

DEVICE ~~OF LICENSING FOR PERMITTING~~ PROGRAM, PROGRAM
TRANSACTION DEVICE AND METHOD ~~FOR PERMITTING-OF~~
LICENSING PROGRAM THEREOF

TECHNICAL FIELD

Embodiments in the present disclosure are related to a method of licensing a program, and more particularly to a method of licensing a program in a cloud.

BACKGROUND

Cloud storage refers to a mode of storing on-line data on the internet, i.e., storing the on-line data in a plurality of virtual servers managed by a third party agent, but not to an exclusive server. A data center provider prepares virtualized resources to store the on-line data at the back end according to customers' demands, provides the customer with a storage pool, and then the customer can use the storage pool to store files or objects. Cloud computing is a kind of computing based on the internet. Through this method, shared software resources and messages can be supplied to the computer and other devices on demand. Cloud computing describes an increasing service based on a new information technology (IT) of the internet, usage and delivery and payment modes, involves dynamic transaction expansion functions provided through the internet, and is usually virtualized resources. A user can access service software and data, and the service provider maintains the basic infrastructure and platform to keep the service operating normally. The service or the software provided by the service provider is usually called "software-on-demand", being charged based on usage time. The user only needs to have low complexity software and hardware equipment to use these services, so this can save costs for the enterprise. Because the application is supplied centrally, updates to the

~~The English translation of Claims amended based on Article 19 PCT
(WO 2015/013974)~~

What is claimed is:

~~1. A method of licensing a program, stored in one of a storage device and a remote server, and including a plurality of executable files including a first executable file having a first header and a second executable file having a second header, the method comprising steps of:~~

~~—causing an OS to receive a program start command to activate the program;~~

~~—causing the OS to store the first header in the storage device for reading, and causing the license verification component to prevent the OS from loading the first executable file into the RAM to be executed;~~

~~—causing the license verification component to work with one of the OS and the remote server to perform a license verification;~~

~~—allowing the first executable file to be loaded into the RAM for execution and causing one of the OS and the storage device to acquire a token when the first executable file passes the license verification; and~~

~~—when the second executable file is to be used, the OS reads the second header and performs another license verification through the license verification component and one of the OS and the remote server, wherein:~~

~~the token includes an anonymous token and a non-anonymous token;~~

~~if the license verification pass is verified, the anonymous token is verified after the program is shut down, the program has a datum restored to a default value; and—~~

~~if the license verification pass is verified by the non-anonymous verification token after the program is shut down, the program has a datum kept in its original state.~~

~~2. The method as in Claim 1, further comprising one of the steps of:~~

~~—causing the OS to read an abort file to terminate a licensing procedure of the program, when there is a license verification failure, or stopping the OS from reading the program and causing the program to generate errors to terminate the licensing procedure when there is the license verification failure; and~~

~~—when the second executable file passes the other license verification, the license verification component allows the second executable file to be loaded into the RAM for execution.~~

~~3. A method of licensing a program, comprising the steps of:~~

~~—causing an OS to receive a program start command to activate the program;~~

~~—causing the license verification component to work with one of the OS and the remote server to perform a license verification before the OS loads the program; and~~

~~—causing one of the OS and the storage device to acquire a token when there is the license verification passes, wherein:~~

~~the token includes an anonymous token and a non-anonymous token;~~

~~if the license verification pass is verified, the anonymous token is verified after the program is shut down, the program has a datum restored to a default value; and~~

~~if the license verification pass is verified by the non-anonymous verification token after the program is shut down, the program has a~~

~~datum kept in its original state.~~

~~4. The method as in Claim 3, wherein:~~

~~the license verification component interrupts the OS from loading the program, and the license verification component allows the OS to continuously load the program after the license verification is passed;~~

~~the anonymous token is used with a public computer, and the non-anonymous token is used with a private computer;~~

~~the license verification includes one selected from a group consisting of a permanent license verification, a lease license verification and a trial license verification;~~

~~when the license verification is one of the lease license verification and the trial license verification, the license verification component cooperates with the remote server to perform the license verification;~~

~~when the license verification is the permanent license verification and the remote server is not available, the license verification coordinates with the OS to perform the license verification.——~~

~~5. A device for licensing a program including a header, comprising:~~

~~a storage device;~~

~~a file system arranged to the storage device;~~

~~an operating system (OS) receiving a program start command to activate the program, and storing the header into the storage device for reading; and~~

~~a license verification component preventing the OS from loading the program to a random access memory (RAM) for execution, and cooperating with one of the OS and a remote server to perform a license—~~

~~verification, wherein the license verification component allows the program to be continuously loaded into the RAM for execution if the license verification passes, wherein the OS reads an abort file to terminate a licensing procedure of the program when there is a license verification failure, or stopping the OS from reading the program and causing the program to generate errors to terminate the licensing procedure when there is the license verification failure.~~

~~6. The device as in Claim 5, wherein:~~

~~the device further includes a device driver, and in response to the license verification pass, the license verification component transmits at least one of a first, a second and a third control messages to control the storage device, the file system and the device driver respectively, so as to allow the program to be stored in the storage device from the remote server, to allow the program to be stored in the file system from the storage device through the device driver, and to allow the program to be loaded into the RAM from the file system for execution through the OS;~~

~~the license verification includes one selected from a group consisting of a permanent license verification, a lease license verification and a trial license verification;~~

~~when the license verification is the permanent license verification, the program is allowed to be used without an expiration date;~~

~~when the license verification is the lease license verification, the program is allowed to be used during a predetermined period of time;~~

~~when the license verification is the trial license verification, the program is available until the expiration date; and~~

~~the license verification further includes one of a network license verification and a telephone license verification, the network license verification uses a first grant code to perform the license verification, the first license code includes a message associated with a personal privacy including one selected from the group consisting of an identification number, birthday and a combination thereof., the telephone license verification uses a telephone number to perform the license verification, the telephone number is used to acquire a second license code when the telephone license verification is performed, and the second license code is used to pass the telephone license verification.~~

~~7. A method of licensing a program, comprising the steps of:~~

- ~~——choosing a specific program;~~
- ~~——performing a license verification by one of a local operation system (OS) itself and a remote server; and~~
- ~~——allowing the OS to load the specific program to a specific storage for execution if the license verification is passed; and~~

~~the OS reads an aborting file to terminate a licensing procedure of the program when there is a license verification failure, or stopping the OS from reading the program and causing the program to generate errors to terminate the licensing procedure when there is the license verification failure.~~

~~8. The method as in Claim 7, wherein:~~

- ~~——the method further includes the steps of:~~
- ~~——causing the program to be stored in a software host from a cloud host; and~~
- ~~——transmitting the program to a local area network host from the~~

~~software host;—~~
~~—the method further includes the steps of:~~
~~——stopping the program from executing, and allowing the program~~
~~to be continuously executed after the license verification passes;—~~
~~——the license verification verifies a personal privacy including one~~
~~selected from the group consisting of an identification number, birthday~~
~~and a combination thereof; and~~
~~the specific storage has a storage path which is selected by the~~
~~subscriber.—~~

~~9. A program transaction device, comprising:~~

~~a first storage component storing a remote program database~~
~~including a plurality of programs;~~

~~a second storage component configured for storage for a local~~
~~operating system (OS), so as to select a specific program from the~~
~~plurality of programs; and~~

~~a license verification component cooperating with one of the local~~
~~OS itself and a remote server to perform a license verification, and~~
~~allowing the specific program to be executed after the license verification~~
~~passes, wherein:~~

~~when the license verification does not pass, the OS reads an abort~~
~~file; and~~

~~the license verification component allows the OS to load the specific~~
~~program into one of the first storage component and the second storage~~
~~component after the license verification passes.~~

~~10. The device as in Claim 9, wherein:~~

~~the first storage component is one of a proxy server hard disk and a—~~

~~cloud hard disk, and the second storage component is a random access memory (RAM);~~

~~the license verification component initially prevents the local OS from loading the program into the RAM, and allows the program to be loaded into the RAM for execution after the license verification passes;~~

~~when the program transaction device is a software host, the remote server is a cloud host, the license verification is performed at the cloud host, and the program is stored in the software host;—~~

~~—when the program transaction device is the software host and the remote server is not available, the license verification is performed at the software host, and the program is stored in a local area network (LAN) computer; and~~

~~when the program transaction device is the LAN computer, the remote server is the software host, the license verification is performed at the software host, and the program is stored in the LAN computer;~~

~~when the license verification is one of a lease license verification and a trial license verification, the license verification component cooperates with the remote server to perform the license verification; and~~

~~when the license verification is a permanent license verification and the remote server is not available, the license verification component cooperates with the local OS to perform the license verification;~~

~~the license verification includes one selected from a group consisting of a permanent license verification, a lease license verification and a trial license verification;~~

~~when the license verification is the permanent license verification,—~~

~~the program is allowed to be used without an expiration date;~~
~~when the license verification is the lease license verification, the~~
~~program is allowed to be used during a predetermined period of time;~~
~~when the license verification is the trial license verification, the~~
~~program is available until the expiration date; and~~
~~the license verification further includes one of a network license~~
~~verification and a telephone license verification, the network license~~
~~verification uses a first grant code to perform the license verification, the~~
~~first license code includes a message associated with a personal privacy~~
~~including one selected from the group consisting of an identification~~
~~number, birthday and a combination thereof., the telephone license~~
~~verification uses a telephone number to perform the license verification,~~
~~the telephone number is used to acquire a second license code when the~~
~~telephone license verification is performed, and the second license code is~~
~~used to pass the telephone license verification.~~

~~11. A device of licensing a program, comprising:~~

~~—— a host including a local OS, a random access memory (RAM) and a~~
~~device driver;~~

~~—— a mobile device coupled with the host and including:~~

~~—— a firmware including the license verification component, wherein~~
~~when the mobile device is coupled to the host, the firmware prevents the~~
~~program from being transmitted to the host from the mobile device, and~~
~~the device driver prevents the OS from loading the program into the~~
~~RAM for execution, the license verification component is activated to~~
~~cause the local OS to cooperate with the firmware to perform a license~~
~~verification by using the device driver, when the license verification—~~

~~passes, the firmware allows the program to be transmitted to the host from the mobile device, and the device driver allows the program to be loaded into the RAM for execution through the local OS, wherein:~~

~~the OS reads an abort file to terminate a licensing procedure of the program when there is a license verification failure, or stops the OS from reading the program and causes the program to generate errors to terminate the licensing procedure when there is the license verification failure.~~

~~12. A method of licensing a program in the program transaction device, the program transaction device includes a host and a mobile device, and the method comprises the steps of:~~

~~——coupling the mobile device and the host;~~

~~——the firmware of the mobile device prevents the program from being transmitted to the host from the mobile device, and the device driver prevents the OS from loading the program into the RAM for execution;~~

~~——the license verification component of the mobile device is activated to cause the local OS to cooperate with the firmware to perform a license verification by using the device driver;—~~

~~——when the license verification passes, the firmware allows the program to be transmitted to the host from the mobile device, and the device driver allows the program to be loaded into the RAM for execution through the local OS; and~~

~~the OS reads an abort file to terminate a licensing procedure of the program when there is a license verification failure, or stops the OS from reading the program and causes the program to generate errors to—~~

~~terminate the licensing procedure when there is the license verification failure.~~

1. A method of licensing a program, stored in at least one of a remote server and a storage device in a local terminal having an operating system (OS), a license verification component and a random access memory (RAM) and including a plurality of executable files including a first executable file having a first header and a second executable file having a second header, the method comprising steps of:

causing the OS to receive a program-start command to activate the program;

causing the OS to store the first header in the storage device, and causing the license verification component to prevent the OS from loading the first executable file in the RAM to be executed;

causing the license verification component to work with at least one of the OS and the remote server to perform a license verification;

allowing the first executable file to be loaded in the RAM for execution when the first executable file passes the license verification; and

when the second executable file is to be used, causing the OS to read the second header and perform another license verification through the license verification component and one of the OS and the remote server.

2. The method as in Claim 1, further comprising one of the steps of:

causing the OS to read an aborting file to terminate a licensing procedure of the program, when there is a license verification failure;

stopping the OS from reading the program and causing the program

to generate errors to terminate the licensing procedure when there is the license verification failure; and

when the second executable file passes the another license verification, causing the license verification component to allow the second executable file to be loaded in the RAM.

3. The method as in Claim 1, further comprising:

causing one of the OS and the storage device to acquire a token when there is a license verification pass.

4. The method as in Claim 3, wherein:

the token includes an anonymous token and a non-anonymous token; and

the anonymous token is used with a public computer, and the non-anonymous token is used with a private computer.

5. The method as in Claim 4, wherein:

if the license verification pass is verified, the anonymous token is verified after the program is shut down, the program has a datum recovered to a default value; and

if the license verification pass is verified by the non-anonymous verification token after the program is shut down, the program has a datum kept in its original state.

6. The method as in Claim 1, wherein:

the license verification includes one selected from a group consisting of a permanent license verification, a lease license verification and a trial license verification;

when the license verification is one of the lease license verification

and the trial license verification, the license verification component cooperates with the remote server to perform the license verification; and
when the license verification is the permanent license verification and the remote server is not available, the license verification coordinates with the OS to perform the license verification.

7. The method as in Claim 1, further comprising the steps of:

choosing the program;
causing the program to be stored in a software host from a cloud host; and
transmitting the program to a local area network host from the software host.

8. A device for licensing a program including a header, comprising:

a storage device in a local terminal having a random access memory (RAM);
a file system configured in the storage device;
an operating system (OS) receiving a starting-program command to activate the program and storing the header into the storage device; and
a license verification component preventing the OS from loading the program in the RAM, and working with at least one of the OS and a remote server to perform a license verification,
wherein after there is a license verification pass, the license verification component allows the program to be loaded in the RAM.

9. The device as in Claim 8, wherein:

the device further includes a device driver;
in response to the license verification pass, the license verification

component transmits at least one of a first, a second and a third control messages to control the storage device, the file system and the device driver respectively.

10. The device as in Claim 9, wherein:

the first control message allows the program to be stored into the storage device from the remote server;

the second control message allows the program to be stored into the file system from the storage device through the device driver; and

the third control message allows the program to be loaded in the RAM from the file system for execution through the OS.

11. The device as in Claim 8, wherein:

the license verification include at least one of a permanent license verification, a lease license verification and a trial license verification;

when the license verification is the permanent license verification, the program is allowed to be used without an expiration date;

when the license verification is the trial license verification, the program is available until the expiration date.

12. The device as in Claim 8, wherein:

the license verification further includes a network license verification;

the network license verification uses a first grant code to perform the license verification; and

the first license code includes a message associated with a personal privacy including one selected from the group consisting of an identification number, birthday and a combination thereof.

13. The device as in Claim 8, wherein:

the license verification further includes a telephone license verification;

the telephone license verification uses a telephone number to perform the license verification; and

the telephone number is used to acquire a second license code when the telephone license verification is performed, and the second license code is used to pass the telephone license verification.

14. A device for licensing a program, comprising:

a storage unit storing and executing a program; and

a license verification component initially causing the program to be halted from execution, and licensing the program for execution when there is a license verification pass.

15. The device as in Claim 14, wherein:

the storage unit includes a first storage component storing a remote program database including a plurality of programs, and a second storage component;

the first storage component is one of a proxy server hard disk and a cloud hard disk, and the second storage component is a random access memory (RAM); and

the license verification component cooperates with at least one of a local operating system (OS) and a remote server to perform a license verification, initially prevents the local OS from loading the program in the RAM, and allows the program to be loaded into the RAM for execution after having the license verification pass.

16. The device as in Claim 14, wherein:

the storage unit includes a random access memory (RAM) having a first memory space and a second memory space, wherein the first memory space is a RAM disk for storage of the program, and the second memory space is used to execute the program;

the license verification component cooperates with at least one of a local operating system (OS) and a remote server to perform a license verification;

when the device is a software host, the remote server is a cloud host, the license verification is performed at the cloud host, and the program is stored in the software host;

when the device is the software host and the remote server is not available, the license verification is performed at the software host, and the program is stored in a local area network (LAN) computer; and

when the device is the LAN computer, the remote server is the software host, the license verification is performed at the software host, and the program is stored in the LAN computer.

17. The device as in Claim 14, wherein:

the license verification component cooperates with at least one of a local operating system (OS) and a remote server to perform a license verification;

when the license verification is one of a lease license verification and a trial license verification, the license verification component cooperates with the remote server to perform the license verification; and

when the license verification is a permanent license verification and the remote server is not available, the license verification component

cooperates with the local OS to perform the license verification.

18. The device as in Claim 14, further comprising:

a host including a local OS, a random access memory (RAM) and a device driver;

a mobile device coupled with the host and including:

a firmware including the license verification component.

19. The device as in Claim 18, wherein:

when the mobile device is coupled to the host, the firmware prevent the program from being transmitted to the host from the mobile device, and the device driver prevents the OS from loading the program into the RAM for execution, the license verification component is activated to cause the local OS to cooperate with the firmware to perform a license verification by using the device driver.

20. The device as in Claim 19, wherein:

when there is the license verification pass, the firmware allows the program to be transmitted to the host from the mobile device, and the device driver allows the program to be loaded in the RAM for execution through the local OS.