[0005] According to an aspect of the present disclosure, a method for managing user login sessions using a server is provided. The method comprises detecting, at a server computing device, a successful login of a user via a login medium, the successful login including a user ID (UID) associated with the user; querying, using the server computing device and a UID, a first database to detect whether a login session queue corresponding to the UID exists in a session cache list, the login session queue comprising a mapping of the UID to at least one session ID; managing, using the server computing device, the user's login status through the login session queue, if the querying detects that the login session queue corresponding to the UID exists in the session cache list, the managing comprising archiving at least one session ID associated with the UID from the login session queue in a second database; and storing, using the server computing device, a session ID in a new login session queue corresponding to the UID in the session cache list if the querying detects an absence of the login session queue corresponding to the UID in the session cache list, the new login queue stored in the first database.

[0006] According to another aspect of the present disclosure, a server computing device for managing user login sessions is provided. The server computing device comprising a query module querying, detecting a successful login of a user via a login medium, the successful login including a user ID (UID) with the user, and using a UID, a first data base to detect whether a login session queue corresponding to the UID exists in a session cache list, the login session queue comprising a mapping of the UID to at least one session ID; a managing module managing the user's login status through the login session queue, if the query module detects that the login session queue corresponding to the UID exists in the session cache list, the managing comprising archiving at least one session ID associated with the UID from the login session queue in a second database; and a first storage module storing a session ID in a new login session queue corresponding to the UID in the session cache list if the query module detects an absence of the login session queue corresponding to the UID in the session cache list, the new login session queue stored in the first database.

[0007] According to yet another aspect of the present disclosure a server is provided. The server comprising a processor a storage medium for tangibly storing thereon program logic for execution by the processor, the stored program logic comprising: detecting logic executed by the processor for detecting a successful login of a user via a login medium, the successful login including a user ID (UID) associated with the user; querying logic executed by the processor for querying, using a UID, a first database to detect whether a login session queue corresponding to

the UID exists in a session cache list, the login session queue comprising a mapping of the UID to at least one session ID; managing logic executed by the processor for managing the user's login status through the login session queue, if the querying detects that the login session queue corresponding to the UID exists in the session cache list, the managing comprising archiving at least one session ID associated with the UID from the login session queue in a second database; and storing logic executed by the processor for storing a session ID in a login session queue corresponding to the UID in the session cache list if the querying detects an absence of the login session queue corresponding to the UID in the session cache list, the new login session queue stored in the first database.

[0008] It is thus clear from the above technical scheme that embodiments of the present disclosure queries, according to the UID, whether there is any existing login session queue corresponding to the UID in the session cache list; if any, the user login status is managed through the login session queue, so that the login status created with a UID can be effectively managed by the legitimate user through the

CLAIMS

1. A method comprising:

detecting, at a server computing device, a successful login of a user via a login medium, the successful login including a user ID (UID) associated with the user;

querying, using the server computing device and a UID, a first database to detect whether a login session queue corresponding to the UID exists in a session cache list, the login session queue comprising a mapping of the UID to at least one session ID;

managing, using the server computing device, the user's login status through the login session queue if the querying detects that the login session queue corresponding to the UID exists in the session cache list, the managing comprising archiving at least one session ID associated with the UID from the login session queue in a second database; and

storing, using the server computing device, a session ID in a new login session queue corresponding to the UID in the session cache list if the querying detects an absence of the login session queue corresponding to the UID in the session cache list, the new login session queue stored in the first database.

2. The method of claim 1, further comprising:

creating the session ID in response to the user's login; and

establishing a mapping relationship between the UID and the session ID.

3. The method of claim 1, managing the user login status through the login session queue further comprising:

determining, using the server computing device, whether a size of the login session queue exceeds a predetermined threshold;

determining, using the server computing device, whether each login session in the login session queue is an invalid login session in the login session queue, deleting each invalid login session from the login session queue, and storing each invalid login session deleted from the login session queue in a first database, if the size of the login session queue is determined to exceed the predetermined threshold; and

storing, using the server computing device, the session ID corresponding to the user's login in the login session queue, if the size of the login session queue is determined not to exceed the predetermined threshold.

4. The method of claim 3, managing the user login status through the login session queue further comprising:

determining, using the server computing device, the user's login permission settings after detecting that the user is performing a password change via a current login medium; and

managing each currently active session ID in the login session queue in accordance with the

login permission settings, comprising:

determining, using the server computing device and for each currently active session ID in the login session queue, whether the currently active session ID is a permitted session ID in accordance with the login permission settings;

keeping, using the server computing device, the currently active session that is identified as permitted in the login session queue, and deleting, from the login session queue, each currently active session ID identified as unpermitted.

5. The method of claim 1, managing the user login status through the login session queue further comprising:

determining, using the server computing device and for each session ID, whether a storage duration of a login session corresponding to the session ID in the login session queue exceeds a predetermined storage cycle;

determining, using the server computing device and for each session ID, that the corresponding login session is an invalid login session in the login session queue if the storage duration exceeds the predetermined storage cycle; and

deleting, using the server computing device and for each invalid login session, the invalid login session from the login session queue and storing the invalid login session in the second database.

6. The method of claim 5, further comprising:

determining, using the server computing device, each session ID in the login session queue having a storage duration not exceeding the predetermined storage cycle as an active session ID in the login session queue; and

storing each determined active session ID in the first database.

7. The method of claim 5, managing the user login status through the login session queue further comprising:

determining, using the server computing device, the user's login permission settings after detecting that the user is performing a password change via a current login medium; and

managing each currently active session ID in the login session queue in accordance with the login permission settings, comprising:

determining, using the server computing device and for each currently active session ID in the login session queue, whether the currently active session ID is a permitted session ID in accordance with the login permission settings;

keeping, using the server computing device, the currently active session that is identified

as permitted in the login session queue, and deleting, from the login session queue, each currently active session ID identified as unpermitted.

8. The method of claim 1, managing the user login status through the login session queue further comprising:

determining, using the server computing device, the user's login permission settings after detecting that the user is performing a password change via a current login medium; and

managing each currently active session ID in the login session queue in accordance with the login permission settings.

9. The method of claim 8, managing each currently active session ID in the login session queue according to the login permission settings further comprising:

determining, using the server computing device and for each currently active session ID in the login session queue, whether the currently active session ID is a permitted session ID in accordance with the login permission settings;

keeping, using the server computing device, the currently active session that is identified as permitted in the login session queue, and deleting, from the login session queue, each currently active session ID identified as unpermitted.

10. A server computing device comprising:

a query module

detecting a successful login of a user via a login medium, the successful login including a user ID (UID) associated with the user, and

querying, using a UID, a first database to detect whether a login session queue corresponding to the UID exists in a session cache list, the login session queue comprising a mapping of the UID to at least one session ID;

a managing module managing the user's login status through the login session queue, if the query module detects that the login session queue corresponding to the UID exists in the session cache list, the managing comprising archiving at least one session ID associated with the UID from the login session queue in a second database; and

a first storage module storing a session ID in a new login session queue corresponding to the UID in the session cache list if the query module detects an absence of the login session queue corresponding to the UID in the session cache list, the new login session queue stored in the first database.

11. The device of claim 10, further comprising:

a creation module creating the session ID in response to the user's login; and

a mapping module establishing a mapping relationship between the UID and the session ID created by the creation module.

12. The device of claim 10, the managing module further comprising:

a first determination unit determining whether a size of the login session queue exceeds a predetermined threshold;

a second determination unit determining whether each login session in the login session queue is an invalid login session in the login session queue and deleting each invalid login session from the login session queue, if the size of the login session queue is determined to exceed the predetermined threshold;

a storage unit storing the session ID corresponding to the user's login in the login session queue, if the size of the login session queue is determined not to exceed the predetermined threshold; and

a second storage module storing, in a first database, each invalid login session identified by the second determination unit.

13. The device of claim 12, the managing module further comprising:

a fifth determination unit determining the user's login permission settings after detecting that the user is performing a password change via a current login medium; and

a managing unit managing each currently active session ID in the login session queue according to the login permission settings in accordance with the login permission settings determined by the fifth determination unit, the managing unit further comprising:

a determination subunit determining, for each currently active session ID in the login session queue, whether the currently active session ID is a permitted session ID in accordance with the login permission settings; and

a managing subunit keeping each currently active session ID that is identified by the determination subunit to be permitted in the login session queue, and deleting, from the login session queue, each currently active session ID that is identified by the determination subunit to be unpermitted.

14. The device of claim 10, the managing module further comprising:

a third determination unit determining, for each session ID, whether a storage duration of a login session corresponding to the session ID in the login session queue exceeds a predetermined storage cycle;

a fourth determination unit determining, for each session ID, that the corresponding login session is an invalid login session in the login session queue, if the login session's storage duration determined by the third determination unit exceeds the predetermined storage cycle;

a deletion unit deleting each invalid login session identified by the fourth determination unit

from the login session queue; and

a third storage module storing each invalid login session deleted from the login session queue by the deletion unit in the second database.

15. The device of claim 14, further comprising:

a determination module determining each session ID in the login session queue having a storage duration not exceeding the predetermined storage cycle as an active session ID in the login session queue; and

a fourth storage module storing each determined active session ID in the first database.

16. The device of claim 14, the managing module further comprising:

a fifth determination unit determining the user's login permission settings after detecting that the user is performing a password change via a current login medium; and

a managing unit managing each currently active session ID in the login session queue according to the login permission settings in accordance with the login permission settings determined by the fifth determination unit, the managing unit further comprising:

a determination subunit determining, for each currently active session ID in the login session queue, whether the currently active session ID is a permitted session ID in accordance with the login permission settings; and

a managing subunit keeping each currently active session ID that is identified by the determination subunit to be permitted in the login session queue, and deleting, from the login session queue, each currently active session ID that is identified by the determination subunit to be unpermitted.

17. The device of claim 10, the managing module further comprising:

a fifth determination unit determining the user's login permission settings after detecting that the user is performing a password change via a current login medium; and

a managing unit managing each currently active session ID in the login session queue according to the login permission settings in accordance with the login permission settings determined by the fifth determination unit.

18. The device of claim 17, the managing unit further comprising:

a determination subunit determining, for each currently active session ID in the login session queue, whether the currently active session ID is a permitted session ID in accordance with the login permission settings; and

a managing subunit keeping each currently active session ID that is identified by the determination subunit to be permitted in the login session queue, and deleting, from the login session queue, each currently active session ID that is identified by the determination subunit to be unpermitted.

19. A server, comprising:

a processor; and

a storage medium for tangibly storing thereon program logic for execution by the processor, the stored program logic comprising:

detecting logic executed by the processor for detecting a successful login of a user via a login medium, the successful login including a user ID (UID) associated with the user;

querying logic executed by the processor for querying, using a UID, a first database to detect whether a login session queue corresponding to the UID exists in a session cache list, the login session queue comprising a mapping of the UID to at least one session ID;

managing logic executed by the processor for managing the user's login status through the login session queue, if the querying detects that the login session queue corresponding to the UID exists in the session cache list, the managing comprising archiving at least one session ID associated with the UID from the login session queue in a second database; and

storing logic executed by the processor for storing a session ID in a login session queue corresponding to the UID in the session cache list if the querying detects an absence of the login session queue corresponding to the UID in the session cache list, the new login session queue stored in the first database.