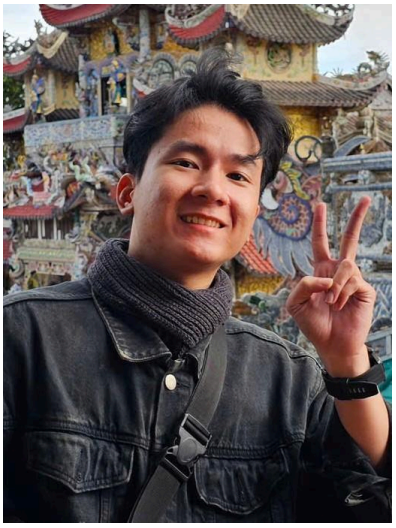
THÔNG TIN CHUNG CỦA NHÓM

- Link YouTube video của báo cáo (tối đa 5 phút):
  https://youtu.be/wwXwhybtof4
- Link slides (dạng .pdf đặt trên Github của nhóm):
  https://github.com/DangHaiThinh2001/Final_Project-CS2205.CH183/blob/main/Th%E1%BB%8Bnh%20%C4%90%E1%BA%B7ng%20H%E1%BA%A3i%20-%20CS2205.NOV2024.DeCuong.FinalReport.Template.Slide.pdf
- *Mỗi thành viên của nhóm điền thông tin vào một dòng theo mẫu bên dưới*
- *Sau đó điền vào Đề cương nghiên cứu (tối đa 5 trang), rồi chọn Turn in*
- *Lớp Cao học, mỗi nhóm một thành viên*

- Họ và Tên: Đặng Hải Thịnh
- MSSV: 240202014



- Lớp: CS2205.CH183
- Tự đánh giá (điểm tổng kết môn): 9/10
- Số buổi vắng: 0
- Số câu hỏi QT cá nhân: 4
- Số câu hỏi QT của cả nhóm: 4
- Link Github:
  https://github.com/DangHaiThinh2001/Final_Project-CS2205.CH183

ĐỀ CƯƠNG NGHIÊN CỨU

TÊN ĐỀ TÀI (IN HOA)

PHÁT HIỆN VÀ NGĂN CHẶN GIAO DỊCH ĐẾN NHỮNG TÀI KHOẢN LỪA ĐẢO SỬ DỤNG HỌC SÂU

TÊN ĐỀ TÀI TIẾNG ANH (IN HOA)

DETECTING & PREVENTING FRAUDULENT TRANSACTIONS USING DEEP LEARNING

TÓM TẮT *(Tối đa 400 từ)*

Sự bùng nổ của công nghệ tài chính mang lại vô số cơ hội nhưng đồng thời cũng đặt ra thách thức nghiêm trọng trong việc kiểm soát các hành vi lừa đảo ngày càng tinh vi và phức tạp. Các phương pháp truyền thống đã trở nên lỗi thời, không theo kịp sự biến đổi linh hoạt của các thủ đoạn lừa đảo hiện đại. Nghiên cứu này đề xuất một phương pháp tiên tiến ứng dụng Deep Learning để phát hiện và ngăn chặn giao dịch đến các tài khoản lừa đảo. Mô hình này có khả năng phân tích khối lượng dữ liệu khổng lồ, nhận diện những hành vi bất thường và đưa ra cảnh báo kịp thời, giúp ngăn chặn tổn thất tài chính trước khi xảy ra. Hệ thống này sẽ được so sánh với các phương pháp truyền thống và được đánh giá trong điều kiện thực tế để đảm bảo tính ứng dụng cao trong các nền tảng thanh toán hiện đại.

GIỚI THIỆU *(Tối đa 1 trang A4)*

Trong bối cảnh chuyển đổi số mạnh mẽ, thanh toán trực tuyến đã trở thành một phần không thể thiếu trong nền kinh tế hiện đại. Tuy nhiên, song song với sự phát triển vượt bậc này là sự gia tăng đáng báo động của các hành vi lừa đảo tài chính. Những thủ đoạn phổ biến như giả mạo danh tính, chiếm đoạt tài khoản, hù dọa, tống tiền, lừa đảo tín dụng… không ngừng thay đổi, gây thiệt hại nặng nề cho cá nhân và tổ chức tài chính. Hầu hết các hệ thống phát hiện lừa đảo hiện nay vẫn dựa trên các quy tắc cố định hoặc mô hình thống kê đơn giản, vốn thiếu tính linh hoạt và không thể theo kịp sự phát triển của các phương thức lừa đảo mới. Những hệ

thống này thường chỉ phản ứng sau khi lừa đảo đã xảy ra, thay vì chủ động nhận diện và ngăn chặn ngay từ đầu. Do đó, cần có một phương pháp mạnh mẽ hơn, có khả năng học hỏi từ dữ liệu và liên tục thích nghi với những hình thức lừa đảo mới. Deep Learning đã chứng minh được tiềm năng vượt trội trong việc phát hiện các bất thường trong dữ liệu lớn, giúp nâng cao hiệu quả nhận diện lừa đảo tài chính. Nghiên cứu này hướng đến việc phát triển một hệ thống phát hiện lừa đảo hiện đại, ứng dụng học sâu để phân tích giao dịch tài chính theo thời gian thực, từ đó nâng cao mức độ an toàn cho các hệ thống thanh toán và bảo vệ người dùng trước những rủi ro tài chính nghiêm trọng.

MỤC TIÊU *(Viết trong vòng 3 mục tiêu)*

1. Phát triển mô hình Deep Learning có khả năng phát hiện và ngăn chặn giao dịch đến tài khoản lừa đảo với độ chính xác cao.
2. Tích hợp mô hình vào hệ thống thanh toán trực tuyến để kiểm tra tính hiệu quả trong môi trường thực tế.
3. So sánh hiệu suất của mô hình với các phương pháp phát hiện lừa đảo truyền thống.

NỘI DUNG VÀ PHƯƠNG PHÁP

1. **Thu thập và xử lý dữ liệu:**

   Thu thập dữ liệu từ nhiều nguồn: Việc thu thập dữ liệu từ nhiều nguồn khác nhau giúp mô hình có thể học được nhiều dạng lừa đảo đa dạng, từ giao dịch ngân hàng truyền thống đến thanh toán điện tử.

   Tiền xử lý dữ liệu:

   - Loại bỏ dữ liệu bị thiếu hoặc nhiễu bằng phương pháp loại bỏ giá trị ngoại biên (outlier) để tránh ảnh hưởng tiêu cực đến quá trình huấn luyện.
   - Chuẩn hóa các đặc trưng số liệu bằng phương pháp Min-Max Scaling nhằm giữ cho tất cả dữ liệu có cùng một phạm vi giá trị, giúp mô hình học tốt hơn.

- Mã hóa các dữ liệu danh mục bằng phương pháp One-Hot Encoding hoặc Embedding để biến đổi dữ liệu văn bản hoặc danh mục thành dạng số, giúp mô hình hiểu được các mối quan hệ giữa các biến đầu vào.

Khai thác đặc trưng:

- Feature Engineering được sử dụng để tạo ra các đặc trưng mới từ dữ liệu thô (ví dụ: tần suất giao dịch theo giờ, giá trị trung bình giao dịch theo tài khoản), giúp mô hình có thêm thông tin quan trọng.
- Áp dụng Principal Component Analysis (PCA) để giảm chiều dữ liệu, giúp loại bỏ các đặc trưng không quan trọng và tăng tốc độ huấn luyện mô hình.

2. **Xây dựng mô hình học sâu:**

Mạng Nơ-ron Hồi tiếp (RNN): Sử dụng RNN, đặc biệt là LSTM, để phân tích chuỗi thời gian của các giao dịch. Điều này giúp mô hình nhận biết các thay đổi bất thường trong hành vi tài chính của một tài khoản theo thời gian.

Mạng Nơ-ron Đồ thị (GNN): Lừa đảo tài chính thường liên quan đến nhiều tài khoản có liên kết với nhau. GNN có thể mô hình hóa các giao dịch dưới dạng một mạng lưới để phát hiện các cụm giao dịch bất thường.

Học không giám sát (Unsupervised Learning):

- Sử dụng Autoencoder để phát hiện các giao dịch bất thường không có nhãn trước đó.
- Áp dụng Isolation Forest để phát hiện các giao dịch lệch chuẩn, giúp phát hiện những giao dịch có mức giá trị hoặc tần suất bất thường.

Học có giám sát (Supervised Learning):

- Sử dụng thuật toán LSTM với Attention Mechanism để dự đoán rủi ro của giao dịch dựa trên lịch sử tài khoản. Giúp mô hình tập trung vào các đặc điểm quan trọng trong chuỗi giao dịch thay vì xử lý tất cả thông tin một cách cứng nhắc.
- Huấn luyện mô hình bằng phương pháp Gradient Descent với Adaptive Learning Rate để tối ưu hóa tốc độ học và tránh overfitting.

3. **Huấn luyện và đánh giá mô hình**

   Chia tập dữ liệu: Sử dụng kỹ thuật k-fold cross-validation để đảm bảo mô hình có thể tổng quát hóa tốt trên dữ liệu mới.

   Tăng cường dữ liệu (Data Augmentation): Dữ liệu lừa đảo thường có số lượng rất ít, do đó cần sử dụng phương pháp SMOTE để tạo thêm các mẫu dữ liệu lừa đảo nhân tạo, giúp cân bằng dữ liệu và cải thiện hiệu suất mô hình.

   Tiêu chí đánh giá mô hình:

   - **Độ chính xác (Accuracy)**: Đo lường khả năng mô hình phân loại chính xác giao dịch khả nghi.
   - **Tỉ lệ phát hiện (Recall)**: Đánh giá khả năng mô hình tìm ra các giao dịch khả nghi mà không bỏ sót.
   - **Chỉ số F1-score**: Cân bằng giữa Precision và Recall để tránh trường hợp mô hình phát hiện sai quá nhiều hoặc bỏ sót giao dịch khả nghi.
   - **AUC-ROC Curve**: Giúp đánh giá hiệu suất mô hình trên nhiều ngưỡng phân loại khác nhau.

4. **Triển khai và thử nghiệm thực tế**

   Xây dựng API tích hợp với hệ thống thanh toán:

   - Sử dụng Flask hoặc FastAPI để xây dựng dịch vụ phát hiện lừa đảo, giúp hệ thống có thể đưa ra quyết định trong thời gian thực.
   - Kết nối API với hệ thống giao dịch để ngăn chặn các giao dịch đáng ngờ ngay lập tức.

   Giám sát và cập nhật mô hình liên tục:

   - Áp dụng kỹ thuật Online Learning để mô hình có thể thích ứng với các thay đổi trong hành vi lừa đảo theo thời gian.
   - Sử dụng Reinforcement Learning để tối ưu hóa các quyết định chặn giao dịch, giảm thiểu các trường hợp chặn nhầm.

   Đánh giá hiệu quả trên dữ liệu thực tế:

   - So sánh số lượng giao dịch bị chặn và số lượng giao dịch lừa đảo chưa được phát hiện để tối ưu hóa quy trình phát hiện lừa đảo.

- Thu thập phản hồi từ tổ chức và người dùng để cải thiện hệ thống.

KẾT QUẢ MONG ĐỢI

1. **Độ chính xác cao trong phát hiện giao dịch lừa đảo:** Hệ thống dự kiến sẽ đạt độ chính xác trên 90% trong việc phân loại các giao dịch đáng ngờ.
2. **Giảm thiểu tổn thất tài chính:** Bằng cách chặn các giao dịch trước khi tiền được chuyển đến tài khoản lừa đảo, hệ thống giúp giảm đáng kể thiệt hại cho khách hàng và tổ chức tài chính.
3. **Phát hiện kịp thời các mô hình lừa đảo mới:** Nhờ khả năng học liên tục, hệ thống có thể nhanh chóng thích nghi và phát hiện các mô hình lừa đảo mới mà các phương pháp truyền thống không kịp nhận diện.
4. **Tích hợp dễ dàng với hệ thống tài chính hiện có:** Hệ thống được thiết kế để có thể triển khai trên nền tảng giao dịch tài chính sẵn có, thông qua các API giúp các tổ chức tài chính dễ dàng tích hợp vào quy trình hiện tại.

TÀI LIỆU THAM KHẢO *(Định dạng DBLP)*

[1]. R Sivarethinamohan: Integration of Deep Learning and Particle Swarm Optimization for Enhanced Accounting Fraud Detection. 2023 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)

[2]. Sepp Hochreiter, Jürgen Schmidhuber: Long Short-Term Memory. Neural Computation (Volume: 9, Issue: 8, 15 November 1997)

[3]. Fawaz Khaled Alarfaj; Shabnam Shahzadi: Enhancing Fraud Detection in Banking with Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention. IEEE Access (Volume: 13) 23 September 2024

[4]. Aayush Sheth; Arjun Nair; Aashutosh Rai; Rupali Sawant**:** Prediction and Analysis of Fraud Detection in Finance: A Deep Learning and Machine Learning based approach. 2024 4th International Conference on Intelligent Technologies

[5]. Min Li; Mengjie Sun; Qianlong Liu; Yumeng Zhang: Fraud Detection Based on Graph Neural Networks with Self-attention. 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology