CLAIMS

1. A computer-implemented method for secure account login into a server, the method comprising:

receiving, by a server and from a computing device, a login request comprising a user name and a password corresponding to a user account and a variable apparatus identifier (ID) (S210) associated with the computing device, wherein the variable apparatus ID is generated by the server during a prior initialization phase based on a static apparatus ID and an additional parameter, and wherein the static apparatus ID is generated by the server based on attribute information of a mobile device including an international mobile equipment identity (IMEI), an Android ID, a MAC address, a serial number (SN) or a vendor identifier (vendor ID);

verifying, by the server in a user account database, the user name and the password in the login request;

storing, by the server in the user account database, mapping relationships between the static apparatus ID and the variable apparatus ID, between the variable apparatus ID and the user name associated with the login request, and between the static apparatus ID and the user name;

receiving, by the server, another login request from the computing device, the another login request based on the variable apparatus ID;

determining, by the server, that the variable apparatus ID corresponds to a user account;

determining, by the server and based on a timestamp included in the variable apparatus ID and a current time of the server, that an update of the variable apparatus ID is necessary (S230);

updating, by the server, the variable apparatus ID associated with the computing device (S240), wherein

updating the variable apparatus ID comprises replacing the variable apparatus ID with an updated apparatus ID, and wherein the updated apparatus ID is generated based on the static apparatus ID and an updated additional parameter; and

transmitting, by the server and to the computing device, an account login permission instruction and the updated variable apparatus ID as automatic login information for a next login request to the server.

2. The computer-implemented method of claim 1, wherein the variable apparatus ID has a

validity period and can identify the mobile device.

3. The computer-implemented method of claim 2, wherein the validity period of the variable apparatus ID varies with an app type.

4. The computer-implemented method of claim 1, wherein determining whether the update is requested comprises:

determining a survival period of the variable apparatus ID based on the timestamp in the variable apparatus ID and the current time of the server;

determining whether the survival period is shorter than a validity period; and

if the survival period is not shorter than the validity period, updating the variable apparatus ID.

5. The computer-implemented method of claim 1, further comprising, in response to determining that the update of the variable apparatus ID is not necessary, sending an account login permission instruction and the variable apparatus ID to the mobile device.

6. The computer-implemented method of claim 1, wherein the variable apparatus ID comprises an apparatus token that has a validity period.

7. The computer-implemented method of claim 1, wherein the variable apparatus ID is generated by the server based on an app, an apparatus ID, a validity period, and a timestamp.

8. The computer-implemented method of claim 7, wherein the apparatus ID is a unique ID generated by the server based on terminal apparatus information of the mobile device.

9. The computer-implemented method of claim 8, wherein the login request comprises a variable apparatus ID and a user name.

10. The computer-implemented method of claim 1, wherein determining that the variable apparatus ID corresponds to a user account comprises:

searching the user account database for an apparatus ID corresponding to the variable apparatus ID, and determining whether the user name is a user name corresponding to the apparatus ID.

11. The computer-implemented method of any one of claims 1 to 10, further comprising, in response to updating the variable apparatus ID, updating the user account database by using the updated variable apparatus ID.

12. A server, comprising:

a receiving unit, configured to perform the method of any one of claims 1 to 11 comprising receiving a login request from a computing device, wherein the login request comprises a user name and a password corresponding to a user account and a variable apparatus ID;

a storage unit, configured to store a user account database including mapping relationships between a static apparatus ID and the variable apparatus ID, between the variable apparatus ID and the user name associated with the login request, and between the static apparatus ID and the user name;

a searching unit, configured to search the user account database for user account information including the mapping relationships;

a determining unit, configured to determine that a variable apparatus ID corresponds to a user account and whether the variable apparatus ID needs to be updated;

an update unit, configured to update the variable apparatus ID based on a timestamp in the variable apparatus ID and a current time of the server; and

a transmitting unit, configured to send an account login permission instruction and an updated variable apparatus ID to the computing device as automatic login information for a next login request to the server.

13. An apparatus for secure account login, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 11.