

WHAT IS CLAIMED IS:

1. A method for verifying a trusted terminal at a server, comprising:
 - determining whether a login terminal of a user matches the trusted terminal of the user recorded locally;
 - determining, when it is determined that the login terminal does not match the trusted terminal of the user recorded locally, whether a login account of the user is associated with a frequent-use login account of the login terminal; and
 - determining that the login terminal is the trusted terminal of the user if Yes.
2. The method according to claim 1, wherein before determining whether a login terminal of a user matches a trusted terminal of the user recorded locally, the method further comprises:
 - identifying a terminal type of the trusted terminal according to hardware information of the trusted terminal;
 - locally classifying the trusted terminal as a handheld trusted terminal when the trusted terminal is identified as a handheld terminal;
 - determining whether a frequent-use time period of the trusted terminal is an office time period or a household time period, when the trusted terminal is identified as a PC terminal;
 - locally classifying the trusted terminal as an office trusted terminal, when the frequent-use time period of the trusted terminal is the office time period; and
 - locally classifying the trusted terminal as a household trusted terminal, when the frequent-use time period of the trusted terminal is the household time period.

3. The method according to claim 1, wherein before determining whether a login account of the user is associated with a frequent-use login account of the login terminal, the method further comprises:

determining whether the number of logins of the login account of the user on the login terminal reaches a threshold;

further determining whether the login account of the user is associated with the frequent-use login account of the login terminal, if Yes; and

determining that the login terminal is an untrusted terminal of the user, if No.

4. The method according to claim 1, wherein determining whether a login account of the user is associated with a frequent-use login account of the login terminal comprises:

querying the frequent-use login account of the login terminal, wherein the frequent-use login account is, among historical login accounts of the login terminal, a login account that the number of logins thereof reaches a threshold;

determining whether the login account of the user and the frequent-use login account were logged-in on a same trusted terminal and whether the numbers of logins of both of the two accounts reach the threshold; and

if Yes, determining that the login account of the user is associated with the frequent-use login account, and locally storing an association relationship between the login account of the user and the historical login accounts.

5. The method according to claim 4, wherein the same trusted terminal is the same household trusted terminal.

6. A device for verifying a terminal at a server, comprising:

a first determining module, used for determining whether a login terminal of a user matches a trusted terminal recorded locally; and

a second determining module, used for determining, when it is determined that the login terminal does not match the trusted terminal recorded locally, whether a login account of the user is associated with a frequent-use login account of the login terminal, and determine that the login terminal is the trusted terminal of the user if Yes.

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

a classification module, used for identifying, before the first determining module determines whether a login terminal of a user matches a trusted terminal of the user recorded locally, a terminal type of the trusted terminal according to hardware information of the trusted terminal;

when the trusted terminal is identified as a handheld terminal, locally classifying the trusted terminal as a handheld trusted terminal;

when the trusted terminal is identified as a PC terminal, determining whether a common time period of the trusted terminal is an office time period or a household time period;

when the common time period of the trusted terminal is the office time period, locally classifying the trusted terminal as an office trusted terminal; and

when the common time period of the trusted terminal is the household time period, locally classifying the trusted terminal as a household trusted terminal.

8. The device according to claim 6, wherein the second determining module is further used for:

determining, before determining whether a login account of the user is associated with a frequent-use login account of the login terminal, whether the number of logins of the login account of the user on the login terminal reaches a threshold;

further determining whether the login account of the user is associated with the frequent-use login account of the login terminal if Yes; and

determining that the login terminal is an untrusted terminal of the user if No.

9. The device according to claim 6, wherein the second determining module is further used for:

querying the frequent-use login account of the login terminal, wherein the frequent-use login account is, among historical login accounts of the login terminal, a login account that the number of logins thereof reaches a threshold;

determining whether the login account of the user and the frequent-use login account were logged-in on a same trusted terminal and whether the numbers of logins of both of the two accounts reach the threshold; and

if Yes, determining that the login account of the user is associated with the frequent-use login account, and locally storing an association relationship between the login account of the user and the historical login accounts.

10. The device according to claim 9, wherein the same trusted terminal is the same household trusted terminal.

11. A device for verifying a trusted terminal, comprising:

a processor; and a memory for storing instructions executable by the processor;

wherein the processor is used for:

determining whether a login terminal of a user matches a trusted terminal of the user recorded locally;

determining, when it is determined that the login terminal does not match the trusted terminal of the user recorded locally, whether a login account of the user is associated with a frequent-use login account of the login terminal; and

determining that the login terminal is the trusted terminal of the user if Yes.

12. A non-transitory computer readable medium that stores a set of instructions that is executable by at least one processor of a terminal device to cause the terminal device to perform a method for verifying a trusted terminal at a server, the method comprising:

determining whether a login terminal of a user matches the trusted terminal of the user recorded locally;

determining, when it is determined that the login terminal does not match the trusted terminal of the user recorded locally, whether a login account of the user is associated with a frequent-use login account of the login terminal; and

determining that the login terminal is the trusted terminal of the user if Yes.

13. The non-transitory computer readable medium according to claim 12, wherein before determining whether a login terminal of a user matches a trusted terminal of the user recorded locally, the method further comprises:

identifying a terminal type of the trusted terminal according to hardware information of the trusted terminal;

locally classifying the trusted terminal as a handheld trusted terminal when the trusted terminal is identified as a handheld terminal;

determining whether a frequent-use time period of the trusted terminal is an office time period or a household time period, when the trusted terminal is identified as a PC terminal;

locally classifying the trusted terminal as an office trusted terminal, when the frequent-use time period of the trusted terminal is the office time period; and

locally classifying the trusted terminal as a household trusted terminal, when the frequent-use time period of the trusted terminal is the household time period.

14. The non-transitory computer readable medium according to claim 12, wherein before determining whether a login account of the user is associated with a frequent-use login account of the login terminal, the method further comprises:

determining whether the number of logins of the login account of the user on the login terminal reaches a threshold;

further determining whether the login account of the user is associated with the frequent-use login account of the login terminal, if Yes; and

determining that the login terminal is an untrusted terminal of the user, if No.

15. The non-transitory computer readable medium according to claim 12, wherein determining whether a login account of the user is associated with a frequent-use login account of the login terminal comprises:

querying the frequent-use login account of the login terminal, wherein the frequent-use login account is, among historical login accounts of the login terminal, a login account that the number of logins thereof reaches a threshold;

determining whether the login account of the user and the frequent-use login account were logged-in on a same trusted terminal and whether the numbers of logins of both of the two accounts reach the threshold; and

if Yes, determining that the login account of the user is associated with the frequent-use login account, and locally storing an association relationship between the login account of the user and the historical login accounts.

16. The non-transitory computer readable medium according to claim 15, wherein the same trusted terminal is the same household trusted terminal.