



(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:

PCT/CN2014/086122

(22) International Filing Date:

9 September 2014 (09.09.2014)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

201310412075.6

11 September 2013 (11.09.2013)

CN

(71) Applicant: **TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED** [CN/CN]; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN).

(72) Inventors: **TANG, Wenliang**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN). **ZENG, Xing**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN). **QIN, Lei**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN). **LIN, Chunyou**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN).

(74) Agent: **ADVANCE CHINA IP LAW OFFICE**; Room 3901, No. 85 Huacheng Avenue, Tianhe District, Guangzhou, Guangdong 510623 (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: METHODS, DEVICES, AND SYSTEMS FOR ACCOUNT LOGIN

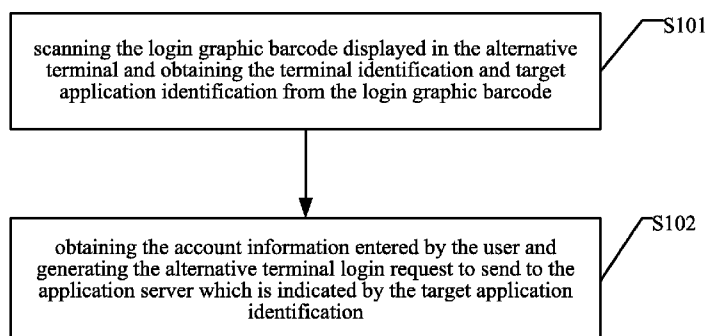


Fig. 1

(57) Abstract: Embodiments of the present disclosure are to provide an account login method, a device and a system thereof. In the method, the user terminal scans the login graphic code displayed in the alternative terminal and obtains the terminal identification and target application identification from the login graphic code. The user terminal obtains the account information and generates an alternative terminal login request to send to an application server which is indicated by the target application identification. The alternative terminal login request includes the account information and the terminal identification. The alternative terminal login request is programmed to request the application server to return the notification message of access permit to the alternative terminal, so the alternative terminal logs in the target application using the account information.



WO 2015/035895 A1

Description

METHODS, DEVICES, AND SYSTEMS FOR ACCOUNT LOGIN

CROSS-REFERENCE TO RELATED APPLICATIONS

[001] This application claims priority to Chinese Patent Application No. 201310412075.6, filed on September 11, 2013, which is hereby incorporated by reference in its entirety.

FIELD

[002] The present disclosure relates to the technology field of computer login application, and more particularly to an account login method, device and system thereof.

BACKGROUND

[003] With the development of computer application technology and network technology, people can sign in the account information including registered username and password anytime so as to log in to various types of servers. Thus, people can exchange information with the other one or more users when logging in all types of instant communication applications, BBS exchange, games, social network and so on.

[004] In the existing login technology, a terminal generally shows a login interface to a user, the user then enters the account information in the username box and password box, according to which the terminal sends a login request to the corresponding server. After the server has verified and passed the account information, the server returns the notice message for access permission which the account information corresponds to, informs the terminal such as the public computer and so on to access services, and returns some information such as the user's friends list, user's role information in the game, messages received at the offline time, and other data, ultimately completes the user's login.

[005] However, due to the presence of various types of viruses and Trojans, in some public environments such as internet cafes, the viruses and Trojans hidden in the unsafe user terminals may run backstage, obtain the user's account information when the user enters the account information including the username and password to sign in. Thus, the user's username and password may be stolen. That is to say, the security of the existing login technology is poor, which may easily causes the information leakage and the loss of user's property.

SUMMARY

[006] Embodiments of the present disclosure are to provide an account login method, device and system. The method, device and system can complete the login of other devices in the safe device, which ensures the security of login to a certain extent.

[007] In a first aspect, the embodiments of the present disclosure provide an account login method implemented in a user terminal. The method includes: the user terminal scans the login graphic code displayed in an alternative terminal and obtains the terminal identification and target application identification from the login graphic code. The user terminal obtains the account information and generates an alternative terminal login request to send the alternative terminal login request to the application server which is indicated by the target application identification. The alternative terminal login request includes the account information and the terminal identification. The alternative terminal login request is programmed to request the application server to return the notification message of access permit to the alternative terminal, so that the alternative terminal logs in the target application using the account information.

[008] In a second aspect, the embodiments of the present disclosure also provide another account login method. In the method, a server receives the alternative terminal login request sent by a user terminal, where the alternative terminal login request includes the account information and terminal identification obtained by the user terminal. The server authenticates the account information in the alternative terminal login request. The server returns a notification message of access permit to the alternative terminal after authenticating the account information, so that the alternative terminal logs in the target application using the account information.

[009] In a third aspect, the embodiments of the present disclosure also provide another account login method. In the method, a user terminal scans a login graphic code displayed in the alternative terminal and obtains the terminal identification and target application identification from the login graphic code. The user terminal obtains the account information and generates the alternative terminal login request to send the alternative terminal login request to the application server that is indicated by the target application identification. The alternative terminal login request includes the obtained account information and terminal identification. The user terminal then receives a notification message of access permit to the alternative terminal from an application server after the account information is authenticated, so that the alternative terminal logs in the target application using the account information.

[010] In a fourth aspect, the embodiments of the present disclosure also provide an account login device. The account login device includes a hardware processor and a non-transitory storage medium accessible to the hardware processor. The non-transitory storage medium configured to store modules including: a scanning module and a processing module. The scanning module is programmed to scan a login graphic code displayed in the alternative terminal and obtaining a terminal identification and a target application identification from the login graphic code. The processing module is programmed to obtain the account information and generating an alternative terminal login request to send the alternative terminal login request to an application server that is

indicated by the target application identification; wherein the alternative terminal login request comprises the account information and the terminal identification. The alternative terminal login request is programmed to request the application server to return the notification message of access permit to the alternative terminal that is indicated by the terminal identification, so that the alternative terminal logs in the target application using the account information.

[011] In a fifth aspect, the embodiments of the present disclosure also provide another account login device that includes a hardware processor and a non-transitory storage medium accessible to the hardware processor. The non-transitory storage medium configured to store modules including: a receiving module, an authentication module, and an access module. The receiving module is programmed to receive an alternative terminal login request sent by a user terminal, where the alternative terminal login request comprises account information and a terminal identification obtained by the user terminal. The authentication module, programmed to authenticate the account information in the alternative terminal login request. The access module is programmed to return a notification message of access permit to the alternative terminal indicated by the terminal identification, so that the alternative terminal logs in the target application using the account information.

[012] In a sixth aspect, the embodiments of the present disclosure also provide an account login system. The system includes: an alternative terminal, a user terminal and a server. The user terminal is programmed to scan the login graphic code displayed in the alternative terminal and obtaining the terminal identification and target application identification from the login graphic code. The user terminal is further programmed to obtain the account information entered by the user and generating the alternative terminal login request to send the alternative terminal login request to the application server which is indicated by the target application identification; therein the alternative terminal login request carries the obtained account information and terminal identification. The application server is programmed to return the notification message of access permit to the alternative terminal indicated by the terminal identification in the alternative terminal login request after authenticating the account information in the received alternative terminal login request, so the alternative terminal logs in the target application using the account information.

[013] According to the graphic code, the embodiments of the present disclosure can provide the related information of the terminal which needs the login account to the other more secure and reliable terminals, such as user's phone and tablet frequently used, and so on. Communicating with the corresponding servers by the secure and reliable terminals and achieving alternative terminal login function by the secure and reliable terminals, that makes users not expose their account information to the computers when they log in the corresponding applications and games on the computers provided by the public places such as internet bars. It improves the security of the account

login, protects the safety of the users' accounts better, and avoids losses caused by account information leakage.

BRIEF DESCRIPTION OF THE DRAWINGS

[014] To explain the technical proposals according to the embodiments of the present disclosure or the prior art, accompanying drawings used in the embodiments or the prior art are briefly described hereunder. Apparently, the following drawings merely illustrate some embodiments of the present disclosure, but for persons skilled in the art, other drawings can be obtained without creative works according to these drawings.

[015] Fig. 1 is an example flowchart of an account login method according to embodiments of the present disclosure;

[016] Fig. 2 is an example flowchart of another account login method according to embodiments of the present disclosure;

[017] Fig. 3 is an example flowchart of another account login method according to embodiments of the present disclosure;

[018] Fig. 4 is an example flowchart of another account login method according to embodiments of the present disclosure;

[019] Fig. 5 is one of the schematic views of the security warning interface according to embodiments of the present disclosure;

[020] Fig. 6 is an example flowchart of another account login method according to embodiments of the present disclosure;

[021] Fig. 7 is an example flowchart of another account login method according to embodiments of the present disclosure;

[022] Fig. 8 is an example flowchart of the account login method according to embodiments of the present disclosure;

[023] Fig. 9 is an example structure schematic view of an account login system according to embodiments of the present disclosure;

[024] Fig. 10 is an example structure schematic view of an account login device according to embodiments of the present disclosure;

[025] Fig. 11 is an example structure schematic view of Processing Module as shown in Fig. 10;

[026] Fig. 12 is another structure schematic view of Processing Module as shown in Fig. 10;

[027] Fig. 13 is another structure schematic view of Processing Module as shown in Fig. 10;

[028] Fig. 14 is an example structure schematic view of another account login device according to embodiments of the present disclosure; and

[029] Fig. 15 is an example structure schematic view of Access module as shown in Fig. 14.

DETAILED DESCRIPTION OF THE DRAWINGS

[030] Reference throughout this specification to “one embodiment,” “an embodiment,” “example embodiment,” or the like in the singular or plural means that one or more particular features, structures, or characteristics described in connection with an embodiment is included in at least one embodiment of the present disclosure. Thus, the appearances of the phrases “in one embodiment” or “in an embodiment,” “in an example embodiment,” or the like in the singular or plural in various places throughout this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures, or characteristics may be combined in any suitable manner in one or more embodiments.

[031] The terminology used in the description of the disclosure herein is for the purpose of describing particular examples only and is not intended to be limiting of the disclosure. As used in the description of the disclosure and the appended claims, the singular forms “a,” “an,” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise. Also, as used in the description herein and throughout the claims that follow, the meaning of “in” includes “in” and “on” unless the context clearly dictates otherwise. It will also be understood that the term “and/or” as used herein refers to and encompasses any and all possible combinations of one or more of the associated listed items. It will be further understood that the terms “may include,” “including,” “comprises,” and/or “comprising,” when used in this specification, specify the presence of stated features, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, operations, elements, components, and/or groups thereof.

[032] As used herein, the term “module” or “unit” may refer to, be part of, or include an Application Specific Integrated Circuit (ASIC); an electronic circuit; a combinational logic circuit; a field programmable gate array (FPGA); a processor (shared, dedicated, or group) that executes code; other suitable hardware components that provide the described functionality; or a combination of some or all of the above, such as in a system-on-chip. The term module or unit may include memory (shared, dedicated, or group) that stores code executed by the processor.

[033] The exemplary environment may include a server, a client, and a communication network. The server and the client may be coupled through the communication network for information exchange, such as sending/receiving identification information, sending/receiving data files such as splash screen images, etc. Although only one client and one server are displayed in the environment, any number of terminals or servers may be included, and other devices may also be included.

[034] The communication network may include any appropriate type of communication network for providing network connections to the server and client or among multiple servers or clients. For example, communication network may include the Internet or other types of computer networks or telecommunication networks, either wired or wireless. In a certain embodiment, the

disclosed methods and apparatus may be implemented, for example, in a wireless network that includes at least one client.

[035] In some cases, the client may refer to any appropriate user terminal with certain computing capabilities, such as a personal computer (PC), a work station computer, a server computer, a hand-held computing device (tablet), a smart phone or mobile phone, or any other user-side computing device. In various embodiments, the client may include a network access device. The client may be stationary or mobile.

[036] A server, as used herein, may refer to one or more server computers configured to provide certain server functionalities, such as database management and search engines. A server may also include one or more processors to execute computer programs in parallel.

[037] A user, as used herein, may refer to one or more persons or things that control a client. The user may control more than one clients or other devices.

[038] The solutions in the embodiments of the present disclosure are clearly and completely described in combination with the attached drawings in the embodiments of the present disclosure. Obviously, the described embodiments are only a part, but not all, of the embodiments of the present disclosure. On the basis of the embodiments of the present disclosure, all other embodiments acquired by those of ordinary skill in the art under the precondition that no creative efforts have been made shall be covered by the protective scope of the present disclosure.

[039] Hereinafter, the technical proposals according to the embodiments of the present disclosure will be clearly and completely described in conjunction with the accompanying drawings. Apparently, the embodiments described are merely a part of embodiments of the present disclosure, but not all embodiments. Persons skilled in the art can obtain all other embodiments without creative works, based on these embodiments, which pertains to the protection scope of the present disclosure.

[040] Fig. 1 illustrates an example flowchart of an account login method according to embodiments of the present disclosure. The method according to the embodiment of the present disclosure may be implemented in a smart phone, a tablet, a smart wearable device, or any other user terminals. The method includes:

[041] S101: A user terminal scans the login graphic code displayed in the alternative terminal and obtaining a terminal identification and a target application identification from the login graphic code. The login graphic code may be a barcode, a two-dimensional code, a two-dimensional code, or any graphical code which may include the necessary identification information.

[042] In the embodiments of the present disclosure, the alternative terminal may be any terminal that the user has not used before. For example, the alternative terminal may be a computer in a public library, an Internet café, a friend's smart phone, or any terminal device in a public place. When the user wants to sign in various accounts like instant communication accounts and games

accounts to access to the corresponding application servers, game servers, etc., in the alternative terminal, the alternative terminal can obtain the current IP address of the alternative terminal and/or other terminal identification when the graphic code login operation is detected. The alternative terminal may then combine with the identification of the application and generates the login graphic code like bar code or two-dimensional code, then displays the login graphic code. The alternative terminal may display the login graphic code along with the log-in user interface of the target application such as the instant communication application.

[043] The alternative terminal may also send the graphic code login request to the corresponding server when the graphic code login operation is detected. The server assigns a unique identification for the alternative terminal according to the graphic code login request, and generates the graphic code including the assigned identification and the target application identification to return to the alternative terminal by which the graphic code is shown to the user.

[044] The user terminal scans the login graphic code displayed in the alternative terminal by calling a photographing module, and resolves the login graphic code to obtain the carried binary information thereof, and ultimately obtains the terminal identification and target application identification of the alternative terminal. The user terminal may confirm the corresponding application server to the application in the present login according to the target application identification thereof. For example, when it is confirmed as an instant communication application according to the target application identification, the corresponding instant communication application server can be confirmed according to the address of the typed of built-in server of the instant communication application.

[045] S102: obtaining the account information entered by the user and generating the alternative terminal login request to send the alternative terminal login request to the application server which is indicated by the target application identification; wherein the alternative terminal login request carries the obtained account information and terminal identification;

[046] Here, the alternative terminal login request is programmed to request the application server to return the notification message of access permit to the alternative terminal which is indicated by the terminal identification in the alternative terminal login request, so the alternative terminal logs in the target application of the alternative terminal using the account information.

[047] The methods of entering the account information by users includes variety, and specifically can be: obtaining the account information including the username and password entered by users by showing a login interface or calling the login interface of the application which has been installed in the present terminal and is corresponding to the target application identification; or detecting the history login account of the target application in the present terminal automatically, then showing the detected history login account to users as a choice, then making the account

information including the corresponding username and password to the history login account chosen by users as the account information entered by users; or further including the username and password entered in the application input box by users in the login graphic code displayed in the alternative terminal, then making the account information including the username and password as account information entered by users, therein to be noted that the user won't click to log in after entering the username and password in the alternative terminal. Because there is no clicking to log in, neither the viruses nor Trojans program at present will be triggered to obtain the account information including the username and password entered by users, so that it basically is also safe relatively.

[048] After detecting the users' login confirmation, the user terminal may combine and/or encrypt the obtained account information and the terminal identification of the alternative terminal in the alternative terminal update request. The user terminal then send the alternative terminal update request to the corresponding application server. Alternatively or additionally, the alternative terminal may also directly combine and/or send encrypt the obtained account information and the terminal identification of the alternative terminal in the alternative terminal update request and then sends directly the alternative terminal update request to the corresponding application server.

[049] After the application server receives the alternative terminal update request, confirming the present login act is the alternative terminal login act needs to achieve to sign in the account information entered by the users in the target application of the alternative terminal of the terminal identification in the alternative terminal update request. Authenticate the account information in the alternative terminal login request; after authenticating the account information, return the notification message of access permit to the alternative terminal which is indicated by the terminal identification in the alternative terminal login request, so the alternative terminal logs in the target application using the account information, and also return the user data such as the user's friends chain, user's role information in the game and the data programmed to receive, sending and processing, ultimately complete the user's login in the alternative terminal. The alternative terminal update request may constitute part of the alternative terminal login request.

[050] According to the graphic code, the embodiments of the present disclosure provide the related information of the terminal which needs the login account to the other more secure and reliable terminals, such as user's phone and tablet frequently used, and so on. Communicating with the corresponding servers by the secure and reliable terminals and achieving alternative terminal login function by the secure and reliable terminals, that makes users not expose their account information to the computers when they log in the corresponding applications and games on the computers provided by the public places such as internet bars. It improves the security of the account login, protects the safety of the users' accounts better, and avoids losses caused by account information leakage.

[051] Fig. 2 shows a flowchart of another account login method according to embodiments of the present disclosure. The method may be applied in a smart phone, a tablet, smart wearable devices, or other user terminals. The method includes:

[052] S201: scanning the login graphic code displayed in the alternative terminal and obtaining a terminal identification and a target application identification from the login graphic code;

[053] The user terminal scans the login graphic code displayed in the alternative terminal by calling Photographing Module, and resolves the login graphic code to obtain the carried binary information thereof, and ultimately obtains the terminal identification and target application identification of the alternative terminal.

[054] S202: detecting a history of login accounts of the target application in the present user terminal, and displaying the detected history of login accounts in the present user terminal.

[055] For example, the history login account may include the account information of the target application which has been logged in by the user in the present user terminal (such as the smart phone and other terminals). The account information includes the username and password programmed to sign in the target application. The user terminal may achieve this automatic entry of the account information intelligently using the history login account. Thus, the user does not need to enter the corresponding account again. If the history account information is not detected, the user terminal may send the login interface directly to inform the user to enter the account information.

[056] S203: confirming the username and password of the selected login account chosen by the user from the displayed history login accounts as the account information entered by the user;

[057] After the user has selected one of the login accounts displayed, the user terminal obtains the selection that identifies the selected login accounts. Step S203 may include: detecting whether the latest login time of the login account selected by the user in the displayed history login accounts has exceeded the preset validity duration or not. If it has not exceeded the preset validity duration, the user terminal directly obtains the selected username and password of the history login account as the account information. If it exceeds the preset validity duration, the user terminal displays an interface including the username of the selected history login account and obtains the password entered by the user. The user terminal then confirms the username of the selected login account and the entered password as the account information.

[058] The period of login validity duration may be a preset duration such as one hour or two hours. During that period, the corresponding information like username and password with the history login account can be obtained directly. Therefore, the user terminal first determines whether it is in the period of login validity duration. If yes, the user terminal may extract the username and password of the history login account directly as the account information. If it is out of the period of login validity duration, the user terminal only extracts the username first. The user terminal may

then display a message and asks the user to re-enter the password to obtain the complete account information including the username and password.

[059] S204: generating the alternative terminal login request according to the confirmed account information entered by the user and the terminal identification. Here, the alternative terminal login request is programmed to request the application server to return the notification message of access permit to the alternative terminal which is indicated by the terminal identification in the alternative terminal login request, so that the alternative terminal logs in the target application using the account information;

[060] S205: sending the alternative terminal login request to the application server which is indicated by the target application identification.

[061] After receiving the alternative terminal update request, the application server confirms that the present login act is an alternative terminal login act. In the alternative terminal login act, the application in the present user terminal does not need to log in. Rather, in the alternative terminal login act, the alternative terminal needs to log in the target application of the alternative terminal using the account information.

[062] The application server may return the notification message of access permit to the alternative terminal indicated by the terminal identification in the alternative terminal login request after authenticating the account information, so that the alternative terminal logs in the target application using the account information. The application server may send the prompt message of the successful validation to the user terminal first, so that the user terminal executes the operation of confirming to log in. Optionally, the user terminal can execute the following S206 to S208.

[063] S206: after receiving the prompt message of the successful validation which is returned by the application server responding to the alternative terminal login request, sending the security warning of whether to allow to log in the alternative terminal;

[064] S207: determining whether to a confirming button in the security warning interface is clicked or not;

[065] S208: if the confirming button is clicked, sending the notice of confirming to log in in the alternative terminal using the account information. The alternative terminal is indicated by the terminal identification in the alternative terminal login request to the application server. The notice of confirming makes the application server return the notification message of access permit to the alternative terminal, so that the alternative terminal logs in the target application using the account information.

[066] Fig. 5 shows one of the schematic views of the security warning interface that may be displayed in the user terminal, where the security warning includes a warning message that the same account may log in the alternative terminal. According to the security warning interface, the user

may determine whether or not to continue logging in the alternative terminal. The user may continue the logging process in the alternative terminal by clicking the confirming button. Alternatively, the user may stop the logging process in the alternative terminal if he does not click the confirming button. It can be further confirmed by the S205 to S207 whether this alternative terminal login operation is a valid user or not, thus the account login security is further ensured.

[067] The embodiments of the present disclosure can provide the terminal information of the terminal which needs login account and application information to the other more secure and reliable terminals, such as user's phone and tablet frequently used, etc.. Communicating with the corresponding servers by the secure and reliable terminals and achieving alternative terminal login function by the secure and reliable terminals, that makes users not expose their account information to the computers when they log in the corresponding applications and games on the computers provided by the public places such as internet bars. It improves the security of the account login, protects the safety of the users' accounts better, and avoids losses caused by account information leakage. Furthermore, it can meet the automation of the account entering by automatically providing the recorded account information in the secure and reliable terminals to the users as a choice, and save the required time to log in in an alternative terminal.

[068] Fig. 3 shows a flowchart of another account login method according to embodiments of the present disclosure. The method according to the embodiment of the present disclosure may be implemented in the smart phone, tablet, smart wearable devices and other user terminals. The method may include:

[069] S301: scanning the login graphic code displayed in the alternative terminal and obtaining the terminal identification and target application identification from the login graphic code;

[070] The user terminal scans the login graphic code displayed in the alternative terminal by calling a photographing module, and resolves the login graphic code to obtain the carried binary information thereof, and ultimately obtains the terminal identification and target application identification of the alternative terminal.

[071] S302: calling the login box to obtain the account information entered by the user, wherein the entered account information includes the username and password.

[072] The login box may be a simple entering box where a user can enter the account information including the username and password. Alternatively, the login box may be the login box of the target application installed in the present terminal. Thus, the user may use the entering box in the present alternative terminal to obtain the account information including the username and password.

[073] S303: generating the alternative terminal login request according to the entered account information and terminal identification;

[074] Here, the alternative terminal login request is programmed to request the application server to return the notification message of access permit to the alternative terminal which is indicated by the terminal identification in the alternative terminal login request, so the alternative terminal logs in the target application of the alternative terminal using the account information.

[075] S304: sending the alternative terminal login request to the application server which is indicated by the target application identification.

[076] After receiving the alternative terminal update request, the application server confirms that the present login act is the alternative terminal login act needs to achieve to sign in the target application of the alternative terminal, which is identified by the terminal identification in the alternative terminal update request.

[077] The application server may return the notification message of access permit to the alternative terminal after authenticating the account information, so that the alternative terminal logs in the target application using the account information. The application server can also send the prompt message of the successful validation to the user terminal first, so that the user terminal executes the operation of confirming to log in. Optionally, the user terminal can execute the following S305 to S307.

[078] S305: after receiving the prompt message of the successful validation which is returned by the application server responding to the alternative terminal login request, sending a security warning of whether to allow the target application to log in the alternative terminal;

[079] S306: determining whether a confirming button in the security warning interface is clicked or not;

[080] S307: if so, sending the notice of confirming to the application server, which makes the application server return the notification message of access permit to the alternative terminal, so the alternative terminal logs in the target application using the account information. The notice of confirming may be programmed to indicate that the user account is ready to sign in the alternative terminal which is indicated by the terminal identification in the alternative terminal login request.

[081] Fig. 5 shows one of the schematic views of the security warning interface that may be displayed in the user terminal. The security warning warns the user that the user account may log in the alternative terminal. According to the security warning interface, the user can determine whether or not there is a need to log in the alternative terminal. It can be further confirmed by the S205 to S207 whether this alternative terminal login operation is a valid user or not, thus the account login security is further ensured.

[082] The embodiments of the present disclosure can provide the terminal information of the terminal which needs login account and application information to the other more secure and reliable terminals, such as user's phone and tablet frequently used, and so on. Communicating with the

corresponding servers by the secure and reliable terminals and achieving alternative terminal login function by the secure and reliable terminals, that makes users not expose their account information to the computers when they log in the corresponding applications and games on the computers provided by the public places such as internet bars. It improves the security of the account login, protects the safety of the users' accounts better, and avoids losses caused by account information leakage. Furthermore, after obtaining the terminal identification and application identification, an input box can be displayed in the terminal to inform the user to enter the corresponding account and password. It makes the operation simple and clear, and is suitable for most of the entry of account information.

[083] Fig. 4 shows a flowchart of another account login method according to embodiments of the present disclosure. The method according to the embodiment of the present disclosure can be applied in the smart phone, tablet, smart wearable devices and other user terminals. The flowchart includes:

[084] S401: scanning the login graphic code displayed in the alternative terminal and obtaining the terminal identification and target application identification from the login graphic code;

[085] S402: obtaining the account information from the login graphic code, where the account information in the login graphic code is the account information entered in the target application login interface of the alternative terminal;

[086] In the embodiments of the present disclosure, the login graphic code may also include the account information. For example, when opening the target application in the alternative terminal, the user may enter the username and password in the target application login box without the need to click the login button. When the user clicks the button for login using the two-dimensional code, the alternative terminal generates the account information including the username and password, terminal identification and the login graphic code of the target application identification. The user terminal scans the login graphic code displayed in the alternative terminal by calling Photographing Module in S410, and resolves the login graphic code to obtain the carried binary information thereof, and ultimately obtains the terminal identification, target application identification and the account information of the alternative terminal.

[087] S403: generating the alternative terminal login request according to the entered account information and terminal identification;

[088] Here, the alternative terminal login request is programmed to request the application server to return the notification message of access permit to the alternative terminal which is indicated by the terminal identification in the alternative terminal login request, so the alternative terminal logs in the target application using the account information.

[089] S404: sending the alternative terminal login request to the application server which is indicated by the target application identification.

[090] The application server may return the notification message of access permit to the alternative terminal indicated by the terminal identification in the alternative terminal login request after authenticating the account information, so the alternative terminal logs in the target application using the account information. It can also send the prompt message of the successful validation to the user terminal first, so that the user terminal executes the operation of confirming to log in. Optionally, the user terminal can execute the following S405 to S407.

[091] S405: after receiving the prompt message of the successful validation which is returned by the application server responding to the alternative terminal login request, sending the a security warning of whether to allow to log in the alternative terminal;

[092] S406: determining whether the confirming button is clicked in the security warning interface or not;

[093] S407: if so, sending the notice of confirming to sign in the account information in the alternative terminal which is indicated by the terminal identification in the alternative terminal login request to the application server, which makes the application server return the notification message of access permit to the alternative terminal which is indicated by the terminal identification in the alternative terminal login request, so the alternative terminal logs in the target application using the account information.

[094] As shown in Fig. 5, it is one of the schematic views of the security warning interface which is sent by the user terminal and can log in the alternative terminal. According to the security warning interface which can log in the alternative terminal, the user can intuitively determine whether or not there is a need to log in the alternative terminal. It can be further confirmed by the S205 to S207 whether this alternative terminal login operation is a valid user or not, thus the account login security is further ensured.

[095] To be noted, the methods of obtaining the user account in the embodiments of Fig. 2 to Fig. 4, may be used independently or be combined. For example, the alternative terminal may only use one of these methods, or use a combination of any two or three methods according to the needs to achieve the same account information login or different accounts information login.

[096] The embodiments of the present disclosure can provide the terminal information of the terminal which needs login account and application information to the other more secure and reliable terminals, such as user's phone and tablet frequently used, and so on. The disclosed methods communicate with the corresponding servers by the secure and reliable terminals and achieve alternative terminal login function by the secure and reliable terminals, which reduces the potential exposure of user account information to the unsecured computers when they log in the corresponding

applications and games on the unsecured computers in public places. It improves the security of the account login, protects the safety of the users' accounts better, and avoids losses caused by account information leakage.

[097] Fig. 6 shows a flowchart of another account login method according to embodiments of the present disclosure. The method according to the embodiment of the present disclosure can be implemented in all kinds of servers for applications, games and so on. The method includes:

[098] S501: receiving the alternative terminal login request sent by the user terminal; where the alternative terminal login request includes the account information and the terminal identification obtained by the user terminal;

[099] The alternative terminal login request is sent by the user terminals such as phones, and programmed to request the application server to return the notification message of access permit to the alternative terminal which is indicated by the terminal identification in the alternative terminal login request, so the alternative terminal logs in the target application using the account information. To the generating and sending process of the alternative terminal login request, the description according to the embodiments of the present disclosure above can be a reference.

[0100] After receiving the alternative terminal login request, the server executes the flow of the alternative terminal login. While receiving the existing ordinary login request, execute the existing login act.

[0101] S502: authenticating the account information in the alternative terminal login request.

[0102] The server may authenticate whether the username and password of the account information in the alternative terminal login request matches the stored username and password for a particular application. If the username and password match, the authentication is successful. Otherwise, the server sends an error warning.

[0103] S503: returning the notification message of access permit to the alternative terminal indicated by the terminal identification in the alternative terminal login request after authenticating the account information, so the alternative terminal logs in the target application using the account information.

[0104] The notification message of access permit is programmed to inform the alternative terminal that it can log in according to the account information received by the present server and at the same time returning some corresponding user data to the account to the public computer and other alternative terminals, which is loaded into the target application by the alternative terminal.

[0105] In addition, optionally, the server may also remind the user in the user terminal whether to confirm to log in the alternative terminal after the authentication is passed, the interface can be referred to Fig. 5. In the embodiment of the present disclosure, the S503 may include: responding to the alternative terminal login request to return the prompt message of the successful validation to the

user terminal; if receiving the notice of confirming to sign in the account information in the alternative terminal which is indicated by the terminal identification in the alternative terminal login request sent by the user terminal, the alternative terminal which is indicated by the terminal identification in the alternative terminal login request returns the notification message of access permit.

[0106] Further, the server may also carry out the following steps when it receives the graphic code login request sent by the alternative terminal. For example, the server may assign a unique identification for the alternative terminal when receiving the graphic code login request of the alternative terminal and generate the graphic code including the unique identification and the target application identification. After that, the server may return the generated graphic code to the alternative terminal.

[0107] After the alternative terminal login request sent by more secure and reliable terminals, such as user's phone and tablet frequently used, and so on, the embodiments achieve alternative terminal login function by verifying the information in the alternative terminal login request of the more secure and reliable terminals. It makes users not expose their account information to the computers when they log in the corresponding applications and games on the computers provided by the public places such as internet bars. It improves the security of the account login, protects the safety of the users' accounts better, and avoids losses caused by account information leakage.

[0108] Fig. 7 shows a flowchart of another account login method according to embodiments of the present disclosure. The method according to the embodiment of the present disclosure can be executed between the user terminals like phone and tablet and servers, and can complete the account login from the alternative terminals like public computers to the servers by the user terminals. The method includes:

[0109] S601: scanning the login graphic code displayed in the alternative terminal by user terminal and obtaining the terminal identification and target application identification from the login graphic code;

[0110] S602: obtaining the account information which is entered by the user by the user terminal and generating the alternative terminal login request to send the alternative terminal login request to the application server which is indicated by the target application identification; therein the alternative terminal login request carries the obtained account information and terminal identification;

[0111] The implementations of the S601 to S602 may refer to the above description of the corresponding embodiments shown in Fig. 1 to Fig. 5.

[0112] S603: returning the notification message of access permit to the alternative terminal indicated by the terminal identification in the alternative terminal login request by the application

server after authenticating the account information in the received alternative terminal login request, so the alternative terminal logs in the target application using the account information.

[0113] The implementation of S603 of the application server and the account information login in the target application using the account information may be referred to the above description of the corresponding embodiments shown in Fig. 1 to Fig. 6.

[0114] According to the graphic code, the embodiments of the present disclosure can provide the related information of the terminal which needs the login account to the other more secure and reliable terminals, such as user's phone and tablet frequently used, and so on. Communicating with the corresponding servers by the secure and reliable terminals and achieving alternative terminal login function by the secure and reliable terminals, that makes users not expose their account information to the computers when they log in the corresponding applications and games on the computers provided by the public places such as internet bars. It improves the security of the account login, protects the safety of the users' accounts better, and avoids losses caused by account information leakage.

[0115] Fig. 8 shows an example flowchart of the account login method according to embodiments of the present disclosure. The embodiments describe the method by the alternative terminals like personal computers, the user terminals like smart phones and the server-side. Specifically, the method includes:

[0116] S1: An alternative terminal opens the two-dimensional code login interface in the computer. The alternative terminal may firstly open the ordinary login interface according to the user's click operation, then displays the two-dimensional code login interface when the user clicks the button programmed to mark the two-dimensional code login on the ordinary login interface.

[0117] S1 is executed by an alternative terminal such as a computer in the public space. S2 to S21 below are all executed by a user terminals such as mobile phone which can initiate the alternative terminal login.

[0118] S2: scanning the two-dimensional code shown on the two-dimensional code login interface by mobile phone. Specifically, in the embodiment of the present disclosure, the two-dimensional code is generated and sent to the computer to show by the server when the server receives the information of the two-dimensional code login of the terminal.

[0119] S3: determining whether the scanning is successful or not by mobile phone; if not scanning successfully, continue to execute the S2; if executing successfully, jump to the S4.

[0120] S4: determining whether the two-dimensional code is legal or not by mobile phone; if being the incorrect two-dimensional code, it is illegal and execute S5; if being legal, execute S6.

[0121] S5: prompting error information by mobile phone, such as showing the message that the two-dimensional code is incorrect.

[0122] Specifically, S1 to S5 above correspond to S101 in Fig. 1 or the S201 in the embodiment in Fig. 2.

[0123] S6: determining whether the present terminal has signed in the account of the application or not by mobile phone; if having not done, confirm the user logs in the application first time and execute S7; if having done, execute S9.

[0124] S7: calling and showing the interface of entering the account and password by mobile phone.

[0125] S8: generating the login information including the account and password when mobile phone receives the click login operation, and jumping to S16.

[0126] S9: determining whether the number of accounts which have signed in the application is more than one or not by mobile phone; if being more than one, execute S10; if being only one, directly execute S11.

[0127] S10: jumping to the account login choosing page on mobile phone, and choosing one login account therefrom by the user.

[0128] S11: determining whether to connect to the net at present or not by mobile phone; if not, execute S12; if yes, jump to S13.

[0129] S12: popping up to prompt that it has failed to connect to the net on mobile phone.

[0130] S13: determining whether the account which is confirmed to need to log in is out of the period of login validity duration or not by mobile phone, which can be determined by determining whether the distance between the last active time after the account has logged in to the present time reaches the time thresholds or not; if yes, the login is out of the period of validity duration; if being out of the period of validity duration, execute S14; if not being out of the period of validity duration, execute S16.

[0131] S14: showing the interface of entering the account and password by mobile phone.

Therein, acquiescently fill the account chosen and confirmed by the S10 in the interface, or fill the account information and password of the account when there is only one account.

[0132] S15: generating the login information including the account and password when mobile phone receives the click login operation, and jumping to S16.

[0133] Specifically, S9 to S15 above are corresponding to S202 to S204 in the embodiment in Fig. 2.

[0134] S16: determining whether the authentication to the account and password by the server is successful or not by mobile phone. That is, after the preceding server sends the login message, the server authenticates the account and password. If successful, return the response of successful login, according to which mobile phone determines whether the authentication is successful or not. If authenticating successfully, execute S18; otherwise, execute S17.

- [0135] S17: giving the prompt information according the failed situation by mobile phone, such as showing that the entered password is wrong and other prompt information.
- [0136] S16 to S17 are corresponding to S205 in the embodiment in Fig. 2.
- [0137] S18: showing the interface of confirming to log in by mobile phone. As the interface shown in Fig.5, the interface of confirming to log in is the security warning interface. S17 to S18 are corresponding to S206 in the embodiment in Fig. 2.
- [0138] S19: determining whether the user chooses to confirm to log in or not by mobile phone. If clicking to choose to log in, execute S21; otherwise, execute S20. The S19 corresponds to the S207 in the embodiment in Fig. 2.
- [0139] S20: sending the message of canceling the login by mobile phone, so that the server interrupts the present alternative terminal login operation.
- [0140] S21: sending the message of confirming the login by mobile phone, which makes the server access the opened application on the computer, and then the application on the computer successfully logs in.
- [0141] S20 to S21 correspond to the S208 in the embodiment in Fig. 2 .
- [0142] According to the graphic code, the embodiments of the present disclosure can provide the related information of the terminal which needs the login account to the other more secure and reliable terminals, such as user's phone and tablet frequently used, and so on. Communicating with the corresponding servers by the secure and reliable terminals and achieving alternative terminal login function by the secure and reliable terminals, that makes users not expose their account information to the computers when they log in the corresponding applications and games on the computers provided by the public places such as internet bars. It improves the security of the account login, protects the safety of the users' accounts better, and avoids losses caused by account information leakage.
- [0143] Hereinafter, the account login device and system according to the embodiments of the present disclosure will be described in detail.
- [0144] Fig. 9 shows an example structure schematic view of an account login system according to embodiments of the present disclosure. The system according to the embodiment of the present disclosure can include a user terminal 1, an alternative terminal 3, and a server 2. The User Terminal 1 may be user terminals having the photographing and scanning function, such as the smart phone, tablet and smart wearable devices. The Alternative terminal 3 may be configured like computers in the public places like internet cafes. The Server 2 may be the servers which can log in by account and are programmed to manage the applications such as instant communication applications, social network, games and so on.

[0145] The User Terminal 1 is programmed to scan the login graphic code displayed in the Alternative terminal 3 and obtaining the terminal identification and target application identification from the login graphic code. The User Terminal 1 is programmed to obtain the account information entered by the user and generating the alternative terminal login request to send the alternative terminal login request to the application server 2 which is indicated by the target application identification, where the alternative terminal login request includes the obtained account information and terminal identification.

[0146] The Application Server 2 is programmed to return the notification message of access permit to the Alternative terminal 3 indicated by the terminal identification in the alternative terminal login request after authenticating the account information in the received alternative terminal login request, so the alternative terminal logs in the target application using the account information.

[0147] Further optionally, the Alternative terminal 3 can generate the graphic code including the terminal identification and target application identification to show to the users according to the identifications such as IP address of itself as the terminal identification, and can also assign a unique terminal identification for the alternative terminal by the Server 2 through sending the graphic code login request to the Server 2, and generate the graphic code including the assigned identification and the target application identification to send to the Alternative terminal 3. The Alternative terminal 3 and Server 2 may further have the following functions:

[0148] The Alternative terminal 3 is programmed to initiate the graphic code login request to the Server 2 when it is detected that the user initiates the graphic code login operation in the user interface of the target application.

[0149] The Server 2 is further programmed to respond to the graphic code login request, assigning a unique identification for the Alternative terminal 3 and generating the login graphic code including the terminal identification and the target application identification to send to the Alternative terminal 3.

[0150] The Alternative terminal 3 is further programmed to display the login graphic code sent by the Server 2. The Alternative terminal 3 is programmed to generate the login graphic code according to the IP address of the alternative terminal and the target application identification and showing the login graphic code.

[0151] According to the graphic code, the embodiments of the present disclosure can provide the related information of the terminal which needs the login account to the other more secure and reliable terminals, such as user's phone and tablet frequently used, and so on. Communicating with the corresponding servers by the secure and reliable terminals and achieving alternative terminal login function by the secure and reliable terminals, that makes users not expose their account information to the computers when they log in the corresponding applications and games on the

computers provided by the public places such as internet bars. It improves the security of the account login, protects the safety of the users' accounts better, and avoids losses caused by account information leakage.

[0152] Fig. 10 shows an example structure schematic view of an account login device 1000 according to embodiments of the present disclosure. The device 1000 according to the embodiment of the present disclosure may be set in the smart phone, tablet, smart wearable devices and other user terminals. The device 1000 includes a hardware processor 1010 and a non-transitory storage medium 1020 configured to store a scanning module 11 and a processing module 12.

[0153] The scanning module 11 is programmed to scan the login graphic code displayed in the alternative terminal and obtaining the terminal identification and target application identification from the login graphic code. The processing module 12 is programmed to obtain the account information entered by the user and generating the alternative terminal login request to send the alternative terminal login request to the application server which is indicated by the target application identification; therein the alternative terminal login request carries the obtained account information and terminal identification. The alternative terminal login request is programmed to request the application server to return the notification message of access permit to the alternative terminal which is indicated by the terminal identification in the alternative terminal login request, so the alternative terminal logs in the target application using the account information.

[0154] The scanning module 11 may scan the login graphic code displayed in the alternative terminal by calling Photographing Module, and resolve the login graphic code to obtain the carried binary information thereof, and ultimately obtain the terminal identification and target application identification of the alternative terminal. The processing module 12 may confirm the corresponding application server to the application in the present login according to the target application identification thereof. For example, when it is confirmed as an instant communication application according to the target application identification, the corresponding instant communication application server can be confirmed according to the address of the type of built-in server of the instant communication application.

[0155] Optionally, the processing module 12 may use the following functional units to achieve it when executing the obtaining account information and the sending alternative terminal login request. The achieving process of each unit can specifically refer to the descriptions of the methods above correspondingly.

[0156] As shown in Fig. 11, the processing module 12 may include: a Detecting Unit 121, a Processing Unit 122, and a First Request Unit 123.

[0157] The detecting unit 121 is programmed to detect the history login account of the application which is indicated by the target application identification in the alternative terminal, and showing the detected history login account to users;

[0158] The processing unit 122 is programmed to confirm the username and password of the history login account chosen from the displayed history login accounts by the user as the account information entered by the user;

[0159] The first request unit 123 is programmed to generate the alternative terminal login request according to the confirmed account information entered by the user and the terminal identification; and sending the alternative terminal login request to the application server which is indicated by the target application identification.

[0160] Here, when implementing specifically, the processing unit 122 can optionally include the following functional subunits:

[0161] Time Detecting Subunit, programmed to detect whether the latest login time of the selected login account chosen by users in the displayed history login accounts has exceeded the preset validity duration or not;

[0162] First Validation Subunit, programmed to obtain the chosen username and password of the history login account directly as the account information entered by the user if it has not exceeded the preset validity duration;

[0163] Second Validation Subunit, programmed to display the interface including the username of the selected login account, obtaining the password entered by the user and confirming the username of the selected login account and the entered password as the account information entered by the user if it has exceeded the preset validity duration.

[0164] As shown in Fig. 12, the processing module 12 can specifically further include: a calling unit 124 and a second request unit 125.

[0165] The calling unit 124 is programmed to call the login box to obtain the account information entered by the user, therein the entered account information includes the username and password. The second request unit 125 is programmed to generate the alternative terminal login request according to the entered account information and terminal identification; sending the alternative terminal login request to the application server which is indicated by the target application identification.

[0166] As shown in Fig. 13, the Processing Module 12 may further include: an obtaining unit 126 and a third request unit 127.

[0167] The obtaining unit 126 is programmed to obtain the account information from the login graphic code, where the account information in the login graphic code is the account information entered in the target application login interface of the alternative terminal. The third request unit 127

is programmed to generate the alternative terminal login request according to the entered account information and terminal identification; sending the alternative terminal login request to the application server which is indicated by the target application identification.

[0168] To be noted, the processing module 12 of the account login device according to the embodiments of the present disclosure can specifically include the structures in the Fig. 11 to Fig. 13 at the same time according to the needs, and it can also include any one or two of the structures in the Fig. 11 to Fig. 13.

[0169] Further optionally, as shown in Fig. 10, the account login device according to the embodiment of the present disclosure may further include a prompt module 13 a judgment module 14, and a notification module 15.

[0170] The prompt module 13 is programmed to send the a security warning of whether allowing to log in the alternative terminal after receiving the prompt message of the successful validation which is returned by the application server responding to the alternative terminal login request.

[0171] The judgment module 14 is programmed to determine whether a confirming button in the security warning interface is clicked or not.

[0172] The notification module 15 is programmed to send the notice of confirming to sign in the account information in the alternative terminal which is indicated by the terminal identification in the alternative terminal login request to the application server if the judgment result of the judgment module is yes, which makes the application server return the notification message of access permit to the alternative terminal which is indicated by the terminal identification in the alternative terminal login request, so the alternative terminal logs in the target application using the account information.

[0173] The specific implementation of the prompt module 13, the judgment module 14, and the notification module 15 above can refer to the descriptions of the methods in the embodiments.

[0174] According to the graphic code, the embodiments of the present disclosure can provide the related information of the terminal which needs the login account to the other more secure and reliable terminals, such as user's phone and tablet frequently used, and so on. Communicating with the corresponding servers by the secure and reliable terminals and achieving alternative terminal login function by the secure and reliable terminals, that makes users not expose their account information to the computers when they log in the corresponding applications and games on the computers provided by the public places such as internet bars. It improves the security of the account login, protects the safety of the users' accounts better, and avoids losses caused by account information leakage.

[0175] Fig. 14 shows an example structure schematic view of another account login device 1400 according to embodiments of the present disclosure. The device 1400 according to the embodiment of the present disclosure can be set in all kinds of application servers and game servers. The device

1400 includes a hardware processor 1410 and a non-transitory storage medium 1420 accessible to the hardware processor. The non-transitory storage medium 1420 is configured to store modules including: a receiving module 21, an authentication module 22, and an access module 23.

[0176] The receiving module 21 is programmed to receive the alternative terminal login request sent by the user terminal; therein the alternative terminal login request carries the account information and terminal identification obtained by the user terminal. The authentication module 22 is programmed to authenticate the account information in the alternative terminal login request. The access module 23 is programmed to return the notification message of access permit to the alternative terminal indicated by the terminal identification in the alternative terminal login request after authenticating the account information, so the alternative terminal logs in the target application using the account information.

[0177] The alternative terminal login request received by the Receiving module 21 is programmed to request the application server to return the notification message of access permit to the alternative terminal which is indicated by the terminal identification in the alternative terminal login request, so the alternative terminal logs in the target application using the account information.

[0178] After receiving the alternative terminal login request, the server executes the alternative terminal login function by the Authentication module 22 and access module 23. While the Receiving module 21 receives the existing ordinary login request, executes the existing login act.

[0179] Optionally, the server may also reminder the user in the user terminal whether to confirm to log in the alternative terminal after the authentication is passed. In the embodiment of the present disclosure, as shown in Fig. 15, the access module 23 may include: an Authentication Prompt Unit 231 and an access unit 232.

[0180] The authentication prompt unit 231 is programmed to respond to the prompt message of the successful validation which is returned to the user terminal by the alternative terminal login request. The access unit 232 is programmed to return the notification message of access permit to the alternative terminal which is indicated by the terminal identification in the alternative terminal login request if receiving the notice of confirming to sign in the account information in the alternative terminal which is indicated by the terminal identification in the alternative terminal login request sent by the user terminal.

[0181] Further, when the Receiving module 21 receives the graphic code login request sent by the alternative terminal, the account login device may further include: an allocation module 24 and a sending module 25.

[0182] The allocation module 24 is programmed to assign a unique identification for the alternative terminal when receiving the graphic code login request of the alternative terminal and generating the graphic code including the unique identification and the target application

identification. The sending module 25 is programmed to return the generated graphic code to the alternative terminal.

[0183] According to the graphic code, the embodiments of the present disclosure can provide the related information of the terminal which needs the login account to the other more secure and reliable terminals, such as user's phone and tablet frequently used, and so on. Communicating with the corresponding servers by the secure and reliable terminals and achieving alternative terminal login function by the secure and reliable terminals, that makes users not expose their account information to the computers when they log in the corresponding applications and games on the computers provided by the public places such as internet bars. It improves the security of the account login, protects the safety of the users' accounts better, and avoids losses caused by account information leakage.

[0184] It's understood for person skilled in the art to accomplish whole or part of steps in the embodiments mentioned above by instructing the related hardware with program. Such program can be stored in a computer-readable storage medium, and can include the flow of the embodiments of all methods above when executing the program. The storage medium may include Disk, CD, Read Only Memory (ROM), Random Access Memory (RAM), etc.

Claims

1. An account login method, comprising:

scanning, by a terminal device, a login graphic code shown in an alternative terminal and obtaining a terminal identification and a target application identification from the login graphic code;

obtaining, by the terminal device, account information in the terminal device and generating an alternative terminal login request to send the alternative terminal login request to an application server that is indicated by the target application identification, wherein the alternative terminal login request comprises the account information and the terminal identification; and

requesting, by the terminal device, the application server to return a notification message of access permit to the alternative terminal, so that the alternative terminal logs in a target application using the account information.

2. The method according to claim 1, further comprising at least one of the following:

obtaining, from the application server, the login graphic code that comprises a first graphic code comprising the terminal identification and the target application identification after the alternative terminal initiates a graphic code login request to the application server corresponding to the target application, and

generating, by the alternative terminal, the login graphic code that comprises a second graphic code according to an IP address of the alternative terminal and the target application identification.

3. The method according to claim 1, wherein obtaining the account information and generating the alternative terminal login request to send the alternative terminal login request to the application server comprises:

detecting, by the terminal device, a history of login accounts of the application in the terminal device, and displaying the detected history of login accounts;

obtaining, by the terminal device, a selection of one of the login accounts and confirming a selected username and a corresponding password of the selected login account as the account information;

generating, by the terminal device, the alternative terminal login request according to the account information and the terminal identification; and

sending, by the terminal device, the alternative terminal login request to the application server that is indicated by the target application identification.

4. The method according to claim 3, wherein obtaining a selection of one of the login accounts and confirming the selected username and password of the selected login account as the account information comprises:

detecting whether a latest login time of the selected login account has exceeded a preset validity duration;

if it has not exceeded the preset validity duration, obtaining the corresponding username and password of the selected login account directly as the account information; and

if it has exceeded the preset validity duration, displaying an interface including the username of the selected login account, obtaining the password entered by a user and confirming the username of the selected login account and the entered password as the account information.

5. The method according to claim 1, wherein obtaining the account information and generating the alternative terminal login request to send the alternative terminal login request to the application server comprises:

calling a login box to obtain the account information entered by a user, wherein the entered account information comprises a username a password;

generating the alternative terminal login request according to the entered account information and terminal identification; and

sending the alternative terminal login request to the application server that is indicated by the target application identification.

6. The method according to any one of claim 1 to claim 5, further comprising:

sending a security warning of allowing to log in the alternative terminal after receiving a prompt message of a successful validation that is returned by the application server responding to the alternative terminal login request;

determining whether a confirming button in the security warning has been clicked; and

if the confirming button is clicked, sending the application server a notice that confirms to log in the alternative terminal using the account information, which makes the application server return the notification message of access permit to the alternative terminal so that the alternative terminal logs in the target application using the account information.

7. An account login method, comprising:

receiving, by a server, an alternative terminal login request sent by a user terminal, wherein the alternative terminal login request comprises account information and a terminal identification;

authenticating, by the server, the account information in the alternative terminal login request;
and

returning, by the server, a notification message of access permit to an alternative terminal indicated by the terminal identification in the alternative terminal login request, so that the alternative terminal logs in a target application using the account information.

8. The method according to claim 7, further comprising:

assigning a unique identification for the alternative terminal when receiving a graphic code login request of the alternative terminal and generating the graphic code comprising the unique identification and a target application identification; and
returning the generated graphic code to the alternative terminal.

9. The method according to claim 7 or claim 8, wherein returning the notification message of access permit to the alternative terminal comprises:

responding to the alternative terminal login request to return a prompt message of a successful validation to the user terminal; and

if receiving a notice of confirming to sign in the account information in the alternative terminal sent by the user terminal, returning the notification message of access permit to the alternative terminal.

10. An account login method, comprising:

scanning, by a user terminal, a login graphic code displayed in an alternative terminal and obtaining a terminal identification and a target application identification from the login graphic code;
obtaining, by the user terminal, account information and generating an alternative terminal login request;

sending, by the user terminal, the alternative terminal login request to an application server that is indicated by the target application identification, wherein the alternative terminal login request comprises the account information and the terminal identification; and

receiving, by the user terminal, a notification message of access permit to the alternative terminal from the application server after the account information is authenticated, so that the alternative terminal logs in a target application using the account information.

11. An account login device, comprising a hardware processor and a non-transitory storage medium accessible to the hardware processor, the non-transitory storage medium configured to store modules comprising:

a scanning module, programmed to scan a login graphic code displayed in an alternative terminal and obtaining a terminal identification and a target application identification from the login graphic code; and

a processing module, programmed to obtain account information and generating an alternative terminal login request to send the alternative terminal login request to an application server that is indicated by the target application identification; wherein the alternative terminal login request comprises the account information and the terminal identification;

wherein the alternative terminal login request is programmed to request the application server to return the notification message of access permit to the alternative terminal that is indicated by the terminal identification, so that the alternative terminal logs in the target application using the account information.

12. The device according to claim 11, wherein the processing module comprises:

a detecting unit, programmed to detect a history of login accounts of the application that is indicated by the target application identification, and displaying the history of login account to users in the account login device;

a processing unit, programmed to obtain a selection of one of the login accounts and confirm a selected username and a corresponding password of the selected login account as the account information; and

a first request unit, programmed to generate the alternative terminal login request according to the account information and the terminal identification; and sending the alternative terminal login request to the application server that is indicated by the target application identification.

13. The device according to claim 12, wherein the processing unit comprises:

a time detecting subunit, programmed to detect whether a login time of the selected login account has exceeded a preset validity duration or not;

a first validation subunit, programmed to obtain a username and a password of the selected login account directly as the account information if it has not exceeded the preset validity duration; and

a second validation subunit, programmed to display an interface including the username of the selected login account, obtaining the password entered by the user and confirming the username of the selected login account and the entered password as the account information if it has exceeded the preset validity duration.

14. The device according to claim 12, wherein the processing unit comprises:

a calling unit, programmed to call a login box to obtain the account information entered by the user, wherein the entered account information includes the username and password; and

a second request unit, programmed to generate the alternative terminal login request according to the account information and terminal identification; sending the alternative terminal login request to the application server that is indicated by the target application identification.

15. The device according to any one of claim 11 to claim 14, comprising:

a prompt module, programmed to send a security warning of allowing to log in the alternative terminal after receiving a prompt message of a successful validation that is returned by the application server responding to the alternative terminal login request;

a judgment module, programmed to determine whether a confirming button in the security warning has been clicked; and

a notification module, programmed to send a notice of confirming to log in the alternative terminal to the application server if the confirming button is clicked, which makes the application server return the notification message of access permit to the alternative terminal, so that the alternative terminal logs in the target application using the account information.

16. An account login device, comprising a hardware processor and a non-transitory storage medium accessible to the hardware processor, the non-transitory storage medium configured to store modules comprising:

a receiving module, programmed to receive an alternative terminal login request sent by a user terminal, wherein the alternative terminal login request comprises account information and a terminal identification obtained by the user terminal;

an authentication module, programmed to authenticate the account information in the alternative terminal login request; and

an access module, programmed to return a notification message of access permit to the alternative terminal indicated by the terminal identification, so that the alternative terminal logs in a target application using the account information.

17. The device according to claim 16, further comprising:

an allocation module, programmed to assign a unique identification for the alternative terminal when receiving a graphic code login request of the alternative terminal and generating the graphic code comprising the unique identification and a target application identification that identifies the target application; and

a sending module, programmed to return the generated graphic code to the alternative terminal.

18. The device according to claim 16 or claim 17, wherein the access module comprises:

an authentication prompt unit, programmed to respond to the alternative terminal login request and return a prompt message of a successful validation to the user terminal; and

an access unit, programmed to return the notification message of access permit to the alternative terminal if receiving a notice of confirming to log in the alternative terminal.

19. An account login system, comprising: an alternative terminal, a user terminal, and an application server, wherein:

the user terminal is programmed to scan a login graphic code displayed in the alternative terminal, and obtaining a terminal identification and a target application identification from the login graphic code;

the user terminal is programmed to obtain account information and generating an alternative terminal login request to send the alternative terminal login request to the application server, wherein the alternative terminal login request comprises the account information and the terminal identification;

the application server is programmed to return a notification message of access permit to the alternative terminal indicated by the terminal identification after authenticating the account information in the received alternative terminal login request, so that the alternative terminal logs in a target application using the account information.

20. The system according to claim 19, wherein:

the alternative terminal is programmed to initiate a graphic code login request to the application server when it is detected that a user initiates a graphic code login operation in a user interface of the target application;

the application server is further programmed to respond to the graphic code login request, assigning a unique identification for the alternative terminal and generating the login graphic code comprising the terminal identification and the target application identification to send to the alternative terminal; and

the alternative terminal is further programmed to display the login graphic code sent by the server.

21. The system according to claim 19, wherein the alternative terminal is programmed to generate the login graphic code according to an IP address of the alternative terminal and the target application identification, and displaying the login graphic code.

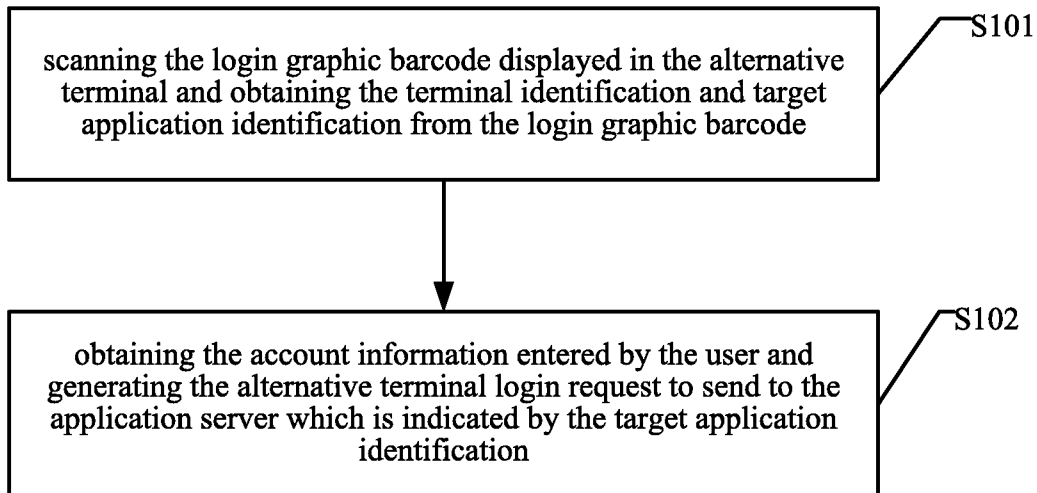


Fig. 1

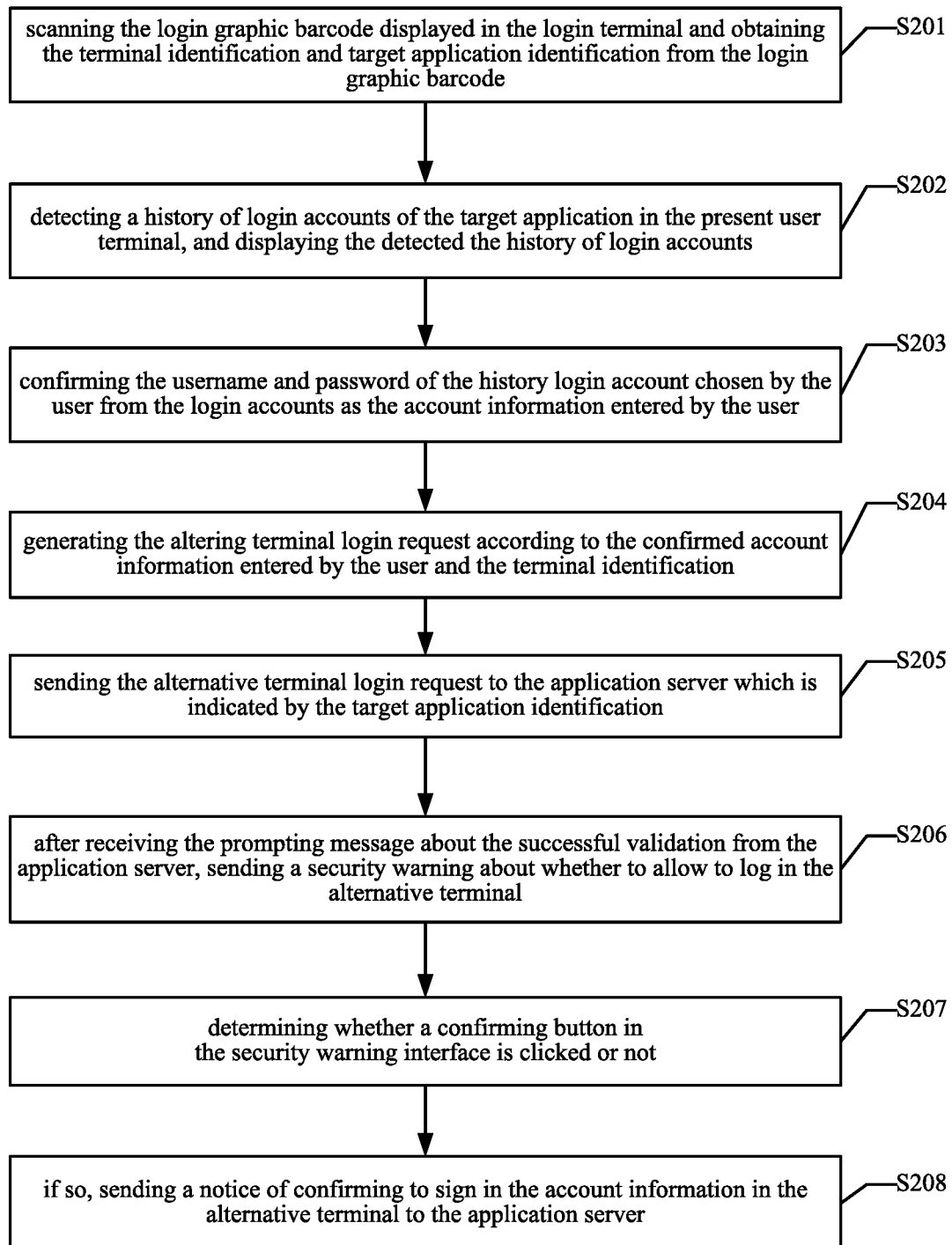


Fig. 2

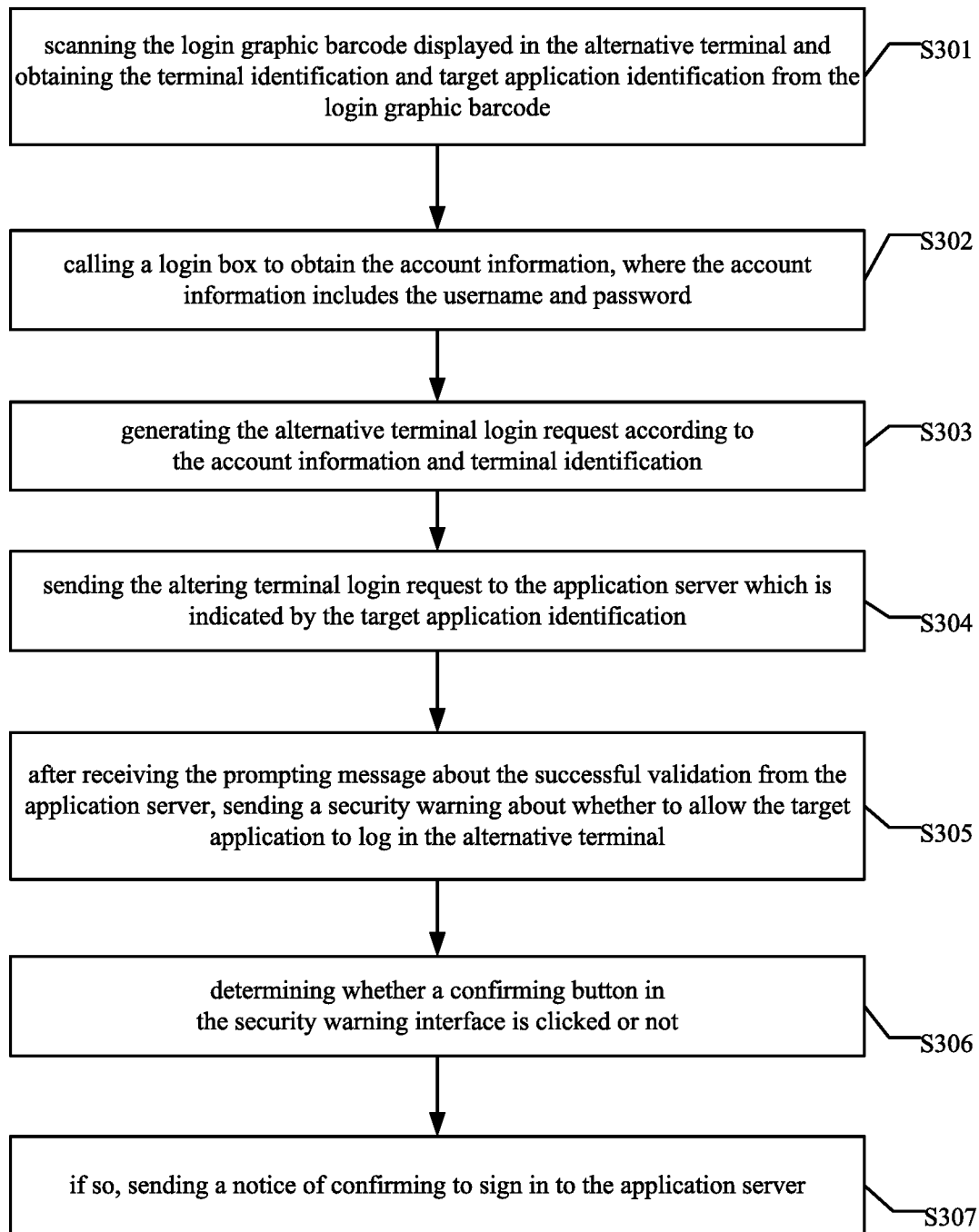


Fig. 3

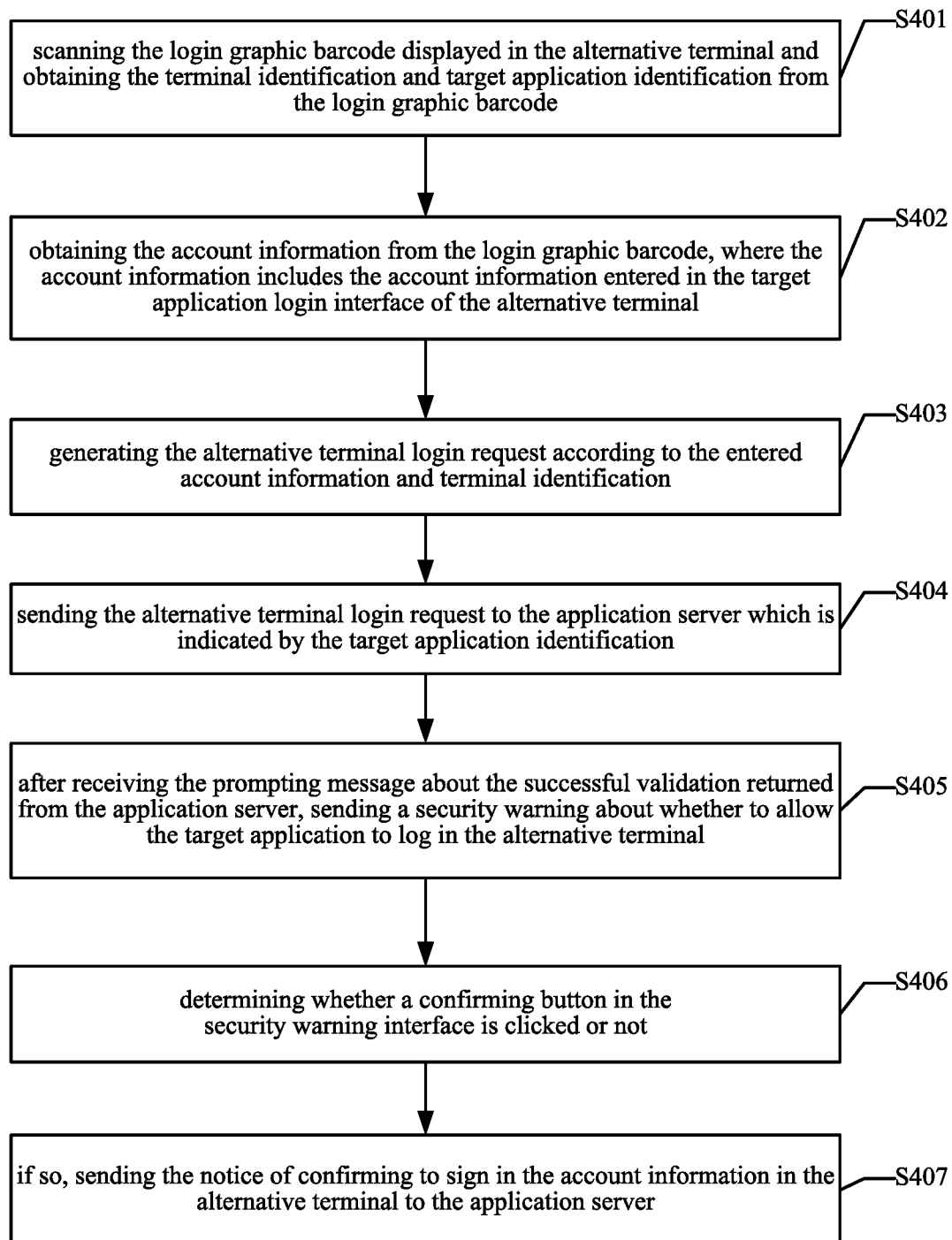


Fig. 4

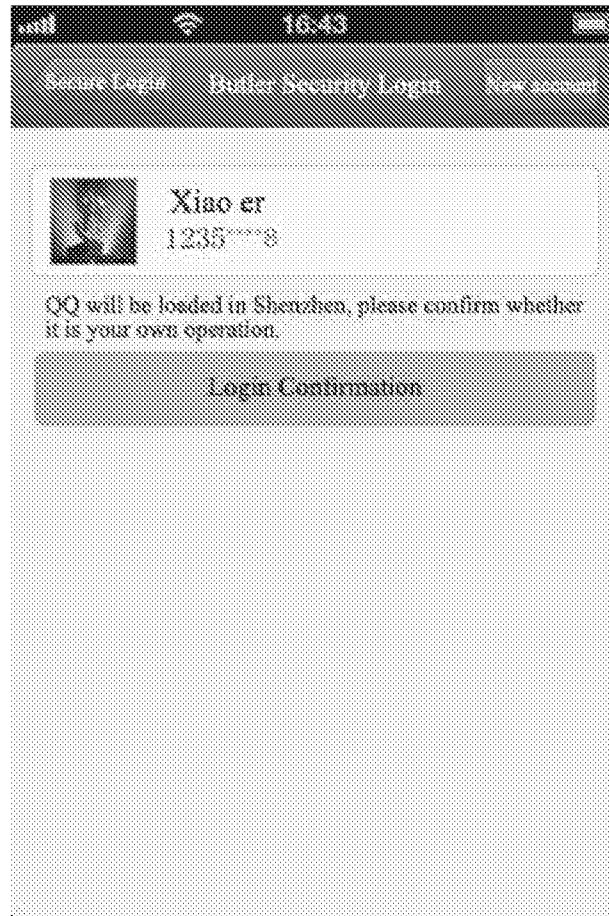


Fig. 5

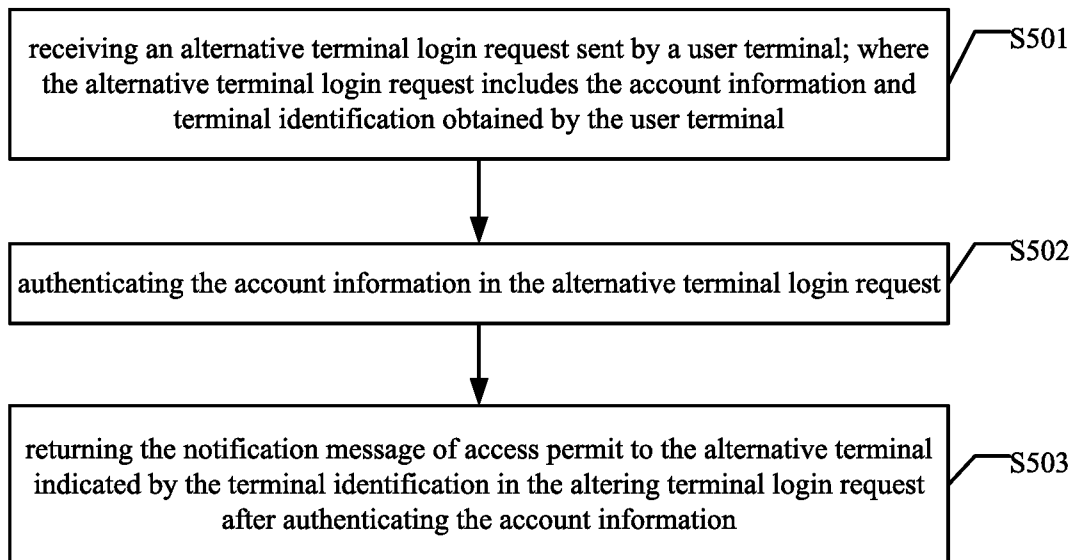


Fig. 6

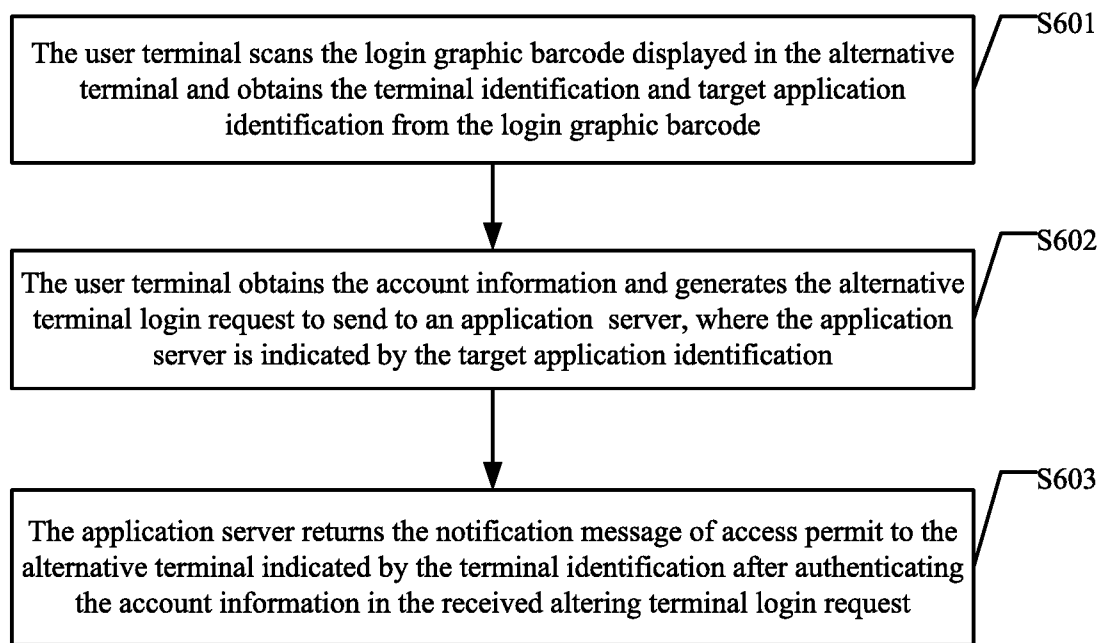


Fig. 7

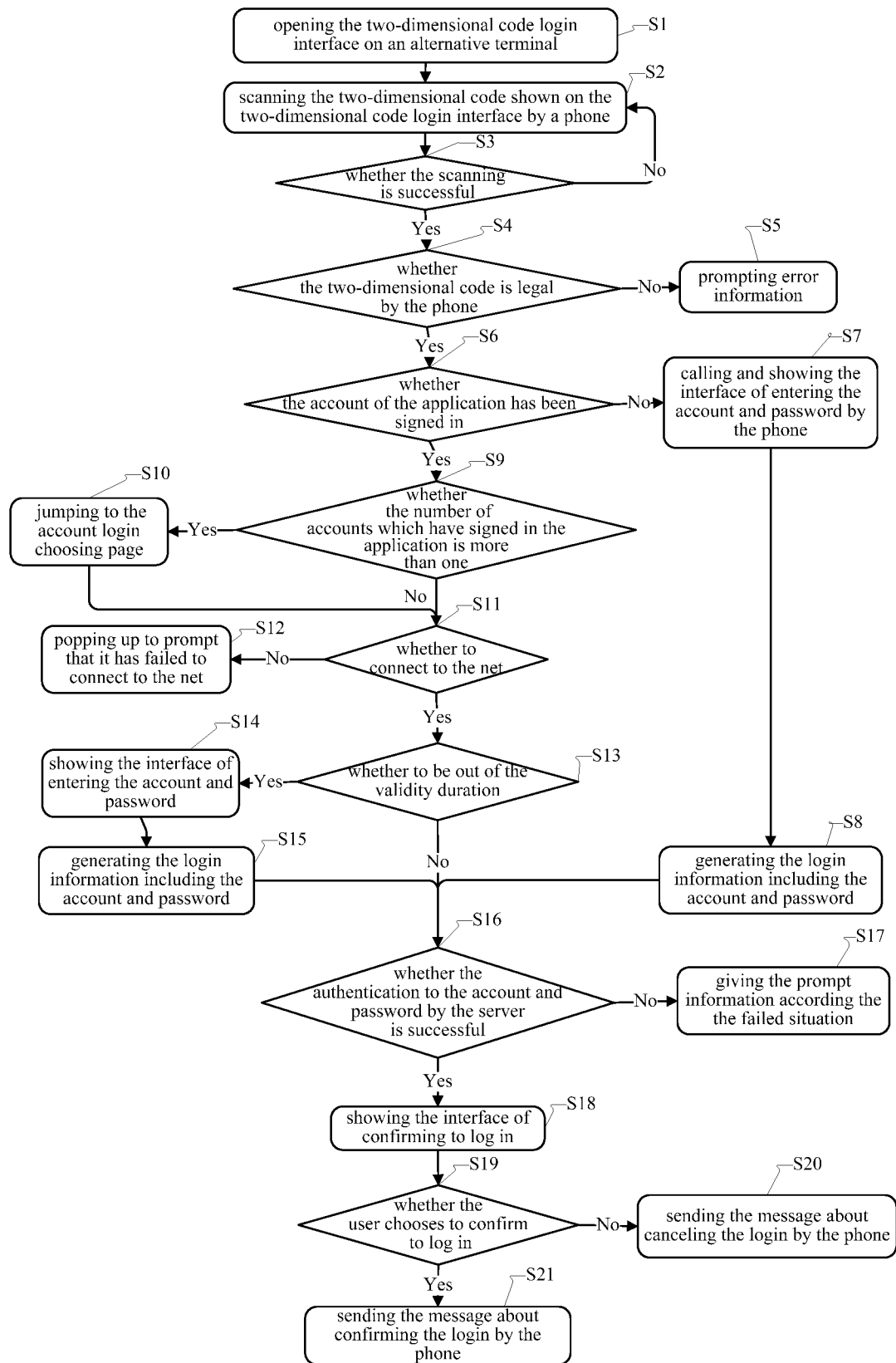


Fig. 8

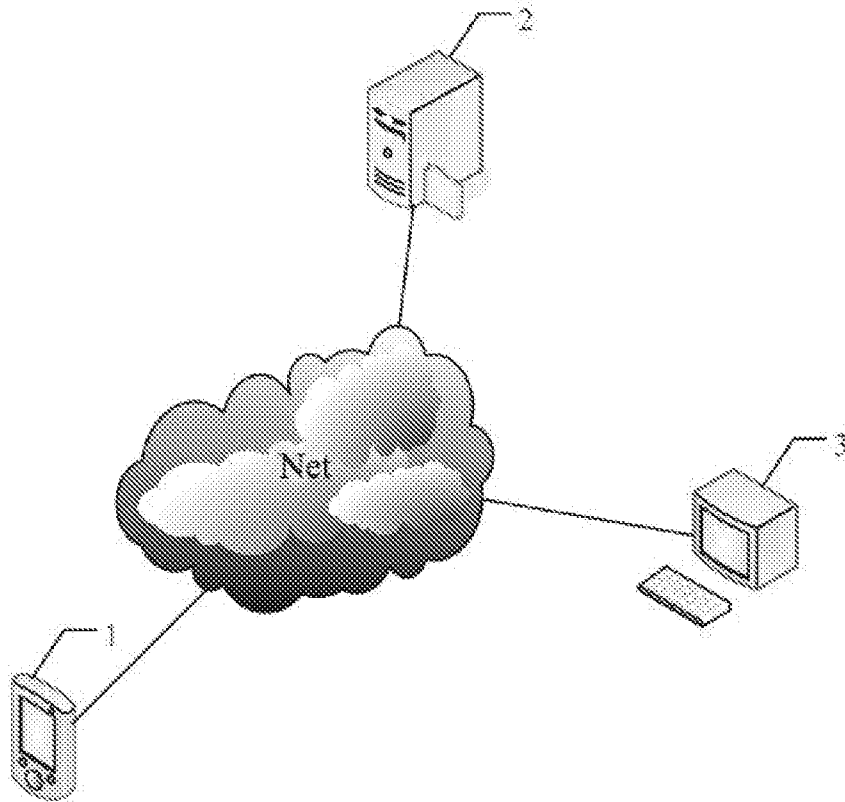


Fig. 9

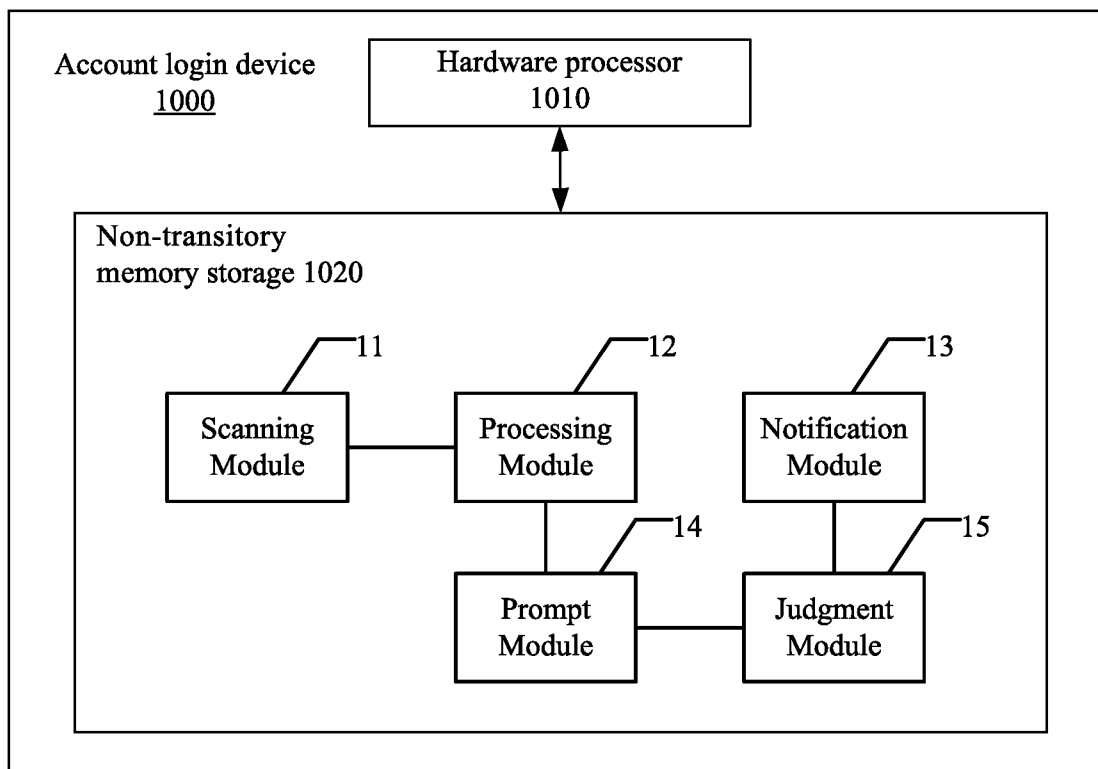


Fig. 10

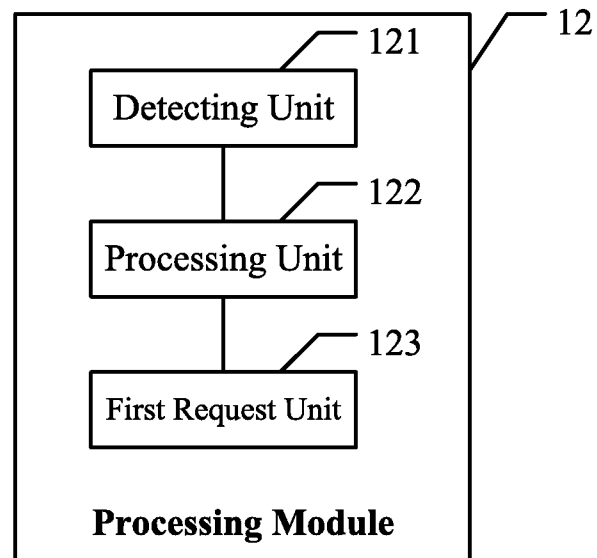


Fig. 11

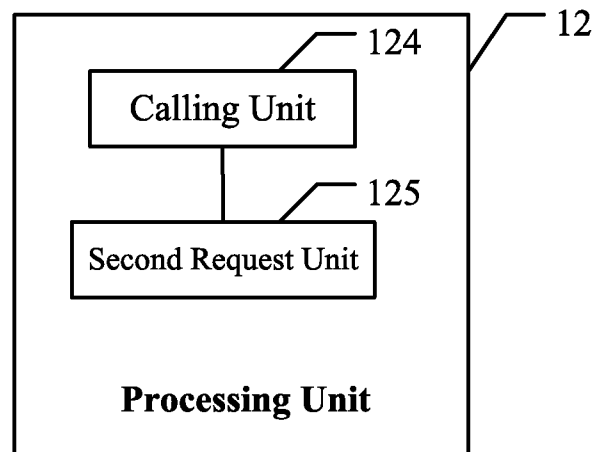


Fig. 12

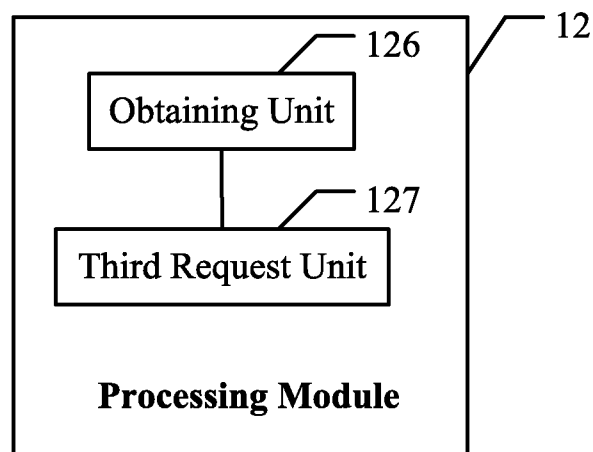


Fig. 13

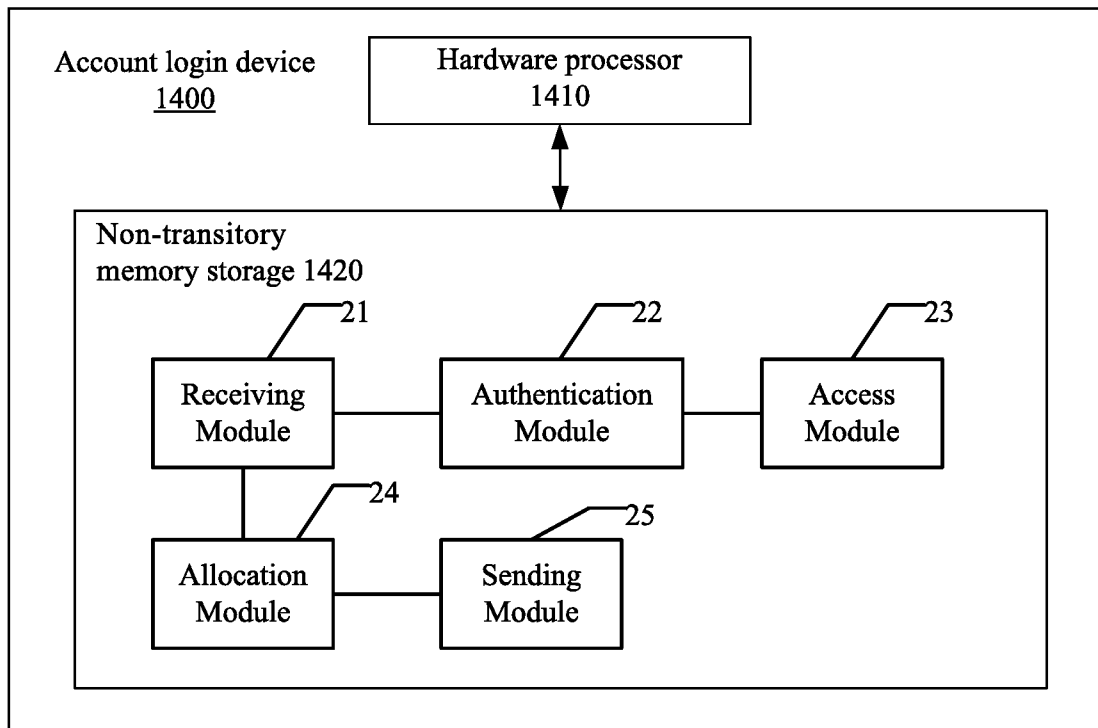


Fig. 14

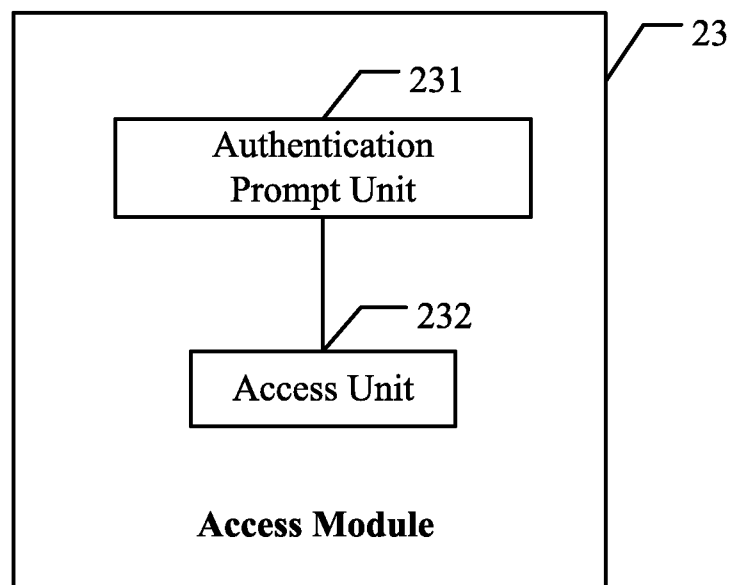


Fig. 15

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/086122

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(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

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)

CPRSABS,CNTXT,VEN,CNKI:two dimension+ code, graphic, code, login, log in, secur+, authenticat+, alternative terminal, second, terminal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103001973 A (BAIDU ON-LINE NETWORK TECHNOLOGY CO., LTD.) 27 March 2013 (2013-03-27) see description, paragraphs 50-131, figures 1-5	1-21
X	CN 103067378 A (BAIDU ON-LINE NETWORK TECHNOLOGY CO., LTD.) 24 April 2013 (2013-04-24) see description, paragraphs 36-117, figures 1-4	1-21
A	CN 1987888 A (CHINA MOBILE COMMUNICATION GROUP CORP.) 27 June 2007 (2007-06-27) the whole document	1-21



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

01 December 2014

Date of mailing of the international search report

10 December 2014

Name and mailing address of the ISA/CN

STATE INTELLECTUAL PROPERTY OFFICE OF THE
P.R.CHINA(ISA/CN)
6,Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088 China

Authorized officer

PANG, Yan

Facsimile No. (86-10)62019451

Telephone No. (86-10)62089462

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2014/086122

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)		Publication date (day/month/year)
CN	103001973	A	27 March 2013	Non	e	
CN	103067378	A	24 April 2013	Non	e	
CN	1987888	A	27 June 2007	CN	1987888	B 13 April 2011