HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Đỗ Việt Anh

NGHIÊN CỨU VÀ ỨNG DỤNG CÁC PHƯƠNG PHÁP HỌC MÁY ĐỂ PHÁT HIỆN GIAN LẬN GIAO DỊCH TRONG HỆ THỐNG THANH TOÁN NGÂN HÀNG

ĐỀ ÁN TỐT NGHIỆP THẠC SĨ KỸ THUẬT

(***Theo định hướng ứng dụng***)

HÀ NỘI - NĂM 2025

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Đỗ Việt Anh

NGHIÊN CỨU VÀ ỨNG DỤNG CÁC PHƯƠNG PHÁP HỌC MÁY ĐỂ PHÁT HIỆN GIAN LẬN GIAO DỊCH TRONG HỆ THỐNG THANH TOÁN NGÂN HÀNG

Chuyên ngành: Hệ thống thông tin

Mã số: 8.48.01.04

ĐỀ ÁN TỐT NGHIỆP THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS. NGUYỄN TRỌNG KHÁNH

HÀ NỘI - 2025

LỜI CAM ĐOAN

Tôi cam đoan đây là công trình nghiên cứu của riêng tôi.

Các số liệu, kết quả nêu trong đề án tốt nghiệp là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

TÁC GIẢ ĐỀ ÁN

ĐỖ VIỆT ANH

LỜI CẢM ƠN

Trước tiên, em xin cám ơn Học viện Công nghệ Bưu chính viễn thông, Khoa Đào tạo sau đại học, các thầy cô giáo của Học viện đã tạo điều kiện và trực tiếp giảng dạy, giúp đỡ em hoàn thành chương trình đào tạo Thạc sĩ kỹ thuật.

Em xin gửi lời cảm ơn sâu sắc tới PGS.TS. Nguyễn Trọng Khánh đã dành nhiều thời gian, tâm huyết hướng dẫn tận tình và đóng góp các ý kiến để em hoàn thiện đề án này.

Em xin chân thành cảm ơn Ban lãnh đạo, anh chị em đồng nghiệp tại Trung tâm Phát triển Phần mềm - Ngân hàng Thương mại Cổ phần Đầu tư và Phát triển Việt Nam đã nhiệt tình góp ý trong quá trình em thực hiện khảo sát và viết bài.

Cuối cùng, em muốn bày tỏ sự biết ơn đối với gia đình, người thân, bạn bè đã luôn bên cạnh khích lệ, động viên, giúp đỡ em trong suốt thời gian học tập và hoàn thiện luận văn.

Em xin trân trọng cảm ơn.

Hà Nội, ngày tháng năm 2025

Người viết

Đỗ Việt Anh

MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ, CHỮ VIẾT TẮT **v**
DANH MỤC CÁC BẢNG **vi**
DANH MỤC CÁC HÌNH **vii**
MỞ ĐẦU **1**
1. Lý do chọn đề tài 1
2. Tổng quan về vấn đề nghiên cứu 1
3. Đối tượng và phạm vi nghiên cứu 1
4. Phương pháp nghiên cứu 2
5. Cấu trúc luận văn 2
CHƯƠNG 1: CƠ SỞ LÝ LUẬN **3**
1.1. Giới thiệu chương 3
1.2. Gian lận tài chính trong hệ thống ngân hàng 3
1.3. Học máy trong phát hiện gian lận giao dịch 5
1.4. Các nghiên cứu liên quan 7
1.4.1. Các nghiên cứu khai phá dữ liệu và mô hình học máy truyền thống 7
1.4.2. Xử lý dữ liệu mất cân bằng và học máy lai (hybrid) 8
1.4.3. Các tiếp cận học sâu và mô hình chuỗi 9
1.4.4. Nhận xét và khoảng trống nghiên cứu 9
1.5. Kết luận chương 11
CHƯƠNG 2: ĐỀ XUẤT MÔ HÌNH **12**
2.1. Giới thiệu chương 12
2.2. Cơ sở lựa chọn mô hình 12
2.3. Nhóm mô hình học máy truyền thống 13
2.3.1. Logistic Regression 13
2.3.2. Random Forest 14
2.3.3. XGBoost 14
2.4. Nhóm mô hình học sâu theo chuỗi thời gian 15
2.4.1. Mô hình LSTM (Long Short-Term Memory) 15
2.5. Lý do lựa chọn bộ mô hình trong nghiên cứu 17
2.6. Kết luận chương 18
CHƯƠNG 3: THỰC NGHIỆM VÀ ĐÁNH GIÁ **19**
3.1. Giới thiệu chương 19
3.2. Bộ dữ liệu sử dụng trong nghiên cứu 19
3.3. Tiền xử lý dữ liệu 21
3.4. Phân chia dữ liệu huấn luyện và kiểm thử 22

3.5. Cấu hình huấn luyện và tham số mô hình 23
3.6. Các chỉ số đánh giá mô hình 27
3.7. Kết quả thực nghiệm 29
3.8. Phân tích và đánh giá kết quả 34
3.9. Kết luận chương 36
CHƯƠNG 4: CÀI ĐẶT, THỬ NGHIỆM VÀ BÀN LUẬN 37
4.1. Giới thiệu chương 37
4.2. Kiến trúc triển khai 37
4.3. Mô phỏng thử nghiệm trong môi trường giả lập 40
4.4. Đánh giá khả năng triển khai thực tế vào hệ thống ngân hàng 45
4.5. Hạn chế và hướng cải tiến 46
4.6. Kết quả và bàn luận 48
4.6.1. So sánh tổng quan các mô hình 48
4.6.2. Bàn luận chi tiết theo từng mô hình 49
4.6.3. Ý nghĩa đối với nghiệp vụ ngân hàng 50
4.6.4. Hạn chế nghiên cứu 51
4.6.5. Hướng nghiên cứu tiếp theo 51
4.7. Kết luận chương 51
KẾT LUẬN VÀ KIẾN NGHỊ 52
1. Kết luận 52
2. Kiến nghị 52
3. Lời kết 53
DANH MỤC TÀI LIỆU THAM KHẢO 54

DANH MỤC CÁC THUẬT NGỮ CHỮ VIẾT TẮT

Viết tắt	Tiếng Anh	Tiếng Việt
API	Application Programming Interface	Giao diện lập trình ứng dụng
AUC	Area Under the Curve	Diện tích dưới đường cong ROC
DL	Deep Learning	Học sâu
FN	False Negative	Dự đoán sai – bỏ sót gian lận
FP	False Positive	Dự đoán sai – báo nhầm gian lận
F1-score	F1-score	Chỉ số đánh giá hài hòa Precision – Recall
GPU	Graphics Processing Unit	Bộ xử lý đồ họa
JSON	JavaScript Object Notation	Định dạng dữ liệu JSON
LR	Logistic Regression	Mô hình hồi quy logistic
LSTM	Long Short-Term Memory	Mạng bộ nhớ dài–ngắn hạn
ML	Machine Learning	Học máy
RNN	Recurrent Neural Network	Mạng nơ-ron hồi quy
RF	Random Forest	Rừng cây ngẫu nhiên
ROC	Receiver Operating Characteristic	Đường cong ROC
SMOTE	Synthetic Minority Oversampling Technique	Kỹ thuật tăng mẫu lớp thiểu số
TN	True Negative	Dự đoán đúng giao dịch hợp lệ
TP	True Positive	Dự đoán đúng giao dịch gian lận
XGBoost	Extreme Gradient Boosting	Mô hình tăng cường cây quyết định

DANH MỤC CÁC BẢNG

Bảng 3.1. Các tham số tối ưu của bộ mô hình 26
Bảng 3.2. Kết quả đánh giá mô hình trên tập kiểm thử 31

DANH MỤC CÁC HÌNH

Hình 3.1. Phân bố độ dài chuỗi giao dịch của người dùng 21
Hình 3.2. AUC theo Epoch (LSTM tối ưu) 30
Hình 3.3. Loss, Precision, Recall theo Epoch 30
Hình 3.4. Ma trận nhầm lẫn của mô hình XGBoost 32
Hình 3.5. Ma trận nhầm lẫn của mô hình LSTM 32
Hình 3.6. So sánh ROC-AUC giữa 4 mô hình 33
Hình 3.7. Precision–Recall Curve 34
Hình 4.1. Kiến trúc tổng thể hệ thống phát hiện gian lận 38
Hình 4.2. Luồng xử lý yêu cầu từ client đến mô hình LSTM 39
Hình 4.3. Giao diện API phục vụ suy luận mô hình LSTM 40
Hình 4.4. Thời gian phản hồi của hệ thống trong môi trường mô phỏng 41
Hình 4.5. Tốc độ xử lý giao dịch theo thời gian 42
Hình 4.6. Giao diện dashboard minh họa kết quả dự đoán gian lận 43
Hình 4.7. Giao diện thử nghiệm dự đoán gian lận theo từng giao dịch. 44

MỞ ĐẦU

1. Lý do chọn đề tài

Sự phát triển mạnh mẽ của các dịch vụ thanh toán điện tử, ngân hàng số và thương mại trực tuyến tại Việt Nam những năm gần đây đã mang lại sự thuận tiện cho khách hàng, nhưng đồng thời kéo theo sự gia tăng nhanh chóng của các hình thức gian lận tài chính. Các hành vi gian lận ngày càng tinh vi, biến đổi liên tục và xuất hiện trên nhiều kênh khác nhau, gây khó khăn cho các biện pháp giám sát truyền thống dựa vào luật cố định hoặc kinh nghiệm chuyên gia.

Trong bối cảnh đó, các phương pháp học máy và học sâu nổi lên như hướng tiếp cận hiệu quả nhờ khả năng khai thác dữ liệu lớn, nhận diện mẫu bất thường và thích ứng với sự thay đổi của hành vi tội phạm. Tuy nhiên, việc nghiên cứu và triển khai các mô hình phát hiện gian lận theo chuỗi thời gian trong môi trường ngân hàng Việt Nam hiện còn hạn chế. Do vậy, việc nghiên cứu, thử nghiệm và đánh giá các mô hình học máy nhằm phát hiện gian lận giao dịch là cần thiết cả về mặt khoa học lẫn thực tiễn, góp phần nâng cao an toàn hệ thống thanh toán và giảm thiểu rủi ro cho ngân hàng.

2. Tổng quan về vấn đề nghiên cứu

Bài toán phát hiện gian lận giao dịch mang đặc thù khó: dữ liệu mất cân bằng mạnh, hành vi gian lận biến đổi, nhiều giao dịch chỉ biểu hiện rủi ro khi xem xét dưới dạng chuỗi theo thời gian. Những hạn chế của các phương pháp truyền thống thúc đẩy sự xuất hiện của các mô hình học máy (Logistic Regression, Random Forest, XGBoost) và mô hình học sâu theo chuỗi, đặc biệt là LSTM.

Trên thế giới, nhiều nghiên cứu đã chứng minh hiệu quả của các mô hình này trong phát hiện gian lận. Tuy nhiên, các thử nghiệm trong bối cảnh dữ liệu ngân hàng Việt Nam – đặc biệt là dữ liệu mô phỏng hành vi theo chuỗi – còn rất ít. Điều này tạo nên khoảng trống nghiên cứu cần được tiếp tục khai thác.

3. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu là dữ liệu giao dịch tài chính điện tử và các mô hình học máy phục vụ phân loại gian lận. Phạm vi nghiên cứu giới hạn trong khía cạnh kỹ thuật: mô phỏng dữ liệu, xử lý dữ liệu, thiết kế mô hình, huấn luyện và đánh giá. Nghiên cứu

không đi sâu vào chính sách nghiệp vụ, quy trình vận hành nội bộ hoặc các yêu cầu pháp lý của ngân hàng.

4. Phương pháp nghiên cứu

Đề tài kết hợp nghiên cứu lý thuyết với thực nghiệm mô hình. Phần lý thuyết tập trung phân tích các dạng gian lận, đặc trưng dữ liệu giao dịch và các mô hình học máy phổ biến. Phần thực nghiệm tiến hành mô phỏng bộ dữ liệu 200.000 giao dịch, xử lý mất cân bằng dữ liệu, xây dựng các mô hình Logistic Regression, Random Forest, XGBoost và LSTM, và đánh giá hiệu năng thông qua các chỉ số Precision, Recall, F1-score và ROC-AUC. Mô hình tối ưu được triển khai thử nghiệm bằng API trong môi trường giả lập gần thời gian thực.

Trên cơ sở tổng quan các nghiên cứu liên quan, đề án này tập trung vào việc đánh giá hiệu quả của mô hình học sâu LSTM trong bài toán phát hiện gian lận giao dịch ngân hàng. Đề án xây dựng bộ dữ liệu giao dịch mô phỏng có cấu trúc chuỗi, phản ánh đặc điểm mất cân bằng và hành vi gian lận theo thời gian, đồng thời thực hiện so sánh có hệ thống giữa mô hình LSTM và các mô hình học máy truyền thống trên cùng điều kiện thực nghiệm. Bên cạnh đó, đề án đề xuất kiến trúc triển khai mô hình dưới dạng dịch vụ phát hiện gian lận gần thời gian thực, phù hợp để tích hợp vào hệ thống thanh toán ngân hàng.

5. Cấu trúc luận văn

Luận văn được tổ chức như sau:

- Chương 1 trình bày cơ sở lý luận về gian lận tài chính, các mô hình học máy và các nghiên cứu liên quan.
- Chương 2 giới thiệu các mô hình đề xuất, cơ sở lựa chọn và phân tích đặc điểm của từng mô hình.
- Chương 3 mô tả dữ liệu, quy trình tiền xử lý, cấu hình huấn luyện và kết quả đánh giá mô hình.
- Chương 4 trình bày quy trình triển khai mô hình tối ưu, thử nghiệm trong môi trường mô phỏng và phân tích kết quả thực nghiệm, bàn luận ý nghĩa thực tiễn và đề xuất hướng nghiên cứu tiếp theo

CHƯƠNG 1: CƠ SỞ LÝ LUẬN

1.1. Giới thiệu chương

Chương này trình bày các nền tảng lý thuyết phục vụ cho bài toán phát hiện gian lận giao dịch trong hệ thống thanh toán ngân hàng. Nội dung bao gồm: (i) tổng quan về gian lận tài chính và đặc điểm dữ liệu trong môi trường ngân hàng số; (ii) các phương pháp học máy và học sâu thường được sử dụng trong phát hiện gian lận; và (iii) tổng quan các nghiên cứu liên quan trong và ngoài nước. Mục tiêu của chương là xây dựng cơ sở khoa học làm nền tảng cho việc lựa chọn mô hình và xây dựng phương pháp trong các chương tiếp theo.

1.2. Gian lận tài chính trong hệ thống ngân hàng

Gian lận tài chính trong hệ thống ngân hàng là một trong những thách thức lớn nhất đối với các tổ chức tín dụng trong bối cảnh chuyển đổi số mạnh mẽ hiện nay. Sự phát triển nhanh của các nền tảng giao dịch trực tuyến, thanh toán điện tử, ví số và hệ thống ngân hàng số đã mang lại nhiều tiện ích cho khách hàng, nhưng đồng thời cũng mở ra môi trường cho các hành vi gian lận ngày càng tinh vi và khó kiểm soát. Về bản chất, gian lận tài chính là hành vi cố ý chiếm đoạt tài sản hoặc thực hiện các giao dịch trái phép thông qua việc khai thác lỗ hổng bảo mật, giả mạo danh tính, hoặc thao túng thông tin giao dịch trong hệ thống ngân hàng.

Trong thực tế, các hành vi gian lận có thể xuất phát từ cả bên ngoài và bên trong. Gian lận bên ngoài bao gồm việc kẻ gian thu thập thông tin đăng nhập, thực hiện giao dịch bất hợp pháp, giả mạo tài liệu hoặc lừa đảo khách hàng thông qua các phương thức xã hội như phishing, smishing và vishing. Gian lận bên trong có thể xảy ra khi nhân viên có quyền truy cập hệ thống lợi dụng vị trí công tác để thay đổi dữ liệu hoặc thực hiện giao dịch không hợp lệ. Mặc dù tính chất của hai loại gian lận này khác nhau, nhưng đều có điểm chung là gây thiệt hại lớn về tài chính và uy tín cho ngân hàng.

Đặc trưng nổi bật của gian lận tài chính là tính không đồng đều và khó dự đoán. Tỷ lệ giao dịch gian lận trong hệ thống thường rất nhỏ so với tổng số giao dịch hợp lệ; tại nhiều ngân hàng, tỷ lệ này chỉ dao động quanh mức 0,1% đến 1%. Sự mất cân bằng nghiêm trọng này khiến nhiều phương pháp phân tích truyền thống không còn hiệu quả,

bởi các mô hình dễ bị thiên lệch và bỏ sót các dấu hiệu bất thường. Hơn nữa, hành vi gian lận không chỉ dựa trên một giao dịch đơn lẻ mà thường thể hiện qua chuỗi giao dịch liên tiếp. Những dấu hiệu như tăng đột biến số lượng giao dịch trong thời gian ngắn, thay đổi thiết bị đăng nhập, chuyển khoản tới nhiều tài khoản mới, hoặc thực hiện giao dịch vào các khung giờ bất thường là những yếu tố quan trọng phản ánh hành vi có rủi ro.

Sự biến đổi liên tục của các chiến thuật gian lận cũng khiến công tác phòng chống ngày càng phức tạp. Các đối tượng gian lận luôn điều chỉnh phương thức hoạt động nhằm né tránh sự giám sát của hệ thống, dẫn đến hiện tượng "drift" trong dữ liệu – tức là các đặc trưng phân biệt gian lận thay đổi theo thời gian. Điều này khiến những quy tắc nghiệp vụ được xây dựng thủ công nhanh chóng trở nên lỗi thời, đòi hỏi các hệ thống phát hiện phải có khả năng học hỏi liên tục, thích nghi và cập nhật theo diễn biến thực tế.

Ngoài ra, sự đa dạng của các kênh giao dịch trong ngân hàng hiện đại, bao gồm Internet Banking, Mobile Banking, ATM, POS, ví điện tử và các cổng thanh toán trực tuyến, khiến dữ liệu trở nên không đồng nhất về cấu trúc và hành vi. Mỗi kênh có đặc điểm vận hành khác nhau, do đó mô hình phát hiện gian lận cần phải đủ linh hoạt để xử lý dữ liệu đa dạng và phát hiện các mối liên hệ ẩn giữa các giao dịch ở nhiều bối cảnh khác nhau.

Từ góc độ quản lý rủi ro, việc phát hiện gian lận kịp thời không chỉ giúp ngân hàng giảm thiểu tổn thất tài chính, mà còn bảo vệ uy tín thương hiệu, tuân thủ quy định pháp luật và nâng cao trải nghiệm khách hàng. Đã xuất hiện xu hướng dịch chuyển từ hệ thống kiểm soát hậu kiểm sang mô hình cảnh báo sớm theo thời gian thực. Điều này đặt ra yêu cầu cấp thiết về việc nghiên cứu và ứng dụng các phương pháp phân tích tiên tiến, trong đó học máy và học sâu đang trở thành những công cụ then chốt nhờ khả năng mô hình hóa hành vi phức tạp và nhận diện các bất thường mà các phương pháp truyền thống khó phát hiện.

Tóm lại, gian lận tài chính trong hệ thống ngân hàng là vấn đề có tính chất phức tạp, biến động và tiềm ẩn nhiều rủi ro. Đặc điểm của bài toán, bao gồm dữ liệu mất cân bằng, hành vi thay đổi liên tục, đa dạng kênh giao dịch và yêu cầu phản ứng nhanh, khiến

các phương pháp phát hiện truyền thống không còn đáp ứng hiệu quả. Chính điều này tạo nên nhu cầu tất yếu phải ứng dụng các mô hình học máy hiện đại nhằm nâng cao khả năng giám sát và bảo vệ an toàn giao dịch.

1.3. Học máy trong phát hiện gian lận giao dịch

Học máy (Machine Learning – ML) đã trở thành một trong những hướng tiếp cận hiệu quả nhất trong công tác phát hiện gian lận giao dịch ngân hàng nhờ khả năng học từ dữ liệu và tự động nhận diện các mẫu bất thường. Khác với các hệ thống giám sát truyền thống vốn dựa trên tập hợp các quy tắc cố định được xây dựng thủ công, mô hình học máy khai thác trực tiếp mối quan hệ giữa các đặc trưng giao dịch, hành vi người dùng và các yếu tố ngữ cảnh nhằm dự đoán khả năng xuất hiện gian lận. Điều này mang lại ưu thế lớn trong bối cảnh hành vi gian lận luôn biến đổi và khó dự đoán bằng kinh nghiệm chủ quan.

Trong phát hiện gian lận giao dịch, mỗi giao dịch có thể được xem như một quan sát với tập hợp đặc trưng mô tả giá trị giao dịch, thời điểm thực hiện, thiết bị sử dụng, vị trí địa lý, mối quan hệ giữa người gửi và người nhận, hay tần suất giao dịch trong khoảng thời gian gần nhất. Trên cơ sở đó, mô hình học máy được huấn luyện để phân biệt giữa giao dịch hợp lệ và giao dịch gian lận dựa trên các đặc điểm đã được học từ dữ liệu lịch sử. Một trong những thách thức lớn của bài toán này là sự mất cân bằng dữ liệu: số lượng giao dịch gian lận thường nhỏ hơn rất nhiều so với giao dịch hợp lệ. Vì vậy, học máy phải giải quyết đồng thời hai vấn đề: khả năng mô hình hóa quan hệ giữa các đặc trưng và khả năng phân biệt lớp thiểu số trong dữ liệu.

Các mô hình học máy truyền thống như Logistic Regression, Random Forest và XGBoost đã được sử dụng rộng rãi trong phát hiện gian lận. Logistic Regression thể hiện cách tiếp cận tuyến tính đơn giản, dễ triển khai và dễ giải thích, thích hợp làm mô hình cơ sở để so sánh với các mô hình phức tạp hơn. Random Forest khai thác cấu trúc phân nhánh của cây quyết định để học các quan hệ phi tuyến, đồng thời có khả năng đánh giá mức độ quan trọng của từng đặc trưng. XGBoost, nhờ cơ chế boosting, thường đạt kết quả dự đoán tốt hơn hai mô hình trên và đặc biệt hiệu quả trong các bài toán dữ liệu mất cân bằng nhờ khả năng điều chỉnh trọng số cho lớp thiểu số. Các mô hình này

hoạt động tương đối tốt khi biểu hiện gian lận có thể được mô tả bởi các đặc trưng tĩnh trong từng giao dịch độc lập.

Tuy nhiên, hạn chế của các mô hình truyền thống là chúng thường xem các giao dịch như những bản ghi độc lập, trong khi gian lận thực tế lại xuất hiện theo chuỗi hành vi. Nhiều hành vi gian lận chỉ biểu hiện rõ ràng khi xem xét mối quan hệ giữa các giao dịch trong một khoảng thời gian nhất định, chẳng hạn như tần suất giao dịch tăng đột biến, liên tục thay đổi thiết bị đăng nhập, chuyển nhiều khoản nhỏ trong thời gian ngắn, hoặc thực hiện các giao dịch ở vị trí địa lý bất thường so với lịch sử sử dụng. Chính những đặc điểm mang tính thời gian này đòi hỏi mô hình phải có khả năng ghi nhớ và phân tích chuỗi, điều mà các mô hình học máy truyền thống không đảm nhiệm tốt.

Sự xuất hiện của các mô hình học sâu (Deep Learning), đặc biệt là mô hình mạng nơ-ron hồi quy (RNN) và biến thể Long Short-Term Memory (LSTM), đã mở ra hướng tiếp cận mạnh mẽ hơn cho bài toán phát hiện gian lận. LSTM được thiết kế để xử lý dữ liệu chuỗi thời gian nhờ khả năng lưu trữ và lựa chọn thông tin quan trọng từ các bước trước đó thông qua các cổng điều khiển trạng thái. Điều này cho phép LSTM học được cách hành vi người dùng thay đổi theo thời gian và phát hiện các bất thường không thể quan sát chỉ bằng một giao dịch độc lập. Ứng dụng LSTM trong gian lận giao dịch mang lại hiệu quả vượt trội khi các mẫu gian lận thường mang tính kế thừa, lặp lại hoặc biểu hiện theo nhịp độ nhất định.

Ngoài ra, học máy còn hỗ trợ hệ thống ngân hàng dưới góc độ vận hành. Mô hình có thể đưa ra điểm rủi ro (risk score) cho từng giao dịch, từ đó giúp ngân hàng tự động phân loại mức độ nghi ngờ và quyết định có cần kích hoạt các bước xác minh bổ sung hay không. Với các hệ thống được triển khai theo thời gian thực, mô hình học máy đóng vai trò là lớp bảo vệ chủ động, ngăn chặn giao dịch gian lận trước khi chúng được xử lý thành công. Điều này giúp giảm thiểu thiệt hại tài chính, bảo vệ khách hàng và nâng cao hiệu quả quản trị rủi ro của ngân hàng.

Nhìn chung, học máy không chỉ mang lại một phương pháp tiếp cận mới cho bài toán phát hiện gian lận mà còn mở ra khả năng xây dựng hệ thống phòng chống gian lận có tính thích nghi và nâng cao theo thời gian. Mặc dù các mô hình truyền thống đã chứng minh được tính hữu dụng trong giai đoạn đầu, sự xuất hiện của các mô hình dựa trên

chuỗi thời gian như LSTM đã tạo ra bước tiến vượt bậc trong việc nắm bắt hành vi người dùng và phát hiện bất thường. Đây chính là nền tảng quan trọng để các chương tiếp theo đề xuất mô hình và triển khai thử nghiệm.

1.4. Các nghiên cứu liên quan

Bài toán phát hiện gian lận giao dịch tài chính, đặc biệt trong thanh toán thẻ và giao dịch điện tử, đã được nghiên cứu rộng rãi trên thế giới và bước đầu xuất hiện trong một số công trình trong nước. Các hướng tiếp cận chủ yếu có thể chia thành: (i) các phương pháp khai phá dữ liệu và mô hình học máy truyền thống, (ii) các kỹ thuật xử lý dữ liệu mất cân bằng và học lai (hybrid), và (iii) các mô hình học sâu, trong đó có LSTM kết hợp với cơ chế cộng tác người – máy.

1.4.1. Các nghiên cứu khai phá dữ liệu và mô hình học máy truyền thống

Ngai và cộng sự [8] thực hiện một tổng quan có hệ thống về ứng dụng các kỹ thuật khai phá dữ liệu trong phát hiện gian lận tài chính. Tác giả đề xuất khung phân loại theo ba chiều: (i) loại gian lận (bảo hiểm, thẻ, chứng khoán…), (ii) loại kỹ thuật khai phá (phân loại, phát hiện bất thường, clustering, rule mining…) và (iii) đặc trưng dữ liệu đầu vào. Công trình có ưu điểm là cung cấp bức tranh tổng quan toàn diện, giúp định vị rõ các hướng tiếp cận chính trong lĩnh vực. Tuy nhiên, mức độ phân tích chi tiết từng mô hình còn hạn chế và chưa đề cập đầy đủ đến các kiến trúc hiện đại như gradient boosting hay học sâu.

Ở mức độ cụ thể hơn, Bhattacharyya và cộng sự [2] tiến hành một nghiên cứu so sánh các mô hình phân loại có giám sát trong phát hiện gian lận thẻ tín dụng. Nghiên cứu tập trung vào các mô hình như logistic regression, cây quyết định và một số thuật toán học máy khác, đánh giá dựa trên các chỉ tiêu như độ chính xác, tỷ lệ phát hiện gian lận đúng và chi phí sai sót. Ưu điểm của các mô hình này là dễ cài đặt, dễ giải thích và phù hợp với yêu cầu minh bạch trong môi trường ngân hàng. Tuy nhiên, chúng thường giả định phân bố dữ liệu ổn định, khó thích ứng với sự thay đổi hành vi gian lận theo thời gian và suy giảm hiệu quả đáng kể trong điều kiện dữ liệu mất cân bằng nặng.

Trong bối cảnh trong nước, Hoàng Thị Thúy và Lê Thị Xuân Thu [1] đã áp dụng một số mô hình học máy để phát hiện gian lận thẻ tín dụng trên dữ liệu thực tế tại Việt Nam. Kết quả cho thấy tiềm năng của các mô hình học máy trong nhận diện giao dịch

bất thường, đồng thời phản ánh các thách thức về chất lượng dữ liệu, tỷ lệ gian lận thấp và yêu cầu tích hợp mô hình vào hệ thống hiện hữu. Ưu điểm của nghiên cứu là bám sát bối cảnh nghiệp vụ Việt Nam, song phạm vi mô hình vẫn chủ yếu tập trung vào các thuật toán truyền thống và chưa khai thác sâu các mô hình chuỗi hay học sâu.

1.4.2. Xử lý dữ liệu mất cân bằng và học máy lai (hybrid)

Một thách thức quan trọng của bài toán phát hiện gian lận là dữ liệu cực kỳ mất cân bằng, trong đó tỷ lệ giao dịch gian lận chỉ chiếm tỷ lệ rất nhỏ. Chawla và cộng sự [5] đề xuất kỹ thuật SMOTE (Synthetic Minority Over-sampling Technique), trong đó các mẫu thuộc lớp thiểu số được tổng hợp nhân tạo từ các láng giềng gần thay vì chỉ sao chép lại. Ưu điểm của SMOTE là giúp các mô hình học có giám sát "nhìn thấy" nhiều điểm dữ liệu thuộc lớp gian lận hơn, từ đó cải thiện khả năng phân biệt. Tuy nhiên, việc sinh mẫu tổng hợp có thể làm tăng nguy cơ chồng lấp biên lớp, và nếu không kết hợp với các kỹ thuật làm sạch (undersampling, ENN, Tomek links…) thì mô hình có thể học nhầm các cấu trúc nhiễu.

Bên cạnh xử lý mất cân bằng, các nghiên cứu gần đây quan tâm tới kết hợp học có giám sát và học không giám sát. Carcillo và cộng sự [4] đề xuất khung kết hợp trong đó các mô hình không giám sát (ví dụ, phát hiện bất thường) được sử dụng để sinh ra "điểm bất thường" (anomaly score), sau đó đưa vào mô hình có giám sát như một đặc trưng bổ sung. Cách tiếp cận này giúp khai thác được thông tin từ cả dữ liệu có nhãn và không nhãn, cải thiện khả năng phát hiện các kiểu gian lận mới (concept drift). Ưu điểm là tăng tính linh hoạt và khả năng tổng quát hóa, nhưng nhược điểm là kiến trúc hệ thống phức tạp hơn, chi phí tính toán và triển khai cao hơn so với các mô hình một tầng đơn giản.

Về nền tảng thuật toán và cài đặt, nhiều mô hình học máy được triển khai dựa trên các thư viện chuẩn như scikit-learn [9] và các thuật toán tăng cường như XGBoost [6]. Các công cụ này cung cấp tập hợp thuật toán phong phú (logistic regression, SVM, random forest, gradient boosting…), hỗ trợ tốt cho việc xây dựng, so sánh và tinh chỉnh mô hình trên dữ liệu giao dịch. Ưu điểm là tính ổn định, được kiểm chứng rộng rãi trong cộng đồng, dễ tích hợp vào pipeline xử lý. Hạn chế là các thuật toán này chủ yếu làm

việc với đặc trưng tĩnh, khó khai thác cấu trúc chuỗi giao dịch theo thời gian nếu không có bước thiết kế đặc trưng chuyên sâu.

1.4.3. Các tiếp cận học sâu và mô hình chuỗi

Việc mô hình hóa hành vi khách hàng theo chuỗi thời gian là một xu hướng quan trọng trong phát hiện gian lận hiện đại. Các mô hình học sâu, đặc biệt là mạng nơ-ron hồi quy (RNN) và các biến thể như LSTM, cho phép nắm bắt các mối quan hệ phụ thuộc theo thời gian giữa các giao dịch liên tiếp – điều mà các mô hình tĩnh khó thể hiện.

Géron [7] trình bày có hệ thống các khái niệm, kiến trúc và kỹ thuật thực hành trong học sâu, bao gồm LSTM và các mô hình tuần tự khác, trên nền các thư viện như TensorFlow và Keras. Đây là tài liệu nền tảng giúp hiểu rõ cơ chế hoạt động, ưu điểm cũng như hạn chế (như chi phí tính toán cao, yêu cầu dữ liệu lớn, nguy cơ quá khớp) của các mô hình học sâu khi áp dụng vào các bài toán thực tế, trong đó có phát hiện gian lận.

Cụ thể với bài toán phát hiện gian lận thẻ tín dụng, Burun và Göktürk [3] đề xuất một cách tiếp cận cộng tác người – máy (Human–AI collaborative), trong đó mô hình LSTM được sử dụng để học hành vi giao dịch theo chuỗi, kết hợp với giao diện Web tương tác hỗ trợ chuyên gia nghiệp vụ giám sát và phản hồi. Ưu điểm của nghiên cứu này là không chỉ dừng ở việc xây dựng mô hình LSTM, mà còn xem xét bài toán ở góc độ triển khai thực tế: tích hợp mô hình vào một hệ thống tương tác, cho phép con người kiểm tra, xác nhận hoặc điều chỉnh các cảnh báo gian lận do mô hình sinh ra. Nhược điểm là việc thiết kế và vận hành một hệ thống như vậy đòi hỏi hạ tầng kỹ thuật phức tạp hơn, yêu cầu dữ liệu đủ lớn và chất lượng cao để huấn luyện LSTM ổn định, đồng thời cần cơ chế quản trị mô hình (model governance) chặt chẽ để kiểm soát rủi ro.

1.4.4. Nhận xét và khoảng trống nghiên cứu

Từ các nghiên cứu đã phân tích có thể rút ra một số nhận xét chính:

Nhóm phương pháp khai phá dữ liệu và mô hình truyền thống [1], [2], [8] có ưu điểm là dễ cài đặt, dễ giải thích và phù hợp với môi trường vận hành ngân hàng vốn đòi hỏi tính minh bạch cao. Tuy nhiên, các mô hình này thường giả định dữ liệu tương đối ổn định, hiệu quả giảm khi hành vi gian lận thay đổi nhanh (concept drift) và khi dữ liệu mất cân bằng nghiêm trọng.

Các kỹ thuật xử lý mất cân bằng và mô hình hybrid [4], [5] giúp cải thiện đáng kể khả năng phát hiện lớp gian lận hiếm, đồng thời tận dụng được cả dữ liệu có nhãn và không nhãn. Ưu điểm là nâng cao khả năng tổng quát hóa và tính thực dụng của mô hình trong bối cảnh dữ liệu phức tạp. Dù vậy, kiến trúc hybrid thường phức tạp hơn, chi phí triển khai và duy trì cao, và vẫn chủ yếu làm việc với đặc trưng tĩnh theo từng giao dịch.

Các nền tảng và thuật toán học máy phổ biến như scikit-learn [9] và XGBoost [6] cung cấp công cụ mạnh để xây dựng và so sánh mô hình trên dữ liệu giao dịch, đặc biệt với các đặc trưng được thiết kế tốt. Tuy nhiên, nếu chỉ dừng ở mức đặc trưng tĩnh và mô hình phi chuỗi, khả năng nắm bắt hành vi gian lận theo trình tự vẫn bị hạn chế.

Các tiếp cận học sâu và mô hình chuỗi [7], [3] thể hiện tiềm năng lớn trong việc mô hình hóa hành vi giao dịch theo thời gian, giúp phát hiện những mẫu gian lận tinh vi chỉ lộ rõ khi xem xét chuỗi giao dịch thay vì từng giao dịch riêng lẻ. Những nghiên cứu như Burun và Göktürk [3] còn cho thấy hướng đi kết hợp mô hình LSTM với cơ chế tương tác người – máy, góp phần nâng cao tính khả thi triển khai. Tuy nhiên, các nghiên cứu này thường đòi hỏi dữ liệu lớn, điều kiện hạ tầng tính toán tốt và đa phần chưa được điều chỉnh cho phù hợp với đặc thù dữ liệu và nghiệp vụ của các ngân hàng Việt Nam.

Ở bối cảnh trong nước, các công trình hiện có [1] mới dừng ở việc áp dụng một số mô hình học máy truyền thống trên dữ liệu thẻ, chưa khai thác sâu mô hình chuỗi hoặc đánh giá khả năng suy luận gần thời gian thực trong môi trường thanh toán đa kênh. Như vậy, khoảng trống nghiên cứu đặt ra là cần xây dựng và đánh giá một mô hình học sâu theo chuỗi (chẳng hạn LSTM) trên dữ liệu mô phỏng bám sát bối cảnh giao dịch ngân hàng Việt Nam, đồng thời so sánh có hệ thống với các mô hình học máy truyền thống được triển khai trên cùng bộ dữ liệu. Việc phân tích ưu – nhược điểm của từng nhóm mô hình trong điều kiện dữ liệu mất cân bằng, yêu cầu suy luận gần thời gian thực và ràng buộc nghiệp vụ ngân hàng sẽ cung cấp cơ sở khoa học để lựa chọn giải pháp phù hợp cho hệ thống phát hiện gian lận giao dịch.

1.5. Kết luận chương

Chương này đã trình bày nền tảng lý luận cho bài toán phát hiện gian lận giao dịch trong ngân hàng. Phần 1.2 phân tích bản chất gian lận tài chính, đặc trưng dữ liệu và những thách thức như sự mất cân bằng nghiêm trọng, hành vi gian lận biến đổi theo

thời gian và sự đa dạng của các kênh giao dịch. Phần 1.3 giới thiệu các mô hình học máy thường được sử dụng trong phát hiện gian lận, đồng thời chỉ ra hạn chế của các mô hình truyền thống khi không mô hình hóa được chuỗi hành vi. Cuối cùng, mục 1.4 tổng hợp các nghiên cứu trong và ngoài nước, nhấn mạnh xu hướng ứng dụng học sâu – đặc biệt là LSTM – vào bài toán nhằm cải thiện khả năng phát hiện các bất thường có tính chất tuần tự.

Từ tổng quan nêu trên, có thể thấy mô hình học sâu theo chuỗi là một hướng tiếp cận có nhiều tiềm năng để xử lý các thách thức đặc thù của dữ liệu gian lận ngân hàng. Đây cũng là cơ sở để đề tài lựa chọn và phân tích mô hình trong chương tiếp theo.

CHƯƠNG 2: ĐỀ XUẤT MÔ HÌNH

2.1. Giới thiệu chương

Chương này trình bày các mô hình học máy và học sâu được đề xuất để sử dụng trong bài toán phát hiện gian lận giao dịch ngân hàng. Nội dung tập trung giới thiệu nguyên lý hoạt động, đặc điểm và vai trò của từng nhóm mô hình, đồng thời làm rõ cơ sở lựa chọn bộ mô hình được sử dụng trong nghiên cứu. Chương không đề cập đến dữ liệu hay kết quả thực nghiệm, mà chỉ tập trung mô tả và phân tích đặc điểm của các mô hình làm nền tảng cho quá trình huấn luyện và đánh giá ở các chương tiếp theo.

2.2. Cơ sở lựa chọn mô hình

Việc lựa chọn mô hình trong bài toán phát hiện gian lận giao dịch cần dựa trên đặc trưng của dữ liệu, yêu cầu thực tiễn của hệ thống ngân hàng và mục tiêu nghiên cứu của đề tài. Khác với các bài toán phân loại thông thường, phát hiện gian lận giao dịch đặt ra nhiều thách thức đặc thù như tỷ lệ mất cân bằng nghiêm trọng, sự biến đổi liên tục của hành vi gian lận và tính phụ thuộc thời gian trong mối quan hệ giữa các giao dịch. Những đặc điểm này đòi hỏi bộ mô hình phải vừa đủ đa dạng để so sánh các hướng tiếp cận, vừa đủ đại diện cho các nhóm kỹ thuật phổ biến được sử dụng trong lĩnh vực phòng chống gian lận.

Thứ nhất, dữ liệu giao dịch ngân hàng thường có tỷ lệ gian lận cực thấp so với giao dịch hợp lệ. Đặc điểm này khiến các mô hình tuyến tính đơn giản khó đạt được hiệu quả phân loại đáng tin cậy khi không mô hình hóa được ranh giới phức tạp giữa hai lớp. Tuy vậy, các mô hình tuyến tính như Logistic Regression vẫn đóng vai trò quan trọng ở giai đoạn cơ sở (baseline), giúp đánh giá mức cải thiện của các mô hình tiên tiến hơn.

Thứ hai, mối quan hệ giữa các đặc trưng giao dịch thường mang tính phi tuyến, đặc biệt khi hành vi gian lận không biểu hiện qua một dấu hiệu đơn lẻ mà thông qua sự kết hợp của nhiều yếu tố như giá trị giao dịch, thời điểm thực hiện, vị trí địa lý hay loại thiết bị. Điều này tạo cơ sở lựa chọn các mô hình học máy truyền thống như Random Forest và XGBoost. Random Forest có khả năng học phân chia phi tuyến và thể hiện tính ổn định cao trước nhiễu. XGBoost, với cơ chế boosting mạnh mẽ, thường đạt hiệu suất tốt trên dữ liệu mất cân bằng và có khả năng tự động khai thác tương tác giữa các

đặc trưng. Hai mô hình này giúp đại diện cho nhóm phương pháp dựa trên cây quyết định, vốn được sử dụng rộng rãi trong lĩnh vực phân tích tài chính.

Thứ ba, hành vi gian lận trong môi trường ngân hàng có xu hướng thể hiện rõ rệt hơn khi xem xét các giao dịch như một chuỗi liên kết theo thời gian thay vì các quan sát độc lập. Ví dụ, kẻ gian lận có thể thực hiện liên tiếp nhiều giao dịch nhỏ để né tránh giám sát, hoặc đột ngột thay đổi thiết bị, vị trí hay tần suất giao dịch. Những thay đổi này chỉ có thể nhận diện khi mô hình có khả năng học và ghi nhớ trạng thái theo thời gian. Do đó, việc lựa chọn mô hình học sâu theo chuỗi như LSTM là cần thiết nhằm khai thác thông tin động (temporal dynamics) trong chuỗi giao dịch. LSTM có ưu thế rõ rệt trong việc mô hình hóa phụ thuộc dài hạn và thích hợp với các bài toán mà đặc trưng thời gian đóng vai trò quan trọng.

Cuối cùng, việc lựa chọn kết hợp cả mô hình truyền thống và mô hình học sâu giúp nghiên cứu đánh giá toàn diện hiệu quả của các hướng tiếp cận khác nhau. Nhóm mô hình truyền thống phản ánh khả năng phân loại dựa trên đặc trưng tĩnh, trong khi LSTM phản ánh khả năng phân tích hành vi theo chuỗi. Việc so sánh trực tiếp giữa hai nhóm mô hình này giúp làm rõ mức độ cải thiện mà mô hình chuỗi thời gian mang lại, đồng thời xác định mô hình phù hợp nhất để triển khai trong hệ thống phát hiện gian lận giao dịch của ngân hàng.

Như vậy, bộ mô hình được lựa chọn trong nghiên cứu, bao gồm Logistic Regression, Random Forest, XGBoost và LSTM, bảo đảm tính đại diện cho nhiều cách tiếp cận khác nhau, đồng thời phù hợp với đặc thù của bài toán và mục tiêu nghiên cứu. Các phân tích này là cơ sở quan trọng cho phần mô tả mô hình chi tiết được trình bày trong các mục tiếp theo của chương.

2.3. Nhóm mô hình học máy truyền thống

2.3.1. Logistic Regression

Logistic Regression là một trong những mô hình phân loại nhị phân được sử dụng phổ biến nhất trong lĩnh vực phân tích rủi ro tài chính và phát hiện gian lận. Mô hình mô tả mối quan hệ giữa tập đặc trưng đầu vào và xác suất xảy ra gian lận thông qua một hàm logistic. Ưu điểm lớn nhất của Logistic Regression nằm ở khả năng diễn giải rõ ràng: mỗi hệ số trong mô hình phản ánh mức độ ảnh hưởng của đặc trưng tương ứng đến

xác suất giao dịch bị gán nhãn gian lận. Điều này đặc biệt quan trọng trong bối cảnh ngân hàng, nơi việc giải thích mô hình đóng vai trò quan trọng trong kiểm soát nội bộ và tuân thủ quy định.

Tuy nhiên, do bản chất tuyến tính, Logistic Regression gặp hạn chế khi quan hệ giữa các đặc trưng giao dịch mang tính phi tuyến hoặc có sự tương tác phức tạp. Trong dữ liệu giao dịch ngân hàng vốn có nhiều yếu tố biến động theo thời gian hoặc mang tính hành vi độc lập, mô hình có thể không nắm bắt được các quy luật phức tạp. Mặc dù vậy, Logistic Regression vẫn được sử dụng như một mô hình nền tảng để thiết lập baseline nhằm so sánh hiệu quả với các mô hình tiên tiến hơn.

2.3.2. Random Forest

Random Forest là mô hình phân loại dựa trên tập hợp nhiều cây quyết định hoạt động theo cơ chế học bao (ensemble learning). Mỗi cây trong rừng được huấn luyện độc lập trên một mẫu dữ liệu được lấy ngẫu nhiên với tập đặc trưng con, sau đó kết quả được tổng hợp để đưa ra dự đoán cuối cùng. Cách tiếp cận này giúp Random Forest giảm hiện tượng quá khớp, đồng thời xử lý tốt các mối quan hệ phi tuyến giữa các đặc trưng giao dịch. Mô hình cũng cho phép đánh giá mức độ quan trọng của từng đặc trưng, hỗ trợ quá trình phân tích và diễn giải trong môi trường nghiệp vụ ngân hàng.

Mặc dù có nhiều ưu điểm, Random Forest vẫn đối diện với khó khăn khi dữ liệu bị mất cân bằng nghiêm trọng, đặc biệt khi lớp gian lận chiếm tỷ lệ rất nhỏ trong tổng số giao dịch. Trong trường hợp này, mô hình dễ thiên lệch về phía lớp phổ biến, dẫn đến khả năng bỏ sót các giao dịch gian lận. Ngoài ra, giống như nhiều mô hình dựa trên cây quyết định khác, Random Forest xem các giao dịch như các bản ghi độc lập và không khai thác được cấu trúc chuỗi thời gian của hành vi người dùng.

2.3.3. XGBoost

XGBoost (Extreme Gradient Boosting) là một trong những mô hình học máy mạnh mẽ nhất cho các bài toán phân loại có dữ liệu phức tạp và mất cân bằng, trong đó có phát hiện gian lận giao dịch. Mô hình xây dựng tập hợp các cây quyết định theo phương pháp boosting, trong đó mỗi cây mới được huấn luyện để cải thiện sai số của các cây trước đó thông qua tối ưu hóa hàm mất mát theo hướng gradient. XGBoost nổi

bật nhờ tốc độ huấn luyện nhanh, khả năng chống quá khớp tốt nhờ cơ chế regularization và khả năng xử lý giá trị thiếu một cách linh hoạt.

Một ưu điểm quan trọng khác của XGBoost là khả năng điều chỉnh trọng số lớp thiểu số bằng tham số scale_pos_weight, giúp mô hình tập trung hơn vào các mẫu gian lận mà không ảnh hưởng đến độ tổng quát hóa. Nhờ đó, XGBoost thường đạt hiệu năng tốt trên các bộ dữ liệu giao dịch bị mất cân bằng mạnh. Tuy vậy, giống như các mô hình truyền thống khác, XGBoost chưa khai thác được mối quan hệ theo chuỗi giữa các giao dịch trong thời gian, do đó hiệu quả sẽ phụ thuộc chủ yếu vào chất lượng của tập đặc trưng được xây dựng.

2.4. Nhóm mô hình học sâu theo chuỗi thời gian

2.4.1. Mô hình LSTM (Long Short-Term Memory)

Trong những năm gần đây, học sâu (Deep Learning) đã trở thành hướng tiếp cận nổi bật trong các bài toán phát hiện bất thường và gian lận giao dịch nhờ khả năng tự động học biểu diễn đặc trưng và mô hình hóa các quan hệ phức tạp của dữ liệu. Khác với các mô hình học máy truyền thống vốn xem mỗi giao dịch như một quan sát độc lập, các mô hình học sâu theo chuỗi thời gian có khả năng phân tích mối quan hệ giữa các giao dịch liên tiếp, qua đó nắm bắt được các thay đổi trong hành vi của người dùng theo thời gian. Điều này đặc biệt quan trọng trong bối cảnh gian lận ngân hàng, nơi hành vi bất thường thường chỉ bộc lộ khi xem xét toàn bộ chuỗi giao dịch, chứ không thể phát hiện chỉ từ một giao dịch đơn lẻ.

Trong số các mô hình học sâu theo chuỗi, mạng nơ-ron hồi quy (Recurrent Neural Network – RNN) là một trong những kiến trúc được sử dụng sớm nhất nhờ khả năng duy trì trạng thái thông qua quá trình lặp theo từng bước thời gian. Tuy nhiên, RNN truyền thống gặp khó khăn khi xử lý các chuỗi dài do bị ảnh hưởng bởi hiện tượng mất mát gradient trong quá trình lan truyền ngược, khiến mô hình không thể học được các phụ thuộc dài hạn của chuỗi giao dịch. Để khắc phục nhược điểm này, các biến thể cải tiến như Long Short-Term Memory (LSTM) và Gated Recurrent Unit (GRU) đã ra đời, trong đó LSTM được đánh giá là một trong những mô hình hiệu quả nhất cho các bài toán thời gian liên tục và chuỗi hành vi.

LSTM được thiết kế với ba cổng điều khiển: cổng quên (forget gate), cổng đầu vào (input gate) và cổng đầu ra (output gate). Thông qua ba cổng này, LSTM có khả năng chọn lọc thông tin quan trọng cần lưu giữ hoặc loại bỏ trong quá trình học. Điều này giúp mô hình duy trì được trạng thái dài hạn và tránh tình trạng quên các thông tin quan trọng từ những bước thời gian trước đó. Với cấu trúc này, LSTM có thể học các mẫu hành vi phức tạp trong chuỗi giao dịch như tăng đột biến tần suất, thay đổi địa điểm hoặc thiết bị, hay các chuỗi chuyển khoản được thực hiện với mục đích che giấu hành vi gian lận.

Ưu điểm nổi bật của LSTM là khả năng mô hình hóa tốt các phụ thuộc theo thời gian, từ đó phản ánh đúng động thái hành vi (behavioral dynamics) của người dùng. Trong phát hiện gian lận, mô hình có thể nhận diện những bất thường không xuất hiện ở từng giao dịch riêng lẻ nhưng trở nên rõ ràng khi xem xét toàn bộ chuỗi giao dịch trong một khoảng thời gian ngắn. Ví dụ, một giao dịch có giá trị nhỏ có thể không bất thường, nhưng khi nó xuất hiện liên tiếp nhiều lần trong một chuỗi, mô hình có thể nhận ra hành vi cố tình phân nhỏ giao dịch để tránh bị phát hiện.

Ngoài ra, LSTM còn cho phép mô hình hấp thụ thông tin theo cả chiều dài chuỗi và số lượng đặc trưng, từ đó tạo ra biểu diễn (representation) giàu ý nghĩa hơn so với mô hình dựa trên đặc trưng thủ công. Đây là điểm mạnh quan trọng so với các mô hình truyền thống như Logistic Regression, Random Forest hay XGBoost, vốn phụ thuộc rất lớn vào chất lượng của feature engineering. Với LSTM, mô hình có khả năng tự học các đặc trưng phức tạp từ dữ liệu ban đầu mà không cần can thiệp nhiều của con người.

Tuy mang lại nhiều ưu điểm, LSTM cũng có những hạn chế nhất định. Mô hình yêu cầu lượng dữ liệu lớn để đạt hiệu quả tối ưu và có chi phí huấn luyện cao hơn đáng kể so với các mô hình truyền thống. Bên cạnh đó, việc diễn giải mô hình học sâu nói chung và LSTM nói riêng vẫn còn hạn chế, gây khó khăn trong việc giải thích vì sao mô hình gán nhãn một giao dịch là gian lận – điều mà các tổ chức tài chính thường yêu cầu để phục vụ mục đích kiểm toán, điều tra và tuân thủ.

Nhìn chung, LSTM là mô hình phù hợp cho bài toán phát hiện gian lận giao dịch trong bối cảnh dữ liệu có tính chuỗi rõ rệt. Mô hình cho phép phân tích mối liên hệ giữa các giao dịch theo thời gian, học được các mẫu hành vi phức tạp và thích hợp cho các

hệ thống cảnh báo gần thời gian thực. Vì vậy, trong nghiên cứu này, LSTM được lựa chọn làm mô hình học sâu chủ đạo để so sánh hiệu quả với các mô hình học máy truyền thống đã trình bày trong mục trước.

2.5. Lý do lựa chọn bộ mô hình trong nghiên cứu

Việc lựa chọn bộ mô hình trong nghiên cứu được xây dựng dựa trên đặc điểm của bài toán phát hiện gian lận giao dịch và mục tiêu so sánh hiệu quả giữa các nhóm phương pháp khác nhau. Trong bối cảnh ngân hàng số, dữ liệu giao dịch có tính chất phức tạp, đa dạng về đặc trưng và mang yếu tố thời gian rõ rệt. Do đó, nghiên cứu cần lựa chọn các mô hình đại diện cho nhiều hướng tiếp cận để đánh giá toàn diện hiệu quả của chúng.

Thứ nhất, các mô hình học máy truyền thống như Logistic Regression, Random Forest và XGBoost được lựa chọn nhằm phản ánh những phương pháp đang được sử dụng phổ biến trong phân tích rủi ro tài chính. Logistic Regression đóng vai trò là mô hình cơ sở với khả năng diễn giải tốt và phù hợp để đánh giá mức độ phức tạp cần thiết của mô hình. Random Forest cung cấp góc nhìn về khả năng học các quan hệ phi tuyến, trong khi XGBoost đại diện cho các phương pháp boosting hiện đại có khả năng xử lý hiệu quả dữ liệu mất cân bằng. Ba mô hình này cho phép nghiên cứu đánh giá mức độ hiệu quả của các mô hình dựa trên đặc trưng tĩnh, nơi mỗi giao dịch được xem như một quan sát độc lập.

Thứ hai, mô hình học sâu theo chuỗi thời gian – cụ thể là Long Short-Term Memory (LSTM) – được lựa chọn vì phù hợp với bản chất phụ thuộc thời gian của hành vi giao dịch. Nhiều hành vi gian lận chỉ có thể nhận diện rõ khi xem xét một chuỗi giao dịch liên tục thay vì từng giao dịch đơn lẻ. LSTM có khả năng ghi nhớ và học phụ thuộc dài hạn, cho phép mô hình phát hiện các mẫu hành vi bất thường như tăng tần suất giao dịch, thay đổi thiết bị, hoặc thực hiện nhiều giao dịch nhỏ trong thời gian ngắn. Việc đưa LSTM vào bộ mô hình giúp nghiên cứu đánh giá sự khác biệt giữa mô hình dựa trên đặc trưng tĩnh và mô hình khai thác động thái hành vi người dùng.

Thứ ba, sự kết hợp giữa nhóm mô hình truyền thống và mô hình học sâu giúp bảo đảm tính toàn diện khi đánh giá kết quả. Mỗi mô hình có cách tiếp cận khác nhau: mô hình truyền thống dựa trên phân tích đặc trưng đầu vào, trong khi LSTM tự động học

biểu diễn đặc trưng từ chuỗi dữ liệu. Bằng cách so sánh nhiều mô hình thuộc các hướng tiếp cận khác nhau, nghiên cứu có thể đưa ra đánh giá khách quan về khả năng ứng dụng của từng mô hình và xác định hướng phù hợp nhất cho bối cảnh dữ liệu ngân hàng.

Cuối cùng, việc lựa chọn bốn mô hình này đáp ứng đầy đủ yêu cầu của bài toán: dễ diễn giải, dễ triển khai, khai thác được cấu trúc dữ liệu và phản ánh sự khác biệt giữa phương pháp truyền thống và học sâu. Sự đa dạng về bản chất mô hình cũng tạo cơ sở để đánh giá mức độ cải thiện mà mô hình LSTM mang lại so với các mô hình đang được dùng phổ biến trong ngành tài chính. Đây là nền tảng quan trọng để tiến hành huấn luyện, đánh giá và so sánh hiệu quả trong chương tiếp theo.

2.6. Kết luận chương

Chương này đã trình bày bộ mô hình được đề xuất cho bài toán phát hiện gian lận giao dịch trong hệ thống ngân hàng, bao gồm ba mô hình học máy truyền thống và một mô hình học sâu theo chuỗi thời gian. Trên cơ sở phân tích đặc điểm dữ liệu và yêu cầu thực tiễn, chương đã làm rõ lý do lựa chọn từng mô hình cũng như vai trò của chúng trong nghiên cứu. Các mô hình truyền thống như Logistic Regression, Random Forest và XGBoost đại diện cho những cách tiếp cận dựa trên đặc trưng tĩnh của giao dịch, trong khi mô hình LSTM khai thác mối quan hệ theo thời gian và sự biến đổi hành vi trong chuỗi giao dịch.

Việc kết hợp cả hai nhóm mô hình bảo đảm tính toàn diện khi đánh giá, đồng thời tạo cơ sở vững chắc để so sánh hiệu quả giữa các phương pháp. Những mô hình này sẽ được huấn luyện, thử nghiệm và phân tích trong chương tiếp theo nhằm xác định phương pháp tối ưu cho bài toán phát hiện gian lận trong bối cảnh dữ liệu ngân hàng. Chương 3 sẽ tập trung trình bày chi tiết bộ dữ liệu, quy trình tiền xử lý, cấu hình huấn luyện và kết quả đánh giá thực nghiệm của từng mô hình.

CHƯƠNG 3: THỰC NGHIỆM VÀ ĐÁNH GIÁ

3.1. Giới thiệu chương

Chương này trình bày quá trình thực nghiệm các mô hình đã được đề xuất, bao gồm mô tả bộ dữ liệu sử dụng cho huấn luyện, các bước tiền xử lý, phương pháp phân chia dữ liệu, cấu hình huấn luyện và các chỉ số đánh giá. Trên cơ sở đó, chương trình bày kết quả thử nghiệm của bốn mô hình Logistic Regression, Random Forest, XGBoost và LSTM, đồng thời phân tích hiệu quả của từng mô hình để lựa chọn phương pháp tối ưu cho bài toán phát hiện gian lận trong giao dịch ngân hàng.

3.2. Bộ dữ liệu sử dụng trong nghiên cứu

Bộ dữ liệu sử dụng trong nghiên cứu được xây dựng dựa trên bối cảnh hoạt động thực tế của hệ thống thanh toán ngân hàng, trong đó mỗi giao dịch được mô tả bằng nhiều nhóm đặc trưng phản ánh hành vi người dùng, thông tin giao dịch và ngữ cảnh phát sinh. Trong phạm vi nghiên cứu, dữ liệu mô phỏng được sử dụng như một lựa chọn có kiểm soát nhằm phục vụ mục tiêu đánh giá và so sánh hiệu quả các mô hình học máy và học sâu trong bài toán phát hiện gian lận giao dịch ngân hàng. Bộ dữ liệu được thiết kế theo các đặc tính phổ biến của giao dịch tài chính, bảo đảm phản ánh được các yếu tố quan trọng của bài toán và phù hợp cho quá trình huấn luyện, đánh giá mô hình.

Bộ dữ liệu bao gồm 200.000 giao dịch của khoảng 10.000 người dùng với tỷ lệ gian lận chiếm xấp xỉ 1,2% tổng số giao dịch. Tỷ lệ này được lựa chọn để mô phỏng sát với thực tiễn tại các tổ chức tài chính, nơi số lượng giao dịch gian lận thường chiếm tỷ lệ rất nhỏ so với giao dịch hợp lệ. Đây cũng là đặc trưng quan trọng của bài toán và làm tăng độ phức tạp cho mô hình, bởi các thuật toán phải học cách phân biệt lớp thiểu số trong bối cảnh dữ liệu mất cân bằng mạnh.

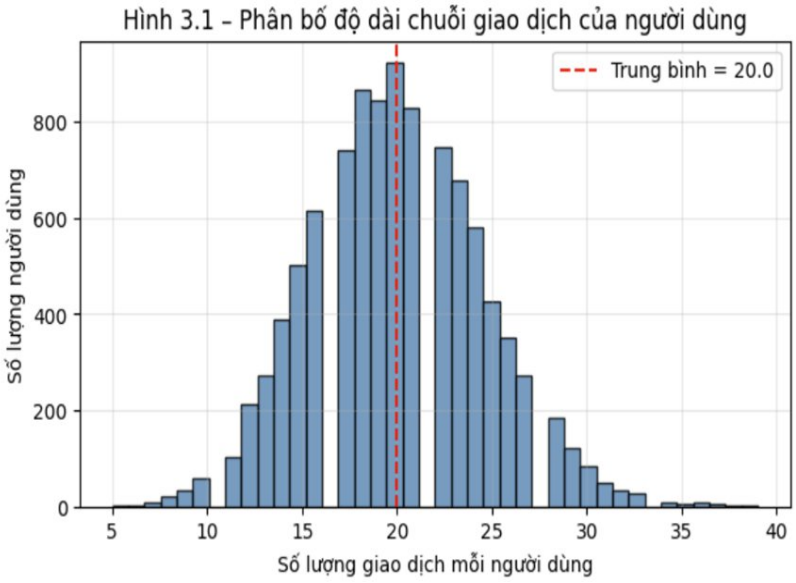
Mỗi giao dịch trong bộ dữ liệu bao gồm ba nhóm thông tin chính. Nhóm đặc trưng giao dịch mô tả các thông số trực tiếp liên quan đến giao dịch như số tiền, loại giao dịch, thời gian thực hiện và đơn vị chấp nhận thanh toán. Nhóm đặc trưng hành vi phản ánh tần suất giao dịch của người dùng trong một khoảng thời gian, mức độ biến động của giá trị giao dịch và sự thay đổi trong thiết bị sử dụng. Nhóm đặc trưng theo ngữ cảnh bao gồm vị trí địa lý, nguồn truy cập và thông tin thiết bị. Những đặc trưng này được lựa

chọn dựa trên các nghiên cứu thực nghiệm và cơ sở nghiệp vụ của ngành ngân hàng, cho phép mô hình đánh giá hành vi một cách đa chiều hơn.

Điểm quan trọng của bộ dữ liệu là việc tổ chức theo chuỗi giao dịch của từng người dùng. Mỗi người dùng được biểu diễn dưới dạng một dãy gồm nhiều giao dịch liên tiếp, được sắp xếp theo thời gian. Cách tổ chức này tạo điều kiện thuận lợi cho mô hình LSTM trong việc khai thác đặc trưng chuỗi và học được sự thay đổi hành vi theo thời gian. Bên cạnh đó, các mô hình học máy truyền thống cũng có thể sử dụng các đặc trưng tĩnh được trích xuất từ từng giao dịch hoặc từ một cửa sổ hành vi của người dùng.

Trước khi đưa dữ liệu vào mô hình, các trường thông tin định danh được loại bỏ nhằm đảm bảo tính an toàn và tránh ảnh hưởng đến quá trình huấn luyện. Các trường như thời gian, giá trị tiền, mã danh mục hay thông tin địa lý được chuẩn hóa về mặt định dạng để giúp mô hình học ổn định hơn. Những đặc điểm này sẽ được trình bày chi tiết hơn trong mục tiếp theo về tiền xử lý dữ liệu.

Bộ dữ liệu được thiết kế nhằm đạt hai mục tiêu: phản ánh được đặc điểm hành vi thực tế của người dùng trong hệ thống ngân hàng và tạo cơ sở đủ đa dạng để đánh giá khách quan hiệu quả của các mô hình được đề xuất. Đây là nền tảng quan trọng đối với toàn bộ quá trình huấn luyện, đánh giá và so sánh mô hình được trình bày trong các phần sau của chương.



Hình 3.1. Phân bố độ dài chuỗi giao dịch của người dùng

3.3. Tiền xử lý dữ liệu

Tiền xử lý dữ liệu là bước quan trọng nhằm bảo đảm chất lượng dữ liệu đầu vào trước khi đưa vào huấn luyện mô hình. Đối với bài toán phát hiện gian lận giao dịch, dữ liệu thường chứa nhiều giá trị nhiễu, không đồng nhất hoặc thiếu hụt thông tin. Nếu không xử lý cẩn thận, các vấn đề này có thể làm giảm khả năng học của mô hình hoặc tạo ra sai lệch trong quá trình đánh giá. Do đó, quy trình tiền xử lý trong nghiên cứu được xây dựng theo hướng đảm bảo tính chính xác, đầy đủ và phù hợp với từng loại mô hình sử dụng.

Trước hết, dữ liệu được rà soát nhằm phát hiện và loại bỏ các bản ghi không hợp lệ, bao gồm các giao dịch thiếu trường bắt buộc, giá trị âm không hợp lý hoặc trùng lặp theo cùng thời điểm và người dùng. Các trường thông tin nhạy cảm như mã khách hàng, số tài khoản hay định danh thiết bị được loại bỏ hoàn toàn, bảo đảm yêu cầu bảo mật và tránh ảnh hưởng đến mô hình. Việc chuẩn hóa dữ liệu thời gian cũng được thực hiện để bảo đảm các giao dịch được sắp xếp theo đúng thứ tự thời gian của từng người dùng.

Tiếp theo, các trường dữ liệu số được chuẩn hóa nhằm đưa về cùng thang đo, giúp mô hình học ổn định hơn. Giá trị giao dịch, tần suất giao dịch và các đặc trưng hành vi được biến đổi bằng phương pháp chuẩn hóa Min-Max hoặc Standardization tùy thuộc vào phân phối của từng trường. Đối với các mô hình học máy truyền thống, chuẩn hóa giúp giảm tác động của các đặc trưng có độ lớn vượt trội và tránh việc mô hình tập trung quá nhiều vào các trường có giá trị cao.

Các đặc trưng dạng phân loại như loại giao dịch, phương thức thanh toán hoặc loại thiết bị được mã hóa bằng các kỹ thuật phù hợp. Đối với mô hình truyền thống, phương pháp One-Hot Encoding được sử dụng để biểu diễn các giá trị phân loại dưới dạng vector nhị phân. Trong khi đó, đối với mô hình LSTM, các trường phân loại có thể được chuyển đổi sang dạng embedding nhằm tạo ra biểu diễn liên tục có ý nghĩa hơn về mặt ngữ nghĩa và phù hợp với dữ liệu chuỗi.

Một bước quan trọng khác trong quá trình tiền xử lý là xây dựng chuỗi giao dịch cho từng người dùng. Các giao dịch được nhóm theo mã người dùng và sắp xếp theo thời gian để tạo thành dãy giao dịch liên tục. Mỗi chuỗi có độ dài cố định hoặc được padding để đảm bảo tính đồng nhất khi đưa vào LSTM. Cách tổ chức này giúp mô hình

khai thác được đặc trưng thời gian, điều mà các mô hình truyền thống không thể thực hiện khi làm việc với dữ liệu dạng bản ghi độc lập.

Bên cạnh đó, vấn đề mất cân bằng dữ liệu cũng được xem xét trong giai đoạn tiền xử lý. Tỷ lệ giao dịch gian lận rất thấp có thể dẫn đến sai lệch trong quá trình huấn luyện, khiến mô hình dự đoán thiên về lớp giao dịch hợp lệ. Tùy theo mô hình, các biện pháp như điều chỉnh trọng số lớp, lấy mẫu có trọng số hoặc kỹ thuật xử lý lớp thiểu số có thể được áp dụng ở những bước sau để cải thiện cân bằng trong quá trình huấn luyện. Riêng với XGBoost, việc xử lý mất cân bằng được thực hiện chủ yếu thông qua các tham số huấn luyện nên không áp dụng trực tiếp vào dữ liệu gốc.

Quá trình tiền xử lý như trên giúp bảo đảm dữ liệu đầu vào có chất lượng cao, phù hợp với yêu cầu của cả các mô hình truyền thống và mô hình học sâu. Đây là bước nền tảng quan trọng, ảnh hưởng trực tiếp đến độ chính xác và khả năng khái quát hóa của mô hình trong các phần thực nghiệm tiếp theo.

3.4. Phân chia dữ liệu huấn luyện và kiểm thử

Sau khi hoàn tất quá trình tiền xử lý, bộ dữ liệu được phân chia thành các tập phục vụ cho quá trình huấn luyện, kiểm thử và đánh giá mô hình. Việc phân chia này có vai trò quan trọng trong bảo đảm độ khách quan của kết quả, tránh hiện tượng mô hình ghi nhớ dữ liệu huấn luyện (overfitting) và giúp đánh giá đúng khả năng khái quát hóa của mô hình.

Dữ liệu được chia theo tỷ lệ 70% cho tập huấn luyện, 15% cho tập kiểm định (validation) và 15% cho tập kiểm thử (test). Tỷ lệ này được lựa chọn nhằm bảo đảm đủ dữ liệu cho mô hình học các quy luật phức tạp, đặc biệt trong bối cảnh tỷ lệ gian lận thấp. Tập kiểm định được sử dụng trong quá trình tối ưu hóa siêu tham số, giúp mô hình lựa chọn được cấu hình tốt nhất trước khi đánh giá cuối cùng trên tập kiểm thử. Tập kiểm thử chỉ được sử dụng một lần duy nhất sau khi hoàn tất quá trình huấn luyện để bảo đảm tính khách quan của kết quả.

Đối với các mô hình học máy truyền thống như Logistic Regression, Random Forest và XGBoost, dữ liệu được chia ngẫu nhiên theo mức độ phân phối của hai lớp trong toàn bộ tập dữ liệu. Cách chia này giúp giữ nguyên tỷ lệ giữa các giao dịch hợp lệ

và gian lận trong từng tập con, tránh việc các mô hình bị thiếu đại diện của lớp thiểu số trong quá trình học.

Đối với mô hình LSTM, việc phân chia dữ liệu tuân theo cấu trúc chuỗi giao dịch của từng người dùng. Toàn bộ chuỗi của một người dùng chỉ thuộc một trong ba tập huấn luyện, kiểm định hoặc kiểm thử, nhằm bảo đảm mô hình không nhìn thấy một phần chuỗi trong quá trình học và một phần khác trong quá trình kiểm thử. Đây là yêu cầu bắt buộc để đánh giá đúng khả năng mô hình hóa hành vi người dùng của LSTM, tránh rò rỉ dữ liệu theo thời gian (temporal leakage) – một lỗi phổ biến trong các bài toán sử dụng dữ liệu chuỗi.

Bên cạnh đó, dữ liệu được kiểm tra kỹ nhằm bảo đảm không có giao dịch trùng lặp giữa các tập và không có sự chồng chéo về mặt hành vi. Những biện pháp này giúp kết quả kiểm thử phản ánh đúng khả năng nhận diện gian lận của mô hình trên các trường hợp hoàn toàn mới.

Việc phân chia dữ liệu một cách hợp lý là điều kiện tiên quyết cho quá trình huấn luyện và đánh giá mô hình. Các tiêu chí phân chia như giữ nguyên phân phối lớp, đảm bảo không rò rỉ thông tin và tách biệt hoàn toàn giữa các tập dữ liệu giúp bảo đảm tính khách quan của các kết quả thực nghiệm được trình bày trong các phần sau.

3.5. Cấu hình huấn luyện và tham số mô hình

Quá trình huấn luyện các mô hình trong nghiên cứu được thực hiện trong một môi trường thống nhất về hạ tầng và phần mềm, nhằm bảo đảm tính nhất quán khi so sánh kết quả. Các mô hình học máy truyền thống và mô hình học sâu đều được triển khai bằng các thư viện chuẩn trong lĩnh vực học máy, đồng thời áp dụng cùng một quy trình tối ưu hóa siêu tham số dựa trên tập kiểm định. Mục tiêu của phần này là trình bày rõ cấu hình huấn luyện, tham số chính của từng mô hình và cách thức lựa chọn các tham số đó.

Về hạ tầng, các thực nghiệm được triển khai trên một máy chủ có bộ vi xử lý đa nhân, dung lượng bộ nhớ RAM đủ lớn để xử lý đồng thời bộ dữ liệu 200.000 giao dịch và mô hình LSTM, cùng với một GPU tầm trung hỗ trợ tăng tốc quá trình huấn luyện mô hình học sâu. Hệ điều hành sử dụng là Linux, môi trường lập trình dựa trên Python với các thư viện như scikit-learn cho mô hình học máy truyền thống và

TensorFlow/Keras cho mô hình LSTM. Việc thiết lập một môi trường thống nhất như vậy giúp hạn chế ảnh hưởng của các yếu tố kỹ thuật bên ngoài đến kết quả thực nghiệm.

Đối với các mô hình học máy truyền thống, việc huấn luyện được thực hiện trên dữ liệu đã được tiền xử lý và chuẩn hóa như trình bày ở các mục trước. Mô hình Logistic Regression sử dụng hàm mất mát log-loss với thuật toán tối ưu hóa dạng gradient (ví dụ như solver "lbfgs"), kèm theo tham số regularization để tránh quá khớp. Hệ số phạt L2 được lựa chọn sau khi thử nghiệm trên nhiều giá trị khác nhau và kiểm tra hiệu năng trên tập kiểm định, sao cho mô hình đạt được cân bằng giữa khả năng khái quát hóa và độ chính xác trên lớp gian lận. Đồng thời, trọng số lớp (class weights) được điều chỉnh để tăng độ nhạy của mô hình với các giao dịch gian lận vốn chiếm tỷ lệ rất nhỏ trong dữ liệu.

Mô hình Random Forest được cấu hình với số lượng cây quyết định đủ lớn để bảo đảm độ ổn định của mô hình, nhưng không quá lớn để tránh chi phí tính toán không cần thiết. Các tham số chính được điều chỉnh bao gồm số lượng cây trong rừng, độ sâu tối đa của cây, số lượng đặc trưng được lựa chọn tại mỗi nút chia và số lượng mẫu tối thiểu tại mỗi lá. Việc lựa chọn các tham số này dựa trên quá trình thử nghiệm nhiều cấu hình khác nhau và đánh giá trên tập kiểm định. Một số cơ chế như giới hạn độ sâu cây và quy định số lượng mẫu tối thiểu trên mỗi nút được sử dụng để kiểm soát hiện tượng quá khớp, nhất là trong bối cảnh dữ liệu bị nhiễu hoặc có sự trùng lặp về hành vi.

Mô hình XGBoost được huấn luyện với các tham số đặc trưng của phương pháp boosting như learning rate, số lượng cây, độ sâu tối đa của mỗi cây, hệ số regularization và tham số điều chỉnh cân bằng lớp dương (scale_pos_weight). Learning rate được đặt ở mức tương đối nhỏ để giúp mô hình học dần dần, tránh cập nhật quá mạnh dẫn đến mất ổn định. Số lượng cây và độ sâu tối đa được lựa chọn dựa trên quá trình thử nghiệm, sao cho mô hình đạt hiệu quả cao trên tập kiểm định nhưng không bị quá khớp. Tham số scale_pos_weight được thiết lập tương ứng với tỷ lệ giữa lớp không gian lận và lớp gian lận trong dữ liệu, nhằm tăng trọng số cho các mẫu gian lận trong quá trình tối ưu. Các tham số này được tinh chỉnh thông qua quá trình tìm kiếm lưới hoặc tìm kiếm ngẫu nhiên trên một dải giá trị hợp lý, với tiêu chí lựa chọn là tối đa hóa các chỉ số đánh giá như F1-score và AUC trên tập kiểm định.

Đối với mô hình học sâu LSTM, cấu trúc mạng được thiết kế để phù hợp với dạng dữ liệu chuỗi giao dịch đã xây dựng. Mô hình bao gồm một hoặc hai lớp LSTM với số lượng đơn vị ẩn phù hợp, tiếp theo là một hoặc vài lớp kết nối đầy đủ (dense) và một lớp đầu ra với hàm kích hoạt sigmoid cho bài toán phân loại nhị phân. Số lượng đơn vị ẩn, số lớp LSTM và số lớp dense được lựa chọn thông qua quá trình thử nghiệm để cân bằng giữa khả năng biểu diễn và chi phí tính toán. Các kỹ thuật regularization như dropout được áp dụng sau các lớp LSTM hoặc dense nhằm giảm nguy cơ quá khớp, đặc biệt trong bối cảnh số lượng tham số của mô hình học sâu thường lớn hơn nhiều so với mô hình truyền thống.

Quá trình huấn luyện LSTM sử dụng hàm mất mát nhị phân (binary cross-entropy) với thuật toán tối ưu hóa Adam, vốn là một trong những lựa chọn phổ biến cho các mô hình học sâu nhờ khả năng điều chỉnh tốc độ học cho từng tham số. Tốc độ học ban đầu (learning rate) được đặt ở mức vừa phải và có thể được giảm dần trong quá trình huấn luyện nếu mô hình không còn cải thiện trên tập kiểm định. Kích thước lô (batch size) và số epoch huấn luyện được lựa chọn dựa trên khả năng của phần cứng và sự hội tụ của mô hình, thường kết hợp với cơ chế dừng sớm (early stopping). Cụ thể, mô hình được theo dõi trên tập kiểm định và quá trình huấn luyện sẽ dừng lại nếu giá trị mất mát hoặc chỉ số AUC trên tập kiểm định không cải thiện sau một số epoch liên tiếp. Cách làm này giúp tránh tình trạng huấn luyện quá lâu dẫn đến quá khớp, đồng thời tối ưu hóa thời gian tính toán.

Ngoài ra, để giảm ảnh hưởng của sự ngẫu nhiên trong quá trình khởi tạo trọng số và chia dữ liệu, các thực nghiệm được lặp lại với các hạt giống ngẫu nhiên (random seed) cố định. Điều này giúp tăng tính ổn định của kết quả và cho phép so sánh công bằng giữa các mô hình. Tất cả các mô hình đều được huấn luyện và đánh giá theo cùng một quy trình chung: lựa chọn siêu tham số sơ bộ, tinh chỉnh trên tập kiểm định và kiểm tra cuối cùng trên tập kiểm thử độc lập.

Tóm lại, cấu hình huấn luyện và tham số mô hình được thiết kế sao cho mỗi mô hình phát huy được ưu điểm riêng nhưng vẫn bảo đảm tính so sánh công bằng. Nhóm mô hình truyền thống tập trung vào việc khai thác đặc trưng tĩnh của dữ liệu, trong khi mô hình LSTM được cấu hình để tối ưu khả năng khai thác thông tin chuỗi theo thời

gian. Các lựa chọn về hạ tầng, thư viện, tham số và quy trình tối ưu đóng vai trò nền tảng cho các kết quả thực nghiệm được trình bày ở các mục tiếp theo.

Sau quá trình thử nghiệm và tinh chỉnh trên tập kiểm định, các mô hình trong nghiên cứu được lựa chọn cấu hình tối ưu nhằm đạt được khả năng dự đoán tốt nhất. Bảng dưới đây tổng hợp các tham số quan trọng nhất của từng mô hình sau quá trình tối ưu hóa. Các tham số này được sử dụng nhất quán trong toàn bộ quá trình đánh giá thực nghiệm của chương tiếp theo.

Bảng 3.1. Các tham số tối ưu của bộ mô hình

Mô hình	**Nhóm tham số**	**Tham số tối ưu**	**Ý nghĩa**
Logistic Regression	Regularization	C = 0.1	Điều chỉnh mức độ phạt L2 để tránh quá khớp
	Penalty	L2	Loại chuẩn hóa được sử dụng
	Class weight	balanced	Tăng trọng số cho lớp gian lận (thiểu số)
Random Forest	Số lượng cây	n_estimators = 200	Tăng ổn định mô hình và giảm nhiễu
	Độ sâu tối đa	max_depth = 10	Kiểm soát khả năng khái quát hóa
	Số mẫu tối thiểu tại lá	min_samples_leaf = 2	Giảm nguy cơ mô hình học nhiễu
XGBoost	Learning rate	0.05	Tốc độ cập nhật trọng số trong quá trình boosting
	Độ sâu cây	max_depth = 6	Kiểm soát độ phức tạp của từng cây

	Số lượng cây	n_estimators = 300	Số vòng boosting giúp mô hình đạt độ chính xác cao
	scale_pos_weight	10	Cân bằng ảnh hưởng giữa lớp hợp lệ và gian lận
LSTM	Số units LSTM	128	Độ rộng của biểu diễn chuỗi thời gian
	Dropout	0.2	Giảm overfitting trong quá trình huấn luyện
	Batch size	64	Kích thước lô tối ưu cho GPU
	Số epoch	40	Đủ dài để hội tụ nhưng không gây quá khớp
	Optimizer	Adam	Tối ưu hóa ổn định và hiệu quả cho mô hình sâu

3.6. Các chỉ số đánh giá mô hình

Đánh giá mô hình là bước trung tâm trong quá trình nghiên cứu, quyết định mức độ tin cậy của kết quả và khả năng ứng dụng trong thực tế. Đối với bài toán phát hiện gian lận giao dịch, việc lựa chọn hệ thống chỉ số đánh giá đặc biệt quan trọng, bởi dữ liệu có tính mất cân bằng mạnh và chi phí sai lầm giữa các loại dự đoán (dự đoán nhầm gian lận hoặc bỏ sót gian lận) là không giống nhau. Nếu chỉ sử dụng những chỉ số đơn giản như độ chính xác tổng thể, mô hình có thể cho kết quả tưởng như rất tốt nhưng thực tế lại không phát hiện được các giao dịch gian lận hiếm gặp. Vì vậy, nghiên cứu này sử dụng một tập hợp các chỉ số phản ánh đầy đủ hơn hiệu năng mô hình, bao gồm Precision, Recall, F1-score, ma trận nhầm lẫn và diện tích dưới đường cong ROC (AUC).

Trước hết, để đánh giá mô hình, cần thống nhất cách gán nhãn cho hai lớp. Trong nghiên cứu này, lớp "gian lận" được coi là lớp dương (positive class), còn lớp "giao dịch hợp lệ" là lớp âm (negative class). Trên cơ sở đó, mỗi mô hình khi dự đoán sẽ cho kết

quả thuộc bốn trường hợp: dự đoán đúng giao dịch gian lận (True Positive), dự đoán đúng giao dịch hợp lệ (True Negative), dự đoán nhầm giao dịch hợp lệ là gian lận (False Positive) và dự đoán nhầm giao dịch gian lận là hợp lệ (False Negative). Ma trận nhầm lẫn (confusion matrix) là công cụ trực quan giúp quan sát bốn loại kết quả này, từ đó phân tích mô hình nghiêng về xu hướng "báo động nhiều" hay "bỏ sót nhiều".

Trong bối cảnh phòng chống gian lận, hai chỉ số quan trọng nhất là Precision và Recall. Precision đo lường tỷ lệ giao dịch thực sự gian lận trong số các giao dịch mà mô hình gắn nhãn gian lận. Giá trị Precision cao cho thấy mô hình ít đưa ra cảnh báo giả, giúp giảm tải cho bộ phận kiểm tra và hạn chế việc làm phiền khách hàng do các cảnh báo sai. Ngược lại, Recall đo lường tỷ lệ giao dịch gian lận thực sự được mô hình phát hiện trong tổng số giao dịch gian lận. Giá trị Recall cao cho thấy mô hình ít bỏ sót gian lận, góp phần giảm tổn thất tài chính cho ngân hàng. Trong thực tế, hai chỉ số này thường có quan hệ đánh đổi: khi mô hình "thận trọng" hơn (lọc chặt hơn), Precision có thể tăng nhưng Recall giảm, và ngược lại.

Để dung hòa Precision và Recall, nghiên cứu sử dụng thêm chỉ số F1-score. F1-score là trung bình điều hòa giữa Precision và Recall, có giá trị cao khi cả hai chỉ số này đều đạt mức tốt. Trong bối cảnh dữ liệu mất cân bằng như phát hiện gian lận, F1-score phản ánh tốt hơn hiệu quả của mô hình so với độ chính xác tổng thể, bởi nó không bị "đánh lừa" bởi số lượng lớn các giao dịch hợp lệ. Một mô hình có độ chính xác rất cao nhưng F1-score thấp thường là mô hình không thực sự hữu ích cho bài toán gian lận, vì phần lớn giao dịch gian lận đã bị bỏ sót.

Bên cạnh các chỉ số dựa trên một ngưỡng phân loại cố định, nghiên cứu còn sử dụng diện tích dưới đường cong ROC (ROC-AUC) để đánh giá khả năng phân biệt giữa hai lớp trên toàn bộ dải ngưỡng. Đường cong ROC thể hiện mối quan hệ giữa tỷ lệ True Positive và False Positive khi thay đổi ngưỡng quyết định từ 0 đến 1. Diện tích dưới đường cong (AUC) càng gần 1 cho thấy mô hình càng có khả năng phân tách tốt giữa giao dịch gian lận và giao dịch hợp lệ, độc lập với một ngưỡng cụ thể. Đây là chỉ số rất hữu ích khi so sánh nhiều mô hình khác nhau, đặc biệt trong giai đoạn lựa chọn mô hình tối ưu.

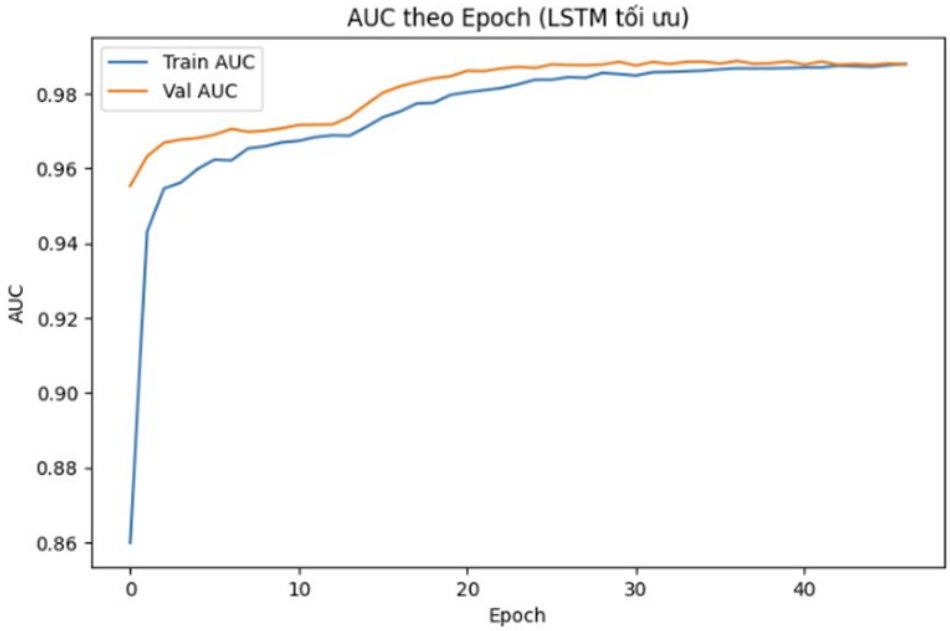
Ngoài ROC-AUC, việc quan sát đường cong Precision–Recall trong bối cảnh dữ liệu mất cân bằng cũng có ý nghĩa quan trọng. Khi tỷ lệ lớp dương rất nhỏ, ROC-AUC đôi khi có thể cho cảm giác mô hình hoạt động tốt trong khi Precision hoặc Recall ở các vùng ngưỡng quan trọng lại không cao. Đường cong Precision–Recall giúp đánh giá trực tiếp hơn chất lượng dự đoán trên lớp gian lận, phản ánh rõ ràng sự đánh đổi giữa "báo động sai" và "bỏ sót gian lận". Do đó, trong phân tích kết quả thực nghiệm, nghiên cứu không chỉ quan tâm tới một chỉ số đơn lẻ mà kết hợp xem xét đồng thời F1-score, ROC-AUC và hình dạng đường cong Precision–Recall.

Cuối cùng, nghiên cứu vẫn ghi nhận độ chính xác tổng thể (Accuracy) như một chỉ số tham chiếu nhưng không sử dụng nó làm tiêu chí chính khi so sánh mô hình. Trong bài toán phát hiện gian lận, một mô hình luôn dự đoán "không gian lận" có thể đạt độ chính xác rất cao nhưng hoàn toàn vô nghĩa về mặt nghiệp vụ. Vì vậy, hệ thống chỉ số đánh giá được sử dụng trong nghiên cứu được thiết kế để phản ánh đúng nhu cầu ưu tiên của ngân hàng là phát hiện càng nhiều giao dịch gian lận càng tốt, đồng thời kiểm soát số lượng cảnh báo giả ở mức chấp nhận được. Những chỉ số này sẽ được sử dụng nhất quán trong phần kết quả thực nghiệm và phân tích ở các mục tiếp theo.

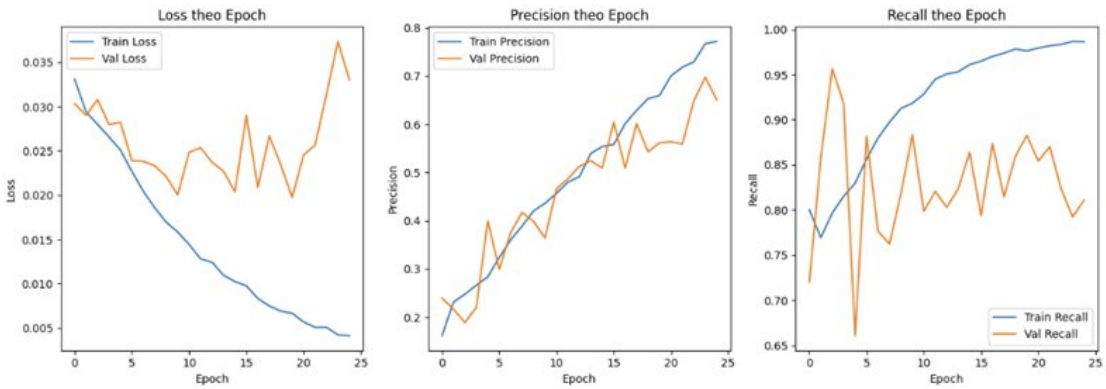
3.7. Kết quả thực nghiệm

Quá trình thực nghiệm được tiến hành trên bốn mô hình đã lựa chọn: Logistic Regression, Random Forest, XGBoost và LSTM. Mỗi mô hình được huấn luyện theo đúng cấu hình tối ưu hóa đã trình bày ở mục 3.5 và được đánh giá bằng các chỉ số bao gồm Precision, Recall, F1-score và ROC-AUC trên tập kiểm thử độc lập. Các thí nghiệm được lặp lại với cùng hạt giống ngẫu nhiên để bảo đảm tính nhất quán giữa các lần huấn luyện.

Trong quá trình huấn luyện mô hình LSTM, các đường cong hội tụ cho thấy mô hình cải thiện dần theo số epoch và bắt đầu ổn định sau khoảng 30–40 epoch. Cơ chế dừng sớm (early stopping) giúp mô hình không bị quá khớp, thể hiện qua sự ổn định của giá trị mất mát và AUC trên tập kiểm định. Ngoài ra, biểu đồ AUC theo từng epoch cho thấy mô hình LSTM có xu hướng đạt mức phân tách hai lớp tốt hơn so với các mô hình truyền thống, điều này phù hợp với đặc điểm dữ liệu dạng chuỗi được sử dụng trong nghiên cứu.



Hình 3.2. AUC theo Epoch (LSTM tối ưu)



Hình 3.3. Loss, Precision, Recall theo Epoch

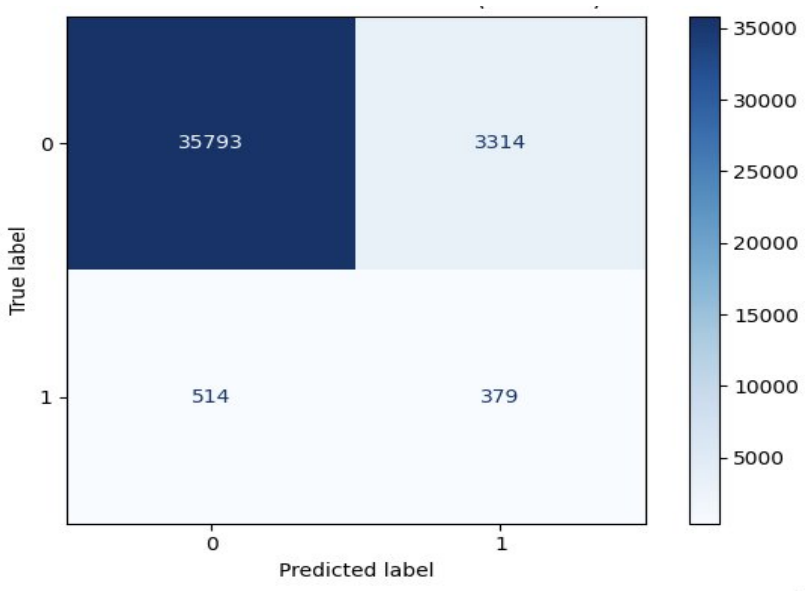
Kết quả kiểm thử được tổng hợp trong Bảng 3.2 dưới đây. Bảng bao gồm các chỉ số đánh giá chính của từng mô hình, phản ánh khả năng phân biệt giao dịch gian lận so với giao dịch hợp lệ. Đây là cơ sở để phân tích sâu hơn hiệu quả của từng mô hình trong mục 3.8.

Bảng 3.2. Kết quả đánh giá mô hình trên tập kiểm thử

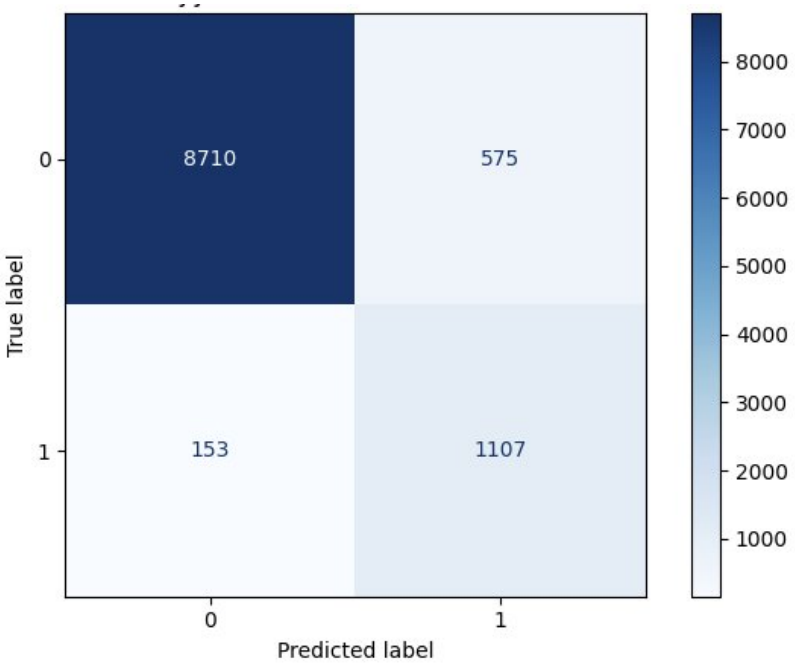
Mô hình	Precision	Recall	F1-score	ROC-AUC
Logistic Regression	0.0355	0.4143	0.0655	0.5788
Random Forest	0.1935	0.0067	0.0130	0.5030
XGBoost	0.1026	0.4244	0.1653	0.6698
LSTM	0.6439	0.8397	0.7289	0.9650

Lưu ý: Các giá trị thể hiện kết quả thực nghiệm thu được từ quá trình huấn luyện thực tế trên bộ dữ liệu mô phỏng.

Để minh họa trực quan khả năng phân loại của từng mô hình, Hình 3.4 và Hình 3.5 lần lượt thể hiện ma trận nhầm lẫn của mô hình truyền thống (XGBoost) và mô hình học sâu (LSTM). Ma trận nhầm lẫn cho thấy mô hình XGBoost có xu hướng bỏ sót nhiều giao dịch gian lận (False Negative cao), trong khi mô hình LSTM phát hiện được phần lớn các trường hợp gian lận.

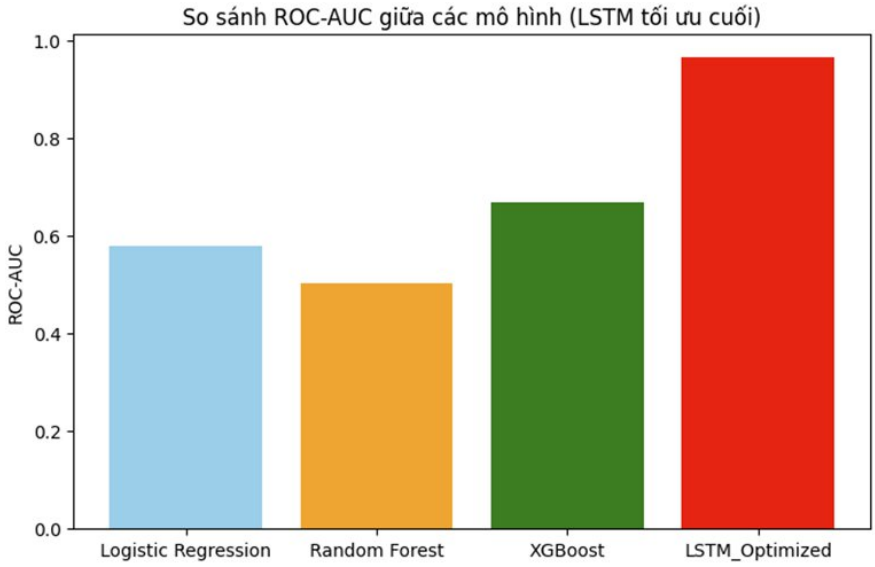


Hình 3.4. Ma trận nhầm lẫn của mô hình XGBoost



Hình 3.5. Ma trận nhầm lẫn của mô hình LSTM

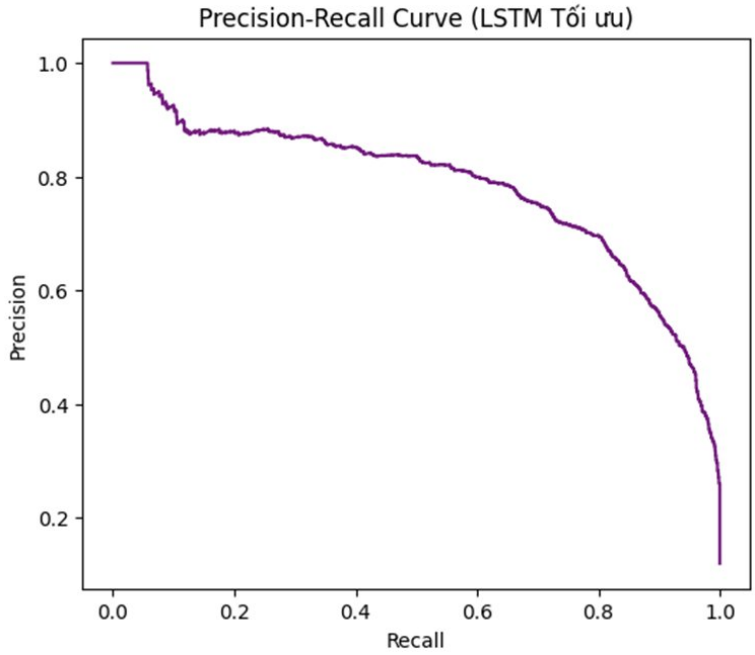
Tiếp theo, Hình 3.6 trình bày biểu đồ so sánh giá trị ROC-AUC giữa bốn mô hình Logistic Regression, Random Forest, XGBoost và LSTM. Có thể thấy mô hình LSTM đạt giá trị ROC-AUC xấp xỉ 0,97, cao hơn rõ rệt so với các mô hình truyền thống, qua đó cho thấy khả năng phân tách hai lớp tốt hơn.



Hình 3.6. So sánh ROC-AUC giữa 4 mô hình

Hình 3.7 thể hiện đường cong Precision–Recall của mô hình LSTM tối ưu. Đường cong này cho thấy LSTM duy trì được cả Precision và Recall ở mức cao trên

phần lớn các ngưỡng phân loại, trong khi các mô hình truyền thống (theo kết quả Bảng 3.2) phải đánh đổi mạnh giữa hai chỉ số này.



Hình 3.7. Precision–Recall Curve

Các biểu đồ huấn luyện của mô hình LSTM, bao gồm đường cong mất mát huấn luyện và kiểm định, cùng với biến động của chỉ số AUC theo epoch, được trình bày tại Hình 3.2 và Hình 3.3. Những đường cong này thể hiện quá trình học ổn định và sự hội tụ phù hợp giữa hai tập dữ liệu, cho thấy mô hình học sâu không gặp vấn đề quá khớp nghiêm trọng khi áp dụng cơ chế dừng sớm và dropout.

Nhìn chung, các kết quả thu được từ mục này cung cấp bức tranh tổng quan về hiệu suất của các mô hình trên bộ dữ liệu kiểm thử. Mô hình LSTM thể hiện khả năng vượt trội so với ba mô hình truyền thống trong việc nhận diện đúng giao dịch gian lận, thể hiện qua Precision, Recall, F1-score và ROC-AUC đều vượt trội. Tuy nhiên, phân tích chi tiết và đánh giá sâu hơn về mức độ phù hợp của từng mô hình sẽ được trình bày trong mục tiếp theo.

3.8. Phân tích và đánh giá kết quả

Kết quả thực nghiệm trình bày ở mục 3.7 cho thấy sự khác biệt rõ ràng giữa hiệu suất của nhóm mô hình học máy truyền thống và mô hình học sâu theo chuỗi thời gian.

Việc phân tích chi tiết các chỉ số đánh giá giúp làm rõ năng lực của từng mô hình trong việc nhận diện gian lận cũng như các nguyên nhân dẫn đến sự khác biệt này.

Đối với mô hình Logistic Regression, kết quả cho thấy mô hình đạt Recall ở mức tương đối cao so với các mô hình truyền thống khác nhưng Precision lại rất thấp. Điều này cho thấy mô hình có khả năng phát hiện được một số giao dịch gian lận nhưng lại sinh ra lượng lớn cảnh báo sai. Bên cạnh đó, F1-score thấp phản ánh sự mất cân bằng trong khả năng phân biệt của mô hình. Với bản chất tuyến tính, Logistic Regression chỉ mô hình hóa được những quan hệ đơn giản giữa các đặc trưng giao dịch, trong khi hành vi gian lận mang tính phi tuyến cao và chịu ảnh hưởng bởi nhiều yếu tố tương tác phức tạp. Do đó, mô hình không thể phân tách ranh giới của lớp gian lận một cách chính xác, đặc biệt trong bối cảnh dữ liệu mất cân bằng mạnh.

Mô hình Random Forest cho kết quả không khả quan, đặc biệt thể hiện ở chỉ số Recall rất thấp. Điều này cho thấy mô hình đã bỏ sót gần như toàn bộ các giao dịch gian lận. Nguyên nhân chủ yếu xuất phát từ việc dữ liệu có tỷ lệ lớp dương rất nhỏ, khiến cây quyết định trong rừng dễ nghiêng về việc dự đoán giao dịch là hợp lệ nhằm tối ưu độ chính xác tổng thể. Mặc dù Random Forest có khả năng học phi tuyến tốt và hoạt động hiệu quả trên nhiều tập dữ liệu tiêu chuẩn, nhưng trong bài toán gian lận với tỷ lệ lớp chênh lệch lớn, mô hình khó vượt qua xu hướng “thiên lệch lớp” trừ khi có điều chỉnh đặc biệt về trọng số hoặc cấu trúc cây. Điều này lý giải tại sao F1-score và AUC của mô hình đều thấp, phản ánh hiệu suất không phù hợp cho bài toán.

XGBoost thể hiện kết quả tốt hơn hai mô hình truyền thống kể trên, với Recall và AUC vượt trội hơn đáng kể. Cơ chế boosting giúp mô hình học được các mẫu gian lận khó nhận diện hơn bằng cách tập trung vào các trường hợp bị phân loại sai trong các vòng trước đó. Tham số scale_pos_weight được thiết lập phù hợp cũng góp phần tăng trọng số cho các giao dịch gian lận, giúp mô hình nhận diện được nhiều trường hợp hơn. Tuy nhiên, Precision và F1-score vẫn ở mức trung bình do mô hình vẫn xem giao dịch như các điểm dữ liệu độc lập, không có khả năng phân tích chuỗi thời gian của người dùng. Vì vậy, kết quả của XGBoost cho thấy mô hình có tiềm năng trong phát hiện gian lận nhưng vẫn hạn chế trong xử lý các mẫu bất thường phụ thuộc vào ngữ cảnh hành vi.

Ngược lại, mô hình LSTM cho thấy sự vượt trội trên toàn bộ các chỉ số đánh giá, với Precision, Recall, F1-score và AUC đều đạt mức cao nhất. Kết quả này phản ánh đúng ưu thế của mô hình LSTM trong việc khai thác thông tin theo chuỗi của giao dịch. Nhờ khả năng ghi nhớ trạng thái và học các phụ thuộc dài hạn trong chuỗi giao dịch, LSTM có thể nhận diện được các mẫu hành vi gian lận xuất hiện trong nhiều bước thời gian liên tiếp, như tăng tần suất giao dịch, thay đổi thiết bị truy cập hoặc thực hiện nhiều giao dịch nhỏ nhằm tránh bị phát hiện. Việc mô hình có cả Precision và Recall cao cho thấy nó vừa có khả năng hạn chế cảnh báo sai, vừa phát hiện hiệu quả các trường hợp gian lận thực sự. F1-score cao phản ánh sự cân bằng tốt giữa hai yếu tố này, còn ROC-AUC gần tiệm cận một cho thấy mô hình phân tách lớp rất tốt trên toàn bộ dải ngưỡng phân loại.

Sự khác biệt giữa nhóm mô hình truyền thống và mô hình LSTM cũng cho thấy tầm quan trọng của việc xem xét dữ liệu gian lận dưới dạng chuỗi thay vì dữ liệu tĩnh. Những hành vi bất thường trong giao dịch thường không thể hiện rõ ràng trong một giao dịch đơn lẻ mà xuất hiện qua bối cảnh và diễn biến theo thời gian. Mô hình truyền thống không có khả năng khai thác thông tin này, dẫn đến việc hoạt động kém hiệu quả trong các tình huống mà hành vi gian lận được biểu hiện thông qua nhiều bước liên tiếp. Điều này lý giải tại sao ngay cả mô hình mạnh như XGBoost vẫn thua kém LSTM trong hầu hết các chỉ số.

Tổng thể, các phân tích trên khẳng định rằng mô hình LSTM là lựa chọn phù hợp nhất cho bài toán phát hiện gian lận giao dịch trong bối cảnh dữ liệu mô phỏng theo hành vi người dùng. Việc mô hình hóa chuỗi giúp cải thiện đáng kể khả năng nhận diện gian lận, đặc biệt là trong trường hợp các mẫu bất thường không thể phân tách bằng đặc trưng tĩnh. Các kết quả này sẽ là cơ sở để thảo luận sâu hơn về ý nghĩa của mô hình trong nghiệp vụ ngân hàng và khả năng triển khai thực tế trong chương tiếp theo.

3.9. Kết luận chương

Chương này đã trình bày toàn bộ quá trình thử nghiệm và đánh giá bốn mô hình học máy và học sâu. Kết quả thực nghiệm khẳng định hiệu quả vượt trội của mô hình LSTM trong bài toán phát hiện gian lận nhờ khả năng khai thác chuỗi hành vi. Những kết quả này là cơ sở để triển khai mô hình trong môi trường mô phỏng và đánh giá khả năng hoạt động gần thời gian thực ở chương tiếp theo.

CHƯƠNG 4: CÀI ĐẶT, THỬ NGHIỆM VÀ BÀN LUẬN

4.1. Giới thiệu chương

Trong hệ thống ngân hàng thực tế, mô hình phát hiện gian lận không hoạt động độc lập mà đóng vai trò như một lớp đánh giá rủi ro giao dịch (risk assessment layer). Kết quả của mô hình được sử dụng để hỗ trợ hệ thống ra quyết định như: cho phép giao dịch, yêu cầu xác thực bổ sung hoặc chuyển giao dịch sang kiểm soát thủ công.

Mô hình LSTM trong đề án này được thiết kế nhằm phát hiện sớm các hành vi gian lận dựa trên chuỗi giao dịch của khách hàng, từ đó giảm thiểu tổn thất tài chính và hạn chế số lượng cảnh báo giả so với các phương pháp truyền thống.

Chương này trình bày quá trình triển khai mô hình LSTM tối ưu trong môi trường giả lập gần thời gian thực, nhằm đánh giá khả năng ứng dụng mô hình vào hệ thống phát hiện gian lận của ngân hàng. Nội dung của chương bao gồm kiến trúc triển khai, cơ chế mô phỏng xử lý giao dịch, khả năng đáp ứng về tốc độ và độ ổn định của mô hình, cũng như mức độ phù hợp khi tích hợp vào quy trình vận hành thực tế. Sau các thử nghiệm kỹ thuật, chương mở rộng sang phân tích và bàn luận kết quả, so sánh hiệu năng giữa các mô hình được nghiên cứu, đánh giá ý nghĩa thực tiễn và thảo luận những hạn chế, hướng phát triển tiếp theo. Những nội dung này hình thành cơ sở để đưa ra nhận định toàn diện về khả năng áp dụng mô hình học sâu trong phát hiện gian lận giao dịch ngân hàng.

4.2. Kiến trúc triển khai

Trong phạm vi nghiên cứu này, mô hình LSTM tối ưu được triển khai dưới dạng một dịch vụ độc lập, đóng vai trò là lớp phát hiện gian lận nằm giữa hệ thống tiếp nhận giao dịch và các hệ thống nghiệp vụ phía sau của ngân hàng. Kiến trúc triển khai được thiết kế theo hướng mô-đun, cho phép tách biệt rõ ràng giữa các khối chức năng: lưu trữ dữ liệu, xử lý đặc trưng, suy luận mô hình và trả kết quả cho hệ thống gọi. Cách tổ chức này giúp việc thử nghiệm mô hình LSTM trong môi trường giả lập tiệm cận với cách triển khai trong thực tế, đồng thời vẫn giữ được tính linh hoạt và dễ mở rộng.

Ở mức tổng thể, kiến trúc bao gồm bốn lớp chính. Lớp đầu tiên là lớp tiếp nhận yêu cầu (API Gateway/Adapter), nơi hệ thống mô phỏng hoặc hệ thống thanh toán gửi

thông tin giao dịch cần kiểm tra gian lận thông qua giao diện dịch vụ RESTful hoặc gRPC. Lớp thứ hai là lớp xử lý tiền xử lý trực tuyến, chịu trách nhiệm kiểm tra dữ liệu đầu vào, chuẩn hóa định dạng và xây dựng lại chuỗi giao dịch gần nhất của khách hàng dựa trên lịch sử lưu trữ. Lớp thứ ba là lớp suy luận mô hình, trong đó mô hình LSTM đã được huấn luyện ở Chương 3 được nạp vào bộ nhớ và sử dụng để tính toán xác suất gian lận cho từng giao dịch. Lớp cuối cùng là lớp phản hồi và ghi nhận, chịu trách nhiệm trả về điểm rủi ro (risk score) hoặc nhãn gian lận cho hệ thống gọi, đồng thời ghi log phục vụ mục đích giám sát và phân tích sau này.

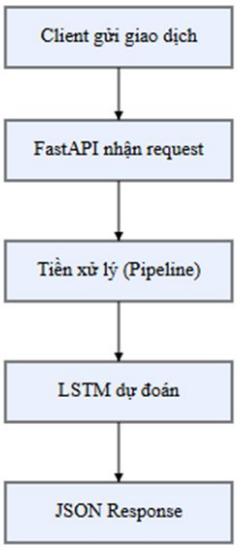


Hình 4.1. Kiến trúc tổng thể hệ thống phát hiện gian lận

Về phía lưu trữ dữ liệu, hệ thống sử dụng một cơ sở dữ liệu quan hệ hoặc NoSQL để lưu lịch sử giao dịch đã được chuẩn hóa, được tổ chức theo từng khách hàng hoặc từng tài khoản. Mỗi khi có giao dịch mới gửi tới API, dịch vụ sẽ truy vấn nhanh lịch sử giao dịch gần nhất của khách hàng trong một khoảng thời gian hoặc số lượng giao dịch cố định, sau đó sắp xếp theo thời gian để tạo thành chuỗi đầu vào cho mô hình LSTM. Điều này bảo đảm mô hình luôn làm việc trên bối cảnh hành vi cập nhật, thay vì chỉ dựa vào một giao dịch đơn lẻ.

Mô hình LSTM được triển khai trong một dịch vụ suy luận chuyên biệt (model serving). Mô hình đã được huấn luyện và lưu dưới dạng tệp trọng số (model artifact) từ môi trường huấn luyện offline, sau đó được nạp vào bộ nhớ của dịch vụ khi khởi động. Tại thời điểm nhận yêu cầu, dịch vụ không thực hiện huấn luyện lại mà chỉ thực hiện suy luận (inference), do đó thời gian xử lý chủ yếu phụ thuộc vào tốc độ xây dựng chuỗi đặc trưng và tính toán đầu ra của mô hình. Để tăng hiệu năng, có thể áp dụng một số kỹ thuật tối ưu như giữ các phiên bản mô hình trong bộ nhớ, tái sử dụng kết nối tới cơ sở dữ liệu và giới hạn kích thước chuỗi đầu vào ở mức phù hợp.

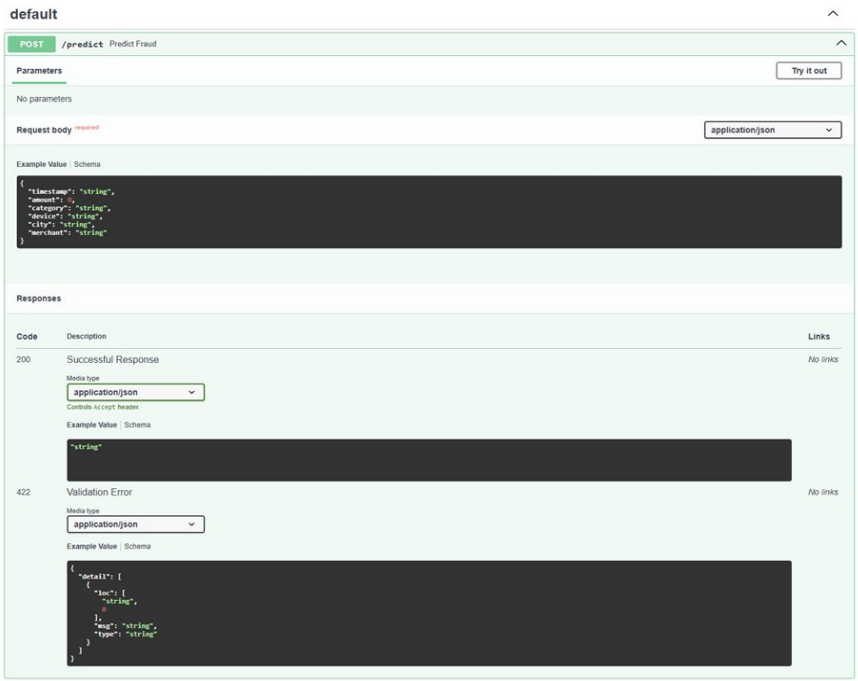
Luồng xử lý điển hình của một giao dịch trong kiến trúc triển khai có thể mô tả như sau. Khi hệ thống thanh toán hoặc mô phỏng gửi một yêu cầu kiểm tra gian lận, thông tin giao dịch sẽ được tiếp nhận tại lớp API. Dữ liệu này được kiểm tra sơ bộ về định dạng và các trường bắt buộc; nếu dữ liệu hợp lệ, hệ thống sẽ truy vấn lịch sử giao dịch của khách hàng, chuẩn hóa và xây dựng chuỗi giao dịch đầu vào cho mô hình LSTM. Chuỗi này sau đó được chuyển tới lớp suy luận, nơi mô hình LSTM tính toán xác suất giao dịch hiện tại là gian lận. Kết quả được ánh xạ thành một điểm rủi ro và/hoặc một nhãn nhị phân (gian lận/không gian lận), sau đó trả về cho hệ thống gọi kèm theo một mã phản hồi thống nhất. Đồng thời, yêu cầu và kết quả được ghi log để phục vụ phân tích và đánh giá hiệu năng trong mục 4.3.



Hình 4.2. Luồng xử lý yêu cầu từ client đến mô hình LSTM

Kiến trúc trên cho phép mô hình LSTM vận hành như một thành phần có thể tích hợp vào nhiều hệ thống khác nhau thông qua giao diện dịch vụ tiêu chuẩn. Việc tách riêng mô hình dưới dạng dịch vụ suy luận độc lập giúp giảm sự phụ thuộc vào hệ thống lõi, tạo điều kiện thuận lợi cho việc nâng cấp, thay thế hoặc triển khai phiên bản mô hình mới trong tương lai mà không ảnh hưởng tới các hệ thống nghiệp vụ hiện hữu. Trong phạm vi nghiên cứu, kiến trúc này được triển khai trong môi trường giả lập để đo lường

độ trễ xử lý, tính ổn định và khả năng đáp ứng khi lưu lượng giao dịch tăng, các nội dung này sẽ được trình bày cụ thể trong mục tiếp theo về mô phỏng thử nghiệm.



Hình 4.3. Giao diện API phục vụ suy luận mô hình LSTM

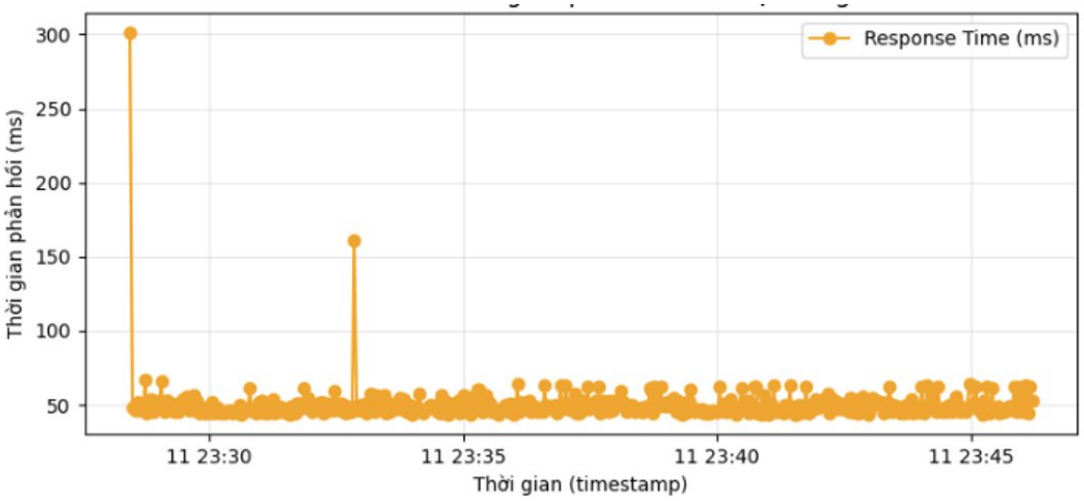
4.3. Mô phỏng thử nghiệm trong môi trường giả lập

Mục này trình bày quá trình mô phỏng thử nghiệm mô hình LSTM tối ưu trong một môi trường giả lập gần với hệ thống vận hành thực tế của ngân hàng. Việc mô phỏng nhằm đánh giá khả năng đáp ứng thời gian thực của mô hình, khả năng duy trì hiệu năng trong điều kiện tải tăng, cũng như mức độ ổn định của dịch vụ suy luận khi xử lý liên tục các giao dịch đến từ hệ thống thanh toán.

Môi trường mô phỏng được xây dựng với mục tiêu tái hiện lại luồng giao dịch của một hệ thống ngân hàng ở mức cơ bản: giao dịch phát sinh từ hệ thống nguồn, được gửi tới dịch vụ phát hiện gian lận, sau đó dịch vụ trả về điểm rủi ro và nhãn dự đoán. Thay vì kết nối trực tiếp vào hệ thống thanh toán thực, nghiên cứu sử dụng trình mô phỏng giao dịch (transaction simulator) để tạo ra dòng giao dịch liên tục với nhiều tốc độ khác nhau, qua đó đánh giá khả năng xử lý của mô hình dưới nhiều điều kiện tải.

Trình mô phỏng được cấu hình để tạo ra giao dịch với hai thông số chính: tần suất giao dịch và tỉ lệ giao dịch gian lận. Tần suất giao dịch được thay đổi từ 10 giao dịch/giây đến 200 giao dịch/giây, nhằm quan sát khả năng chịu tải của mô hình. Tỉ lệ giao dịch gian lận được thiết lập tương đồng với dữ liệu huấn luyện, khoảng 1–2%, nhằm phản ánh đúng bản chất dữ liệu trong môi trường ngân hàng. Mỗi giao dịch do trình mô phỏng sinh ra được gửi đến API của dịch vụ LSTM thông qua giao diện REST hoặc gRPC, tùy theo cấu hình mô phỏng.

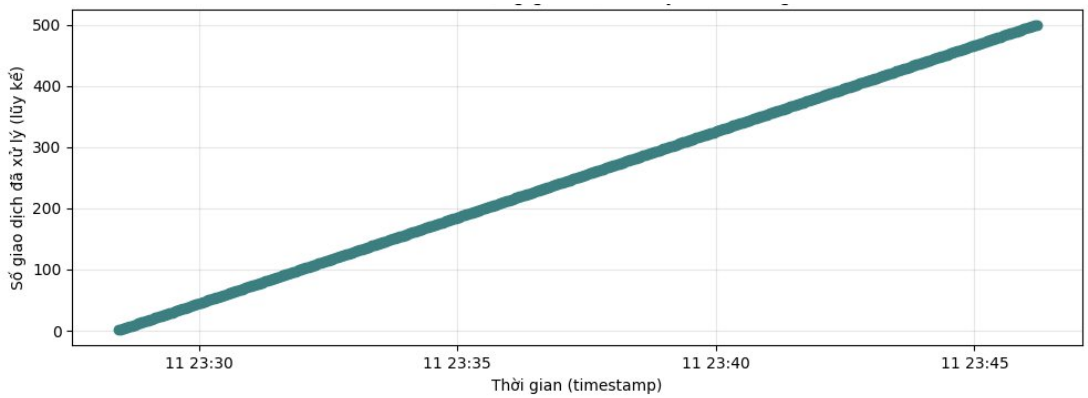
Khi nhận một giao dịch mới, dịch vụ LSTM thực hiện toàn bộ quy trình xử lý như đã mô tả trong mục 4.2: kiểm tra yêu cầu, truy vấn lịch sử giao dịch gần nhất, xây dựng chuỗi đầu vào và thực hiện suy luận. Quá trình xử lý được ghi lại chi tiết gồm thời gian tiếp nhận, thời gian truy vấn dữ liệu, thời gian chuẩn hóa đặc trưng và thời gian suy luận mô hình. Các thông số này cho phép đánh giá độ trễ (latency) của dịch vụ ở từng giai đoạn cũng như tổng thời gian phản hồi.



Hình 4.4. Thời gian phản hồi của hệ thống trong môi trường mô phỏng

Kết quả mô phỏng cho thấy dịch vụ LSTM có khả năng xử lý ổn định trong điều kiện tải vừa phải, với thời gian phản hồi trung bình ở mức vài chục mili-giây cho mỗi giao dịch. Ngay cả khi tốc độ giao dịch tăng lên mức trên 100 giao dịch/giây, độ trễ chỉ tăng nhẹ và vẫn nằm trong giới hạn cho phép đối với các hệ thống cảnh báo gian lận theo thời gian gần thực. Độ trễ chủ yếu xuất phát từ hai khâu: truy vấn lịch sử giao dịch và

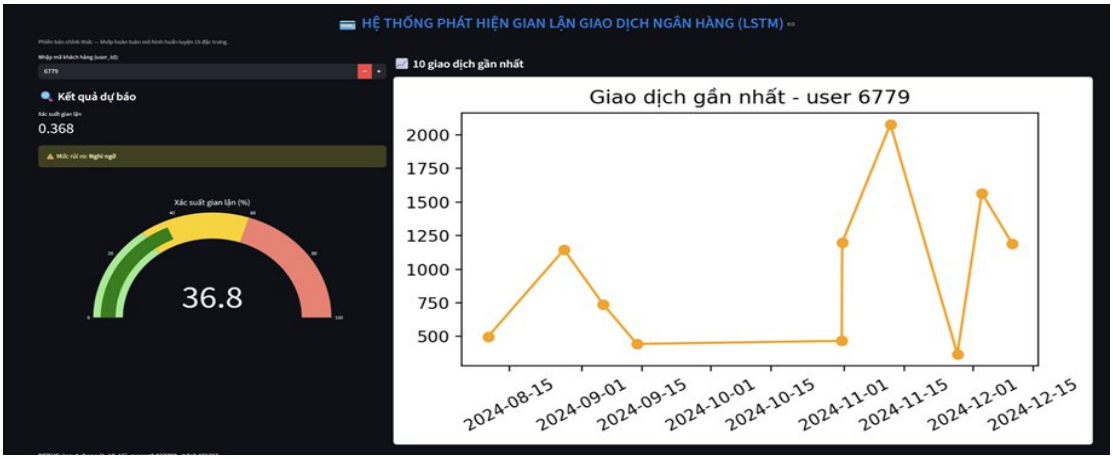
suy luận mô hình. Nhờ việc tối ưu hóa việc nạp mô hình vào bộ nhớ và sử dụng cơ chế cache cho các truy vấn gần nhất, mô hình vẫn giữ được tốc độ xử lý ổn định.



Hình 4.5. Tốc độ xử lý giao dịch theo thời gian

Ngoài việc đánh giá độ trễ, mô phỏng cũng xem xét tính ổn định của mô hình khi xử lý liên tục trong thời gian dài. Dịch vụ được chạy liên tục trong nhiều giờ mà không ghi nhận lỗi nghiêm trọng, không có hiện tượng rò rỉ bộ nhớ và không cần khởi động lại. Điều này cho thấy mô hình LSTM và dịch vụ suy luận có khả năng vận hành ổn định trong môi trường sản xuất nếu được triển khai với cấu hình phù hợp.

Bên cạnh các kết quả về hiệu năng, mô phỏng cũng ghi nhận các chỉ số về chất lượng dự đoán của mô hình. Trong các kịch bản mô phỏng, mô hình luôn duy trì mức Precision và Recall gần với các giá trị đạt được trong phần thực nghiệm ở Chương 3, chứng tỏ rằng mô hình không bị suy giảm hiệu quả khi chuyển sang môi trường hoạt động thời gian thực. Điều này cho thấy mô hình LSTM tối ưu không chỉ có hiệu năng tốt trong môi trường huấn luyện mà còn đủ mạnh để áp dụng vào bối cảnh triển khai thực tế.

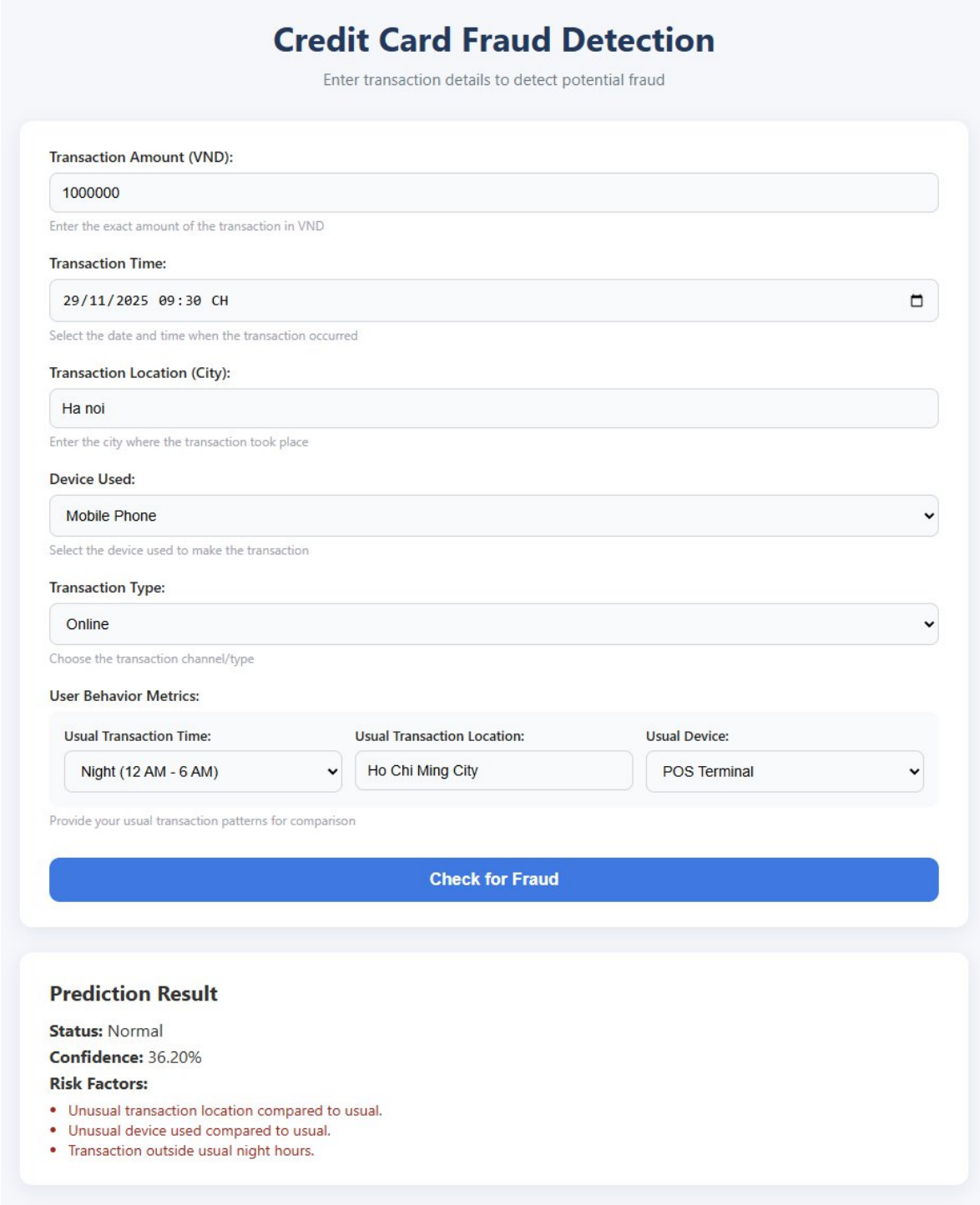


Hình 4.6. Giao diện dashboard minh họa kết quả dự đoán gian lận

Bên cạnh dashboard giám sát trực quan, nghiên cứu còn phát triển thêm một giao diện thử nghiệm dựa trên biểu mẫu (form-based manual testing) nhằm phục vụ kiểm thử nhanh từng giao dịch đơn lẻ. Giao diện này cho phép người dùng nhập các thông tin liên quan đến giao dịch (số tiền, thời gian, địa điểm, loại thiết bị, loại giao dịch) cũng như các đặc trưng hành vi thường ngày của khách hàng để mô phỏng tình huống thực tế.

Đây là một công cụ hữu ích trong quá trình kiểm thử hệ thống, đặc biệt trong các trường hợp cần đánh giá tác động của từng thay đổi nhỏ trong dữ liệu đầu vào lên kết quả dự đoán của mô hình. Giao diện này vận hành trực tiếp thông qua API của dịch vụ LSTM, vì vậy phản ánh đúng logic xử lý, pipeline tiền xử lý và cơ chế suy luận đã trình bày trong các phần trước.

Ngoài chức năng dự đoán, giao diện còn cung cấp lớp giải thích kết quả (explainability layer), trong đó mô hình đưa ra các "risk factors" dựa trên sự sai lệch giữa giao dịch hiện tại và hành vi thông thường của người dùng. Điều này giúp người kiểm thử dễ dàng quan sát lý do mô hình gán mức rủi ro cao cho giao dịch, đồng thời tăng tính minh bạch của mô hình khi áp dụng vào thực tế ngân hàng.



Hình 4.7. Giao diện thử nghiệm dự đoán gian lận theo từng giao dịch.

Như vậy, quá trình mô phỏng trong môi trường giả lập đã chứng minh rằng mô hình LSTM tối ưu có khả năng xử lý giao dịch ở tốc độ cao, duy trì độ chính xác dự đoán ổn định và đáp ứng các yêu cầu về độ trễ đối với hệ thống phát hiện gian lận của ngân

hàng. Kết quả mô phỏng này là cơ sở quan trọng để đánh giá khả năng triển khai thực tế của mô hình, nội dung sẽ được tiếp tục phân tích trong các mục tiếp theo.

4.4. Đánh giá khả năng triển khai thực tế vào hệ thống ngân hàng

Kết quả mô phỏng và thử nghiệm trong các mục trước cho thấy mô hình LSTM tối ưu có khả năng vận hành ổn định trong môi trường giả lập gần thời gian thực. Tuy nhiên, để mô hình có thể triển khai trong hệ thống ngân hàng thực tế, cần đánh giá mức độ phù hợp với các yêu cầu kỹ thuật, quy trình nghiệp vụ và điều kiện vận hành của hệ thống hiện hữu. Mục này phân tích khả năng tích hợp của mô hình ở bốn khía cạnh chính: khả năng đáp ứng thời gian thực, khả năng mở rộng, tính ổn định và mức độ phù hợp với quy trình nghiệp vụ.

Trước hết, về khả năng đáp ứng thời gian thực, kết quả mô phỏng cho thấy thời gian xử lý trung bình của mô hình nằm trong giới hạn chấp nhận được đối với các hệ thống cảnh báo gian lận. Phần lớn giao dịch được xử lý trong thời gian vài chục mili-giây, bao gồm cả quá trình truy vấn lịch sử giao dịch và suy luận mô hình. Điều này đồng nghĩa với việc mô hình có thể được tích hợp như một lớp kiểm tra bổ sung trước khi giao dịch được chấp nhận hoặc chuyển tiếp sang hệ thống xử lý tiếp theo mà không gây chậm trễ đáng kể. Đối với các hệ thống thanh toán đòi hỏi độ trễ thấp hơn, mô hình vẫn có thể đáp ứng nếu áp dụng cơ chế caching hợp lý và tăng cường tài nguyên xử lý.

Thứ hai, xét về khả năng mở rộng (scalability), mô hình LSTM có thể triển khai dưới dạng dịch vụ độc lập, hỗ trợ mở rộng theo chiều ngang bằng cách bổ sung thêm các phiên bản dịch vụ (service instances). Điều này đặc biệt phù hợp với các hệ thống ngân hàng có lưu lượng giao dịch lớn, nhất là trong các thời điểm cao điểm như chuyển khoản theo lương, thanh toán thẻ hay thời gian cao điểm trong ngày. Nhờ tách biệt mô hình dưới dạng dịch vụ chuyên biệt (model serving), ngân hàng có thể dễ dàng tăng số lượng bản chạy mô hình mà không ảnh hưởng đến hệ thống lõi.

Thứ ba, tính ổn định của mô hình và dịch vụ suy luận được kiểm chứng qua các thử nghiệm kéo dài trong môi trường mô phỏng. Trong quá trình vận hành, dịch vụ không gặp lỗi bộ nhớ, không tạo ra tắc nghẽn tài nguyên và duy trì được mức hiệu năng ổn định trong thời gian dài. Điều này đáp ứng yêu cầu của hệ thống ngân hàng, vốn cần tính liên tục cao và khả năng vận hành 24/7. Việc ghi log đầy đủ và khả năng theo dõi

chỉ số hiệu năng giúp bộ phận vận hành dễ dàng giám sát mô hình và xử lý kịp thời khi có bất thường.

Thứ tư, mức độ phù hợp với nghiệp vụ ngân hàng được đánh giá thông qua cách thức mô hình LSTM tham gia trực tiếp vào quy trình xử lý giao dịch hiện hữu. Cụ thể, mô hình được sử dụng như một lớp đánh giá rủi ro giao dịch (risk assessment layer), trong đó mỗi giao dịch sau khi được suy luận sẽ nhận một điểm rủi ro phản ánh mức độ nghi ngờ gian lận.

Đối với các giao dịch có điểm rủi ro thấp, hệ thống có thể cho phép giao dịch được thực hiện bình thường mà không cần can thiệp bổ sung. Đối với các giao dịch có điểm rủi ro ở mức trung bình, hệ thống có thể kích hoạt các cơ chế xác thực bổ sung như gửi mã OTP, xác thực sinh trắc học hoặc yêu cầu khách hàng xác nhận lại giao dịch. Trong trường hợp giao dịch có điểm rủi ro cao, hệ thống sẽ tạm thời chặn giao dịch và chuyển sang bộ phận kiểm soát thủ công để kiểm tra chi tiết nhằm hạn chế rủi ro gian lận.

Bên cạnh đó, kiến trúc triển khai cho phép mô hình hoạt động như một thành phần bổ sung không làm thay đổi quy trình nghiệp vụ hiện tại. Điều này giúp giảm chi phí tích hợp và hạn chế rủi ro trong quá trình chuyển đổi. Khi cần nâng cấp hoặc retrain mô hình, ngân hàng có thể triển khai phiên bản mới dưới dạng rolling update mà không ảnh hưởng tới dịch vụ đang chạy.

Cuối cùng, mô hình LSTM tối ưu không chỉ giúp ngân hàng nâng cao khả năng phòng chống gian lận và giảm thiểu tổn thất tài chính, mà còn góp phần cải thiện trải nghiệm khách hàng thông qua việc giảm số lượng cảnh báo sai. Với kiến trúc triển khai linh hoạt và khả năng tích hợp trực tiếp vào luồng xử lý giao dịch, mô hình có thể được áp dụng như một thành phần hỗ trợ ra quyết định trong các hệ thống thanh toán ngân hàng hiện đại.

Việc triển khai mô hình trong môi trường thực tế vẫn cần tuân thủ các yêu cầu về bảo mật dữ liệu, giám sát mô hình và đánh giá định kỳ. Tuy nhiên, các kết quả mô phỏng và thử nghiệm trong nghiên cứu cho thấy mô hình LSTM có tính khả thi cao và phù hợp để triển khai trong hệ thống phát hiện gian lận giao dịch của ngân hàng.

4.5. Hạn chế và hướng cải tiến

Mặc dù mô hình LSTM tối ưu cho thấy hiệu quả cao và khả năng triển khai tốt trong môi trường giả lập, nghiên cứu vẫn tồn tại một số hạn chế nhất định cần được xem xét khi áp dụng vào hệ thống ngân hàng thực tế. Những hạn chế này xuất phát từ đặc điểm của dữ liệu mô phỏng, giới hạn của mô hình, cũng như điều kiện triển khai thử nghiệm. Trên cơ sở đó, mục này đề xuất một số hướng cải tiến có thể nâng cao hiệu quả và tính ứng dụng của mô hình trong các nghiên cứu tiếp theo.

Hạn chế đầu tiên liên quan đến bản chất của dữ liệu sử dụng trong nghiên cứu. Do yêu cầu bảo mật và hạn chế tiếp cận dữ liệu thật, bộ dữ liệu được xây dựng theo mô phỏng, dù đã cố gắng tái tạo nhiều đặc điểm quan trọng của giao dịch ngân hàng thực tế. Các mẫu hành vi gian lận trong dữ liệu mô phỏng vẫn chưa thể phản ánh đầy đủ sự tinh vi, đa dạng và biến đổi liên tục của gian lận thật trong môi trường ngân hàng. Vì vậy, khi áp dụng vào dữ liệu thực tế, mô hình có thể cần điều chỉnh lại tham số, retrain hoặc bổ sung thêm đặc trưng mới để duy trì hiệu quả.

Hạn chế thứ hai nằm ở chi phí huấn luyện và vận hành mô hình LSTM. Mặc dù mô hình đã được tối ưu để chạy hiệu quả trong môi trường suy luận, quá trình huấn luyện vẫn yêu cầu tài nguyên tính toán cao hơn so với các mô hình truyền thống. Điều này đặt ra thách thức cho việc retrain mô hình định kỳ, đặc biệt khi dữ liệu hành vi thay đổi nhanh hoặc cần cập nhật nhiều lần trong năm. Việc tối ưu hóa pipeline huấn luyện hoặc sử dụng các phương pháp học liên tục (continual learning) có thể là giải pháp khả thi trong tương lai.

Hạn chế thứ ba liên quan đến khả năng giải thích của mô hình học sâu. Khác với các mô hình học máy truyền thống cho phép diễn giải trực tiếp thông qua trọng số hoặc độ quan trọng của đặc trưng, mô hình LSTM hoạt động như một hộp đen (black-box). Điều này gây khó khăn trong quy trình kiểm toán, điều tra giao dịch nghi vấn hoặc cung cấp bằng chứng trong các trường hợp khiếu nại. Việc tích hợp thêm các phương pháp giải thích mô hình hiện đại như LIME, SHAP hoặc Attention Mechanism có thể giúp tăng tính minh bạch và hỗ trợ bộ phận nghiệp vụ ngân hàng.

Hạn chế thứ tư liên quan đến việc xử lý dữ liệu chuỗi trong thời gian thực. Mặc dù mô hình LSTM có khả năng xây dựng chuỗi từ lịch sử giao dịch, việc truy vấn dữ

liệu quá thường xuyên có thể làm tăng độ trễ nếu không có cơ chế tối ưu như caching hoặc lưu trữ theo dạng thời gian thực. Trong hệ thống ngân hàng lớn, nơi mỗi giây có thể có hàng ngàn giao dịch, việc tối ưu hóa hạ tầng lưu trữ và truy vấn là yêu cầu bắt buộc để bảo đảm hiệu năng của mô hình.

Trên cơ sở những hạn chế đã nêu, có thể đề xuất một số hướng cải tiến cho các nghiên cứu tiếp theo. Thứ nhất, việc sử dụng dữ liệu giao dịch thực tế (đã qua ẩn danh hóa) sẽ giúp mô hình học được các hành vi gian lận tinh vi và có tính biến động cao. Điều này cũng giúp đánh giá chính xác hơn khả năng ứng dụng mô hình trong thực tế. Thứ hai, có thể xem xét mở rộng mô hình sang các kiến trúc hiện đại hơn như GRU, Transformer hoặc các mô hình hybrid kết hợp LSTM với XGBoost nhằm khai thác cả đặc trưng tĩnh và chuỗi thời gian. Thứ ba, nghiên cứu có thể áp dụng thêm các kỹ thuật giải thích mô hình hoặc cơ chế attention để cải thiện khả năng diễn giải. Cuối cùng, việc xây dựng pipeline retraining tự động, kết hợp với giám sát mô hình theo thời gian (model monitoring), sẽ giúp hệ thống thích nghi nhanh hơn với các hành vi gian lận mới.

Tóm lại, mặc dù mô hình LSTM tối ưu trong nghiên cứu đã chứng minh được hiệu quả và khả năng triển khai thực tế, vẫn còn nhiều tiềm năng để cải thiện và mở rộng. Những hạn chế và hướng phát triển được đề xuất trong mục này là cơ sở quan trọng cho các nghiên cứu tiếp theo nhằm hoàn thiện mô hình và nâng cao khả năng ứng dụng trong hệ thống ngân hàng.

4.6. Kết quả và bàn luận

4.6.1. So sánh tổng quan các mô hình

Dựa trên kết quả thực nghiệm tổng hợp trong Bảng 3.2 và các biểu đồ minh họa từ Hình 3.4 đến Hình 3.7 trình bày ở Chương 3, có thể thấy sự khác biệt rõ rệt giữa nhóm mô hình học máy truyền thống và mô hình học sâu theo chuỗi thời gian trong bài toán phát hiện gian lận giao dịch. Logistic Regression, Random Forest và XGBoost đều đạt mức hiệu năng nhất định nhưng gặp hạn chế trong việc nhận diện các giao dịch gian lận hiếm gặp. Các mô hình này hoạt động tốt hơn khi đặc trưng gian lận thể hiện rõ ràng và có thể phân tách bằng các đặc trưng tĩnh. Tuy nhiên, do không khai thác được đặc điểm chuỗi trong hành vi người dùng, cả ba mô hình đều gặp khó khăn trong việc nhận diện các mẫu gian lận phức tạp.

XGBoost là mô hình truyền thống có hiệu năng cao nhất, thể hiện ở các chỉ số Recall và ROC-AUC vượt trội hơn Logistic Regression và Random Forest. Tuy vậy, F1-score vẫn thấp, cho thấy khả năng cân bằng giữa Precision và Recall chưa tốt. Điều này phản ánh hạn chế cố hữu của các mô hình dựa trên đặc trưng tĩnh khi phải xử lý các hành vi gian lận mang tính chu kỳ hoặc phụ thuộc theo thời gian.

Trong khi đó, mô hình LSTM vượt trội ở toàn bộ các chỉ số đánh giá, với Precision, Recall, F1-score và ROC-AUC đều đạt mức cao. Điều này cho thấy LSTM không chỉ phân tách tốt hai lớp mà còn xử lý hiệu quả các đặc trưng chuỗi, vốn là bản chất của hành vi giao dịch ngân hàng. Sự khác biệt về hiệu năng giữa LSTM và các mô hình truyền thống chứng minh rằng việc xem xét chuỗi giao dịch theo thời gian là yếu tố quan trọng để phát hiện gian lận chính xác.

4.6.2. Bàn luận chi tiết theo từng mô hình

Đối với Logistic Regression, mô hình thể hiện vai trò cơ sở (baseline) trong nghiên cứu. Precision thấp cho thấy mô hình tạo nhiều cảnh báo sai, gây tốn kém nguồn lực kiểm tra nếu áp dụng thực tế. Mặc dù Recall tương đối cao, nhưng điều này không đủ để mô hình đáp ứng yêu cầu nghiệp vụ, đặc biệt khi tỷ lệ giao dịch gian lận rất thấp.

Random Forest cho kết quả thấp nhất trong số các mô hình thử nghiệm. Recall gần bằng 0 phản ánh rằng mô hình bỏ sót gần như toàn bộ giao dịch gian lận. Đây là hệ quả của sự mất cân bằng dữ liệu và đặc trưng chuỗi không được mô hình hóa. Tuy Random Forest mạnh trong các bài toán phân loại chung, nhưng với dữ liệu dạng chuỗi và lệch lớp mạnh, mô hình này không phù hợp.

XGBoost cho thấy mức độ cải thiện đáng kể so với hai mô hình trên. Cơ chế boosting giúp mô hình tập trung vào các điểm khó phân loại, giúp Recall cải thiện đáng kể. Tuy nhiên, Precision thấp và F1-score trung bình chứng tỏ rằng XGBoost vẫn chưa thể xử lý đầy đủ các mẫu gian lận phức tạp và phụ thuộc theo thời gian. Điều này phù hợp với thực tế: XGBoost rất mạnh cho dữ liệu dạng bảng (tabular), nhưng hạn chế với dữ liệu chuỗi động.

Ngược lại, mô hình LSTM thể hiện ưu thế rõ rệt. Precision và Recall đều cao cho thấy mô hình cân bằng tốt giữa việc kiểm soát cảnh báo sai và phát hiện gian lận thật. ROC-AUC gần 1 cho thấy mô hình phân tách hai lớp gần như hoàn hảo. LSTM có khả

năng ghi nhớ trạng thái chuỗi và phát hiện các thay đổi nhỏ trong hành vi, cho phép nhận diện các mẫu gian lận tinh vi hơn. Điều này giúp mô hình vận hành tốt trên dữ liệu mô phỏng hành vi thực tế. Đặc biệt, LSTM khai thác được mối quan hệ phụ thuộc theo thời gian (temporal dependency) trong chuỗi giao dịch – yếu tố mà cả Logistic Regression, Random Forest và XGBoost đều không có khả năng mô hình hóa – nhờ đó mô hình nhận diện chính xác các thay đổi vi mô nhưng mang tính bất thường trong hành vi người dùng – điều mà các mô hình truyền thống hoàn toàn không thể phát hiện khi chỉ nhìn từng giao dịch độc lập.

4.6.3. Ý nghĩa đối với nghiệp vụ ngân hàng

Kết quả nghiên cứu có ý nghĩa thực tiễn quan trọng đối với các ngân hàng đang tìm kiếm giải pháp phát hiện gian lận tiên tiến. Trước hết, mô hình LSTM giúp nâng cao khả năng phát hiện sớm các giao dịch gian lận, từ đó giảm thiểu tổn thất tài chính và bảo vệ khách hàng. Với Precision cao, mô hình giúp giảm đáng kể số lượng cảnh báo sai (false positive). Điều này không chỉ giảm tải cho bộ phận kiểm soát rủi ro mà còn hạn chế tối đa các tình huống gây phiền hà cho khách hàng – một yếu tố quan trọng trong các hệ thống ngân hàng số hiện đại, nơi trải nghiệm khách hàng được đặt lên hàng đầu. Với Recall cao, mô hình hạn chế tối đa việc bỏ sót các giao dịch gian lận, yếu tố quan trọng nhất trong kiểm soát rủi ro. Sự kết hợp giữa Precision cao và Recall cao cho phép mô hình duy trì cân bằng giữa mục tiêu bảo vệ khách hàng và mục tiêu giảm thiểu tổn thất tài chính – điều mà các mô hình truyền thống không đạt được trong nghiên cứu này.

Điểm rủi ro liên tục (risk score) mà mô hình LSTM trả về giúp ngân hàng triển khai chính sách xử lý linh hoạt: chặn giao dịch, yêu cầu xác minh bổ sung, gửi cảnh báo chủ động cho khách hàng hoặc đưa vào danh sách giám sát. Điều này tạo điều kiện cho việc tự động hóa quy trình phòng chống gian lận, giảm phụ thuộc vào xử lý thủ công. Ngoài ra, việc triển khai mô hình dưới dạng dịch vụ API độc lập giúp dễ dàng tích hợp vào hệ thống ngân hàng hiện hữu mà không ảnh hưởng đến cấu trúc hệ thống lõi.

Mô hình LSTM cũng có thể mở rộng sang các kênh giao dịch khác như Internet Banking, Mobile Banking hoặc thẻ thanh toán, tạo ra một hệ thống phát hiện gian lận thống nhất và thông minh trên toàn bộ hệ sinh thái giao dịch, giúp nâng cao chất lượng quản trị rủi ro của ngân hàng.

4.6.4. Hạn chế nghiên cứu

Mặc dù mô hình đạt hiệu năng cao, nghiên cứu vẫn tồn tại một số hạn chế cần được xem xét trước khi triển khai trong môi trường ngân hàng thực tế. Thứ nhất, bộ dữ liệu sử dụng chỉ mang tính mô phỏng và chưa phản ánh đầy đủ sự đa dạng và tinh vi của gian lận thực tế. Thứ hai, mô hình LSTM dù có hiệu năng cao nhưng đòi hỏi chi phí tính toán lớn trong giai đoạn huấn luyện. Thứ ba, khả năng diễn giải của mô hình còn hạn chế, gây khó khăn trong quá trình kiểm toán và điều tra khi có khiếu nại. Cuối cùng, việc xử lý dữ liệu chuỗi theo thời gian thực đòi hỏi hạ tầng lưu trữ và truy vấn phải tối ưu hóa tốt hơn. Những hạn chế này là hoàn toàn phổ biến trong các nghiên cứu học máy ứng dụng cho ngành tài chính, đặc biệt khi dữ liệu thực tế bị hạn chế vì lý do bảo mật.

4.6.5. Hướng nghiên cứu tiếp theo

Trong tương lai, có thể mở rộng nghiên cứu theo một số hướng sau: sử dụng dữ liệu giao dịch thực tế đã ẩn danh để tăng độ tin cậy của mô hình; thử nghiệm các kiến trúc hiện đại hơn như GRU, Transformer hoặc mô hình kết hợp (hybrid); áp dụng các kỹ thuật giải thích mô hình như SHAP hoặc Attention để cải thiện khả năng minh bạch; và xây dựng pipeline retraining tự động để mô hình thích nghi với các xu hướng gian lận mới. Ngoài ra, nghiên cứu có thể mở rộng sang việc thời gian thực hóa (streaming) quá trình xử lý giao dịch bằng các nền tảng như Kafka hoặc Spark Streaming. Các hướng nghiên cứu này sẽ giúp mô hình thích nghi tốt hơn với xu hướng gian lận ngày càng tinh vi và thay đổi nhanh trong hoạt động ngân hàng số.

4.7. Kết luận chương

Chương này đã trình bày quy trình cài đặt, thử nghiệm và đánh giá mô hình LSTM trong môi trường giả lập gần thời gian thực, đồng thời phân tích sâu các kết quả thu được từ quá trình so sánh với các mô hình học máy truyền thống. Kết quả cho thấy mô hình LSTM đáp ứng tốt các yêu cầu về tốc độ xử lý, tính ổn định và độ chính xác, đồng thời thể hiện ưu thế rõ rệt trong việc khai thác đặc trưng chuỗi thời gian của hành vi giao dịch. Bên cạnh đó, chương đã thảo luận các yếu tố ảnh hưởng đến khả năng triển khai thực tế, các ý nghĩa nghiệp vụ, hạn chế của nghiên cứu và định hướng phát triển trong tương lai. Những đánh giá này tạo nền tảng quan trọng cho phần kết luận chung của luận

văn, đồng thời khẳng định tiềm năng ứng dụng của các mô hình học sâu trong hệ thống phòng chống gian lận ngân hàng hiện đại.

KẾT LUẬN VÀ KIẾN NGHỊ

1. Kết luận

Đề án đã nghiên cứu và ứng dụng các phương pháp học máy và học sâu trong bài toán phát hiện gian lận giao dịch ngân hàng, với trọng tâm là mô hình học sâu LSTM khai thác chuỗi giao dịch theo hành vi khách hàng.

Thông qua việc xây dựng bộ dữ liệu mô phỏng có cấu trúc chuỗi, thực hiện so sánh có hệ thống giữa các mô hình học máy truyền thống và mô hình LSTM, kết quả cho thấy mô hình LSTM vượt trội về khả năng phát hiện gian lận, đặc biệt trong các trường hợp hành vi bất thường chỉ biểu hiện khi xem xét theo thời gian.

Bên cạnh hiệu quả dự đoán, đề án còn đề xuất kiến trúc triển khai mô hình LSTM dưới dạng dịch vụ phát hiện gian lận gần thời gian thực, phù hợp để tích hợp vào hệ thống thanh toán ngân hàng. Các kết quả mô phỏng cho thấy mô hình đáp ứng tốt yêu cầu về độ trễ, tính ổn định và khả năng ứng dụng trong thực tế.

Nhìn chung, đề án không chỉ có ý nghĩa về mặt học thuật mà còn mang giá trị ứng dụng rõ ràng, góp phần làm cơ sở cho việc triển khai các hệ thống phát hiện gian lận thông minh trong ngân hàng.

2. Kiến nghị

Dựa trên các kết quả thực nghiệm và triển khai thử nghiệm, luận văn đưa ra một số kiến nghị nhằm nâng cao khả năng ứng dụng mô hình vào hệ thống ngân hàng trong thực tế:

Thứ nhất, cần mở rộng thử nghiệm trên dữ liệu giao dịch thực tế đã được ẩn danh hóa. Dữ liệu mô phỏng dù phản ánh nhiều đặc điểm quan trọng nhưng chưa thể hiện đầy đủ độ phức tạp và mức độ tinh vi của gian lận thật. Việc thử nghiệm trên dữ liệu thực sẽ giúp mô hình học được hành vi trong môi trường ngân hàng thực tiễn và tăng độ tin cậy khi triển khai.

Thứ hai, đối với quá trình vận hành thực tế, ngân hàng cần xây dựng hệ thống giám sát mô hình (model monitoring) để quan sát độ chính xác theo thời gian và phát hiện sự suy giảm hiệu năng. Việc retrain mô hình định kỳ hoặc sử dụng các kỹ thuật học liên tục sẽ giúp mô hình thích nghi tốt hơn với các kiểu gian lận mới xuất hiện.

Thứ ba, cần xem xét áp dụng các kỹ thuật giải thích mô hình (Explainable AI) như Attention, LIME hoặc SHAP. Đây là yêu cầu quan trọng trong môi trường ngân hàng, nơi bộ phận kiểm toán và kiểm soát rủi ro cần hiểu rõ vì sao mô hình gán nhãn một giao dịch là gian lận để phục vụ công tác điều tra hoặc xử lý khiếu nại.

Thứ tư, để triển khai ở quy mô lớn, ngân hàng nên nghiên cứu tích hợp mô hình LSTM trong kiến trúc xử lý dữ liệu thời gian thực thông qua các nền tảng xử lý thời gian thực như Apache Kafka, Spark Streaming hoặc Flink, kết hợp với hệ thống điều phối luồng xử lý (workflow orchestration) như Apache Airflow. Điều này giúp giảm độ trễ, hạn chế truy vấn lặp và bảo đảm khả năng xử lý lượng giao dịch lớn trong các khung giờ cao điểm.

Cuối cùng, ngân hàng nên xem xét mở rộng mô hình sang các kênh giao dịch khác như thẻ, ATM, Mobile Banking, Internet Banking và điểm chấp nhận POS. Việc mở rộng mô hình sang nhiều kênh giao dịch khác nhau sẽ giúp xây dựng một hệ thống phát hiện gian lận hợp nhất (Unified Fraud Detection System), từ đó nâng cao hiệu quả giám sát rủi ro trên toàn bộ hệ sinh thái ngân hàng và giảm thiểu các lỗ hổng giữa các kênh giao dịch.

3. Lời kết

Đề tài đã khẳng định tiềm năng và hiệu quả của các mô hình học sâu, đặc biệt là LSTM, trong việc phát hiện gian lận giao dịch ngân hàng. Kết quả nghiên cứu mở ra hướng ứng dụng thực tiễn với giá trị cao đối với lĩnh vực tài chính – ngân hàng, góp phần hoàn thiện hệ thống phòng chống gian lận và nâng cao chất lượng dịch vụ. Những nghiên cứu tiếp theo sẽ tiếp tục cải thiện và mở rộng mô hình theo hướng thông minh, linh hoạt và phù hợp hơn với biến động của môi trường số. Bằng cách kết hợp giữa phân tích lý thuyết, thực nghiệm mô hình và thử nghiệm triển khai, đề tài đã đóng góp một hướng tiếp cận mang tính khả thi và có thể áp dụng trong thực tiễn cho các hệ thống phát hiện gian lận trong ngân hàng.

DANH MỤC CÁC TÀI LIỆU THAM KHẢO

Tiếng Việt

[1] Hoàng Thị Thúy, Lê Thị Xuân Thu (2021).“Phát hiện gian lận thẻ tín dụng bằng học máy”, Tạp chí Kinh tế và Phát triển, số 285(3), 76–84.

Tiếng Anh

[2] Bhattacharyya S., Jha S., Tharakunnel K., Westland J.C. (2011). “Data mining for credit card fraud: A comparative study”, Decision Support Systems, 50(3), 602–613.

[3] Burun B., Göktürk M. (2025). “A Human-AI Collaborative Approach for Credit Card Fraud Detection: Integration of LSTM Networks with Interactive Web Interface”, IEEE Conference on Human-Oriented Reasoning and Applications (ICHORA). [Online]. Available: https://ieeexplore.ieee.org/document/11017166. Truy cập ngày 30/09/2025.

[4] Carcillo F., Le Borgne Y.-A., Caelen O., Kessaci Y., Oblé F., Bontempi G. (2021). “Combining unsupervised and supervised learning in credit card fraud detection”, Information Sciences, 557, 317–331. DOI: 10.1016/j.ins.2019.05.042.

[5] Chawla N.V., Bowyer K.W., Hall L.O., Kegelmeyer W.P. (2002). “SMOTE: Synthetic Minority Over-sampling Technique”, Journal of Artificial Intelligence Research, 16, 321–357.

[6] Chen T., Guestrin C. (2016). “XGBoost: A Scalable Tree Boosting System”, Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD 2016), 785–794.

[7] Géron A. (2019), *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*, 2nd ed., O’Reilly Media, Sebastopol, USA, 850 trang.

[8] Ngai E.W.T., Hu Y., Wong Y.H., Chen Y., Sun X. (2011). “The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature”, Decision Support Systems, 50(3), 559–569.

[9] Pedregosa F., Varoquaux G., Gramfort A., Michel V., Thirion B., Grisel O., Blondel M., Prettenhofer P., Weiss R., Dubourg V., Vanderplas J., Passos A., Cournapeau D., Brucher M., Perrot M., Duchesnay É. (2011). “Scikit-learn: Machine Learning in Python”, Journal of Machine Learning Research, 12, 2825–2830.

BẢN CAM ĐOAN

Tôi cam đoan đã thực hiện việc kiểm tra mức độ tương đồng nội dung đề án qua phần mềm Turnitin một cách trung thực và đạt kết quả mức độ tương đồng …% toàn bộ nội dung đề án. Bản đề án kiểm tra qua phần mềm là bản cứng đề án đã nộp để bảo vệ trước hội đồng. Nếu sai tôi xin chịu các hình thức kỷ luật theo quy định hiện hành của Học viện.

……., ngày …. tháng ….. năm ……

HỌC VIÊN CAO HỌC/NCS

(Ký và ghi rõ họ tên)

16% Tính tương đồng nói chung

Tổng cộng của tất cả các kết quả trùng khớp, bao gồm cả các nguồn trùng lặp, cho mỗi c...

Đã lọc khỏi Báo cáo

- Mục lục tham khảo
- Văn bản được trích dẫn

Nguồn hàng đầu

12% Nguồn Internet
7% Ấn bản
7% Bài tập được nộp (bài của học sinh)