RESEARCH DETAIL

MODEL FOR MONITORING SUSPICIOUS INDIVIDUAL CUSTOMERS IN BANKS.

An application of big data technology in bank and financial fields.

PROJECT OVERVIEW

- The main objective is to predict and identify the risk of using bank accounts for illegal financial activities such as telecommunication fraud, gambling, selling or renting accounts through machine learning techniques
- The project divides the business scenarios into four areas: suspicious customer detection, unusual transaction detection, anti-money laundering detection and fraud detection,
- This project selects two machine learning algorithms, Random Forest and Self-Encoder, and explains in detail the rationale for their selection, their advantages, feature engineering and the main learning process

PROJECT BACKGROUND

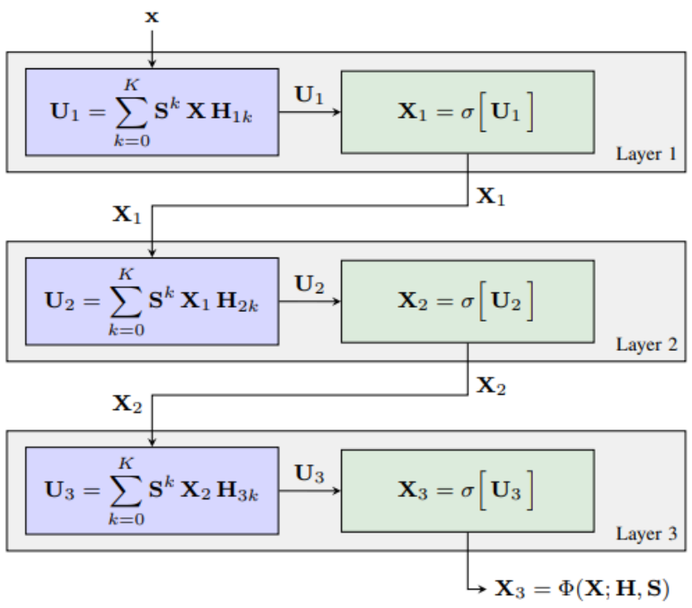
- With the popularity of Internet-based financial services, financial crimes, especially illegal financial activities such as telecommunication fraud, Internet gambling, money-laundering and fraud, are also on the rise.
- Advances in big data and machine learning technologies have provided the financial industry with new tools to improve the efficiency and accuracy of monitoring suspicious activity. By analysing large volumes of transaction data, machine learning models are able to identify normal transaction patterns and identify suspicious behaviour that deviates from the norm.

PROBLEM TO SOLVE

- How machine learning algorithms can analyse data such as customer identifiers, occupations, places of residence and more to identify potentially suspicious customers?
- How to monitor and identify unusual trading behaviour in client accounts?
- How to identify possible money laundering by analysing transaction patterns?
- How to achieve real-time monitoring of suspicious fund flows and rapid manual review and intervention when suspicious activity is detected?

GNN MODEL CONSTRUCTION

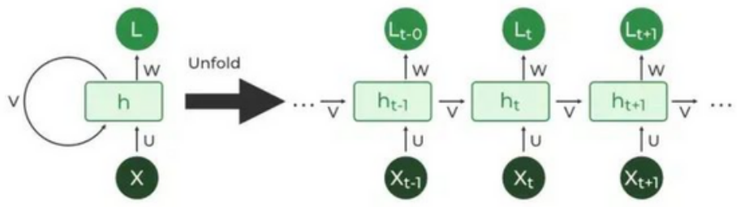
Use a graph convolutional network (GNN) or other graph neural network structure to learn complex patterns of accounts and transactions.The model will learn an embedded representation of the node (account) that captures as much information as possible about the node's neighbourhood (transactions and other accounts associated with it).The embedded representation of each account is passed through a downstream classifier (e.g., logistic regression, neural network) to predict whether the account is involved in fraudulent behaviour.



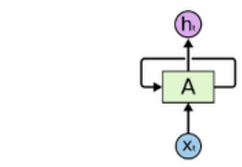
With the node-embedded representation of the GNN, we can capture the transaction patterns and network structure among different accounts, and thus effectively detect abnormal transactions or accounts with higher risks.

RNN MODEL CONSTRUCTION

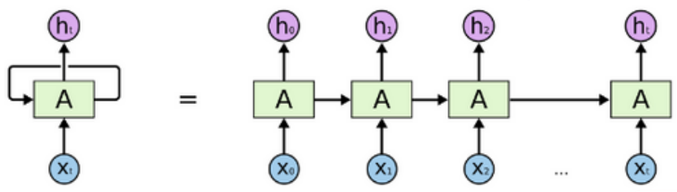
EThe ability of RNNs to process sequential data is utilised to extract features from the customer's transaction history. These features may include changes in transaction patterns, unusual increases in transaction frequency, frequency of large transactions, etc.



Training RNN models using historical transaction data. This data should include both normal transactions and transactions that have been flagged as suspicious so that the model learns to distinguish between the two.



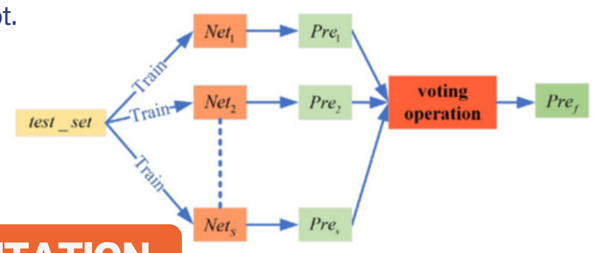
Recurrent Neural Networks have loops.



An unrolled recurrent neural network.

LSTM MODEL CONSTRUCTION

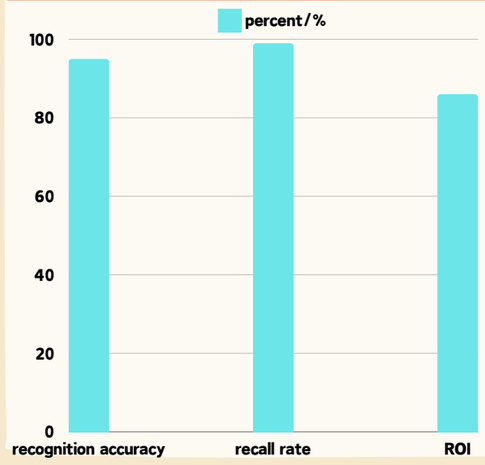
The trained LSTM model can be used to monitor the trading behaviour of customers in real time. The model will analyse the sequence of transactions and predict whether a transaction is suspicious or not.

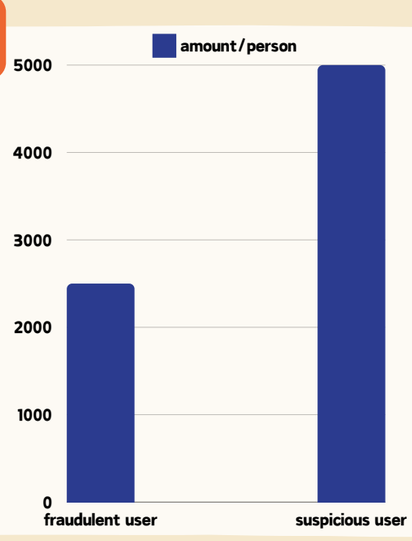


CITATION

1.Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
2.Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., ... & Zheng, X. (2016). TensorFlow: Large-scale machine learning on heterogeneous systems.
3.Olah, C. (2015). Understanding LSTM Networks. http://colah.github.io/posts/2015-08-Understanding-LSTMs/

PROJECT OUTCOMES





CONCLUSION

- The project analyses customers' identity information, occupation, place of residence, through machine learning models to identify potentially suspicious customers.
- By monitoring the trading behaviour of customer accounts, the model is able to identify unusual transactions that do not match the customer's historical trading behaviour or do not match the trading behaviour of similar accounts
- The project aims to achieve real-time monitoring of suspicious fund flows and enable rapid manual review and intervention when anomalies are detected

contact me :19302010047@fudan.edu.cn