

CLAIMS

1. An authentication method, comprising:
 - constructing a graph to represent a set of data, the set of data comprising identities and known relationships between the identities, wherein each node in the graph corresponds to each of the identities and each edge in the graph corresponds to each of the known relationships;
 - predicting unknown relationships between the identities using a model that is trained based on a link prediction algorithm;
 - updating the graph to further comprise at least one new edge that corresponds to a predicted relationship, wherein the updated graph comprises at least one node that corresponds to an identity with a known fraudster label;
 - labeling at least one other identity with a fraudster label based on a label propagation algorithm, wherein the fraudster label is propagated from the known fraudster label; and
 - refusing authentication of the at least one other identity with the fraudster label.
2. The method as claimed in claim 1, wherein the model is trained based on the link prediction algorithm with the set of data.
3. The method as claimed in claim 2, wherein the predicted relationship and the at least one fraudster label are added to the set of data to form a revised set of data, and wherein the method further comprises re-training the model based on the link prediction algorithm with the revised set of data.
4. The method as claimed in any one of the preceding claims, wherein the known relationships are based on similarity of a characteristic of the identities.
5. The method as claimed in claim 4, wherein the characteristic of the identities comprises: biometric data, identity document data and/or personal electronic device data.
6. An authentication system, comprising:
 - a processor module; and
 - a memory module including computer program code;

the memory module and the computer program code configured to, with the processor module, cause the system at least to:

construct a graph to represent a set of data, the set of data comprising identities and known relationships between the identities, wherein each node in the graph corresponds to each of the identities and each edge in the graph corresponds to each of the known relationships;

predict unknown relationships between the identities using a model that is trained based on a link prediction algorithm;

update the graph to further comprise at least one new edge that corresponds to a predicted relationship, wherein the updated graph comprises at least one node that corresponds to an identity with a known fraudster label;

label at least one other identity with the fraudster label based on a label propagation algorithm, wherein the fraudster label is propagated from the known fraudster label; and

refuse authentication of the at least one other identity with the fraudster label.

7. The system as claimed in claim 7, wherein the model is trained based on the link prediction algorithm with the set of data.

8. The system as claimed in claim 8, wherein the predicted relationship and the at least one fraudster label are added to the set of data to form a revised set of data, and wherein the system is further caused to re-train the model based on the link prediction algorithm with the revised set of data.

9. The system as claimed in any one of claims 7 to 9, wherein the known relationships are based on similarity of a characteristic of the identities.

10. The system as claimed in claim 10, wherein the characteristic of the identities comprises: biometric data, identity document data and/or personal electronic device data.