CLAIMS

1. A system for early fake account detection, the system comprising:

one or more processors; and

a memory having instructions stored therein, the instructions, when executed by the one or more processors, cause the one or more processors to:

for each predetermined time step of a sequence of predetermined time steps

collect user registration signals when a user registers for an account;

collect booking signals when the user books a ride hailing service using the account;

collect transaction signals when the user makes a transaction using the account;

collect clickstream data when the user interacts with the account; and

concatenate the user registration signals, the booking signals, the transaction signals and the clickstream data to obtain a vector of signals; and

determine whether the account is fake using a sequence of vectors of signals comprising the vector of signals for each predetermined time step.

2. The system of claim 1, wherein the system is optimized for early detection time.

3. The system of claim 1 or 2, wherein the sequence of vectors of signals is obtained by concatenating the vectors of signals for each predetermined time step.

4. The system of any one of claims 1 to 3, wherein the sequence of vectors of signals is used as an input to a machine learning model, and the one or more processors are configured to use the machine learning model to determine whether the account is fake.

5. The system of claim 4, wherein the machine learning model is trained for both prediction accuracy and detection time.

6. The system of any one of claims 1 to 5, wherein the one or more processors are configured to determine whether the account is fake given the sequence of vectors of signals of a predetermined length T.

7. The system of claim 4, wherein the one or more processors are configured to process the sequence of vectors of signals and embed the sequence of vectors of signals into a hidden state to obtain an intermediate output, wherein the intermediate output is a hazard rate, and wherein the hazard rate indicates an instantaneous probability that an account ban is triggered.

8. The system of claim 6, wherein the one or more processors are configured to add paddings to the sequence of vectors of signals if a current time step is less than the predetermined length T of the predetermined time steps.

9. A method for early fake account detection, the method comprising using one or more processors to:

for each predetermined time step of a sequence of predetermined time steps

collect user registration signals when a user registers for an account;

collect booking signals when the user books a ride hailing service using the account;

collect transaction signals when the user makes a transaction using the account; and

collect clickstream data when the user interacts with the account;

concatenate the user registration signals, the booking signals, the transaction signals and the clickstream data to obtain a vector of signals; and

determine whether the account is fake using a sequence vectors of signals comprising the vector of signals for each predetermined time step.

10. The method of claim 9, wherein the method is optimized for early detection time.

11. The method of claim 9 or 10, wherein the vector of signals is obtained for each predetermined time step.

12. The method of any one of claims 9 to 11, wherein the sequence of vectors of signals is used as an input to a machine learning model, and the method further comprises using the one or more processors to use the machine learning model to determine whether the account is fake.

13. The method of claim 12, comprising simultaneously optimizing the machine learning model for prediction accuracy and detection time.

14. The method of claim 13, wherein the method further comprises using the one or more processors to determine whether the account is fake given the sequence of vectors of signals of a predetermined length T.

15. The method of claim 12, wherein the method further comprises using the one or more processors to process the sequence of vectors of signals and embed the sequence of vectors of signals into a hidden state to obtain an intermediate output, wherein the intermediate output is a hazard rate, and wherein the hazard rate indicates an instantaneous probability that an account ban is triggered.

16. The method of claim 14, wherein the method further comprises using the one or more processors to add paddings to the sequence of vectors of signals if a current time step is less than the predetermined length T of the predetermined time steps.

17. A non-transitory computer-readable medium storing computer executable code comprising instructions for early fake account detection according to any one of claims 9 to 16.

18. A computer executable code comprising instructions for early fake account detection according to any one of claims 9 to 16.