

CLAIMS

What is claimed is:

1. A computer-implemented method for identifying fraudulent transactions, comprising:
 - identifying, by a server, an operation sequence and time difference information associated with a transaction, wherein the operation sequence comprises a plurality of operations at a plurality of time points, and wherein the time difference information comprises a time difference between the time points of each two adjacent operations included in the transaction; and
 - predicting, by the server, a probability that the transaction is a fraudulent transaction based on a result provided by a deep learning network, wherein the deep learning network comprises a feature embedding subnetwork and a classifier subnetwork, comprising:
 - obtaining an operation embedding representation of each time point of the operation sequence, wherein the operation embedding representation of each time point of the operation sequence is an output at each corresponding time point of the feature embedding subnetwork, wherein an input to the feature embedding subnetwork is the operation sequence associated with the transaction;
 - obtaining a time difference embedding representation of each corresponding time point of the operation sequence, wherein the time difference embedding representation of each corresponding time point of the operation sequence is an output at each corresponding time point of the same feature embedding subnetwork, wherein an input to the feature embedding subnetwork is the time difference information associated with the transaction;
 - obtaining a combined embedding representation of the transaction by combining the operation embedding representation of each time point of the operation sequence and the time difference embedding representation of each corresponding time point of the operation sequence, comprising:
 - calculating a similarity between each pair of the operation embedding representation and the time difference embedding representation that corresponds to a specific time point; and

combining more than one operation features based on the calculated similarity to obtain the combined embedding representation of the transaction; and

predicting, by the classifier subnetwork, the probability that the transaction is a fraudulent transaction based on the combined embedding representation of the transaction.

2. The computer-implemented method of claim 1, further comprising training the deep learning network, wherein training the deep learning network comprises:

obtaining a black sample associated with a fraudulent transaction and a white sample associated with a non-fraudulent transaction;

separately extracting, from the black sample and from the white sample, an operation sequence and time difference information;

obtaining an operation embedding representation and a time difference embedding representation of the black sample and the white sample, comprising performing a feature conversion and a selection on each of the operation sequences and on each of the time difference information that are extracted from the black sample and the white sample to obtain a plurality of operation features and a plurality of time difference features;

obtaining a combined embedding representation of the transaction, comprising:

calculating a similarity between each pair of the operation feature and the time difference feature that corresponds to a specific time point;

combining more than one operation features based on the calculated similarity to obtain a combined operation feature; and

training the deep learning network through classification based on the combined operation feature.

3. The computer-implemented method of claim 2, wherein performing the feature conversion and the selection on each of the operation sequences and each of the time difference information comprises:

performing the feature conversion on each of the operation sequences and each of the time difference information to obtain an initial operation feature and an initial time feature; and

separately performing a dimension reduction and an irrelevant feature removal on the initial operation feature and the initial time feature to select the plurality of operation features and the plurality of time difference features.

4. The computer-implemented method of claim 2, wherein calculating a similarity between each pair of the operation feature and the time difference feature that corresponds to a specific time point comprises calculating an inner product of an operation feature matrix that includes the plurality of operation features and a time difference feature matrix that includes the plurality of time difference features to obtain a similarity between each of the operation features and the time difference features.

5. The computer-implemented method of claim 2, wherein the plurality of operation features are combined by calculating a sum of corresponding similarities.

6. The computer-implemented method of claim 2, wherein the deep learning network is trained based on at least one of a recurrent neural network (RNN) algorithm, a long short-term memory (LSTM) algorithm, a gated recurrent unit (GRU) algorithm, and a simple recurrent unit (SRU) algorithm.

7. An apparatus for identification of a fraudulent transaction, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 6.