

CLAIMS

What is claimed is:

1. A computer-implemented method for identity proofing, the method comprising:
training a space segmentation model associated with historical data of identities, wherein the historical data comprises attributes of the identities, values of the attributes of the identities, and time stamps related to activities of the identities;
receiving data corresponding to a new identity, wherein the data comprises attributes of the new identity, values of the attributes of the new identity, and time stamps related to activities of the new identity;
calculating, for the new identity and the historical data of identities, occurrence times of the values of the attributes between a first time stamp and a second time stamp;
segmenting the new identity from the historical data of identities using the space segmentation model based on the occurrence times, wherein the new identity is isolated after a number of segmentation times; and
proofing authenticity of the new identity based on the number of segmentation times.
2. The method as claimed in claim 1, wherein the occurrence times of the values of the attributes between a first time stamp and a second time stamp are represented as a vector.
3. The method as claimed in claim 1 or 2, wherein the occurrence times are adjusted based on text frequency.
4. The method as claimed in any one of the preceding claims, wherein between the first time stamp and the second time stamp is in a form of a sliding time window.
5. The method as claimed in any one of the preceding claims, further comprising:
determining if the data received comprises data corresponding to an image of an identity document; and
in response to the data received is determined to comprise data corresponding to an image of an identity document, extracting the attributes of the new identity and the values of the attributes of the new identity from the image.

6. The method as claimed in claim 5, wherein determining if the data received comprises data corresponding to an image of an identity document is based on a classification algorithm.
7. The method as claimed in claim 5 or 6, wherein extracting the attributes of the new identity and the values of the attributes of the new identity from the image is based on an optical character recognition (OCR) algorithm.
8. The method as claimed in any one of the preceding claims, wherein the trained space segmentation model comprises a tree model.
9. The method as claimed in any one of the preceding claims, the method further comprising:
 - updating the historical data of identities by including the new identity.
10. The method as claimed in any one of the preceding claims, wherein the attribute of the identities is selected from the group comprising name, date of birth, place of birth, height, weight, identity document number, and address.
11. The method as claimed in any one of the preceding claims, wherein the activity of the identities is selected from the group comprising registration, updating information, logging in, logging out, and identity proofing.
12. The method as claimed in claim 11, wherein the identity proofing comprises a Know Your Customer (KYC) process.
13. A system for identity authentication, the system comprising:
 - one or more processors; and
 - one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any one of claims 1 to 12.
14. An apparatus for identity authentication, the apparatus comprising a plurality of modules for performing the method of any one of claims 1 to 12.