Claims

1. An apparatus for real-time detection of fraudulent digital transactions, comprising:

a transceiver module arranged to receive information data of a digital transaction;

a model generator module arranged to dynamically generate a predictive model for fraud detection based collectively on historical information data relating to identified fraudulent transactions and the received information data; and

a fraud detection module having a plurality of anomaly detection modules arranged to respectively process the received information data differently to generate a plurality of scores, which are aggregated to provide an aggregated score to enable real-time determination of whether the digital transaction is a fraudulent digital transaction, wherein the plurality of anomaly detection modules include a predictive anomaly detection module configured to process the received information data using the predictive model to generate a first score;

a semantic anomaly detection module configured to convert the historical information data into anomaly graph structures for storing in an anomaly schema graph database, wherein the received information data is configured to be converted into semantic graph structures and compared with the anomaly graph structures from the anomaly schema graph database to generate a second score; and

a velocity detection module configured to match the received information data to a dynamic group to generate a third score, wherein the plurality of scores include the first score, the second score and the third score

2. The apparatus of claim 1, wherein the fraud detection module further includes an aggregation module configured to aggregate the plurality of scores to provide the aggregated score.

3. The apparatus of any preceding claims, wherein the transceiver module includes being configured to transmit the aggregated score to a payment server from which the digital transaction originates.

4. The apparatus of any preceding claims, wherein the plurality of scores

are arranged to be normalised, prior to being aggregated.

5. The apparatus of any preceding claims, wherein the model generator module includes being configured to use machine learning to dynamically generate the predictive model.

6. The apparatus of any preceding claims, wherein the model generator module includes:

a data transformation module to process the received information data into an associated data representation with reference to a predetermined format;

an extraction module to extract respective values of predetermined data fields in the data representation; and

a model building module to generate the predictive model based on the extracted values.

7. The apparatus of any preceding claims, wherein the fraud detection module is further configured to provide an anomaly score, further comprising:

a recommender module arranged to receive the anomaly score and compare the anomaly score with a threshold value to generate a signal,

wherein based on the generated signal, the recommender module is configured to trigger at least one rule from a fraud rules database, and a weightage value associated with the triggered rule is provided to at least the first anomaly detection module to enable the first anomaly detection module to use the weightage value to process information data of a new digital transaction received.

8. The apparatus of claim 7, wherein the at least one rule includes a plurality of rules, and respective weightage values are associated with respective rules, and; wherein the weightage values are combined and normalized into a single weightage value which is provided to the first anomaly detection module.

9. The apparatus of any preceding claims, wherein a second anomaly detection module is configured to process the received information data using semantic anomaly detection or velocity detection with temporal analysis to generate a second score.

10. The apparatus of any preceding claims, wherein the aggregated score is

compared against a predetermined threshold value, in which the aggregated score being greater than the threshold value indicates a fraudulent digital transaction, and the aggregated score being smaller than the threshold value indicates a non-fraudulent digital transaction.

11. The apparatus of any preceding claims, wherein the apparatus includes a computing device.

12. A method performed by an apparatus for real-time detection of fraudulent digital transactions, the apparatus includes a transceiver module, a model generator module, and a fraud detection module having a plurality of anomaly detection modules, the method comprises:

(i) receiving information data of a digital transaction by the transceiver module;

(ii) dynamically generating a predictive model for fraud detection by the model generator module based collectively on historical information data relating to identified fraudulent transactions and the received information data; and

(iii) respectively processing the received information data differently by the plurality of anomaly detection modules to generate a plurality of scores, wherein the plurality of anomaly detection modules includes a predictive anomaly detection module configured to process the received information data using the predictive model to generate a first score;

a semantic anomaly detection module configured to convert the historical information data into anomaly graph structures for storing in an anomaly schema graph database, wherein the received information data is configured to be converted into semantic graph structures and compared with the anomaly graph structures from the anomaly schema graph database to generate a second score; and

a velocity detection module configured to match the received information data to a dynamic group to generate a third score, wherein the plurality of scores include the first score, the second score and the third score, which are aggregated to provide an aggregated score to enable real-time determination of whether the digital transaction is a fraudulent digital transaction.

13. The method according to claim 12, wherein the fraud detection module further includes an aggregation module configured to aggregate the plurality of scores to provide the aggregated score.

14. The method according to claim 12, wherein the semantic graph structures include concept nodes and relation nodes.