(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 July 2016 (07.07.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/107555 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/CN2015/099497

(22) International Filing Date:
29 December 2015 (29.12.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201410840830.5 29 December 2014 (29.12.2014) CN

(71) Applicant: **HANGZHOU H3C TECHNOLOGIES CO., LTD.** [CN/CN]; 466 Changhe Road, Binjiang District, Hangzhou, Zhejiang 310052 (CN).

(72) Inventor: **LUO, Youchun**; Room 730, Oriental Electronic BLD., NO.2, Chuangye Road, Shangdi Information Industry Base, Haidian District, Beijing 100085 (CN).

(74) Agent: **BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**; Room 1209, B block of Jiahua Building, No.9 Shangdi 3rd Street, Haidian District, Beijing 100085 (CN).

(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).

Published:

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

(54) Title: LOADING STORAGE MEDIUM

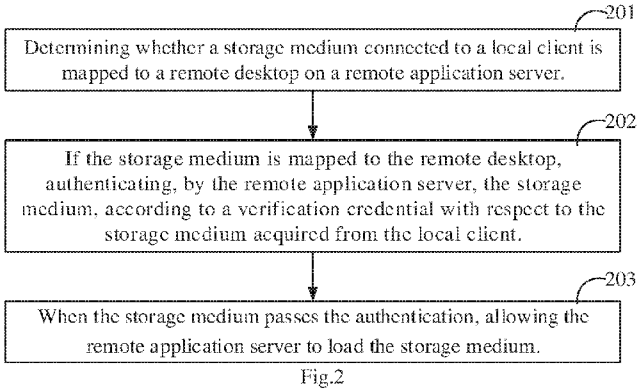

Fig.2

(57) Abstract: In one example, a method comprises determining whether a storage medium connected to a local client is mapped to a remote desktop on a remote application server. If the storage medium is mapped to the remote desktop, the storage medium may be authenticated according to verification credential with respect to the storage medium acquired from the local client. The storage medium may be loaded when the storage medium passes the authentication.

WO 2016/107555 A1

Loading Storage Medium

Background

[0001] With the development of virtualization technology, mobile office becomes more and more pervasive in enterprises. In a mobile office, a user, such as an employee, may be assigned a virtual desktop which runs on a remote server. The remote desktop may store data and certain applications and settings which may be accessed by the user using a local client device which connects to the remote server over a network. While mobile office brings efficiency to enterprises, it also brings security concern to enterprises.

Brief Description of the Drawings

[0002] Fig.1 is a scenario schematic illustrating an application of the present disclosure in loading storage medium;

[0003] Fig.2 is a flowchart illustrating a method for loading storage medium according to an example of the present disclosure;

[0004] Fig.3 is a flowchart illustrating a method for loading storage medium according to an example of the present disclosure;

[0005] Fig.4 is a diagram illustrating hardware structure of an apparatus in which a loading storage medium apparatus is installed according to an example of the present disclosure;

[0006] Fig.5 a diagram illustrating a loading storage medium apparatus according to an example of the present disclosure.

Detailed Description

[0007] After a storage medium connected to a local client is mapped to a remote application desktop (hereinafter, also be referred as "remote desktop") on a remote application server, the storage medium is usually authenticated by the local client. After the storage medium passes the authentication, the remote application server is allowed to access data stored in the storage medium. Since the data loaded from the storage medium by the remote application server is decrypted on the local client, the data may be easily leaked if it is intercepted in transmission. With respect to such condition, the present disclosure provides a method and apparatus for enhancing the security of a storage medium in a mobile office.

[0008] For simplicity and illustrative purposes, the present disclosure is described by referring mainly to an example and figures thereof. In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure as well as its objects, features and advantages.

[0009] In an example of the present disclosure, referring to Fig.1, the scenario schematic of an application of the present disclosure in loading storage medium is illustrated. In Fig.1, the

storage medium 101 may for example be an encrypted removable hard disk, optical disk, removable flash storage, a universal serial bus memory and so on. The local client 102 may be a handset, iPad, laptop, or desktop computer and so on. The remote application server 103 is used for distributing various types of office application software to the local client and authenticating the storage medium. The storage medium administration server 104 is used for identifying the identity of the storage medium. In order to realize mobile office, a mobile office application may be installed in the local client 102, and by initiating the mobile office application on the local client 102, the user may open the remote desktop on the remote application server 103 and access the office application distributed on the remote application server 103.

[0010] In an example, when a user opens the remote desktop on a remote application server, the storage medium 101 connected to the local client 102 may be mapped to the remote desktop on the remote application server. That is, in response to a user opening the remote desktop on the remote application server, a mapping relationship between the storage medium and the remote desktop is built. Thus, based on the mapping relationship between the storage medium and the remote desktop, the remote application server in which the remote desktop is installed may authenticate the storage medium according to verification credential with respect to the storage medium acquired from the local client. And then, when the storage medium passes the authentication, the remote application server may be allowed to access the storage medium such as load data from the storage medium. In this way, since the storage medium is authenticated by the remote application server but not the local client, the data loaded by the remote application server from the storage medium can be decrypted into plaintext by the remote desktop but remains encrypted during the remote application server accessing the storage medium, so as to upgrade the use security of the storage medium.

[0011] Referring to Fig.2, a flowchart of an example of the method for loading storage medium in the present disclosure, the example is illustrated from the side of a remote application server, which may include:

[0012] Block 201, determining whether a storage medium connected to a local client is mapped to a remote desktop on a remote application server.

[0013] For example, when a storage medium is connected to a local client and a user opens the remote desktop on a remote application server, the storage medium connected to the local client may be mapped to the remote desktop through Universal Serial Bus (USB) mapping supported by Remote Desktop Protocol (RDP). In the meantime, since the storage medium mapped to the remote desktop on the remote application server remains encrypted and to be authenticated, the remote application server cannot use the storage medium yet.

[0014] Block 202, if the storage medium is mapped to the remote desktop, authenticating, by

the remote application server, the storage medium, according to a verification credential with respect to the storage medium acquired from the local client. For example the verification credential may be stored on the local client, or input by a user, and acquired by the remote application server.

[0015] In an example, when the storage medium is connected to the local client and the user opens the remote desktop on the remote application server, the local client may pop up a dialog box to require the user to input verification credential, and after the user inputs the verification credential in the dialog box, the local client may send the verification credential to the remote application server.

[0016] In an example, when a storage medium is connected to the local client and the user opens the remote desktop on the remote application server, the local client may further read the unique identifier of the storage medium, and send the unique identifier of the storage medium to the remote application server. For example, the unique identifier may be "USB/VID_152D&PID_2339", VID represents a provider code, and PID represents a product code. In another example, the local client may send the unique identifier of the storage medium together with the verification credential to the remote application server after the user inputs the verification credential into the dialog box popped up in the local client.

[0017] In order to enhance the security in loading storage medium, according to an example, after acquiring the unique identifier of the storage medium, the remote application server may determine whether the identity information of the storage medium mapped to the remote desktop on the remote application server and the unique identifier of the storage medium match each other or not, and if they match, send the identity information of the storage medium to a storage medium administration server. Then, the storage medium administration server may determine whether the identity information of the storage medium is consistent with the preset identity information of storage medium, and if yes, it indicates that the storage medium is identified, and the storage medium administration server may send its own identity information and a loading policy to the remote application server. Wherein, the preset identity information of storage medium means the identity information of the storage medium which is stored in the storage medium administration server in advance. The loading policy means a loading policy which is stored in the storage medium administration server in advance and relates to how the storage medium shall be loaded by the local client or the remote application server, and so on. For example, the loading policy may be: reading operation on the storage medium, writing operation on the storage medium, or reading and writing operation on the storage medium.

[0018] After receiving the identity information of the storage medium administration server, in order to avoid illegal attacks in the meantime, the remote application server may further

determine whether the identity information of the storage medium administration server is consistent with the preset identity information of storage medium administration server, and if yes, it indicates that the storage medium administration server is authenticated. Wherein, the preset identity information of storage medium administration server refers to a legal server that may be used to identify the identity of the storage medium that can be accessed by the remote application server. In general, the preset identity information of storage medium administration server is stored in the remote application server in advance.

[0019] If the identity of the storage medium and the identity of the storage medium administration server in the remote application server are authenticated, it means the mapped storage medium is legal and the remote application server may be allowed to access the storage medium. At this time, the remote application server may further authenticate the verification credentials with respect to the storage medium acquired from the local client, and if the storage medium passes the authentication, Block 203 may be executed; otherwise, the remote application server may return an error report about the verification credential to the local client, so as to inform the user to input correct verification credential. Wherein, the verification credential may be an encryption code of the storage medium, and the authentication process may be that: after acquiring the verification credential input from the local client, the remote application server may compare the verification credential with information about the verification credential extracted by the remote application server, and if they are consistent with each other, it means the storage medium is authenticated, i.e., passes the authentication.

[0020] At block 203, the storage medium passes the authentication, allowing the remote application server to load the storage medium.

[0021] In an example, when the storage medium passes the authentication, the remote application server may load the storage medium according to the loading policy acquired from the storage medium administration server.

[0022] As can be seen from the above, when a storage medium connected to a local client is mapped to a remote desktop on a remote application server, through authenticating the storage medium by the remote application server, the present disclosure may effectively prevents data leaks during the remote application server accessing data in the storage medium, so as to upgrade the use security of the storage medium.

[0023] Referring to Fig.3, a flowchart of another example of the method for loading storage medium in the present disclosure, the example illustrates the interactions among local client, remote application server and storage medium administration server, so as to describe the process for loading the storage medium in details. In the practice, a credible mobile storage medium agent AGENT may be deployed on the remote application server, and the agent

AGENT digitally communicates with the local client and the storage medium administration server so as to execute a method provided in the present disclosure. The method may include following blocks:

[0024] Block 301, after a storage medium is connected to a local client, the user may open the remote desktop on the remote application server by initiating a mobile office application on the local client.

[0025] Block 302, the local client reads the unique identifier of the storage medium.

[0026] Block 303, the storage medium connected to the local client is mapped to a remote desktop on the remote application server through USB mapping supported by RDP.

[0027] Block 304, the local client requests the user to input a verification credential, e.g. through a dialog box.

[0028] Block 305, after the user inputs the verification credential, the local client sends the unique identifier of the storage medium and the verification credential to the agent AGENT on the remote application server.

[0029] Block 306, the agent AGENT determines whether the identity information of the storage medium and the unique identifier of the storage medium match each other or not.

[0030] Block 307, if they match, the agent AGENT sends the identity information of the storage medium to the storage medium administration server.

[0031] Block 308, the storage medium administration server determines whether the identity information of the storage medium is consistent with a preset identity information of storage medium, and if yes, it indicates that the identity of the storage medium passes the identification, and Block 309 may be executed. Otherwise, it indicates that the identity of the storage medium does not pass the identification, and Block 314 may be executed.

[0032] Block 309, the storage medium administration server sends its own identity information and a loading policy to the agent AGENT.

[0033] Block 310, the agent AGENT determines whether the identity information of the storage medium administration server is consistent with preset identity information of storage medium administration server, and if yes, this indicates that the identity information of the storage medium administration server passes the identification, and Block 311 may be executed. Otherwise, this indicates that the identity information of the storage medium administration server does not pass the identification, and Block 315 may be executed.

[0034] Block 311, the agent AGENT authenticates the verification credential with respect to the storage medium acquired from the local client, and if the storage medium passes the authentication, Block 312 may be executed, and otherwise, Block 313 may be executed.

[0035] Block 312, the agent AGENT loads the storage medium according to the loading

policy.

[0036] In the present example, when the storage medium is loaded successfully, the agent AGENT may inform the remote desktop on the remote application server, so as to allow the remote desktop to access the storage medium through an explorer normally.

[0037] Block 313, the agent AGENT returns an error report about verification credential to the local client, so as to inform the user to input correct verification credential.

[0038] Block 314, the storage medium administration server sends a report about the identity information of the storage medium not passing identification to the remote application server, and Block 315 is executed.

[0039] Block 315, it indicates that the remote application server cannot load the storage medium.

[0040] As seen from the above, when a storage medium connected to a local client is mapped to a remote desktop on a remote application server, through authenticating the storage medium by the remote application server, the present disclosure may help to effectively prevents data leaks during the remote application server accessing data in the storage medium and thereby upgrade the security of the mobile office.

[0041] The present disclosure also provides an example of an apparatus for loading storage medium, in correspondence with the method for loading storage medium described above.

[0042] The example of the present disclosure of the apparatus for loading storage medium may be realized by software or hardware or the combination of both. As an example of being realized by software, the apparatus may be an apparatus in a logical sense and formed by the processor of the apparatus reading corresponding machine readable instructions from non-transitory storage to internal memory and operating these instructions. In a hardware sense, as illustrated in Fig.4, the apparatus for loading storage medium in the present disclosure may comprise a processor 401, a network interface 402 and a storage 403, and may further comprise other hardware parts, such as a chip for forwarding messages and so on. And in terms of the hardware structure, the apparatus may be a distributed apparatus and comprise multiple interface cards, so as to perform the extension of message processing in hardware level.

[0043] Referring to Fig.5, a block diagram of the apparatus for loading storage medium in an example of the present disclosure is illustrated, and the example is described from the side of a remote application server. As shown in Fig.5, the apparatus may comprise:

a determining unit 510, configured to determine whether a storage medium connected to a local client is mapped to a remote desktop on a remote application server;

an authenticating unit 520, configured to authenticate the storage medium, according to

verification credential with respect to the storage medium which is acquired from the local client when the determination result of the determining unit 510 is YES; and

a loading unit 530, configured to load the storage medium, when the storage medium passes the authentication.

[0044] In an alternative example, the apparatus may further comprise a matching unit 540, which is configured to:

before the authenticating unit authenticates the storage medium according to the verification credential, determine whether the identity information of the storage medium mapped to the remote desktop on the remote application server and the unique identifier of the storage medium acquired from the local client match each other or not; and

if they match, send the identity information of the storage medium to a storage medium administration server, so as to allow the storage medium administration server to identify the storage medium.

[0045] In another alternative example, the apparatus may further comprise a receiving unit 550, which is configured to

receive the identity information of the storage medium administration server and a loading policy of the storage medium acquired from the storage medium administration server, when the storage medium is identified by the storage medium administration server.

[0046] In another alternative example, the apparatus may further comprise a determining unit 560, which is configured to

determine whether the received identity information of the storage medium administration server is consistent with preset identity information of storage medium administration server, and

if it is, cause the authenticating unit to authenticate the storage medium according to the verification credential with respect to the storage medium acquired from the local client, and

when the storage medium passes the authentication, cause the loading unit to load the storage medium according to the loading policy sent from the storage medium administration server.

[0047] The description about an example of the apparatus is basically in correspondence with that of the method, and the detailed description is omitted and may be referenced to the description about the example of the method. The above-described example of apparatus is only illustrative, wherein the units described as separate components may or may not be physically

separate, and the component described as a displaying unit may or may not be a physical unit and can be located in one location or distributed to a plurality of networking units. Those skilled in the art may readily implement the present disclosure without any inventive effort and may select some or all of the modules or units to implement according to practical needs.

[0048] The present disclosure provides a machine readable storage medium corresponding to the method for loading storage medium as above, which is stored with machine readable instructions which are executed by processor to:

determine whether a storage medium connected to a local client is mapped to a remote desktop on a remote application server;

authenticate the storage medium, according to verification credential with respect to the storage medium acquired from the local client when the storage medium is mapped to the remote desktop; and

load the storage medium, when the storage medium passes the authentication.

[0049] The machine readable instructions are further executed by the processor to:

before authenticating the storage medium according to the verification credential with respect to the storage medium acquired from the local client, determine whether the identity information of the storage medium mapped to the remote desktop on the remote application server and the unique identifier of the storage medium acquired from the local client match each other or not; and

if they match, send the identity information of the storage medium to a storage medium administration server, so as to allow the storage medium administration server to identify the storage medium.

[0050] The machine readable instructions are further executed by the processor to:

when the storage medium is identified by the storage medium administration server, receive the identity information of the storage medium administration server and the loading policy of the storage medium from the storage medium administration server.

[0051] The machine readable instructions are further executed by the processor to:

determine whether the received identity information of the storage medium administration server is consistent with preset identity information of storage medium administration server, and

if it is, authenticate the storage medium, according to the verification credential with respect to the storage medium acquired from the local client, and when the storage medium is

identified, load the storage medium, according to the loading policy sent from the storage medium administration server.

[0052] As seen from the above, when a local client opens a remote desktop on a remote application server, through mapping a storage medium connected to the local client to the remote desktop and authenticating the storage medium by the remote application server, the present disclosure effectively prevents data leaks during the remote application server accessing the data in the storage medium, so as to upgrade the use security of the storage medium.

[0053] The above are only preferred examples of the present disclosure is not intended to limit the disclosure within the spirit and principles of the present disclosure, any changes made, equivalent replacement, or improvement in the protection of the present disclosure should contain within the range.

[0054] The methods, processes and units described herein may be implemented by hardware (including hardware logic circuitry), software or firmware or a combination thereof. The term 'processor' is to be interpreted broadly to include a processing unit, ASIC, logic unit, or programmable gate array etc. The processes, methods and functional units may all be performed by the one or more processors; reference in this disclosure or the claims to a 'processor' should thus be interpreted to mean 'one or more processors'.

[0055] Further, the processes, methods and functional units described in this disclosure may be implemented in the form of a computer software product. The computer software product is stored in a storage medium and comprises a plurality of instructions for making a processor to implement the methods recited in the examples of the present disclosure.

[0056] The figures are only illustrations of an example, wherein the units or procedure shown in the figures are not necessarily essential for implementing the present disclosure. Those skilled in the art will understand that the units in the device in the example can be arranged in the device in the examples as described, or can be alternatively located in one or more devices different from that in the examples. The units in the examples described can be combined into one module or further divided into a plurality of sub-units.

[0057] Although the flowcharts described show a specific order of execution, the order of execution may differ from that which is depicted. For example, the order of execution of two or more blocks may be changed relative to the order shown. Also, two or more blocks shown in succession may be executed concurrently or with partial concurrence. All such variations are within the scope of the present disclosure.

[0058] It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the above-described examples, without departing from the broad general scope of the present disclosure. The present disclosure are, therefore, to be considered in

all respects as illustrative and not restrictive.

[0059] The foregoing disclosure is merely illustrative of preferred examples of the disclosure but is not intended to limit the disclosure, and any modifications, equivalent substitutions, adaptations, thereof made without departing from the spirit and scope of the disclosure shall be encompassed in the claimed scope of the appended claims.

CLAIMS

1. A method for loading storage medium, comprising:

determining whether a storage medium connected to a local client is mapped to a remote desktop on a remote application server;

authenticating, by the remote application server, the storage medium according to a verification credential with respect to the storage medium sent from the local client, when the storage medium is mapped to the remote desktop; and

loading the storage medium, by the remote application server, when the storage medium passes the authentication.

2. The method according to claim 1, further comprising:

before authenticating the storage medium, determining, by the remote application server, whether the identity information of the storage medium mapped to the remote desktop on the remote application server and the verification credential of the storage medium acquired from the local client match each other or not;

if they match, sending the identity information of the storage medium to a storage medium administration server, so as to allow the storage medium administration server to authenticate the storage medium.

3. The method according to claim 2, further comprising:

if the storage medium passes the authentication by the storage medium administration server, receiving, by the remote application server, the identity information of the storage medium administration server and a loading policy of the storage medium from the storage medium administration server.

4. The method according to claim 3, further comprising:

determining, by the remote application server, whether the received identity information of the storage medium administration server is consistent with a preset identity information of storage medium administration server,

if it is consistent, authenticating the storage medium, by the remote application server, according to the verification credential of the storage medium sent from the local client, and loading the storage medium according to the loading policy when the storage medium passes the authentication.

5. An apparatus for loading storage medium, applied on a remote application server, comprising:

a determining unit to determine whether a storage medium connected to a local client is mapped to a remote desktop on the remote application server ;

an authenticating unit to authenticate the storage medium, according to verification credential with respect to the storage medium which is acquired from the local client, when the determination result of the determining unit is YES; and

a loading unit to load the storage medium, when the storage medium passes the authentication.

6. The apparatus according to claim 5, further comprising:

a matching unit to

before the authenticating unit authenticates the storage medium, determine whether the identity information of the storage medium mapped to the remote desktop on the remote application server and the unique identifier of the storage medium acquired from the local client match each other or not; and

if they match, send the identity information of the storage medium to a storage medium administration server, so as to allow the storage medium administration server to identify the storage medium.

7. The apparatus according to claim 6, further comprising:

a receiving unit to, after the storage medium has been authenticated by the storage medium administration server, receive the identity information of the storage medium administration server and a loading policy of the storage medium from the storage medium administration server.

8. The apparatus according to claim 7, further comprising a determining unit which is to

determine whether the received identity information of the storage medium administration server is consistent with preset identity information of storage medium administration server, and

if it is, allow the authenticating unit to authenticate the storage medium according to the acquired verification credential with respect to the storage medium, and allow the loading unit to load the storage medium according to the loading policy when the storage medium passes the authentication.

9. A non-transitory machine readable storage medium storing machine readable instructions, which are executable by a processor to:

determine whether a storage medium connected to a local client is mapped to a remote desktop on a remote application server ;

if the storage medium is mapped to the remote desktop, authenticate the storage medium, according to verification credential with respect to the storage medium which is acquired from the local client; and

load the storage medium when the storage medium passes the authentication.

10. The machine readable storage medium according to claim 9, wherein the machine readable instructions are further executable by the processor to:

before authenticating the storage medium according to the verification credential, determine whether the identity information of the storage medium mapped to the remote desktop on the remote application server and the unique identifier of the storage medium acquired from the local client match each other or not; and

if they match, send the identity information of the storage medium to a storage medium administration server, so as to allow the storage medium administration server to authenticate the storage medium.

11. The machine readable storage medium according to claim 10, wherein the machine readable instructions are further executed by the processor to:

when the storage medium is authenticated by the storage medium administration server, receive the identity information of the storage medium administration server and a loading policy of the storage medium from the storage medium administration server.

12. The machine readable storage medium according to claim 11, wherein the machine readable instructions are further executed by the processor to:

determine whether the received identity information of the storage medium administration server is consistent with preset identity information of storage medium administration server, and

if it is consistent, authenticate the storage medium according to the verification credential with respect to the storage medium acquired from the local client, and load the storage medium according to the loading policy when the storage medium passes the authentication.

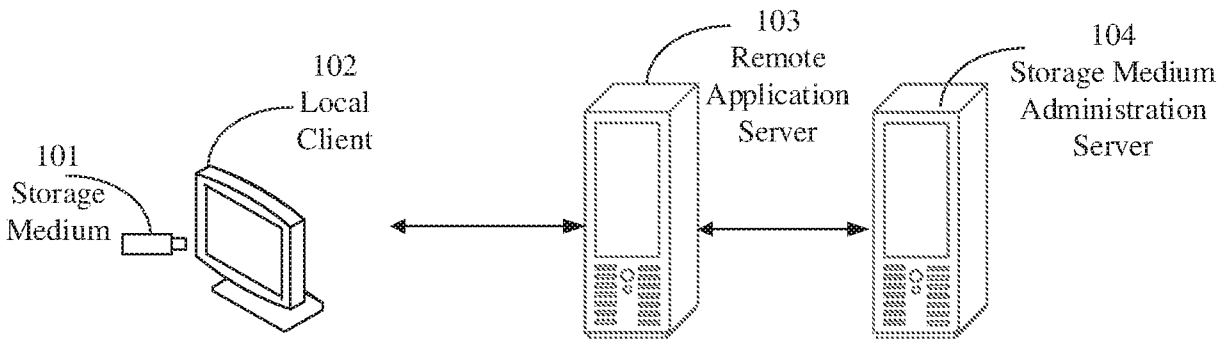
101
Storage
Medium
102
Local
Client
103
Remote
Application
Server
104
Storage Medium
Administration
Server

Fig.1

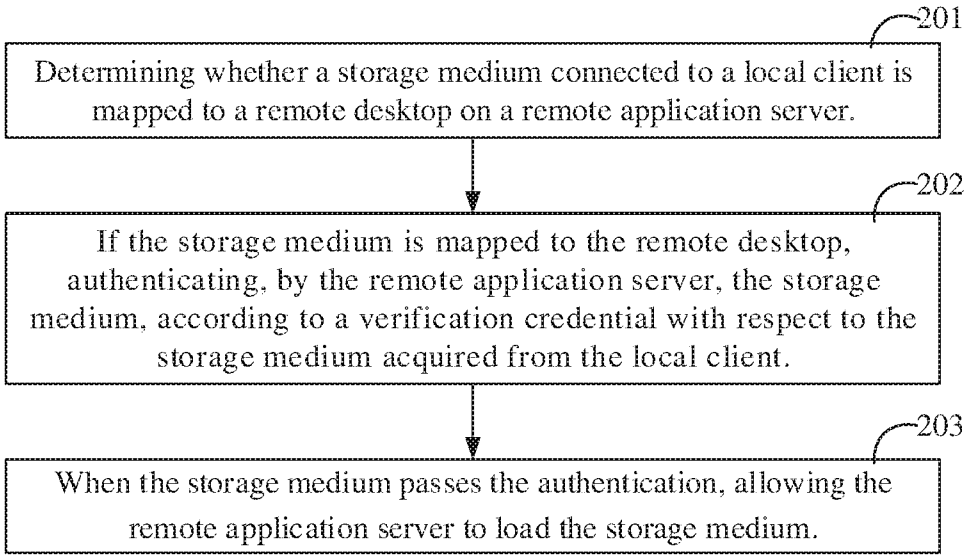
201
Determining whether a storage medium connected to a local client is mapped to a remote desktop on a remote application server.
202
If the storage medium is mapped to the remote desktop, authenticating, by the remote application server, the storage medium, according to a verification credential with respect to the storage medium acquired from the local client.
203
When the storage medium passes the authentication, allowing the remote application server to load the storage medium.

Fig.2

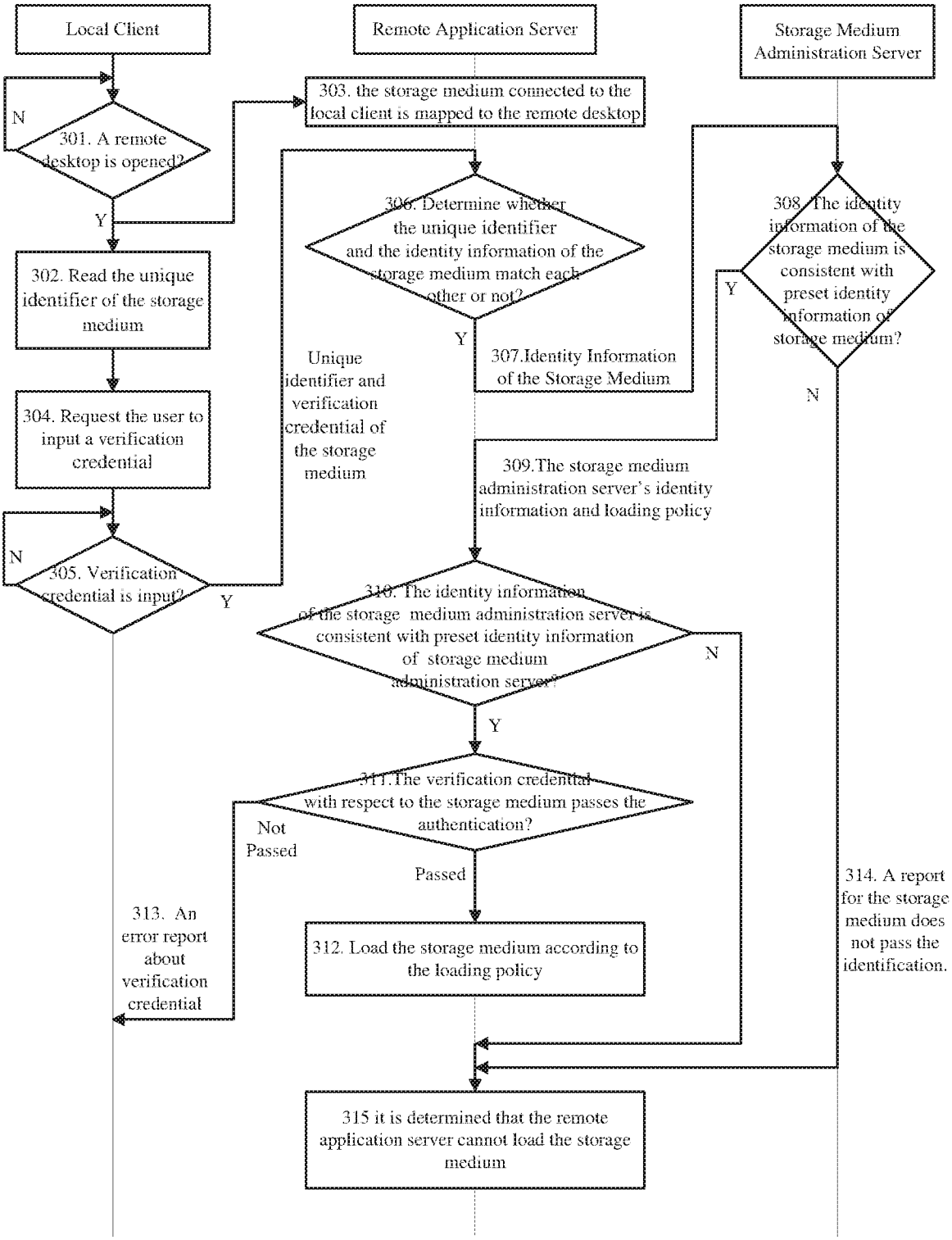
Local Client
Remote Application Server
Storage Medium Administration Server
301. A remote desktop is opened?
N
Y
302. Read the unique identifier of the storage medium
303. the storage medium connected to the local client is mapped to the remote desktop
304. Request the user to input a verification credential
305. Verification credential is input?
N
Y
Unique identifier and verification credential of the storage medium
306. Determine whether the unique identifier and the identity information of the storage medium match each other or not?
Y
307.Identity Information of the Storage Medium
308. The identity information of the storage medium is consistent with preset identity information of storage medium?
Y
N
309.The storage medium administration server's identity information and loading policy
310. The identity information of the storage medium administration server is consistent with preset identity information of storage medium administration server?
N
Y
311.The verification credential with respect to the storage medium passes the authentication?
Not Passed
Passed
313. An error report about verification credential
312. Load the storage medium according to the loading policy
314. A report for the storage medium does not pass the identification.
315 it is determined that the remote application server cannot load the storage medium

Fig.3

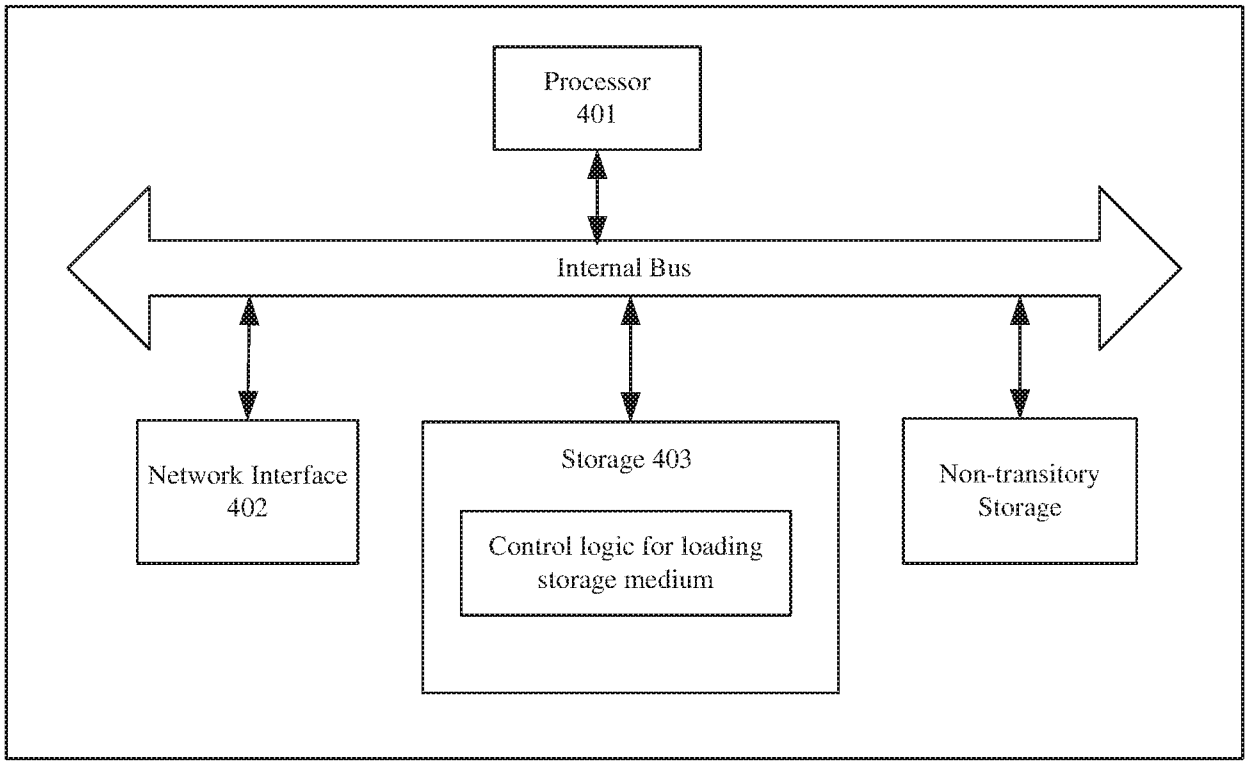
Processor
401
Internal Bus
Network Interface
402
Storage 403
Control logic for loading storage medium
Non-transitory Storage

Fig.4

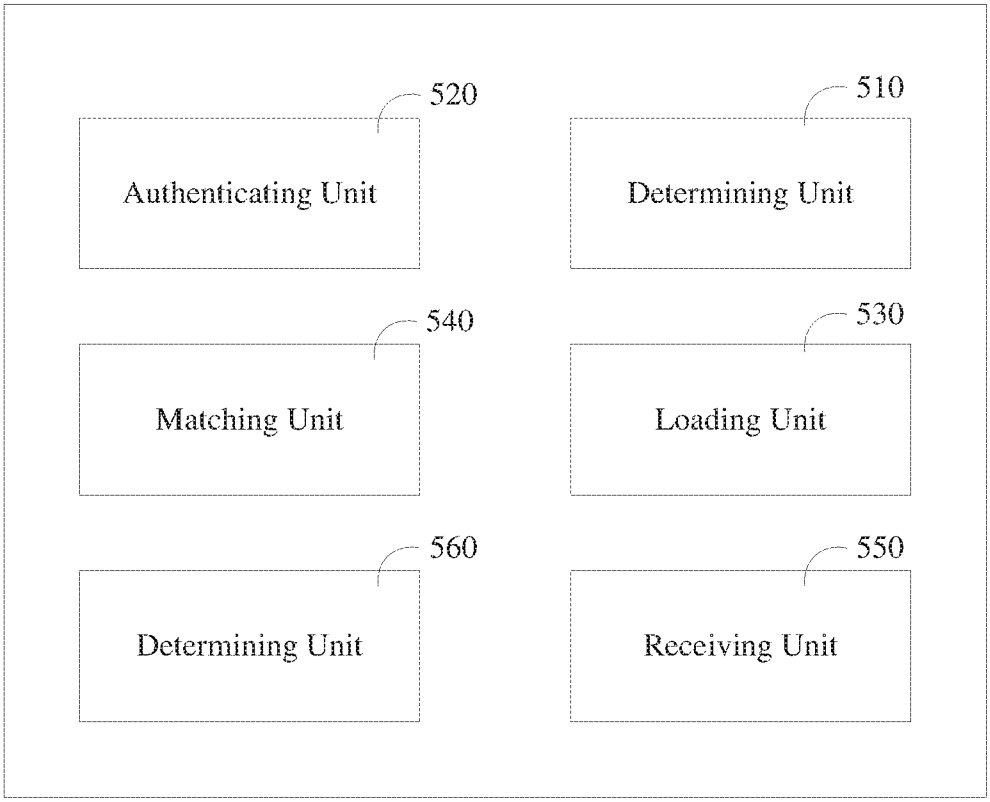
520
Authenticating Unit
510
Determining Unit
540
Matching Unit
530
Loading Unit
560
Determining Unit
550
Receiving Unit

Fig.5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/099497

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W

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)

WPI,EPODOC,CNKI,CNPAT,IEEE:determine, storage, medium, local, client, map, remote, desktop, application, server, authenticate, verification, match, load

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101272242 A (ZTE CORPORATION) 24 September 2008 (2008-09-24) description, page 3, paragraph 10 to page 7, paragraph 2	1, 5, 9
X	CN 102685245 A (BEIJING MAIPU YINGSUI TECHNOLOGY CO., LTD.) 19 September 2012 (2012-09-19) description, paragraphs [0043]-[0088]	1, 5, 9
A	CN 103685267 A (XIAOMI TECHNOLOGY CO., LTD.) 26 March 2014 (2014-03-26) the whole document	1-12
A	CN 103188301 A (PEKING UNIVERSITY FOUNDER GROUP CO., LTD. ET AL.) 03 July 2013 (2013-07-03) the whole document	1-12
A	WO 2014130742 A1 (THE DIGITAL MARVELS, INC.) 28 August 2014 (2014-08-28) the whole document	1-12

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 February 2016	**24 March 2016**

Name and mailing address of the ISA/CN	Authorized officer
STATE INTELLECTUAL PROPERTY OFFICE OF THE P.R.CHINA **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088, China**	**TANG,Guangqiang**
Facsimile No. **(86-10)62019451**	Telephone No. **(86-10)61648266**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/099497

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 101272242 A	24 September 2008	None	
CN 102685245 A	19 September 2012	None	
CN 103685267 A	26 March 2014	None	
CN 103188301 A	03 July 2013	None	
WO 2014130742 A1	28 August 2014	US 2015381735 A1	31 December 2015