CLAIMS

1. A method for service implementation based on a virtual reality scenario, the method comprising:

receiving a target service which is initiated by a user in the virtual reality scenario of a virtual reality client terminal and requires a security authentication, wherein the virtual reality scenario includes a virtual checkout button;

determining that the virtual reality client terminal is currently worn by a real person based on at least one of eye-blinking recognition or heartbeat recognition;

in response to determining that the virtual reality client terminal is currently worn by a real person, presenting a notification in the virtual reality scenario to perform biometric authentication;

invoking an eye recognition hardware to collect an eye physiological feature of the user for the biometric authentication, wherein the eye recognition hardware comprises a sensor, lenses, and a plurality of cameras;

comparing the eye physiological feature of the user with a pre-stored eye physiological feature sample of the user;

determining whether the target service passes the security authentication at least partially with reference to a result of comparison between the eye physiological feature of the user and the pre-stored eye physiological feature sample; and

executing the target service when the target service passes the security authentication.

2. The method of claim 1, wherein the eye physiological feature comprises an eyeprint feature and an iris feature.

3. The method of claim 1, wherein the lenses correspond to locations of eyes of the user, and the plurality of cameras are uniformly distributed around the lenses.

4. The method of claim 1, wherein the eye recognition hardware further comprises a plurality of LED light sources with a one-to-one correspondence to the plurality of cameras and uniformly distributed around the lenses.

5. The method of claim 4, wherein the eye recognition hardware comprises:

a preset brightness detection hardware configured to detect brightness of a collection environment of the eye recognition hardware to obtain a brightness value.

6. The method of claim 5, further comprising:

invoking the eye recognition hardware to collect the eye physiological feature of the user;

determining whether the brightness value is lower than a preset threshold; and

if the brightness value is lower than the preset threshold, invoking the plurality of LED light sources to perform one-to-one light compensation on the plurality of cameras.

7. The method of claim 4, wherein when the eye physiological feature is an iris feature, a camera is an infrared camera; and an LED light source is an infrared LED light source.

8. The method of claim 1, wherein the virtual reality scenario comprises a preset virtual element, and the preset virtual element is used for triggering the target service requiring security authentication.

9. The method of claim 8, further comprising:

recognizing, by using preset sensing hardware, an interaction operation performed by the user on the preset virtual element in the virtual reality scenario; and

determining that the user initiates the target service requiring security authentication when it is recognized that the interaction operation performed by the user on the preset virtual element is a preset interaction operation.

10. The method of claim 1, further comprising:

recognizing a voice instruction sent by the user; and

determining, when an execution instruction for the target service requiring security authentication is recognized from the voice instruction of the user, that the user initiates the target service requiring security authentication.

11. The method of claim 1, further comprising:

performing a bioassay on the user; and

outputting an eye physiological feature collection prompt to the user in a user view of the virtual reality scenario when the user passes the bioassay before invoking the eye recognition hardware to collect the eye physiological feature of the user.

12. The method of claim 2, wherein a camera is a microspur camera.

13. The method of claim 1, wherein comparing the eye physiological feature of the user with a pre-stored eye physiological feature sample of the user comprises:

sending a verification request for the eye physiological feature of the user to a service server terminal, the verification request carrying the eye physiological feature of the user and account information of the user, wherein the service server terminal searches a preset eye physiological feature library for an eye physiological feature sample bound to the account information of the user, and compares the eye physiological feature of the user with the eye physiological feature sample.

14. The method of claim 1, wherein determining whether the target service passes the security authentication comprises:

determining, in response to a comparison result that the eye physiological feature of the user matches the pre-stored eye physiological feature sample, that the target service passes the security authentication; or

performing further security verification on the target service in response to a comparison result that the eye physiological feature of the user matches the pre-stored eye physiological feature sample, and after the security verification is successful, determining that the target service passes the security authentication.

15. An apparatus for service implementation based on a virtual reality scenario, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 14.