CLAIMS

1. A method for encrypting data, the method comprising:

collecting, by a data provider server, user data at a back end;

receiving, by the data provider server and from a modeling server, a second dimension of data features, wherein the second dimension of data features are selected by the modeling server according to one or more modeling demands of the modeling server;

collecting, by the data provider server and from the collected user data, a number of user private data as a number of data samples;

generating, by the data provider server, a target matrix comprising a first dimension based on the number of data samples and the second dimension of data features, the data features corresponding to the data samples, the data samples being associated with a user;

performing, by the data provider server, an encryption calculation on the target matrix based on a principal component analysis (PCA) algorithm to generate an encryption matrix comprising the first dimension and a third dimension that is smaller than the second dimension, wherein performing the encryption calculation on the target matrix further comprises:

separately performing zero averaging on values of vectors corresponding to the data features in the target matrix;

calculating a covariance matrix that corresponds to the target matrix and that is obtained after the zero averaging;

calculating eigenvalues of the covariance matrix and eigenvectors corresponding to the eigenvalues;

sorting the eigenvectors based on the eigenvalues, and extracting the third dimension of eigenvectors with the largest eigenvalues to generate a projection matrix comprising the second dimension and the third dimension; and

multiplying the target matrix by the projection matrix to obtain the encryption matrix; and

transmitting, by the data provider server, the encryption matrix to the modeling server executing a machine-learning model, wherein the encryption matrix is used to train the machine-

learning model for assessing a transaction risk of the user.

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

locally storing the projection matrix as the encryption matrix.

3. The method according to claim 2, wherein performing the encryption calculation further comprises:

determining whether the projection matrix is locally stored;

in response to determining that the projection matrix is locally stored, multiplying the target matrix by the projection matrix to obtain the encryption matrix; and

in response to determining that the projection matrix is not locally stored, performing encryption calculation on the target matrix based on the PCA algorithm to obtain the encryption matrix.

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

determining whether the data features change in terms of a dimension, or meanings represented by the data features change; and

in response to determining that the data features change in terms of a dimension, or meanings represented by the data features change, performing encryption calculation on the target matrix based on the PCA algorithm again, and updating the locally stored projection matrix based on the projection matrix.

5. The method according to claim 1, wherein the machine-learning model comprises a supervised machine-learning algorithm configured to generate a reliability score for the user.

6. An apparatus for encrypting data, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 5.