

CLAIMS

What is claimed is:

1. A system for determining a fraud risk score associated with a transaction, the system comprising:
 - a server including an electronic processor configured to:
 - determine a plurality of rules based on a plurality of transactions over time,
 - extract one or more features of the transaction,
 - select, based on the plurality of rules, a plurality of fraud risk features from the one or more extracted features, wherein the plurality of fraud risk features include at least one selected from the group comprising a non-categorical fraud risk feature and a categorical fraud risk feature, each non-categorical fraud risk feature of the plurality of fraud risk features is associated with a fraud risk feature value, and each categorical fraud risk feature of the plurality of fraud risk features is associated with a categorical variable value,
 - determine, for each categorical fraud risk feature of the plurality of fraud risk features, a fraud risk feature value by transforming the categorical variable value associated with the categorical fraud risk feature using feature encoding,
 - determine an outlying fraud risk feature value of the fraud risk feature values associated with the plurality of fraud risk features,
 - transform one or more fraud risk feature values of the plurality of fraud risk features based on one or more of feature encoding, scaling, and standardization, the one or more fraud risk feature values including the outlying fraud risk feature value, and
 - determine the fraud risk score based on the one or more of the transformed fraud risk feature values.
2. The system according to claim 1, wherein the electronic processor is configured to select a plurality of fraud risk features from the one or more extracted features by using a feature selection technique or a clustering algorithm.

3. The system according to claim 1, wherein the electronic processor is configured to determine a fraud risk score based on the one or more of the transformed fraud risk feature values by executing an eXtreme Gradient Boosting tree algorithm to analyze the one or more of the transformed fraud risk feature values and generate the fraud risk score.

4. The system according to claim 1, wherein the electronic processor is configured to flag fraud risk features that are associated with low quality data.

5. The system according to claim 1, wherein the plurality of rules include a traffic rule, an anchor rule, or both, wherein the traffic rule is a rule pertaining to a user's traffic with respect to the transaction and the anchor rule is a measurement of activity observed against a specific anchor that has been at least one selected from the group comprising labeled as suspect, associated with a high-risk score, and known to be fraudulent .

6. The system according to claim 1, wherein the electronic processor is further configured to compare the fraud risk score to a predetermined threshold to determine a further action to take.

7. A method for determining a fraud risk score associated with a transaction, the method comprising:

determining a plurality of rules based on a plurality of transactions over time,

extracting one or more features of the transaction,

selecting, based on the plurality of rules, a plurality of fraud risk features from the one or more extracted features, wherein the plurality of fraud risk features include at least one selected from the group comprising a non-categorical fraud risk feature and a categorical fraud risk feature, each non-categorical fraud risk feature of the plurality of fraud risk features is associated with a fraud risk feature value, and each categorical fraud risk feature of the plurality of fraud risk features is associated with a categorical variable value,

determining, for each categorical fraud risk feature of the plurality of fraud risk features, a fraud risk feature value by transforming the categorical variable value associated with the categorical fraud risk feature using feature encoding,

determining an outlying fraud risk feature value of the fraud risk feature values associated with the plurality of fraud risk features,

transforming one or more fraud risk feature values of the plurality of fraud risk features based on one or more of scaling, and standardization, the one or more fraud risk feature values including the outlying fraud risk feature value, and

determining the fraud risk score based on the one or more of the transformed fraud risk feature values.

8. The method according to claim 7, wherein selecting a plurality of fraud risk features from the one or more extracted features includes using a feature selection technique or a clustering algorithm to select the plurality of fraud risk features.

9. The method according to claim 7, wherein determining a fraud risk score based on the one or more of the transformed fraud risk feature values includes executing an eXtreme Gradient Boosting tree algorithm to analyze the one or more of the transformed fraud risk feature values and generate the fraud risk score.

10. The method according to claim 7, the method further comprising flagging fraud risk features that are associated with low quality data.

11. The method according to claim 7, wherein the plurality of rules include a traffic rule, an anchor rule, or both, wherein the traffic rule is a rule pertaining to a user's traffic with respect to the transaction and the anchor rule is a measurement of activity observed against a specific anchor that has been at least one selected from the group comprising labeled as suspect, associated with a high-risk score, and known to be fraudulent.

12. The method according to claim 7, the method further comprising comparing the fraud risk score to a predetermined threshold to determine a further action to take.

13. A non-transitory computer-readable medium with computer-executable instructions stored thereon executed by an electronic processor included in a server to perform a method of determining a fraud risk score associated with a transaction, comprising:

determining a plurality of rules based on a plurality of transactions over time,

extracting one or more features of the transaction,

selecting, based on the plurality of rules, a plurality of fraud risk features from the one or more extracted features, wherein the plurality of fraud risk features include at least one selected from the group comprising a non-categorical fraud risk feature and a categorical fraud risk feature, each non-categorical fraud risk feature of the plurality of fraud risk

features is associated with a fraud risk feature value, and each categorical fraud risk feature of the plurality of fraud risk features is associated with a categorical variable value,

determine, for each categorical fraud risk feature of the plurality of fraud risk features, a fraud risk feature value by transforming the categorical variable value associated with the categorical fraud risk feature using feature encoding,

determining an outlying fraud risk feature value of the fraud risk feature values associated with the plurality of fraud risk features,

transforming one or more fraud risk feature values of the plurality of fraud risk features based on one or more of feature encoding, scaling, and standardization, the one or more fraud risk feature values including the outlying fraud risk feature value, and

determining the fraud risk score based on the one or more of the transformed fraud risk feature values.

14. The non-transitory computer-readable medium according to claim 13, wherein selecting a plurality of fraud risk features from the one or more extracted features includes using a feature selection technique or a clustering algorithm to select the plurality of fraud risk features.

15. The non-transitory computer-readable medium according to claim 13, wherein determining a fraud risk score based on the one or more of the transformed fraud risk feature values includes executing an eXtreme Gradient Boosting tree algorithm to analyze the one or more of the transformed fraud risk feature values and generate the fraud risk score.

16. The non-transitory computer-readable medium according to claim 13, the method further comprising flagging fraud risk features that are associated with low quality data.

17. The non-transitory computer-readable medium according to claim 13, wherein the plurality of rules include a traffic rule, an anchor rule, or both, wherein the traffic rule is a rule pertaining to a user's traffic with respect to the transaction and the anchor rule is a measurement of activity observed against a specific anchor that has been at least one selected from the group comprising labeled as suspect, associated with a high-risk score, and known to be fraudulent.

18. The non-transitory computer-readable medium according to claim 13, the method further comprising comparing the fraud risk score to a predetermined threshold to determine a further action to take.