CROSS-TERMINAL LOGIN-FREE METHOD AND DEVICE

Technical field

The present application relates to the field of computers, and in particular, to a cross-terminal login-free method and device.

Background art

Nowadays, a terminal user usually has multiple terminal devices or multiple types of terminal devices, such as multiple mobile phones, multiple PADs, or multiple computers. When switching from one terminal device to another terminal device to log into an account, a user needs to reenter an account and a password for login, which is not only inconvenient but also prone to error.

In the prior art, a method for implementing automatic login across terminal devices is as follows: if a user who uses a computer for login switches to another terminal device for login, a login web page on the computer generates a QR code including an account and a password. The user scans the QR code by using an APP such as Wechat capable of scanning QR codes. After the scanning, the terminal device to which the user switches logs into the account automatically.

During implementation of the present application, the inventor finds that the prior art has at least the following problems:

The login-free method in the prior art is relative troublesome, and it requires a terminal device to open an APP capable of scanning and find the corresponding scanning function to scan a QR code. If the terminal device does not have an APP capable of scanning a QR code, automatic login cannot be realized. Besides, if the QR code is acquired by others, it threatens the security of the user's account.

Summary of the Invention

The objective of the present invention is to provide a cross-terminal login-free method and device. A server queries a relationship of unique identification information between a terminal device that is logging in at a login IP address and a terminal device that has successfully logged in at the same login IP address and a relationship between the unique identification information

and a user login ID of the terminal device that has logged in successfully, so that the terminal device logs in automatically.

A cross-terminal login-free method, which includes:

acquiring, by a server, a login request that is sent by a terminal device and carries unique identification information and a login Internet Protocol (IP) address of the terminal device;

querying, by the server according to the IP address in the login request, whether there exists a terminal device that has logged in successfully at the same IP address in server-stored corresponding relationships among unique identification information, login IP addresses, and user login identities (IDs) of terminal devices that have logged in successfully;

if yes, querying, by the server, whether a corresponding relationship of unique identification information between the terminal device sending the login request and the terminal device that has logged in successfully exists in server-stored corresponding relationships of unique identification information between terminal devices according to the unique identification information in the login request; and

if yes, sending, by the server to a browser corresponding to a current login page of the terminal device, a data cookie corresponding to a user login ID of the terminal device that has logged in successfully, so that the terminal device logs in automatically.

The step of acquiring, by a server, a login request that is sent by a terminal device and carries unique identification information and a login IP address of the terminal device specifically includes:

acquiring, by the server, the login request that is sent by the terminal device when accessing the login page and carries the unique identification information and the login IP address of the terminal device, the unique identification information and the login IP address of the terminal device being acquired by the login page by calling, with JavaScript (JS), a FLASH tool plug-in of the current login page.

A cross-terminal login-free method, which includes:

sending, by a terminal device when accessing a login page, a login request carrying unique

identification information and a login IP address of the terminal device to a server; and

acquiring, by the terminal device, a query result that is obtained by the server according to the login request and includes a user login ID of a terminal device that has logged in successfully, so that the terminal device logs in according to the query result.

The step of sending, by a terminal device when accessing a login page, a login request carrying unique identification information and a login IP address of the terminal device to a server specifically includes:

adding, by the terminal device when accessing the login page, the unique identification information and the login IP address of the terminal device to the login request and sending the login request to the server, the unique identification information and the login IP address of the terminal device being acquired by the login page by calling, with JS, a software FLASH tool plug-in of the current login page.

The terminal device logs in according to the query result and specifically includes:

the terminal device automatically logs in by using a data cookie which is in a browser corresponding to the current login page and is corresponding to the user login ID of the terminal device that has logged in successfully, the user login ID being obtained according to the query result and sent by the server.

A server, which includes:

an acquisition module configured to acquire a login request that is sent by a terminal device and carries unique identification information and a login Internet Protocol (IP) address of the terminal device;

a first query module configured to query, according to the IP address in the login request, whether there exists a terminal device that has logged in successfully at the same IP address in server-stored corresponding relationships among unique identification information, login IP addresses, and user login identities (IDs) of terminal devices that have logged in successfully;

a second query module configured to: if yes, query whether a corresponding relationship of unique identification information between the terminal device sending the login request and the

terminal device that has logged in successfully exists in server-stored corresponding relationships of unique identification information between terminal devices according to the unique identification information in the login request; and

a sending module configured to: if yes, send, to a browser corresponding to a current login page of the terminal device, a data cookie corresponding to a user login ID of the terminal device that has logged in successfully, so that the terminal device logs in automatically.

The acquisition module is specifically configured to:

acquire the login request that is sent by the terminal device when accessing the login page and carries the unique identification information and the login IP address of the terminal device, the unique identification information and the login IP address of the terminal device being acquired by the login page by calling, with JavaScript (JS), a FLASH tool plug-in of the current login page.

A terminal device, which includes:

a sending module configured to send, when the terminal device accesses a login page, a login request carrying unique identification information and a login IP address of the terminal device to a server; and

an acquisition module configured to acquire a query result that is obtained by the server according to the login request and includes a user login ID of a terminal device that has logged in successfully, so that the terminal device logs in according to the query result.

The sending module is specifically configured to:

when the login page is accessed, add the unique identification information and the login IP address of the terminal device to the login request and send the login request to the server, the unique identification information and the login IP address of the terminal device being acquired by the login page by calling, with JS, a software FLASH tool plug-in of the current login page.

The terminal device logs in according to the query result and specifically includes:

the terminal device automatically logs in by using a data cookie which is in a browser corresponding to the current login page and is corresponding to the user login ID of the terminal

device that has logged in successfully, the user login ID being obtained according to the query result and sent by the server.

Compared with the prior art, the embodiments of the present application have at least the following advantages:

In the present application, according to server-stored corresponding relationships of unique identification information between terminal devices and a corresponding relationship, which is stored after a terminal device logs in successfully, among a login IP address, unique identification information, and a user login ID of the terminal device, the server queries, by using a login IP and unique identification information of a terminal device that is currently logging in, a corresponding relationship between unique identification information of a terminal device that has successfully logged in at the login IP and the unique identification information of the terminal device, to determine whether the terminal device that is currently logging in is related to the terminal device that has logged in successfully. If yes, the terminal device that is currently logging in acquires the user login ID of the terminal device that has logged in successfully, so as to log in automatically. In this way, the login process of a terminal device that carries out cross-terminal login is simple, and the terminal device that carries out login does not need to have particular software or hardware, thus reducing requirement limits on a terminal for cross-terminal login. Meanwhile, the terminal device that carries out login should have a same login IP address with a terminal device that has successfully logged in, thereby guaranteeing security of user information.

Brief Description of the Drawings

FIG. 1 is a first flowchart of a cross-terminal login-free method according to an embodiment of the present application;

FIG. 2 is a second flowchart of a cross-terminal login-free method according to an embodiment of the present application;

FIG. 3 is a schematic diagram of a login-free process according to an embodiment of the present application;

FIG. 4 is a schematic structural diagram of a server according to an embodiment of the present application; and

FIG. 5 is a schematic structural diagram of a terminal device according to an embodiment of the present application.

Detailed Description of the Embodiments

In the present application, a server queries a relationship of unique identification information between a terminal device that logs in at a login Internet Protocol (IP) address and a terminal device that has successfully logged in at the same login IP address and a relationship between the unique identification information and a user login identity (ID) of the terminal device that has successfully logged in, so that the terminal device logs in automatically.

The technical solutions in the present application are clearly and completed described with reference to the accompanying drawings in the present application. Apparently, the described embodiments are merely some of rather than all embodiments of the present application. All other embodiments obtained by those of ordinary skill in the art on the basis of the embodiments in the present application without paying creative efforts belong to the protection scope of the present application.

FIG. 1 shows a first embodiment of a cross-terminal login-free method according to the present application. The method includes:

Step 101: A server acquires a login request that is sent by a terminal device and carries unique identification information and a login IP address of the terminal device.

The unique identification information may be a Media Access Control (MAC) address, or may be other exclusive identification information of the terminal device. For example, when the terminal device is a mobile terminal such as a mobile phone, the exclusive identification information thereof may be an International Mobile Equipment Identification Number (IMEI) or an International Mobile Subscriber Identification Number (IMSI), or the like. When the terminal device is a fixed terminal such as a desktop computer, the exclusive identification information thereof may be an ID number of a piece of hardware thereof.

The step of acquiring, by a server, a login request that is sent by a terminal device and carries unique identification information and a login IP address of the terminal device specifically includes:

acquiring, by the server, the login request that is sent by the terminal device when accessing the login page and carries the unique identification information and the login IP address of the terminal device, the unique identification information and the login IP address of the terminal device being acquired by the login page by calling, with JavaScript (JS), a FLASH tool plug-in of the current login page.

Step 102: The server queries, according to the IP address in the login request, whether there exists a terminal device that has logged in successfully at the same IP address in server-stored corresponding relationships among unique identification information, login IP addresses, and user login IDs of terminal devices that have logged in successfully; if yes, step 103 is performed; otherwise, the process is ended.

The server queries whether IP addresses of the terminal device that is currently logging in and the terminal device that has successfully logged in are the same, so as to prove whether the terminal devices are terminal devices in a same local area network, thus guaranteeing the security of user login information.

Step 103: The server queries whether a corresponding relationship of unique identification information between the terminal device sending the login request and the terminal device that has logged in successfully exists in server-stored corresponding relationships of unique identification information between terminal devices according to the unique identification information in the login request; if yes, step 104 is performed; otherwise, the process is ended.

If the corresponding relationship exists, it indicates that there exists a terminal device that has successfully logged in at the same login IP address, and the terminal device that is currently logging in may automatically log in by using the user login ID during login of the terminal device that has successfully logged in. Before the login, it is further necessary to query whether there is a corresponding relationship between the unique identification information of the

terminal device that is currently logging in and the unique identification information of the terminal device that has successfully logged in. If yes, it indicates that the terminal devices are different terminal devices of a same user, or terminal devices associated with each other; if no, it indicates that the terminal devices are merely terminal devices of different users in a same local area network, or terminal devices that are not associated with each other.

When a terminal device logs in successfully, the server may store, in the form of a corresponding relationship, unique identification information, a login IP address and a user login ID of the terminal device that logs in successfully.

Corresponding relationships between unique identification information of different terminal devices stored by the server may be obtained in the following manners:

Manner 1:

A user sends unique identification information of his/her terminal device to a server. The server generates a QR code and sends the QR code to another terminal device, so that the terminal device acquires unique identification information of the other device. Alternatively, the terminal device generates a QR code from its own unique identification information and then sends the QR code to another terminal device, and the terminal device sends a corresponding relationship between unique identification information of the different terminal devices to the server.

Manner 2:

A user connects different terminal devices by means of Bluetooth. A terminal device acquires unique identification information of another terminal device, and sends a corresponding relationship between its own unique identification information and the unique identification information of the other terminal device to a server.

Manner 3: A terminal device sends its own unique identification information to a Near Field Communication (NFC) device, which sends a corresponding relationship of unique identification information between terminal devices to a server. Certainly, the terminal device may also send its own unique identification information to another device, which sends a corresponding

relationship of unique identification information between the terminal devices to the server.

Step 104: The server sends, to a browser corresponding to a current login page of the terminal device, a data cookie corresponding to a user login ID of the terminal device that has logged in successfully, so that the terminal device logs in automatically.

FIG. 2 shows a second embodiment of a cross-terminal login-free method according to the present application. The method includes:

Step 201: When accessing a login page, a terminal device sends a login request carrying unique identification information and a login IP address of the terminal device to a server.

When opening a login page in a browser thereof, the terminal device may automatically send a login request that carries unique identification information and a login IP address of the terminal device to a server, so that the terminal device automatically logs in according to a user login ID of another terminal device that has logged in successfully at the same login IP.

The step of sending, by a terminal device when accessing a login page, a login request carrying unique identification information and a login IP address of the terminal device to a server specifically includes:

adding, by the terminal device when accessing the login page, the unique identification information and the login IP address of the terminal device to the login request and sending the login request to the server, the unique identification information and the login IP address of the terminal device being acquired by the login page by calling, with JS, a software FLASH tool plug-in of the current login page.

Step 202: The terminal device acquires a query result that is obtained by the server according to the login request and includes a user login ID of a terminal device that has logged in successfully, so that the terminal device logs in according to the query result.

Specifically, after receiving the login request that is sent by the terminal device and carries the unique identification information and the login IP, the server queries, according to the IP address, whether there exists a terminal device that has logged in successfully at the same IP address. If yes, the server further queries whether a corresponding relationship between the

unique identification information of the terminal device that is currently logging in and the unique identification information of the terminal device that has logged in successfully exists in server-stored corresponding relationships between unique identification information of different terminal devices. If yes, it indicates that the terminal device currently logging in and the terminal device that has logged in successfully are different terminal devices of a same user. According to the found unique identification information of the terminal device that has logged in successfully, the server finds a user login ID of the user who has logged in successfully, so that the terminal device currently logging in automatically logs in according to the user login ID.

The terminal device logs in according to the query result and specifically includes:

The terminal device automatically logs in by using a data cookie which is in a browser corresponding to the current login page and is corresponding to the user login ID of the terminal device that has logged in successfully, the user login ID being obtained according to the query result and sent by the server.

Compared with the prior art, the embodiments of the present application have at least the following advantages:

In the present application, according to server-stored corresponding relationships of unique identification information between terminal devices and a corresponding relationship, which is stored after a terminal device logs in successfully, among a login IP address, unique identification information, and a user login ID of the terminal device, the server queries, by using a login IP and unique identification information of a terminal device that is currently logging in, a corresponding relationship between unique identification information of a terminal device that has successfully logged in at the login IP and the unique identification information of the terminal device, to determine whether the terminal device that is currently logging in is related to the terminal device that has logged in successfully. If yes, the terminal device that is currently logging in acquires the user login ID of the terminal device that has logged in successfully, so as to log in automatically. In this way, the login process of a terminal device that carries out cross-terminal login is simple, and the terminal device that carries out login does not need to have

particular software or hardware, thus reducing requirement limits on a terminal for cross-terminal login. Meanwhile, the terminal device that carries out login should have a same login IP address with a terminal device that has successfully logged in, thereby guaranteeing security of user information.

To further illustrate the technical idea of the present application, the technical solution of the present application is described in combination with a specific application scenario. In an actual application, changes in specific scenarios do not affect the protection scope of the present application.

Specifically, it is assumed that a user has two terminal devices. One is a mobile terminal: a mobile phone, and the other is a fixed terminal: a computer.

First, a corresponding relationship between the terminal devices is established. The user is ready to login by using the computer. A current login page acquires a MAC address of the computer through a set FLASH tool plug-in and sends the MAC address to a server. The server generates a QR code according to the MAC address and issues the QR code to the computer. The user scans the QR code by using the mobile phone, to acquire the MAC address of the computer. The mobile phone sends its own MAC address and the acquired MAC address of the computer to the server. The server establishes a corresponding relationship according to the MAC address of the mobile phone and the MAC address of the computer.

FIG. 3 shows a schematic diagram of a computer login-free process during cross-terminal login. By means of an APP in a mobile phone, a user logs in to a website corresponding to the APP. After the login succeeds, the mobile phone sends its own MAC address, a login IP address of the mobile phone, and a login ID of the user to a server. The server saves the information.

The computer uses a browser to open an access login page of the corresponding website that the APP of the mobile phone logs on to. The login page of the website invokes FLASH of the current page by using JS, to acquire a MAC address and a login IP address of the computer, and sends the MAC address and the login IP address of the computer to the server. The server searches, according to the login IP address of the computer, whether there exists a terminal

device that logs in successfully at the same IP address. If the IP address of the mobile phone is the same as the IP address of the computer, it indicates that the mobile phone and the computer are connected to a network at a same port in a same local area network. The server searches for a login MAC address of the mobile phone according to the IP address of the mobile phone, and determines, according to the MAC address of the computer, whether there is a corresponding relationship between the MAC address of the computer and the MAC address of the mobile phone. If yes, it indicates that the mobile phone and the terminal are terminal devices of a same user or terminal devices associated with each other. The server finds, according to the MAC address of the mobile phone, a user login ID that is used when the user logs in through the mobile phone. The server finds, according to the user login ID, a corresponding cookie that is used when the user logs in through the mobile phone. The server sends the cookie to the browser on the computer. The computer logs in automatically according to the cookie in the browser.

Based on the application conception the same as the foregoing method, the present application further provides a server. As shown in FIG. 4, the server includes:

an acquisition module 41 configured to acquire a login request that is sent by a terminal device and carries unique identification information and a login Internet Protocol (IP) address of the terminal device;

a first query module 42 configured to query, according to the IP address in the login request, whether there exists a terminal device that has logged in successfully at the same IP address in server-stored corresponding relationships among unique identification information, login IP addresses, and user login identities (IDs) of terminal devices that have logged in successfully;

a second query module 43 configured to: if yes, query whether a corresponding relationship of unique identification information between the terminal device sending the login request and the terminal device that has logged in successfully exists in server-stored corresponding relationships of unique identification information between terminal devices according to the unique identification information in the login request; and

a sending module 44 configured to: if yes, send, to a browser corresponding to a current login

page of the terminal device, a data cookie corresponding to a user login ID of the terminal device that has logged in successfully, so that the terminal device logs in automatically.

The acquisition module is specifically configured to:

acquire the login request that is sent by the terminal device when accessing the login page and carries the unique identification information and the login IP address of the terminal device, the unique identification information and the login IP address of the terminal device being acquired by the login page by calling, with JavaScript (JS), a FLASH tool plug-in of the current login page.

Based on the application conception the same as the foregoing method, the present application further provides a terminal device. As shown in FIG. 5, the terminal device includes:

a sending module 51 configured to send, when the terminal device accesses a login page, a login request carrying unique identification information and a login IP address of the terminal device to a server; and

an acquisition module 52 configured to acquire a query result that is obtained by the server according to the login request and includes a user login ID of a terminal device that has logged in successfully, so that the terminal device logs in according to the query result.

The sending module is specifically configured to:

when the login page is accessed, add the unique identification information and the login IP address of the terminal device to the login request and send the login request to the server, the unique identification information and the login IP address of the terminal device being acquired by the login page by calling, with JS, a software FLASH tool plug-in of the current login page.

The terminal device logs in according to the query result and specifically includes:

the terminal device automatically logs in by using a data cookie which is in a browser corresponding to the current login page and is corresponding to the user login ID of the terminal device that has logged in successfully, the user login ID being obtained according to the query result and sent by the server.

Compared with the prior art, the embodiments of the present application have at least the

following advantages:

In the present application, according to server-stored corresponding relationships of unique identification information between terminal devices and a corresponding relationship, which is stored after a terminal device logs in successfully, among a login IP address, unique identification information, and a user login ID of the terminal device, the server queries, by using a login IP and unique identification information of a terminal device that is currently logging in, a corresponding relationship between unique identification information of a terminal device that has successfully logged in at the login IP and the unique identification information of the terminal device, to determine whether the terminal device that is currently logging in is related to the terminal device that has logged in successfully. If yes, the terminal device that is currently logging in acquires the user login ID of the terminal device that has logged in successfully, so as to log in automatically. In this way, the login process of a terminal device that carries out cross-terminal login is simple, and the terminal device that carries out login does not need to have particular software or hardware, thus reducing requirement limits on a terminal for cross-terminal login. Meanwhile, the terminal device that carries out login should have a same login IP address with a terminal device that has successfully logged in, thereby guaranteeing security of user information.

Those skilled in the art may understand that modules in the device in the embodiment may be distributed in the apparatus of the embodiment according to the description of the embodiment, or corresponding changes may be made so that the modules are located in one or more apparatuses different from this embodiment. The modules in the foregoing embodiment may be combined into one module, or may be further split into multiple sub-modules.

Through the description of the foregoing implementation, those skilled in the art may clearly understand that the present application may be implemented by means of software plus a necessary hardware platform, and certainly may also be implemented by hardware. However, the former is a better implementation in most cases. Based on such an understanding, the essence of technical solution of the present application, or the part contributing to the prior art, may be

embodied in the form of a software product. The computer software product is stored in a storage medium, and includes several instructions so as to enable a device (which may be a mobile phone, a personal computer, a server, a network device, or the like) to execute the methods in the embodiments of the present application.

Described above are merely preferred implementations of the present application. It should be pointed out that, for those of ordinary skill in the art, several improvements and modifications may further be made without departing from the principle of the present application. These improvements and modifications should also be regarded as the protection scope of the present application.

Disclosed above are merely some specific embodiments of the present application. However, the present application is not limited thereto. Any changes that can be conceived of by those skilled in the art should fall into the protection scope of the present application.

CLAIMS

1. A method for automatic login across terminal devices, comprising:

receiving, by a server, a login request that is sent by a first terminal device, the login request comprising unique identification information and a login Internet Protocol (IP) address of the terminal device;

obtaining, by the server, relationships between unique identification information for the first terminal device and a second terminal device that has logged in successfully, comprising:

receiving, at the server, unique identification information of the first terminal device;

generating, by the server, a quick response code using the received unique identification information of the first terminal device;

sending, from the server and to the first terminal device for display, the generated quick response code, so that the generated quick response code is accessible by the second terminal device to derive the unique identification information of the first terminal device;

receiving, at the server, unique identification information of the second terminal device and the unique identification information of the first terminal device sent by the second terminal device to establish the relationships between the first terminal device and the second terminal device;

determining, by the server and according to the IP address in the login request, the second terminal device is at the same IP address as the first terminal device; and

in response to determining that the second terminal device is at the same IP address as the first terminal device, sending, by the server and to a browser corresponding to a current login page of the first terminal device, a data cookie corresponding to a user login ID of the second terminal device that has logged in successfully, so that the first terminal device logs in automatically.

2. The method of claim 1, further comprising, in response to the first terminal device logging in successfully, storing, at the server and in the form of a corresponding relationship, unique identification information, the login IP address and a user login ID of the first terminal device.

3. The method of claim 1, wherein the server obtains the relationships between unique identification information for the first terminal device and the second terminal device, from the second terminal device.

4. The method of claim 1, wherein the unique identification information and the login IP

address in the login request from the first terminal device is obtained by the login page by calling, with JavaScript (JS), a FLASH tool plug-in of the current login page.

5. A server comprising multiple modules configured to perform the method of any one of claims 1 to 4.

6. A system comprising:

one or more computers and one or more storage devices storing instructions that are operable, when executed by the one or more computers, to cause the one or more computers to perform the method of any one of claims 1 to 4.

7. A computer storage medium encoded with computer program instructions that when executed by one or more computers cause the one or more computers to perform operations the method of any one of claims 1 to 4.