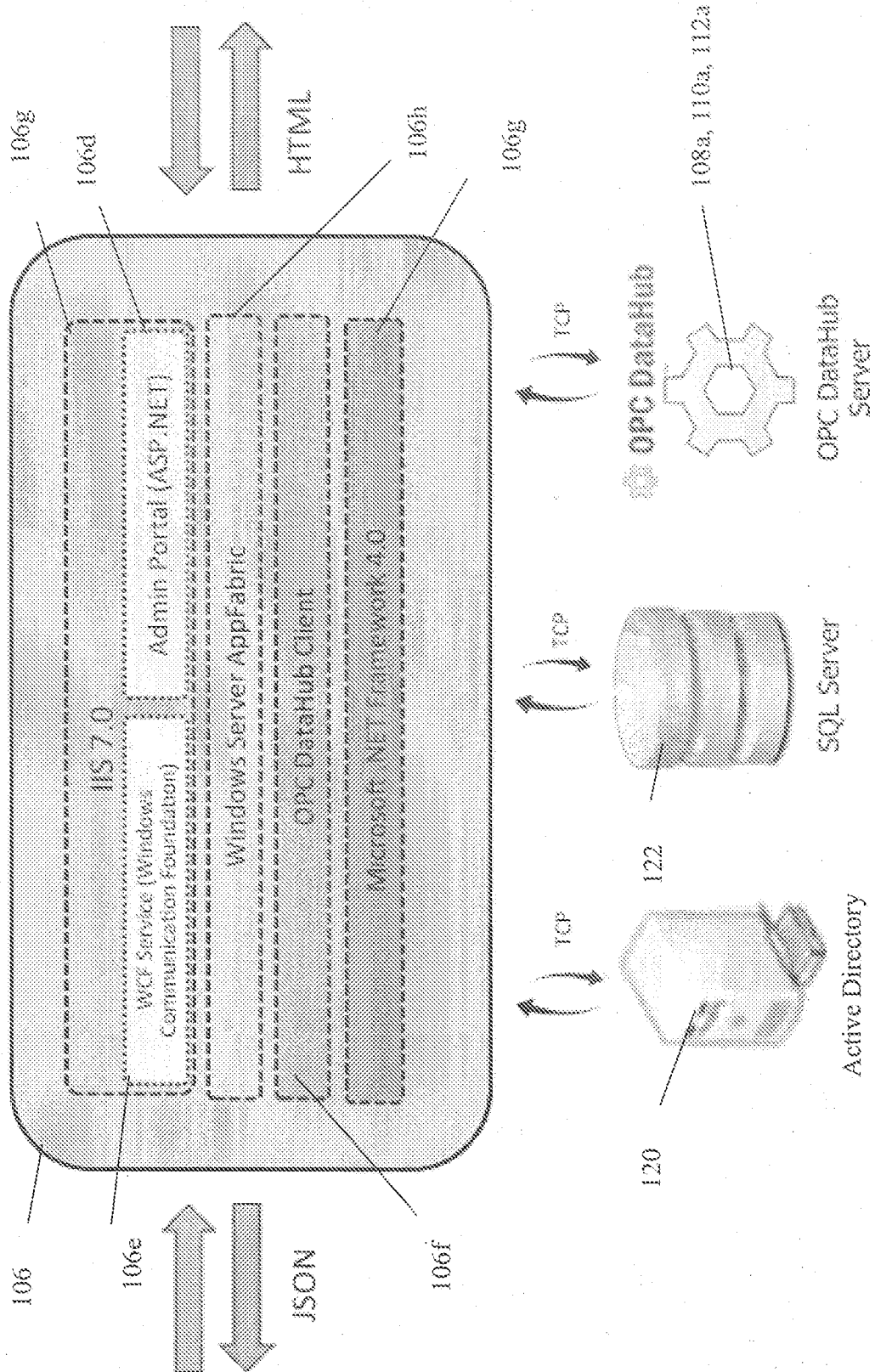


Figure 2

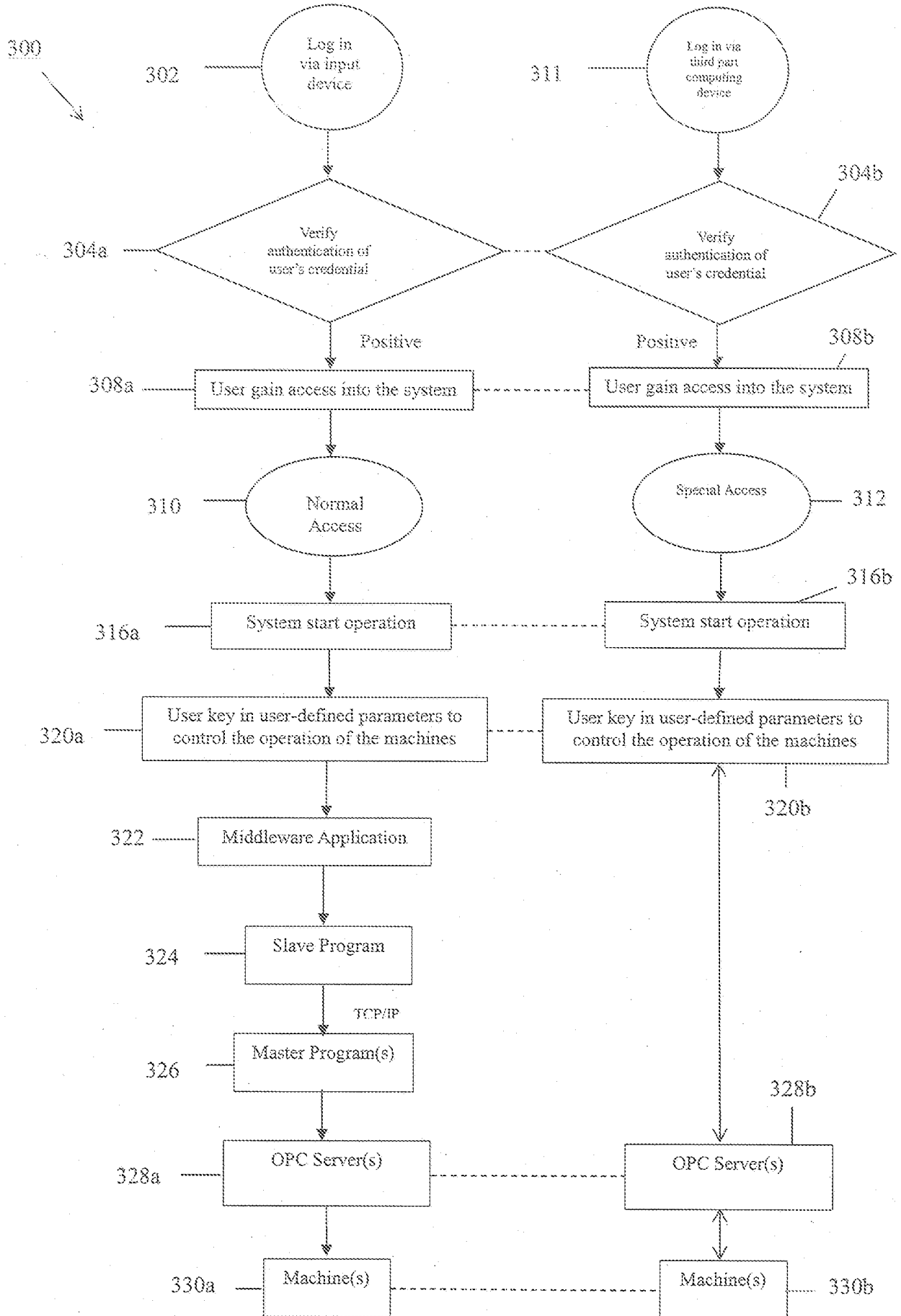


Figure 3

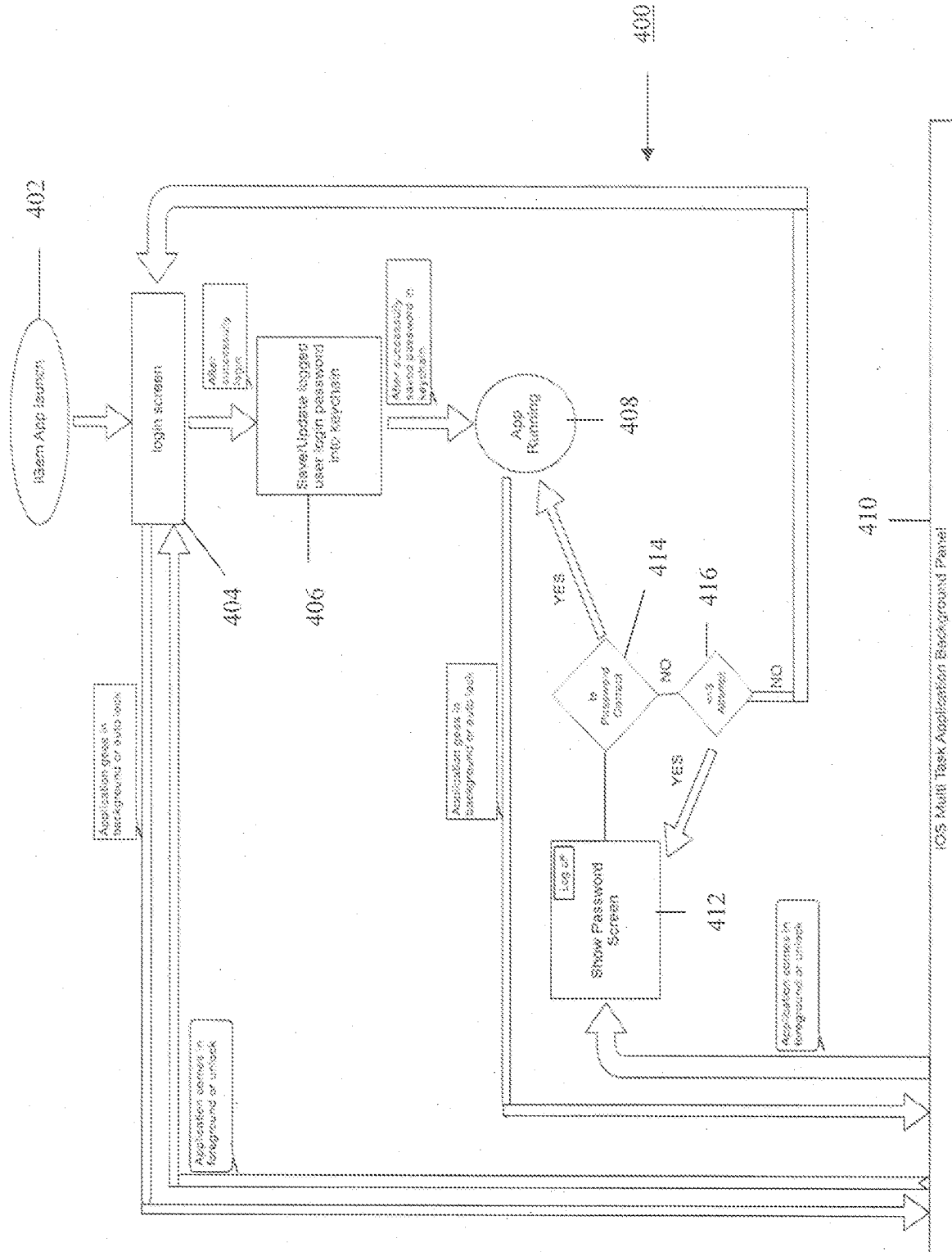



Figure 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SG2015/000141

A. CLASSIFICATION OF SUBJECT MATTER		
G06F 17/30 (2006.1)		
According to International Patent Classification (IPC)		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) G06F17/00		
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) Databases: EPODOC, WPI, English Patent Full-text, FAMPAT Keywords: remote control, monitor, database management, master slave, data exchange, replicate, verify, authentication and other related terms		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/0090937 A1 (MOORE G. ET AL.) 28 April 2005 Paras.[0010],[0012], [0016], [0019],[0021], [0024]-[0025], [0033]-[0034] and [0048]-[0049]; Figs. 1-2	1-24
A	US 2013/0297868 A1 (YIN J. ET AL.) 7 November 2013 The whole document	
A	US 6023507 A (WOOKEY M. J.) 8 February 2000 The whole document	
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> 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 12/01/2016 (day/month/year)	Date of mailing of the international search report 12/01/2016 (day/month/year)
Name and mailing address of the ISA/SG  Intellectual Property Office of Singapore 51 Bras Basah Road #01-01 Manulife Centre Singapore 189554 Email: pct@ipos.gov.sg	Authorized officer <p style="text-align: center;"><u>HONG</u> Lei (Dr)</p> IPOS Customer Service Tel. No.: (+65) 6339 8616

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SG2015/000141**C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6088659 A (KELLEY R. H. ET AL.) 11 July 2000 The whole document	
A	US 2007/0113276 A1 (SHOJI K. ET AL.) 17 May 2007 The whole document	
A	US 6460141 B1 (OLDEN E.M.) 1 October 2002 The whole document	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SG2015/000141

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005/0090937 A1	28/04/2005	AU 2004285129 A1	12/05/2005
		BRP I0415728 A	19/12/2006
		CA 2542771 A1	12/05/2005
		CN 1871432 A	29/11/2006
		DK 1678421 T3	27/07/2015
		EP 1678421 A1	12/07/2006
		ES 2543589 T3	20/08/2015
		WO 2005042971 A1	12/05/2005
US 2013/0297868 A1	07/11/2013	CA 2871313 A1	07/11/2013
		WO 2013165532 A1	07/11/2013
US 6023507 A	08/02/2000	NONE	
US 6088659 A	11/07/2000	AU 750837 B2	01/08/2002
		AU 9386498 A	29/03/1999
		CA 2303064 A1	18/03/1999
		EP 1019857 A1	19/07/2000
		US 6199068 B1	06/03/2001
		WO 9913426 A1	18/03/1999
US 2007/0113276 A1	17/05/2007	CN 1853173 A	25/10/2006
		EP 1657645 A1	25/10/2006
		JP 4576336 B2	04/11/2010
		KR 20060055541 A	23/05/2006
		WO 2005017758 A1	24/02/2005
US 6460141 B1	01/10/2002	NONE	