CLAIMS

What is claimed is:

1. A method for operating an Internet of Things device, comprising:

receiving, by user equipment, a first random number from an Internet of Things device, wherein the first random number is generated by and stored in the Internet of Things device;

receiving, by the user equipment, an operation instruction for the Internet of Things device from a user;

identifying, by the user equipment, a biometric feature of the user;

verifying, by the user equipment, an identity of the user based on the biometric feature;

signing, by the user equipment if the identity of the user is verified successfully, the operation instruction by using a first user key of the user;

transmitting, by the user equipment, both a second random number and the signed operation instruction to the Internet of Things device;

verifying, by the Internet of Things device, a signature for the signed operation instruction by using a second user key of the user, wherein the second user key and the first user key constitute a key pair;

comparing, by the Internet of Things device after the signature is verified successfully, the second random number received from the user equipment with the first random number generated by the Internet of Things device;

executing, by the Internet of Things device, the operation instruction only when the second random number received by the Internet of Things device from the user equipment and the first random number generated by the Internet of Things device are consistent and if the signature is verified successfully; and

invalidating, by the Internet of Things device, the first random number after the operation instruction is executed.

2. The method according to claim 1, wherein the first user key is a user private key of the user, and the second user key is a user public key of the user.

3. The method according to claim 1, wherein the first user key and the second user key are the same user key of the user.

4. The method according to claim 1, further comprising:

binding, by the user equipment, the Internet of Things device before the Internet of Things device is operated.

5. The method according to claim 4, wherein the binding, by the user equipment, the Internet of Things device further comprises:

identifying, by the user equipment, the biometric feature of the user;

verifying, by the user equipment, the identity of the user based on the biometric feature; and

transmitting, by the user equipment, the second user key to the Internet of Things device if the identity of the user is verified successfully.

6. The method according to claim 1, wherein the method further comprises generating, by the user equipment, the first user key and the second user key.

7. The method according to claim 6, wherein the generating, by the user equipment, the first user key and the second user key further comprises:

entering, by the user equipment, the biometric feature of the user, and

generating, by the user equipment, the first user key and the second user key for the user after the biometric feature is entered.

8. The method according to claim 1, wherein the first user key and the second user key are stored in a secure environment of the user equipment, and the secure environment is a trusted execution environment (TEE) or a hardware secure element (SE).

9. A system, comprising:

user equipment, having a biometric feature identification capability and being configured to:

receive a first random number from an Internet of Things device, wherein the first random number is generated by and stored in the Internet of Things device;

receive an operation instruction for the Internet of Things device from a user;

identify a biometric feature of the user;

verify an identity of the user based on the biometric feature;

sign, if the identity of the user is verified successfully, the operation instruction by using a first user key of the user; and

transmit both a second random number and the signed operation instruction to the Internet of Things device; and

an Internet of Things device, configured to:

receive the signed operation instruction from the user equipment;

verify a signature for the signed operation instruction by using a second user key of the user, wherein the second user key and the first user key constitute a key pair;

compare, after the signature is verified successfully, the second random number received from the user equipment with the first random number generated by the Internet of Things device;

execute the operation instruction only when the second random number received by the Internet of Things device from the user equipment and the first random number generated by the Internet of Things device are consistent and if the signature is verified successfully; and

invalidate the first random number after the operation instruction is executed.

10. The system according to claim 9, further comprising:

binding the user equipment to the Internet of Things device before the Internet of Things device is operated.

11. The system according to claim 10, wherein the binding comprises:

identifying, by the user equipment, the biometric feature of the user;

verifying, by the user equipment, the identity of the user based on the biometric feature; and

transmitting, by the user equipment, the second user key to the Internet of Things device if the identity of the user is verified successfully.

12. The system according to claim 9, wherein the first user key and the second user key are generated by the user equipment.

13. The system according to claim 12, wherein the generating, by the user equipment, the first user key and the second user key further comprises:

entering, by the user equipment, the biometric feature of the user, and

generating, by the user equipment, the first user key and the second user key for the user after the biometric feature is entered.

14. The system according to claim 9, wherein the user equipment comprises a secure environment, the first user key and the second user key are stored in the secure environment, and the secure environment is a trusted execution environment (TEE) or a hardware secure element (SE).

15. The system according to claim 9, wherein the system further comprises a router, and the user equipment communicates with the Internet of Things by using the router.

16. A computer-readable storage medium storing instructions, the instructions, when executed by a computer device, causing the computer device to perform the method according to any one of claims 1 to 8.