Claims

1. A method for obtaining data authorization, performed by a trusted computing center; the trusted computing center comprises a data storage center and multiple trusted computing nodes, the data storage center maintains at least multiple encrypted shards of first private data of a first provider, wherein the multiple encrypted shards are obtained by splitting the first private data to be stored into multiple private shards and encrypting the multiple private shards using respective encryption keys; the method comprises:

receiving, by any first computing node among the multiple trusted computing nodes, an authentication request from the first provider;

Returning authentication information to the first provider, wherein the authentication information comprises at least a first code hash of a first computation logic running on the first computing node;

Receiving a channel establishment request sent by the first provider after determining that the first computing node has passed trusted authentication and the first code hash has passed correctness verification;

Establishing a first trusted channel with the first provider based on the channel establishment request; and

Obtaining, via the first trusted channel, a target encryption key from the respective encryption keys corresponding to the multiple encrypted shards, wherein the target encryption key corresponds to a target encrypted shard among the multiple encrypted shards, thereby obtaining authorization to compute the target encrypted shard corresponding to the target encryption key based on the first computation logic.

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

encrypting, by the first computing node, the target encryption key using a private key corresponding to the first computing node and the first computation logic;

Storing the encrypted target encryption key in the data storage center.

3. The method according to claim 2, wherein the trusted computing center further comprises a management center for managing the multiple trusted computing nodes; the data storage center also maintains respective key identifiers corresponding to the multiple encrypted shards; the method further comprises:

receiving, by the first computing node, a computation request from the management center;

In response to the computation request, reading the encrypted target encryption key from the data storage center, decrypting it using a decryption key corresponding to the private key to obtain the target encryption key;

Based on the key identifier of the target encryption key, reading a corresponding target encrypted shard from the data storage center, decrypting it using the target encryption key to obtain a corresponding target plaintext shard; and

Computing on the target plaintext shard and other plaintext shards based on the first computation logic.

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

determining, by the first computing node from the multiple trusted computing nodes, a second computing node belonging to the same role category as the first computing node;

Sharing the target encryption key with the second computing node, so that the second computing node obtains authorization to compute the target encrypted shard based on the first computation logic.

5. The method according to claim 1, wherein the correctness verification comprises comparing the first code hash with a target code hash of a target computation logic that is pre-stored and reviewed by the first provider.

6. A method for obtaining data authorization, performed by a trusted computing center; the trusted computing center comprises a data storage center, multiple trusted computing nodes, and respective proxy nodes; the data storage center maintains at least multiple encrypted shards of first private data of a first provider, wherein the multiple encrypted shards are obtained by splitting the first private data to be stored into multiple private shards and encrypting the multiple private shards using respective encryption keys; the method comprises:

obtaining, by each proxy node from the first provider, the encryption keys corresponding to the multiple encrypted shards;

sending, by any first proxy node among the proxy nodes, an authentication request to a corresponding first computing node, and receiving authentication information returned by the first computing node, wherein the authentication information comprises at least a first code hash of a first computation logic running on the first computing node;

performing, by the first proxy node based on the authentication information, trusted authentication on the first computing node, and determining whether the first code hash is verifiably stored;

When the trusted authentication passes and the first code hash is verifiably stored, establishing, by the first proxy node, a first trusted channel with the first computing node;

sending, by the first proxy node, a target encryption key obtained among the encryption keys corresponding to the multiple encrypted shards to the first computing node through the first trusted channel; and

obtaining, by the first computing node, authorization to compute the target encrypted shard corresponding to the target encryption key based on the first computation logic.

7. The method according to claim 6, wherein determining whether the first code hash is verifiably stored comprises:

Obtaining from the first computing node a certificate of verifiable storage pre-stored on it, wherein the certificate of verifiable storage includes at least a second code hash of the first computation logic;

Comparing the first code hash with the second code hash; if the comparison result matches, determining that the first code hash is verifiably stored.

8. The method according to claim 7, wherein the certificate of verifiable storage is received and forwarded to the first computing node by a third party or administrator recognized by the trusted computing center after the second code hash is provided to a verifiable storage center.

9. The method according to claim 8, wherein the trusted computing center further comprises a code storage center, which maintains at least the first computation logic; the method further comprises:

receiving, by the code storage center, a data retrieval request from the first provider, which includes at least the second code hash obtained by the first provider from the verifiable storage center;

In response to the data retrieval request, providing, by the code storage center, the first computation logic to the first provider for the first provider to review the legitimacy of the first computation logic.

10. A method for obtaining data authorization, involving a trusted computing center; the trusted computing center comprises a data storage center, multiple trusted computing nodes, and respective proxy nodes corresponding to the trusted computing nodes; the data storage center maintains at least multiple encrypted shards of first private data of a first provider, wherein the multiple encrypted shards are obtained by

splitting the first private data to be stored into multiple private shards and encrypting the multiple private shards using respective encryption keys; the method is performed by any first proxy node among the proxy nodes, comprising:

Obtaining from the first provider a target encryption key from the respective encryption keys corresponding to the multiple encrypted shards;

Sending an authentication request to a corresponding first computing node;

Receiving authentication information returned by the first computing node, wherein the authentication information comprises at least a first code hash of a first computation logic running on the first computing node;

Performing, based on the authentication information, trusted authentication on the first computing node, and determining whether the first code hash is verifiably stored;

When the trusted authentication passes and the first code hash is verifiably stored, establishing a first trusted channel with the first computing node; and

Sending the target encryption key to the first computing node through the first trusted channel; thereby the first computing node obtains authorization to compute the target encrypted shard corresponding to the target encryption key based on the first computation logic.

11. An apparatus for obtaining data authorization, disposed in any first computing node of a trusted computing center; the trusted computing center comprises a data storage center and multiple trusted computing nodes, the data storage center maintains at least multiple encrypted shards of first private data of a first provider, wherein the multiple encrypted shards are obtained by splitting the first private data to be stored into multiple private shards and encrypting the multiple private shards using respective encryption keys; the apparatus comprises:

a receiving unit, configured to receive an authentication request from the first provider;

a sending unit, configured to return authentication information to the first provider, wherein the authentication information at least comprises a first code hash of a first computing logic running in the first computing node;

the receiving unit is further configured to receive a channel establishment request sent by the first provider after determining that the first computing node passes trusted authentication and the first code hash passes correctness verification;

an establishment unit, configured to establish a first trusted channel with the first provider according to the channel establishment request; and

the receiving unit is further configured to receive, through the first trusted channel, target encryption keys corresponding to the multiple encrypted shards to obtain permission to perform computation on a target encrypted shard corresponding to the target encryption key based on the first computing logic.

12. The apparatus according to claim 11, further comprising:

an encryption unit, configured to encrypt the target encryption key using a private key corresponding to the first computing node and the first computing logic;

a storage unit, configured to store the encrypted target encryption key to the data storage center.

13. The apparatus according to claim 12, wherein the trusted computing center further comprises a management center for managing the multiple trusted computing nodes; the data storage center also maintains respective key identities corresponding to the multiple encrypted shards; the apparatus further comprises: a reading unit and a computing unit;

the receiving unit is further configured to receive a computation request from the management center;

the reading unit is configured to, in response to the computation request, read the encrypted target encryption key from the data storage center, decrypt it using a decryption key corresponding to the private key to obtain the target encryption key;

the reading unit is further configured to, based on the key identity of the target encryption key, read a corresponding target encrypted shard from the data storage center, decrypt it using the target encryption key to obtain a corresponding target plaintext shard; and

the computing unit is configured to perform computation on the target plaintext shard and other plaintext shards based on the first computing logic.

14. The apparatus according to claim 11, further comprising:

a determining unit, configured to determine, from the multiple trusted computing nodes, a second computing node that belongs to the same role category as the first computing node;

a sharing unit, configured to share the target encryption key with the second computing node, so that the second computing node obtains permission to perform computation on the target encrypted shard based on the first computing logic.

15. The apparatus according to claim 11, wherein the correctness verification comprises comparing the first code hash with a target code hash of a target computing logic that is pre-stored and reviewed by the first provider.

16. A system for obtaining data authorization, comprising a data storage center, multiple trusted computing nodes, and corresponding proxy nodes; the data storage center maintains at least multiple encrypted shards of first private data of a first provider, wherein the multiple encrypted shards are obtained by splitting the first private data to be stored into multiple private shards and encrypting the multiple private shards using respective encryption keys;

the proxy nodes are configured to obtain, from the first provider, encryption keys corresponding to the multiple encrypted shards;

any first proxy node among the proxy nodes is configured to send an authentication request to a corresponding first computing node, and receive authentication information returned by the first computing node, wherein the authentication information at least comprises a first code hash of a first computing logic running in the first computing node;

the first proxy node is further configured to perform trusted authentication on the first computing node based on the authentication information, and determine whether the first code hash is verifiably stored;

the first proxy node is further configured to, when the trusted authentication passes and the first code hash is verifiably stored, establish a first trusted channel with the first computing node;

the first proxy node is further configured to send a target encryption key received to the first computing node through the first trusted channel; and

the first computing node is configured to obtain permission to perform computation on a target encrypted shard among the multiple encrypted shards corresponding to the target encryption key based on the first computing logic.

17. The system according to claim 16, wherein the first proxy node is specifically configured to:

obtain a certificate of verifiable storage stored in advance in the first computing node, wherein the certificate of verifiable storage at least comprises a second code hash of the first computing logic;

compare the first code hash with the second code hash, and if the comparison result is

consistent, determine that the first code hash is verifiably stored.

18. The system according to claim 17, wherein the certificate of verifiable storage is received and forwarded to the first computing node by the trusted third party or administrator after the trusted third party or administrator provides the second code hash to a verifiable storage center.

19. The system according to claim 18, wherein the system further comprises a code storage center that maintains at least the first computing logic;

the code storage center is configured to receive a data acquisition request from the first provider, wherein the data acquisition request at least comprises the second code hash acquired by the first provider from the verifiable storage center;

the code storage center is further configured to provide the first computing logic to the first provider in response to the data acquisition request for the first provider to review the legitimacy of the first computing logic.

20. An apparatus for obtaining data authorization, disposed in any first proxy node of a trusted computing center; the trusted computing center comprises a data storage center, multiple trusted computing nodes, and corresponding proxy nodes; the data storage center maintains at least multiple encrypted shards of first private data of a first provider, wherein the multiple encrypted shards are obtained by splitting the first private data to be stored into multiple private shards and encrypting the multiple private shards using respective encryption keys; the apparatus comprises:

an obtaining unit, configured to obtain, from the first provider, a target encryption key among encryption keys corresponding to the multiple encrypted shards;

a sending unit, configured to send an authentication request to a corresponding first computing node;

a receiving unit, configured to receive authentication information returned by the first computing node, wherein the authentication information at least comprises a first code hash of a first computing logic running in the first computing node;

a determining unit, configured to perform trusted authentication on the first computing node based on the authentication information, and determine whether the first code hash is verifiably stored;

an establishment unit, configured to, when the trusted authentication passes and the first code hash is verifiably stored, establish a first trusted channel with the first computing node;

the sending unit is further configured to send the target encryption key to the first computing node through the first trusted channel; so that the first computing node obtains permission to perform computation on a target encrypted shard among the multiple encrypted shards corresponding to the target encryption key based on the first computing logic.

21. A computer readable storage medium, storing a computer program, wherein when the computer program is executed in a computer, the computer program causes the computer to perform the method according to any one of claims 1-10.

22. A computing device comprising a memory and a processor, wherein the memory stores executable code which when executed by the processor causes the computing device to perform the method according to any one of claims 1-10.