**HỌC VIỆN NGÂN HÀNG**

**KHOA CÔNG NGHỆ THÔNG TIN VÀ KINH TẾ SỐ**

**BÁO CÁO TỔNG KẾT**

**ĐỀ TÀI THAM DỰ CUỘC THI “SINH VIÊN NGHIÊN CỨU KHOA HỌC”**

**CẤP KHOA NĂM HỌC 2024-2025**

**TÊN ĐỀ TÀI: CHÌA KHÓA BẢO MẬT: GIẢI PHÁP PHÁT HIỆN GIAN LẬN BẰNG PHƯƠNG PHÁP HỌC MÁY VÀ XÁC THỰC THÔNG MINH CHO GIAO DỊCH MOBILE BANKING**

**LĨNH VỰC: NGÂN HÀNG**

**CHUYÊN NGÀNH: CÔNG NGHỆ THÔNG TIN**

***Hà Nội, Tháng 5 Năm 2025***

MỤC LỤC

[DANH MỤC BẢNG BIỂU iii](#_Toc197731785)

[DANH MỤC HÌNH ẢNH iv](#_Toc197731786)

[DANH MỤC NHỮNG TỪ VIẾT TẮT v](#_Toc197731787)

[PHẦN MỞ ĐẦU 1](#_Toc197731788)

[1. Lý do chọn đề tài 1](#_Toc197731789)

[2.Mục tiêu nghiên cứu 2](#_Toc197731790)

[3.Đối tượng nghiên cứu 2](#_Toc197731791)

[4.Nhiệm vụ nghiên cứu 3](#_Toc197731792)

[5. Phạm vi nghiên cứu 3](#_Toc197731793)

[6. Ý nghĩa nghiên cứu 3](#_Toc197731794)

[7.Cấu trúc bài nghiên cứu 5](#_Toc197731795)

[CHƯƠNG I.CƠ SỞ LÝ THUYẾT VỀ HỌC MÁY VÀ CÔNG NGHỆ XÁC THỰC THÔNG MINH TRONG PHÁT HIỆN GIAN LẬN MOBILE BANKING 6](#_Toc197731796)

[1.1. Tổng quan về gian lận trong giao dịch Mobile Banking 6](#_Toc197731797)

[1.1.1. Khái niệm và đặc điểm của giao dịch Mobile Banking 6](#_Toc197731798)

[1.1.3.Tầm quan trọng của phát hiện gian lận và bảo mật trong hệ thống Mobile Banking 10](#_Toc197731799)

[1.2.Cơ sở lý thuyết về học máy 13](#_Toc197731800)

[1.2.1.Khái niệm và phân loại học máy 13](#_Toc197731801)

[1.2.2.Vai trò học máy trong phát hiện gian lận giao dịch 15](#_Toc197731802)

[1.3. Công nghệ xác thực thông minh trong Mobile Banking 16](#_Toc197731803)

[1.3.1.Khái niệm về xác thực thông minh 16](#_Toc197731804)

[1.3.2. Ưu điểm và thách thức khi triển khai xác thực thông minh trong Mobile Banking 16](#_Toc197731805)

[TIỂU KẾT CHƯƠNG I 18](#_Toc197731806)

[Chương II. Thực trạng công tác phát hiện gian lận hiện nay và các phương pháp bảo mật trong giao dịch Mobile Banking 19](#_Toc197731807)

[2.1. Thực trạng công tác phát hiện gian lận hiện nay 19](#_Toc197731808)

[2.1.1.Các ngân hàng trên thế giới 19](#_Toc197731809)

[2.1.2.Các ngân hàng tại Việt Nam 22](#_Toc197731810)

[2.2.Thực trạng về các phương pháp bảo mật trong giao dịch Mobile Banking 23](#_Toc197731811)

[2.2.1. Các ngân hàng trên thế giới 23](#_Toc197731812)

[2.2.2.Các ngân hàng Việt Nam 25](#_Toc197731813)

[TIỂU KẾT CHƯƠNG II 28](#_Toc197731814)

[Chương III. MÔ HÌNH PHÁT HIỆN GIAN LẬN VÀ XÁC THỰC THÔNMINH TRONG GIAO DỊCH MOBILE BANKING 29](#_Toc197731815)

[3.1 .Mô hình nghiên cứu GCD-GNN 29](#_Toc197731816)

[3.2 .Dữ liệu nghiên cứu 33](#_Toc197731817)

[3.3.Quy trình nghiên cứu 34](#_Toc197731818)

[3.3.1.Tiền xử lý dữ liệu 35](#_Toc197731819)

[3.3.3.Huấn luyện 38](#_Toc197731820)

[3.3.4.Đánh giá mô hình 38](#_Toc197731821)

[3.4.Mô hình cá nhân hóa cho sinh viên 40](#_Toc197731822)

[TIỂU KẾT CHƯƠNG III 41](#_Toc197731823)

[CHƯƠNG IV. MÔ HÌNH BẢO MẬT TRONG MOBILE BANKING 42](#_Toc197731824)

[4.1.Tổng quan mô hình bảo mật trong MOBILE BANKING 42](#_Toc197731825)

[4.2. Quy trình giao dịch trên Mobile Banking 44](#_Toc197731826)

[4.2.2.Quy trình xác thực bằng IMEI 49](#_Toc197731827)

[4.2.3.Quy trình xác thực bằng VNEID 51](#_Toc197731828)

[4.3. Đánh giá mô hình bảo mật 53](#_Toc197731829)

[4.3.1.Đánh giá hiệu quả bảo mật 53](#_Toc197731830)

[4.3.2.Đánh giá tính khả thi triển khai 55](#_Toc197731831)

[4.4.Giải pháp 56](#_Toc197731832)

[TIỂU KẾT CHƯƠNG IV 58](#_Toc197731833)

[KẾT LUẬN 61](#_Toc197731834)

[Tài liệu tham khảo 63](#_Toc197731835)

DANH MỤC BẢNG BIỂU

[Bảng 1.1. Các loại học máy 15](#_Toc30595)

[Bảng 3.1 : Bảng thuộc tính dữ liệu thực tế 33](#_Toc22110)

[Bảng 3.2: Quy trình xử lý dữ liệu 33](#_Toc13230)

[Bảng 4.1 :Bảng Quy trình xác thực bằng cccd 45](#_Toc7816)

[Bảng 4.2:Bảng Quy trình xác thực bằng IMB 46](#_Toc17478)

[Bảng 4.3: Bảng quy trình xác thực bằng VNEID 48](#_Toc5145)

DANH MỤC HÌNH ẢNH

[Hình 1.1: Báo cáo gian lận theo phương thức thanh toán 11](#_Toc17837)

[Hình 1.2: Tương tác giữa người dùng và máy chủ ngân hàng, cùng với các tệp quyền APK trong ngân hàng di động 13](#_Toc24887)

[Hình 1.3. Phân loại phương pháp học máy 15](#_Toc890)

[Hình 2.1.Mẫu hình sử dụng dịch vụ Mobile banking 20](#_Toc27908)

[Hình 2.2. Tần suất gian lận ngân hàng ở Ấn Độ 21](#_Toc29340)

[Hình 2.3. Số lượng vụ án Pral được ngân hàng Handian lưu giữ 21](#_Toc488)

[Hình 3.1: Dữ liệu giao dịch của cụm sinh viên 30](#_Toc7092)

[Hình 3.2: Quy trình nghiên cứu 32](#_Toc30436)

[Hình 3.3: Hình ảnh kết quả thử nghiệm trên 2 bộ dữ liệu T-Finance và FDCompCN 34](#_Toc18861)

[Hình 4.1: Quy trình giao dịch trong Mobile Banking 42](#_Toc6457)

[Hình 4.2: Trang chủ và màn hình giao dịch 42](#_Toc25476)

[Hình 4.3: Xác thực mã pin và otp 43](#_Toc16362)

[Hình 4.4: Màn hình lựa chọn xác thực khi có giao dịch bất thường 44](#_Toc27240)

[Hình 4.5: Quy trình xác thực bằng cccd 44](#_Toc27656)

[Hình 4.6: Màn hình xác thực cccd 45](#_Toc25422)

[Hình 4.7: Quy trình xác thực bằng IMEI 46](#_Toc19134)

[Hình 4.8: Màn hình xác thực imei 47](#_Toc10136)

[Hình 4.9: Quy trình xác thực bằng VNEID 47](#_Toc9914)

[Hình 4.10: Màn hình xác thực bằng VNEID 49](#_Toc15023)

DANH MỤC NHỮNG TỪ VIẾT TẮT

|  |  |
| --- | --- |
| **Từ viết tắt** | **Giải nghĩa** |
| AI | Artificial Intelligence – Trí tuệ nhân tạo |
| ANN | Artificial Neural Network – Mạng nơ-ron nhân tạo |
| AUC | Area Under Curve – Diện tích dưới đường cong |
| FDCompCN | Fraud Detection Computation China Network (giả định theo mô hình thử nghiệm) |
| GNN | Graph Neural Network – Mạng nơ-ron đồ thị |
| HMM | Hidden Markov Model – Mô hình Markov ẩn |
| MFA | Multi-Factor Authentication – Xác thực đa yếu tố |
| ML | Machine Learning – Học máy |
| OTP | One-Time Password – Mật khẩu dùng một lần |
| PIN | Personal Identification Number – Mã định danh cá nhân |
| PoV | Proof of Voting – Cơ chế đồng thuận dựa trên bỏ phiếu |
| PR-AUC | Precision-Recall Area Under Curve – Diện tích dưới đường cong chính xác-thu hồi |
| ROC | Receiver Operating Characteristic – Đặc tính vận hành máy thu |
| SVM | Support Vector Machine – Máy vector hỗ trợ |
| T-Finance | Tên bộ dữ liệu dùng trong mô hình phát hiện gian lận (giả định) |
| XGBoost | Extreme Gradient Boosting – Tăng cường độ dốc cực đại |

PHẦN MỞ ĐẦU

1. Lý do chọn đề tài

Trong kỷ nguyên chuyển đổi số, sự bùng nổ của công nghệ số, các giao dịch tài chính qua thiết bị di động (Mobile Baking) đang ngày càng trở nên phổ biến trên thế giới nói chung và Việt Nam nói riêng. Tại Việt Nam, theo báo cáo Ngân hàng Nhà nướ**c(2023), g**iao dịch thanh toán qua di động đạt gần 7,96 tỷ, với giá trị vượt 55,10 triệu tỷ đồng, tăng 59,86% về số lượng và 12,73% về giá trị so với năm 2021. Sự tiện lợi, nhanh chóng của Mobile Banking đã thay đổi thói quen giao dịch tài chính của hàng triệu người dùng. Tuy nhiên, song với sự phát triển vượt trội đó thì các hình thức gian lận trong giao dịch ngân hàng điện tử cũng ngày càng tình vi và phức tạp, gây thiệt hại lớn cho cả ngân hàng và khách hàng.Theo báo cáo của LexisNexis Risk Solutions (2023), tổn thất do gian lận trong giao dịch tài chính toàn cầu đã tăng 16% so với năm trước, trong đó Mobile Banking chiếm tỷ trọng đáng kể. Từ đó đòi hỏi tính cấp thiết của các giải pháp trong việc phòng ngừa gian lận.

Tính an toàn của Mobile Banking không chỉ phụ thuộc vào các biện pháp bảo mật truyền thống mà còn yêu cầu các phương pháp dự đoán sớm và phát hiện bất thường trong hành vi giao dịch. Nhiều nghiên cứu đã chỉ ra rằng các phương pháp truyền thống trong phòng chống gian lận, vốn dựa trên luật lệ cố định (rule-based systems), ngày càng bộc lộ những hạn chế trước sự tinh vi của các kỹ thuật tấn công hiện đại. Srivastava et al. (2008) đã chứng minh rằng việc ứng dụng các mô hình học máy, cụ thể là Hidden Markov Model (HMM), có thể phát hiện hiệu quả các mẫu gian lận trong dữ liệu giao dịch tài chính. Bên cạnh đó, Nguyen et al. (2022) cũng nhấn mạnh rằng việc kết hợp học máy với các cơ chế xác thực thông minh, như xác thực đa yếu tố (Multi-Factor Authentication - MFA) hoặc xác thực hành vi người dùng (Behavioral Biometrics), không chỉ làm tăng độ chính xác trong phát hiện gian lận mà còn nâng cao trải nghiệm người dùng thông qua giảm thiểu tỷ lệ báo động giả (false positive rate).

Mặc dù các hướng nghiên cứu trên đã đạt được nhiều thành tựu, tổng quan tài liệu cho thấy vẫn tồn tại những khoảng trống tri thức cần tiếp tục khai thác. Cụ thể, đa số các mô hình học máy phát hiện gian lận hiện hành chủ yếu xử lý dữ liệu tĩnh, thiếu sự kết hợp với yếu tố xác thực liên tục theo hành vi người dùng. Ngoài ra, các nghiên cứu ứng dụng chủ yếu tập trung tại thị trường nước ngoài, trong khi hành vi giao dịch và thói quen sử dụng Mobile Banking tại Việt Nam có những đặc thù riêng, chưa được nghiên cứu đầy đủ. Do đó, việc phát triển mô hình phát hiện gian lận dựa trên học máy, đồng thời kết hợp các kỹ thuật xác thực thông minh trong bối cảnh người dùng Việt Nam, là một nhu cầu thiết thực cả về lý luận lẫn thực tiễn.

Trong bối cảnh đó, đề tài "*Chìa khóa bảo mật: Giải pháp phát hiện gian lận bằng phương pháp học máy và xác thực thông minh cho giao dịch Mobile Banking*" có tính cấp thiết và ý nghĩa thực tiễn sâu sắc. Đề tài hướng đến việc phát triển một giải pháp phát hiện gian lận toàn diện, kết hợp hài hòa giữa khả năng dự báo của học máy và độ tin cậy của các phương thức xác thực tiên tiến, đồng thời thử nghiệm và hiệu chỉnh phù hợp với môi trường giao dịch tại Việt Nam.

Từ những phân tích nêu trên, có thể khẳng định rằng việc thực hiện nghiên cứu này là cần thiết nhằm góp phần hoàn thiện lý luận, mở rộng thực tiễn ứng dụng công nghệ bảo mật trong lĩnh vực ngân hàng số, cũng như đáp ứng yêu cầu cấp bách của xã hội về đảm bảo an toàn tài chính trong kỷ nguyên số hóa.

2.Mục tiêu nghiên cứu

Nghiên cứu đề tài "Chìa khóa bảo mật: Giải pháp phát hiện gian lận bằng phương pháp học máy và xác thực thông minh cho giao dịch Mobile Banking" nhằm mục tiêu:

Thứ nhất, phân tích và đánh giá các phương pháp học máy hiện đang được ứng dụng trong phát hiện gian lận giao dịch Mobile Banking.

Thứ hai, xây dựng mô hình phát hiện gian lận giao dịch Mobile Banking dựa trên các kỹ thuật học máy tiên tiến, có khả năng phát hiện các hành vi gian lận với độ chính xác cao và thời gian xử lý nhanh.

Thứ ba, đề xuất phương án tích hợp các cơ chế xác thực thông minh (vào hệ thống phát hiện gian lận nhằm nâng cao hiệu quả bảo mật và giảm thiểu tỷ lệ cảnh báo giả.

Thứ tư, đề xuất các khuyến nghị và hướng phát triển nhằm hoàn thiện giải pháp phát hiện và ngăn chặn gian lận trong giao dịch Mobile Banking, phù hợp với hành vi người dùng tại Việt Nam.

3.Đối tượng nghiên cứu

Thứ nhất, các giao dịch tài chính thực hiện trên nền tảng Mobile Banking, bao gồm cả các giao dịch hợp lệ và các giao dịch có dấu hiệu gian lận.

Thứ hai, các kỹ thuật học máy và xác thực thông minh được ứng dụng trong việc phát hiện và phòng chống gian lận giao dịch điện tử.

Thứ ba. các đặc điểm hành vi người dùng trong quá trình thực hiện giao dịch Mobile Banking, phục vụ cho việc tích hợp giải pháp xác thực hành vi vào mô hình phát hiện gian lận.

4.Nhiệm vụ nghiên cứu

Hệ thống hóa các cơ sở lý thuyết về gian lận giao dịch tài chính và các phương pháp học máy áp dụng trong phát hiện gian lận giao dịch Mobile Banking.

Đánh giá các phương pháp học máy hiện có và chọn lựa các thuật toán phù hợp cho bài toán phát hiện gian lận trong môi trường Mobile Banking.

Thu thập và tiền xử lý dữ liệu giao dịch từ các nguồn dữ liệu giả lập hoặc thực tế, phục vụ cho việc huấn luyện mô hình học máy.

Xây dựng mô hình phát hiện gian lận giao dịch Mobile Banking ứng dụng các thuật toán học máy, và tinh chỉnh mô hình để tối ưu độ chính xác và hiệu suất.

Đề xuất các giải pháp tích hợp xác thực thông minh (như xác thực hành vi người dùng, sinh trắc học) để cải thiện tính bảo mật và giảm thiểu tỷ lệ cảnh báo giả.

Thực nghiệm và đánh giá hiệu quả của mô hình trên bộ dữ liệu thử nghiệm, từ đó phân tích kết quả và đề xuất các giải pháp hoàn thiện hệ thống phát hiện gian lận.

5. Phạm vi nghiên cứu

6. Ý nghĩa nghiên cứu

Trong bối cảnh chuyển đổi số mạnh mẽ và sự phát triển vượt bậc của ngân hàng di động (Mobile banking), các giao dịch tài chính điện tử ngày càng trở nên phổ biến, đồng thời cũng đối mặt với những nguy cơ gian lận và tấn công mạng ngày càng tinh vi. Đặc biệt, các hình thức lừa đảo qua mạng như giả mạo danh tính, chiếm đoạt tài khoản, tấn công trung gian (man-in-the-middle), phần mềm độc hại hay kỹ thuật xã hội (social engineering) đã trở thành mối đe dọa trực tiếp đối với người dùng và hệ thống ngân hàng. Trong bối cảnh đó, việc nghiên cứu và triển khai các giải pháp bảo mật hiện đại không chỉ là nhu cầu cấp thiết mà còn là điều kiện tiên quyết để đảm bảo an toàn thông tin, nâng cao niềm tin của khách hàng và phát triển bền vững hệ thống ngân hàng số.

Đề tài **“Chìa khóa bảo mật: Giải pháp phát hiện gian lận bằng phương pháp học máy và xác thực thông minh cho giao dịch Mobile Banking”** có ý nghĩa thực tiễn và khoa học sâu sắc.

Về mặt lý luận, đề tài góp phần hệ thống hóa cơ sở khoa học về các kỹ thuật học máy (machine learning) và sinh trắc học trong lĩnh vực bảo mật giao dịch tài chính, đặc biệt là ngân hàng di động( Mobile banking). Việc ứng dụng học máy giúp xây dựng các mô hình phát hiện gian lận tự động, có khả năng học hỏi từ dữ liệu và phát hiện các hành vi bất thường với độ chính xác cao. Trong khi đó, xác thực thông minh bao gồm các phương pháp xác thực sinh trắc học (vân tay, khuôn mặt, giọng nói), xác thực hành vi (behavioral biometrics) và xác thực đa yếu tố (MFA) sẽ đóng vai trò then chốt trong việc xác minh danh tính người dùng một cách nhanh chóng và an toàn, hạn chế tối đa khả năng giả mạo hoặc truy cập trái phép.

Về mặt thực tiễn, đề tài hướng đến việc đề xuất mô hình kết hợp giữa phát hiện gian lận và xác thực thông minh để nâng cao khả năng bảo vệ các giao dịch Mobile banking. Giải pháp được xây dựng có thể áp dụng vào hệ thống ngân hàng hiện hữu, góp phần nâng cao hiệu quả phòng chống gian lận, giảm thiểu tổn thất tài chính và rủi ro pháp lý. Đồng thời, đề tài cũng giúp cải thiện trải nghiệm người dùng nhờ vào các phương thức xác thực thân thiện, tiện lợi và bảo mật cao. Kết quả nghiên cứu có thể làm cơ sở tham khảo cho các tổ chức tài chính, công ty fintech và cơ quan quản lý trong việc xây dựng chính sách và hệ thống an toàn thông tin phù hợp với xu thế ngân hàng số trong thời đại công nghệ 4.0.

Tóm lại, đề tài không chỉ có ý nghĩa về mặt khoa học khi góp phần mở rộng ứng dụng của trí tuệ nhân tạo và bảo mật thông tin trong lĩnh vực tài chính ngân hàng, mà còn mang lại giá trị thực tiễn rõ rệt trong việc xây dựng các giải pháp bảo mật tiên tiến, thích ứng với sự phát triển của nền kinh tế số và nhu cầu bảo vệ người tiêu dùng trong môi trường giao dịch điện tử ngày càng phức tạp.

7.Cấu trúc bài nghiên cứu

Ngoài phần mở đầu mô tả ngắn gọn tính cấp thiết, mục tiêu, đối tượng và phạm vi nghiên cứu cũng như phương pháp nghiên cứu , bài nghiên cứu gồm có 4 chương:

Chương I: Cơ sở lý thuyêt về học máy và công nghệ xác thực thông minh trong phát hiện gian lận Mobile Banking.

Chương II: Thực trạng công tác phát hiện gian lận hiện nay và các phương pháp bảo mật trong giao dịch Mobile Banking.

Chương III: Mô hình phát hiện gian lận và xác thực thông minh trong giao dịch Mobile Banking

Chương IV: Giải pháp và kiến nghị cho Mô hình phát hiện gian lận giao dịch Mobile Banking.

**PHẦN NỘI DUNG**

CHƯƠNG I.CƠ SỞ LÝ THUYẾT VỀ HỌC MÁY VÀ CÔNG NGHỆ XÁC THỰC THÔNG MINH TRONG PHÁT HIỆN GIAN LẬN MOBILE BANKING

1.1. Tổng quan về gian lận trong giao dịch Mobile Banking

1.1.1. Khái niệm và đặc điểm của giao dịch Mobile Banking

Mobile Banking hayNgân hàng di động được hiểu là một hình thức cung cấp dịch vụ ngân hàng qua các thiết bị di động như điện thoại thông minh hoặc máy tính bảng, cho phép khách hàng thực hiện các giao dịch mà không bị giới hạn bởi thời gian hay địa điểm. Khác với thanh toán di động – vốn chủ yếu dùng để thanh toán các giao dịch nhỏ tại điểm bán – ngân hàng di động bao gồm một phạm vi chức năng rộng hơn như kiểm tra số dư, chuyển khoản, thanh toán hóa đơn và quản lý tài khoản. So với các phương thức truyền thống như giao dịch tại quầy hay qua máy tính, ngân hàng di động được đánh giá cao nhờ tính tiện lợi và hiệu quả mà nó mang lại (Laukkanen, 2017).Hay theo ***(***Pousttchi & Schurig)Mobile banking là một nhánh của ngân hàng điện tử, tận dụng tối đa các đặc điểm của thương mại di động. Hình thức ngân hàng này cung cấp cho người dùng nhiều dịch vụ thường xuyên có sẵn 24/7. Các dịch vụ này bao gồm khả năng kiểm tra số dư tài khoản, xem lịch sử giao dịch, thanh toán hóa đơn điện tử, gửi séc từ xa, thực hiện các giao dịch P2P (peer-to-peer) và chuyển tiền (Pousttchi & Schurig, 2004). Mặc dù có thể có một số hạn chế về các loại tài khoản hoặc số tiền có thể truy cập hoặc thực hiện giao dịch, nhưng lợi thế chính của mobile banking vẫn là tính linh hoạt và bảo mật, cho phép khách hàng thực hiện các giao dịch ngân hàng từ bất kỳ đâu (Bank of America, n.d.; EverBank, n.d.; Digital Savings & Checking, n.d.).

1.1.2 Các hình thức gian lận phổ biến trong Mobile Banking

Gian lận được định nghĩa là hành vi lừa đảo trái phép hoặc phạm tội nhằm thu lợi tài chính hoặc cá nhân. Trong các giao dịch kỹ thuật số, gian lận có thể xảy ra qua điện thoại hoặc trên các trang web, khi chủ thẻ cung cấp số thẻ, ngày hết hạn và mã xác minh thẻ (Randhawa et al., 2018).

Gian lận là một vấn đề quan trọng mà các tổ chức tài chính phải đối mặt, và do những kẻ gian lận ngày càng tinh vi hơn, việc nhận biết hoặc phát hiện các chiến lược của họ không phải là nhiệm vụ dễ dàng (Wei, Li, Cao, Ou, & Chen, 2012).

Theo Mudiri (2023), trong bối cảnh dịch vụ tài chính di động, gian lận được hiểu là hành vi có chủ ý và có mục đích nhằm đạt được lợi ích bất chính (dưới dạng tiền mặt hoặc tiền điện tử), làm tổn thất doanh thu của người khác, hoặc gây tổn hại đến uy tín của các bên liên quan trong hệ sinh thái dịch vụ tài chính di động.

***Các hình thức giai lận phổ biến trong giao dịch ngân hàng di động:***

*Lừa đảo do chính người tiêu dùng gây ra*

Trong lĩnh vực ngân hàng di động, một trong những hình thức gian lận phổ biến nhất hiện nay là lừa đảo do chính người tiêu dùng gây ra. Những hành vi này thường do kẻ gian giả làm khách hàng để thực hiện các thủ đoạn tinh vi nhằm chiếm đoạt tiền hoặc tài sản thông qua hệ thống giao dịch điện tử..( My PIN is 4321 của Ignacio Mas (n.d.)) Phương pháp chính để quản lý loại lừa đảo này là thông qua các hoạt động giáo dục người tiêu dùng.*Các loại gian lận phổ biến do người tiêu dùng gây ra như:*

*Thứ nhất*, lừa đảo qua tin nhắn (Phishing): Một số người gửi tin nhắn SMS giả mạo ngân hàng, có thể từ điện thoại cá nhân hoặc qua máy tính. Những tin nhắn này được thiết kế trông rất giống thật để đánh lừa người nhận, khiến họ tin rằng yêu cầu trong tin nhắn là hợp lệ.

*Thứ hai,* khách hàng lừa đảo sau khi làm quen với nhân viên ngân hàng –Một số khách hàng giả vờ thân thiết, tạo mối quan hệ với nhân viên ngân hàng rồi lợi dụng sự tin tưởng đó để lừa lấy tiền mặt hoặc tiền điện tử.

*Thứ ba,* Khách hàng lừa đảo thông qua mối quan hệ với nhân viên đại lý trong giao dịch mobile banking –Một số khách hàng có hành vi gian lận bằng cách chủ động xây dựng mối quan hệ thân thiết với nhân viên đại lý. Sau khi tạo được lòng tin, họ thực hiện các hành vi lừa đảo nhằm chiếm đoạt tiền mặt hoặc tiền điện tử thông qua các giao dịch mobile banking, như yêu cầu hỗ trợ chuyển tiền, rút tiền hoặc xử lý các giao dịch giả mạo.

***Gian lận do ngân hàng gây ra***

Theo Mudiri (2023), gian lận do ngân hàng thực hiện là loại gian lận phát sinh từ bên trong mạng lưới ngân hàng, khi chính các ngân hàng hoặc nhân viên của họ đóng vai trò là tác nhân gây ra. Các hình thức gian lận có thể bao gồm nhân viên lừa đảo ngân hàng, ngân hàng cấp trên lừa ngân hàng cấp dưới, ngân hàng lừa khách hàng hoặc thậm chí là lừa nhà cung cấp dịch vụ tài chính di động. Loại gian lận này thường xảy ra phổ biến ở giai đoạn đầu khi triển khai dịch vụ, do những sơ hở trong việc thiết kế giá cả và sản phẩm, và nó có xu hướng thay đổi về hình thức, đối tượng và mức độ ảnh hưởng theo thời gian (Mudiri, 2023).

Các hình thức gian lận do ngân hàng thực hiện bao gồm:

Thứ nhất, nhân viên lừa đảo chính ngân hàng mình là hành vi gian lận xảy ra khi nhân viên được giao trách nhiệm quản lý hoặc vận chuyển tiền mặt lợi dụng vị trí công việc để chiếm đoạt tài sản rồi bỏ trốn. Đây là một hình thức gian lận nội bộ, thường xảy ra trong các tổ chức tài chính hoặc mạng lưới đại lý nơi mà việc kiểm soát trực tiếp và liên tục còn hạn chế, đặc biệt khi nhân viên nắm giữ quyền tiếp cận tiền mặt lớn mà không có cơ chế giám sát chặt chẽ.

Thứ hai, giao dịch chia nhỏ để trục lợi hoa hồng là hành vi trong đó nhân viên ngân hàng cố ý chia một giao dịch gửi tiền có giá trị lớn thành nhiều giao dịch nhỏ hơn nhằm gia tăng tổng số tiền hoa hồng hoặc tiền thưởng nhận được từ hệ thống. Mặc dù hành động này không gây thiệt hại trực tiếp cho khách hàng (vì họ không phải trả phí khi gửi tiền), nhưng nó làm sai lệch dữ liệu giao dịch, gia tăng chi phí vận hành cho ngân hàng và ảnh hưởng đến tính minh bạch của hệ thống tài chính. Đây là một hình thức gian lận nội bộ dựa trên việc lợi dụng cơ chế trả thưởng theo từng giao dịch.

Thứ ba, gian lận từ phía ngân hàng cấp cao là hành vi gian lận xảy ra khi ngân hàng cấp trên (hoặc chi nhánh quản lý) cố tình khai báo sai hoặc che giấu thông tin về mức hoa hồng thực tế được chi trả cho các ngân hàng cấp dưới (hoặc phòng giao dịch).

***Giân lận liên quan đến đối tác kinh doanh***

Theo Mudiri (2024), gian lận do đối tác kinh doanh gây ra được mô tả là các hành vi lừa đảo xuất phát từ mạng lưới của đối tác kinh doanh, bao gồm các mối quan hệ doanh nghiệp với người tiêu dùng (B2C), người tiêu dùng với doanh nghiệp (C2B) và các thương nhân. Các hành vi này có thể do nhân viên thực hiện đối với tổ chức kinh doanh, khách hàng, hoặc do các doanh nghiệp đối tác thực hiện đối với nhà cung cấp dịch vụ tiền di động. Loại gian lận này thường phổ biến hơn trong giai đoạn gia tăng giá trị của quá trình triển khai, chủ yếu do sự phát triển của các mối quan hệ đối tác kinh doanh trong giai đoạn này. Tuy nhiên, gian lận liên quan đến đối tác kinh doanh vẫn đang ở giai đoạn sơ khai vì việc áp dụng các giao dịch kinh doanh còn trong giai đoạn khởi đầu.

*Các hình thức gian lận phổ biến liên quan đến đối tác kinh doanh bao gồm:*

*Thứ nhất, Nhân viên doanh nghiệp lừa đảo khách hàng:* Là hành vi gian lận trong đó nhân viên của doanh nghiệp (đối tác cung cấp dịch vụ mobile banking) lợi dụng quyền truy cập hệ thống hoặc sự thiếu hiểu biết của khách hàng để chiếm đoạt tiền từ tài khoản mobile banking của khách hàng, thường thông qua việc đăng ký dịch vụ không có sự đồng ý, giả mạo giao dịch, hoặc thay đổi thông tin liên kết.

*Thứ hai,* Là hành vi trong đó nhân viên nội bộ của doanh nghiệp sử dụng quyền truy cập hệ thống mobile banking để thực hiện các giao dịch gian lận, như tạo tài khoản giả mạo, điều chỉnh dữ liệu giao dịch, hoặc chuyển tiền bất hợp pháp từ tài khoản công ty sang tài khoản cá nhân, gây thiệt hại tài chính trực tiếp cho chính doanh nghiệp.

***Gian lận liên quan đến hệ thống***

Theo Mudiri (2024), gian lận liên quan đến hệ thống bao gồm các hoạt động gian lận khai thác điểm yếu trong hệ thống và quy trình của dịch vụ tài chính di động. Loại gian lận này ảnh hưởng đến nhiều bên liên quan như ngân hàng, doanh nghiệp và nhà cung cấp dịch vụ tiền di động, đặc biệt khi hệ thống thiếu các biện pháp kiểm soát hiệu quả trong xử lý giao dịch. Gian lận hệ thống thường xảy ra nhiều nhất ở giai đoạn kích hoạt giao dịch và tiếp tục gia tăng trong giai đoạn gia tăng giá trị của triển khai dịch vụ.

Các hành vi gian lận chính bao gồm:

Thứ nhất, chia sẻ mật khẩu/PIN : Trong môi trường ngân hàng số, Mobile Banking cho phép người dùng thực hiện các giao dịch tài chính như chuyển tiền, thanh toán hóa đơn, hoặc truy vấn tài khoản ngay trên thiết bị di động. Để đảm bảo an toàn, mỗi người dùng được cấp một tài khoản cá nhân kèm theo mã PIN, mật khẩu hoặc mã xác thực một lần (OTP). Những thông tin này được xem là bảo mật cá nhân tuyệt đối, nhằm ngăn ngừa truy cập trái phép và gian lận.Tuy nhiên, trong thực tế, nhiều cá nhân và tổ chức có thói quen chia sẻ thông tin bảo mật như mã PIN hoặc tài khoản với người khác vì lý do tiện lợi hoặc thiếu hiểu biết về rủi ro. Hành vi này tạo ra lỗ hổng nghiêm trọng về an ninh, làm mất khả năng kiểm soát truy cập và khiến việc xác định trách nhiệm trở nên khó khăn khi xảy ra gian lận.

Thứ hai, mật khẩu yếu và độ mạnh của mã PIN giao dịch: Trong giao dịch điện tử, đặc biệt là qua các nền tảng như **Mobile Banking**, **mã PIN và mật khẩu** đóng vai trò quan trọng trong việc **xác thực người dùng** và **bảo vệ tài khoản khỏi truy cập trái phép**. Tuy nhiên, **mật khẩu yếu** – chẳng hạn như dãy số đơn giản, năm sinh, số điện thoại hoặc thông tin cá nhân dễ đoán – làm giảm đáng kể độ an toàn của hệ thống bảo mật.Khi người dùng sử dụng các mã PIN dễ đoán, đặc biệt là các thông tin có thể bị người thân, bạn bè hoặc kẻ xấu biết đến, nguy cơ bị truy cập trái phép và***gian lận tài chính***tăng cao. Việc đặt mật khẩu yếu thường xuất phát từ tâm lý chủ quan, muốn dễ nhớ hoặc do thiếu hiểu biết về rủi ro bảo mật.

Thứ ba, tạo người dùng giả mạo và không tồn tại trên nền tảng dịch vụ tài chính di động: Trong hệ thống giao dịch Mobile Banking, quản trị viên hệ thống thường có quyền cao nhất để tạo, cấp quyền và kiểm soát người dùng trong nội bộ ngân hàng hoặc tổ chức tài chính. Nếu các quyền này không được kiểm soát chặt chẽ, rủi ro tạo tài khoản giả mạo, không tồn tại hoặc không được ủy quyền là rất cao.Hành vi tạo người dùng giả nhằm mục đích gian lận thường đi kèm với việc gán quyền thực hiện và phê duyệt giao dịch, từ đó dễ dàng rút tiền, chuyển khoản bất hợp pháp, gây thất thoát tài chính nghiêm trọng cho tổ chức. Đây là một dạng gian lận hệ thống, thường xảy ra từ bên trong, do người có quyền truy cập kỹ thuật thực hiện.

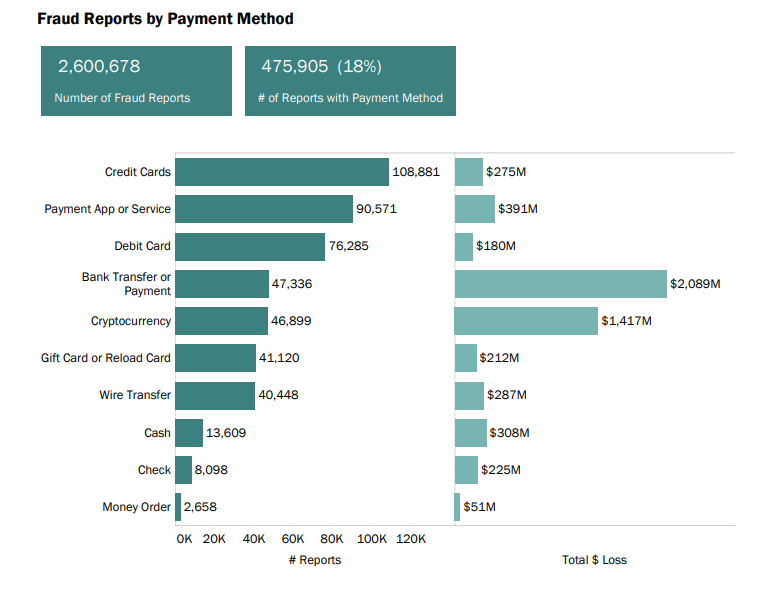
Thứ tư, người dùng cá nhân với nhiều quyền truy cập: Gian lận do quyền truy cập đa vai trò xảy ra khi một cá nhân được cấp nhiều quyền hạn trong hệ thống (ví dụ: khởi tạo và xác minh giao dịch), dẫn đến việc lạm dụng quyền để thực hiện các hành vi gian lận. Điều này thường xuất phát từ việc thiếu phân tách nhiệm vụ (segregation of duties) hoặc quản lý truy cập không chặt chẽ, cho phép một người kiểm soát toàn bộ quy trình giao dịch mà không có sự giám sát.

Thứ năm, Gian lận trên nhiều kênh truy cập: Gian lận trên nhiều kênh truy cập trong hệ thống giao dịch mobile banking xảy ra khi các cá nhân trái phép khai thác các kênh truy cập như ứng dụng di động, máy tính, hoặc chứng chỉ bảo mật để thực hiện giao dịch bất hợp pháp. Nguyên nhân thường xuất phát từ việc quản lý bảo mật yếu kém, chẳng hạn như không thu hồi quyền truy cập, không vô hiệu hóa chứng chỉ bảo mật trên thiết bị bị mất hoặc bị xâm phạm, hoặc không cập nhật thông tin truy cập sau khi nhân viên bị sa thải, dẫn đến việc lạm dụng thông tin để thực hiện gian lận.

1.1.3.Tầm quan trọng của phát hiện gian lận và bảo mật trong hệ thống Mobile Banking

Theo Mudiri (2024), gian lận không chỉ xuất hiện trong dịch vụ tài chính di động mà còn phổ biến ở tất cả các loại hình dịch vụ tài chính. Tuy nhiên, do dịch vụ tài chính di động là một trong những phương thức tiềm năng để thúc đẩy tài chính toàn diện và mở rộng dịch vụ tài chính đến thị trường đại chúng, gian lận trong lĩnh vực này mang lại những hệ lụy sâu rộng. Gian lận tác động mạnh mẽ đến hệ sinh thái tiền di động theo nhiều cách khác nhau.

Hình 1.1: Báo cáo gian lận theo phương thức thanh toán



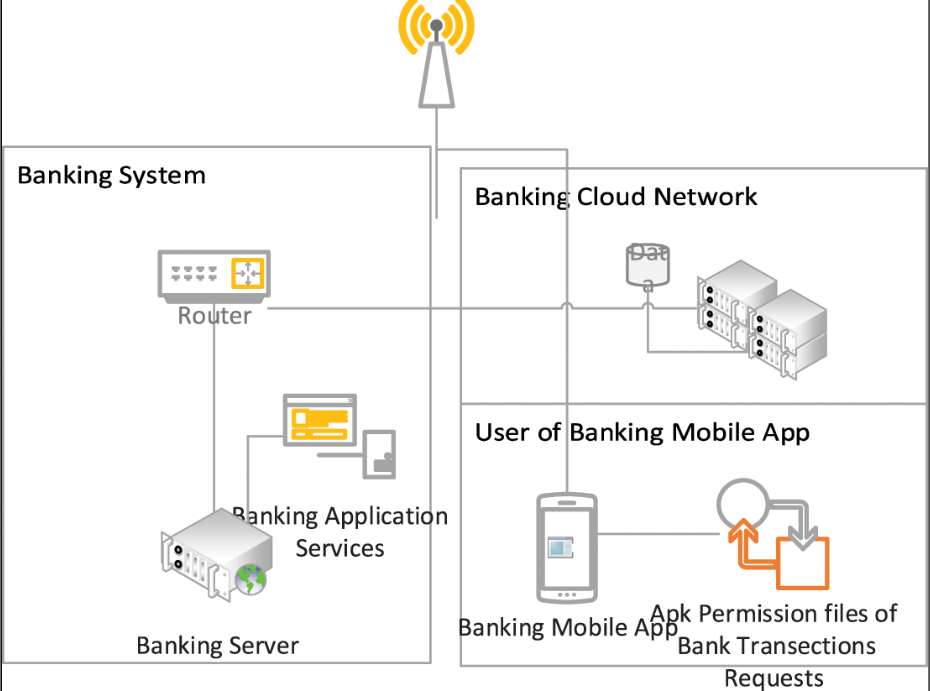
*Nguồn:* ***Consumer Sentinel Network Data Book 2024***

Đồ thị trên được trích từ ***“Consumer Sentinel Network Data Book 2024”*** của Ủy ban Thương mại Liên bang Hoa Kỳ (FTC), bản báo cáo thường niên công bố dữ liệu khiếu nại của người tiêu dùng trong năm trước. Biểu đồ “Fraud Reports by Payment Method” tổng hợp ***2.600.678*** báo cáo gian lận, trong đó có ***475.905*** vụ ghi rõ phương thức thanh toán (chiếm 18%). Trục bên trái thể hiện số lượng báo cáo phân theo 10 phương thức (từ Thẻ tín dụng nhiều nhất với 108.881 vụ đến Phiếu chuyển tiền ít nhất với 2.658 vụ), trong khi trục bên phải cho biết tổng giá trị thiệt hại (triệu USD) tương ứng với từng phương thức. Đặc biệt, ***Chuyển khoản/ngân hàng (Bank Transfer or Payment)*** không chỉ nằm trong nhóm trung bình về số vụ (47.336 báo cáo) mà còn ghi nhận ***thiệt hại cao nhất – lên tới 2.089 tỷ USD***, cho thấy mỗi vụ gian lận qua hình thức này thường có giá trị rất lớn. Rõ ràng, gian lận liên quan đến dịch vụ tài chính di động đang trở thành một vấn đề ngày càng nghiêm trọng. Vậy nên cần đặc biệt chú trọng đến các biện pháp bảo mật trong hệ thống chuyển khoản ngân hàng.

Theo báo cáo của Liên minh chống lừa đảo toàn cầu (GASA), trong năm 2023, có đến 70% người dân Việt Nam từng bị các đối tượng lừa đảo nhắm đến ít nhất một lần mỗi tháng. Thiệt hại tài chính từ các vụ lừa đảo này được ước tính lên đến 16,2 tỷ USD, chủ yếu diễn ra qua hình thức cuộc gọi và tin nhắn giả mạo. Nạn nhân thường bị dụ dỗ để cung cấp thông tin bảo mật như tên truy cập, mật khẩu, mã OTP hoặc số thẻ, dẫn đến mất quyền kiểm soát tài khoản hoặc thiết bị cá nhân (GASA, 2023).

Phát hiện gian lận và bảo mật trong mobile banking đóng vai trò vô cùng quan trọng đối với sự tồn tại và phát triển bền vững của dịch vụ tài chính di động. Khi gian lận không được kiểm soát, nó không chỉ làm giảm lòng tin của người dùng mà còn gây tổn thất lớn cho các tổ chức cung cấp dịch vụ, từ đó ảnh hưởng nghiêm trọng đến sự tăng trưởng của số lượng người đăng ký và các khoản đầu tư vào hệ thống. Một hệ thống bảo mật mạnh mẽ và khả năng phát hiện gian lận kịp thời sẽ tạo ra một môi trường an toàn, giúp người tiêu dùng yên tâm giao dịch và thúc đẩy sự tham gia của các tổ chức doanh nghiệp lớn. Hơn nữa, việc phát hiện gian lận giúp bảo vệ toàn bộ hệ sinh thái tài chính di động, ngăn chặn các hành vi bất hợp pháp như rửa tiền và tài trợ khủng bố. Do đó, bảo mật và khả năng phát hiện gian lận không chỉ là yếu tố cần thiết để bảo vệ lợi ích của người sử dụng mà còn là nền tảng để duy trì sự ổn định và phát triển của thị trường mobile banking trong tương lai.

Hình 1.2: Tương tác giữa người dùng và máy chủ ngân hàng, cùng với các tệp quyền APK trong ngân hàng di động



1.2.Cơ sở lý thuyết về học máy

1.2.1.Khái niệm và phân loại học máy

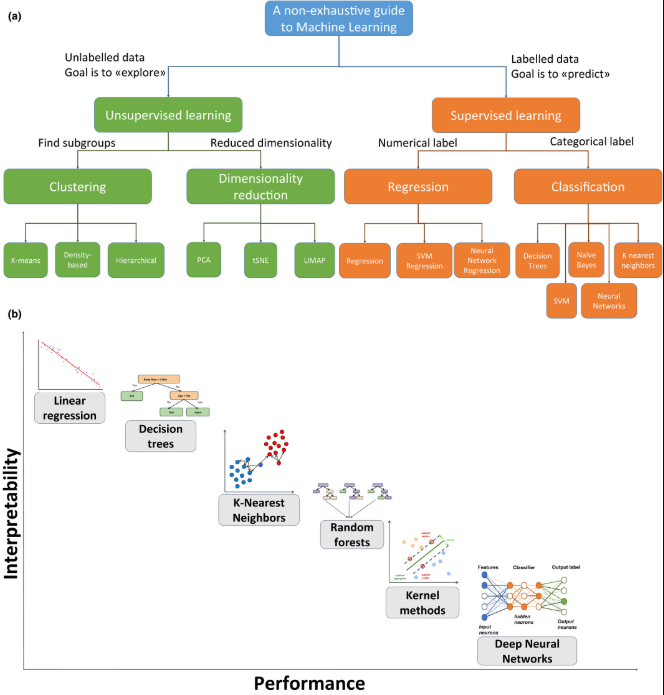
Theo một chương trong sách của IGI Global, máy học là một kỹ thuật cho phép máy tính học hỏi từ dữ liệu mà không cần được lập trình rõ ràng, thông qua việc nghiên cứu và phát triển các thuật toán có khả năng học và đưa ra dự đoán. Ngoài ra, máy học được xem là một nhánh của trí tuệ nhân tạo, chứ không phải ngược lại (Dutta et al., 2023).

Các kỹ thuật học máy (ML) hỗ trợ việc xây dựng các mô hình đánh giá và dự đoán nhằm phân loại giao dịch tài chính là thông thường hay gian lận (Costa et al., 2021). Theo Alqudah và Yaseen (2020), học máy được xem là một phương pháp phân tích dữ liệu, cho phép máy tính tự cập nhật hoặc điều chỉnh hành động dựa trên việc dự đoán sự kiện hoặc kiểm soát máy móc (dos Santos & dos Santos, 2022; Moreira et al., 2022).

Bảng 1.1. Các loại học máy

|  |  |
| --- | --- |
| **Loại học máy** | **Đặc điểm** |
| Học có giám sát | Dữ liệu huấn luyện có nhãn, mô hình học từ đó để dự đoán đầu ra cho dữ liệu mới. |
| Học không giám sát | Dữ liệu không có nhãn, mô hình tự tìm ra cấu trúc, tiềm ẩn trong dữ liệu. |
| Học tăng cường | Cung cấp phản hồi đào tạo bằng cách sử dụng cơ chế khen thưởng. Quá trình học diễn ra như một máy móc hoặc tác nhân tương tác với môi trường và thử nhiều phương pháp khác nhau để đạt được kết quả. Tác nhân được khen thưởng hoặc trừng phạt khi đạt đến trạng thái mong muốn hoặc không mong muốn. |

Hình 1.3. Phân loại phương pháp học máy



1.2.2.Vai trò học máy trong phát hiện gian lận giao dịch

Một số nghiên cứu gần đây đã đề xuất hướng tiếp cận mới trong việc phát hiện gian lận trong giao dịch di động bằng cách tích hợp mô hình học sâu Bi-3DQRNN với công nghệ blockchain dựa trên cơ chế đồng thuận Proof of Voting (PoV), nhằm tăng cường hiệu quả phát hiện và đảm bảo tính bảo mật cho các giao dịch tài chính (Soleymanzadeh et al., 2024).

Halvaiee và Akbari (2014) đã nghiên cứu một mô hình mới có tên là Mô hình Phát hiện Gian lận dựa trên Hệ thống Miễn dịch Nhân tạo (AFDM). Họ áp dụng Thuật toán Lấy cảm hứng từ Hệ thống Miễn dịch (AIRS) để nâng cao độ chính xác trong việc phát hiện gian lận. Kết quả nghiên cứu cho thấy AFDM cải thiện độ chính xác lên đến 25%, giảm chi phí đến 85% và giảm thời gian phản hồi của hệ thống đến 40% so với các thuật toán cơ bản.

Bahnsen và cộng sự (2016) đã phát triển một chiến lược tổng hợp giao dịch, tạo ra các tính năng mới dựa trên phân tích hành vi định kỳ của thời gian giao dịch bằng phân phối von Mises. Họ cũng đề xuất một tiêu chí đánh giá mới dựa trên chi phí để đánh giá các mô hình phát hiện gian lận thẻ tín dụng. Sử dụng tập dữ liệu thẻ tín dụng thực tế, họ kiểm tra tác động của các tập hợp tính năng khác nhau đến kết quả. Đặc biệt, họ mở rộng chiến lược tổng hợp giao dịch để tạo ra các tính năng mới dựa trên phân tích hành vi định kỳ của giao dịch.

Porwal và Mukund (2018) đề xuất một phương pháp sử dụng các kỹ thuật phân cụm để phát hiện giá trị ngoại lai trong tập dữ liệu lớn, có khả năng thích ứng với các mẫu thay đổi. Phương pháp này dựa trên giả định rằng hành vi hợp lệ của người dùng không thay đổi theo thời gian và các điểm dữ liệu đại diện cho hành vi này có chữ ký không gian nhất quán trong các nhóm khác nhau. Họ chỉ ra rằng hành vi gian lận có thể được phát hiện thông qua việc xác định sự thay đổi trong dữ liệu. Ngoài ra, họ cho rằng diện tích dưới đường cong độ chính xác-thu hồi (PR-AUC) là một tiêu chí đánh giá hiệu quả hơn so với ROC.

Olowookere và Adewale (2020) đề xuất một khung công tác kết hợp tiềm năng của các kỹ thuật học tập tổng hợp meta-learning và mô hình học nhạy cảm với chi phí để phát hiện gian lận. Kết quả đánh giá trên dữ liệu chưa được huấn luyện cho thấy bộ phân loại tổng hợp nhạy cảm với chi phí đạt giá trị AUC chấp nhận được và hiệu quả hơn so với các bộ phân loại tổng hợp thông thường.

1.3. Công nghệ xác thực thông minh trong Mobile Banking

1.3.1.Khái niệm về xác thực thông minh

Trong hệ thống máy tính, xác thực (gọi tắt là “auth”) là quá trình xác minh người dùng là người mà họ tuyên bố. Hầu hết các hệ thống xác thực đều dựa vào các yếu tố xác thực, bao gồm các mục (thẻ quẹt), đặc điểm (quét dấu vân tay) hoặc bit thông tin (mã PIN) mà chỉ người dùng mới có.

Vậy xác thực thông minh là một phương pháp xác định danh tính người dùng được cải tiến bằng cách kết hợp nhiều yếu tố xác thực và công nghệ hiện đại như trí tuệ nhân tạo (AI), học máy (ML), sinh trắc học (biometrics) và phân tích hành vi để tăng cường tính bảo mật đồng thời nâng cao trải nghiệm của người dùng.

1.3.2. Ưu điểm và thách thức khi triển khai xác thực thông minh trong Mobile Banking

Ưu điểm

Bảo mật vẫn là ưu tiên hàng đầu trong ngân hàng di động và các công nghệ xác thực sinh trắc học đang đi đầu trong chiến lược này. Nhận dạng vân tay, nhận diện khuôn mặt và nhận diện giọng nói ngày càng được áp dụng rộng rãi để bảo vệ quyền truy cập vào ứng dụng ngân hàng và xác minh giao dịch. Theo báo cáo của Kissflow Banking Technology, những công nghệ này không chỉ nâng cao mức độ bảo mật mà còn mang đến trải nghiệm người dùng dễ dàng và thân thiện hơn.

Xác thực sinh trắc học ngày càng trở thành giải pháp then chốt trong việc bảo vệ ngân hàng di động trước các nguy cơ gian lận và trộm cắp danh tính. Bằng cách sử dụng các đặc điểm sinh học để xác minh danh tính, ngân hàng có thể giảm thiểu đáng kể nguy cơ truy cập trái phép. Đồng thời, tính tiện lợi của xác thực sinh trắc học giúp loại bỏ việc phải nhớ mật khẩu phức tạp, mang lại trải nghiệm người dùng đơn giản và nhanh chóng. Khi các mối đe dọa mạng ngày càng tinh vi, xác thực sinh trắc học chính là một lớp bảo vệ mạnh mẽ, đảm bảo an toàn tuyệt đối cho dữ liệu của khách hàng.

Ngoài ra thì việc phân tích hành vi người dùng bằng trí tuệ nhân tạo giúp phát hiện các mô hình bất thường theo thời gian thực, từ đó cảnh báo và ngăn chặn kịp thời những hành vi bất thường.

**Thách thức**

Mặc dù xác thực thông minh mang lại nhiều lợi ích rõ rệt, nhưng quá trình triển khai trong Mobile Banking cũng đối mặt với không ít thách thức. Trước hết, chi phí đầu tư ban đầu là một rào cản lớn, bởi việc tích hợp các công nghệ như AI, học máy hay sinh trắc học đòi hỏi hạ tầng kỹ thuật hiện đại và nhân sự có chuyên môn cao. Bên cạnh đó, tính tương thích và khả năng tích hợp hệ thống cũng là vấn đề đáng quan tâm, đặc biệt với các ứng dụng ngân hàng cũ hoặc sử dụng hệ thống phân tán. Ngoài ra, xác thực thông minh phần lớn phụ thuộc vào thiết bị người dùng và kết nối mạng ổn định; do đó, với những khách hàng sử dụng điện thoại đời cũ hoặc sống ở khu vực có tín hiệu yếu, trải nghiệm có thể bị gián đoạn. Một thách thức quan trọng khác là mối lo ngại về quyền riêng tư khi các hệ thống thu thập và xử lý dữ liệu sinh trắc học hay hành vi người dùng. Cuối cùng, dù được xem là tiên tiến, nhưng xác thực thông minh vẫn có thể bị vượt qua bởi các kỹ thuật giả mạo tinh vi như deepfake hay tấn công giả lập hành vi, đặt ra yêu cầu ngày càng cao trong việc nâng cấp công nghệ bảo mật.

TIỂU KẾT CHƯƠNG I

Chương I cung cấp thông tin về cơ sở lý thuyết về học máy và công nghệ xác thực thông minh trong phát hiện gian lận Mobile Banking một cách cụ thể và và rõ ràng. Đồng thời cũng nêu ra vai trò của học máy trong việc phát hiện gian lận và lợi ích cũng như thách thức khi triển khai xác thực thông minh trong Mobile Banking giúp người đọc có cái nhìn tổng quan hơn về học máy.

Chương II. Thực trạng công tác phát hiện gian lận hiện nay và các phương pháp bảo mật trong giao dịch Mobile Banking

Thực trạng công tác phát hiện gian lận hiện nay

2.1.1.Các ngân hàng trên thế giới

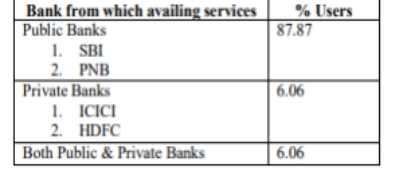
2.1.

**Ấn Độ**

Ngành ngân hàng ở Ấn Độ đã trải qua một chặng đường dài để đạt được vị trí như hiện tại đó là một hệ thống ngân hàng hoạt động hiệu quả và kỷ luật, góp phần hỗ trợ và thúc đẩy kinh tế phát triển.

Theo thống kê thì trong số những người dùng dịch vụ ngân hàng di động thì có tới 87,87% người sử dụng dịch vụ ngân hàng di động từ các ngân hàng công, chính phủ. Ngân hàng nhà nước Ấn Độ là nhà cung cấp dịch vụ ngân hàng di động lớn nhất, tiếp đến là ngân hàng Punjab.

Hình 2.1.Mẫu hình sử dụng dịch vụ Mobile banking

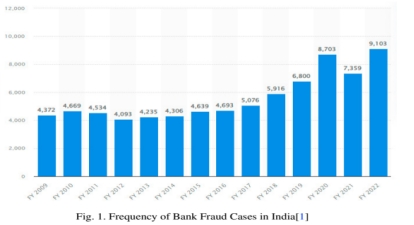


*Nguồn : Goyal, V., Pandey, U. S., & Batra, S. (2012).*

Trong khi hoạt động của các ngân hàng ngày càng phát triển mạnh mẽ thì vấn đề gian lận tài chính trong hệ thống ngân hàng cũng ngày càng gia tăng và những kẻ lừa đảo ngày càng hoạt động tinh vi hơn và được coi là tội phạm có tổ chức.

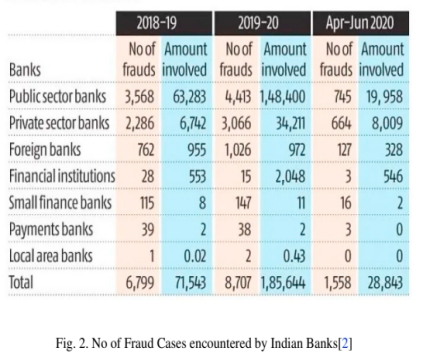
Dưới đây là tần suất các vụ gian lận ngân hàng ở Ấn Độ từ năm 2009 đến 2022.

Hình 2.2. Tần suất gian lận ngân hàng ở Ấn Độ

**

*Nguồn:Singh, J., Singh, G., Gahlawat, M., & Prabha, C. (2022).*

Hình 2.3. Số lượng vụ án Pral được ngân hàng Handian lưu giữ



*Nguồn:Singh, J., Singh, G., Gahlawat, M., & Prabha, C. (2022).*

Theo dữ liệu của ngân hàng Dự Trữ Ấn Độ, tính đến ngày 31 tháng 3 năm 2021, các ngân hàng hoạt động đã thiệt hại 4,92 nghìn tỷ Rupee trong các vụ gian lận

Điều này làm cho các ngân hàng lớn như SBI, ICICI hay PNB càng phải nâng cao cảnh giác và bảo mật, tìm kiếm phương pháp phát hiện gian lận bằng các thuật toán học máy như Decision Tree, ANN, XGBoost.

***Trung Quốc***

Là một trong những quốc gia đi đầu về lính vực khoa học công nghệ, Trung Quốc đã áp dụng trí tuệ nhân tạo (AI) để tăng cường bảo mật cho các hệ thống và đặc biệt là ngân hàng. Ví dụ như Ngân hàng di động đầu tiên của Tung Quốc - Webank đang phát triển mô hình mới về trí tuệ nhân tạo có tên là học liên kết ( federated learning) để tăng cường bảo vệ thông tin và quyền riêng tư của khách hàng***.***Bên cạnh đó, để ngăn chặn và phát hiện gian lận thì China UnionPay - tổ chức thanh toán quốc gia của Trung Quốc đã sử dụng các kỹ thuật phân tích dữ liệu nâng cao và học máy để phân tích lượng lớn dữ liệu giao dịch như thời gian thực và xác định các hoạt động đáng ngờ. Ngoài ra còn sử dụng nhiều quy tắc và mô hình phát hiện gian lận khác nhau để xác định các giao dịch có khả năng gian lận. Các mô hình này dựa trên phân tích thống kê và có thể được cập nhật theo thời gian thực dựa trên dữ liệu mở. China UnionPay đã triển khai các công nghệ xác thực sinh trắc học như nhận dạng khuôn mặt và quét dấu vân tay để giúp ngăn ngừa gian lận bằng cách xác minh danh tính của khách hàng.

***Indonesia***

Các ngân hàng Indonesia đã áp dụng trí tuệ nhân tạo (AI) để cải thiện hoạt động của họ. Chẳng hạn, học máy có thể phân tích giao dịch thông qua trực quan hóa đồ thị để hỗ trợ ra quyết định dựa trên dữ liệu và phát hiện hành vi bất thường của khách hàng nhằm giảm thiểu gian lận (Afriyie et al., 2023). Công nghệ học máy cũng có khả năng phát hiện các mẫu gian lận và tấn công mạng. Liên quan đến mục tiêu của nghiên cứu này, các công nghệ AI được khách hàng sử dụng bao gồm quét khuôn mặt cho giao dịch, lệnh giọng nói, trợ lý ảo trong ngân hàng di động, chatbot cho dịch vụ thông tin, dấu vân tay và sinh trắc học cho quá trình xác thực và ủy quyền. Việc áp dụng AI có thể đơn giản hóa giao dịch của khách hàng; tuy nhiên, nhiều trở ngại đang cản trở việc sử dụng công nghệ này. Thông qua các cuộc phỏng vấn chuyên sâu với các chuyên gia ngân hàng Indonesia, nghiên cứu đã xác định bốn yếu tố chính ngăn cản khách hàng chấp nhận AI tại Indonesia, nhấn mạnh tầm quan trọng của nghiên cứu này.

Theo nghiên cứu, nhận thức về rủi ro và niềm tin của khách hàng liên quan đến trí tuệ nhân tạo (AI) trong lĩnh vực ngân hàng tại Indonesia chịu ảnh hưởng bởi một số yếu tố chính. Thứ nhất, nhiều khách hàng tại Indonesia thiếu hiểu biết về cách AI hoạt động trong các dịch vụ ngân hàng, dẫn đến sự thiếu tin tưởng hoặc do dự khi sử dụng các dịch vụ dựa trên AI. Các rủi ro tiềm ẩn bao gồm thiên kiến trong thuật toán, deepfake, và các quyết định tự động hóa bởi AI (phỏng vấn, tháng 9 năm 2024). Thứ hai, vấn đề bảo mật và quyền riêng tư dữ liệu của khách hàng là mối quan ngại lớn. Mặc dù AI có thể nâng cao hiệu quả và cá nhân hóa dịch vụ, khách hàng lo lắng về cách dữ liệu của họ được sử dụng và lưu trữ, cũng như nguy cơ rò rỉ hoặc lạm dụng thông tin cá nhân (phỏng vấn, tháng 9 năm 2024). Về chuẩn mực chủ quan, nhiều người xung quanh khách hàng, như bạn bè, gia đình hoặc đồng nghiệp, bày tỏ lo ngại về quyền riêng tư và bảo mật dữ liệu, khiến họ ngần ngại sử dụng các dịch vụ dựa trên AI (phỏng vấn, tháng 9 năm 2024). Thứ ba, khoảng cách số tại Indonesia vẫn là một vấn đề lớn. Việc tiếp cận internet nhanh và đáng tin cậy còn hạn chế, cùng với trình độ kỹ năng số thấp, khiến các dịch vụ dựa trên AI kém hấp dẫn với khách hàng (phỏng vấn, tháng 9 năm 2024). Khoảng cách số ảnh hưởng đến khả năng sử dụng công nghệ và nhận thức của khách hàng về tính hữu ích của AI, đặc biệt khi khách hàng gặp khó khăn trong việc sử dụng ứng dụng AI do hạn chế về truy cập internet hoặc thiếu kỹ năng số. Cuối cùng, các chính sách và quy định liên quan đến sử dụng AI trong ngành ngân hàng Indonesia chưa hoàn thiện, gây ra sự bất định về quy định và cản trở các ngân hàng áp dụng rộng rãi công nghệ AI (phỏng vấn, tháng 9 năm 2024). Do đó, các ngân hàng cần đảm bảo sự rõ ràng và chắc chắn về quy định AI.

2.1.2.Các ngân hàng tại Việt Nam

Theo quy định mới của Ngân hàng Nhà nước Việt Nam, các tổ chức cung ứng dịch vụ thanh toán hiện nay bắt buộc phải triển khai các biện pháp kiểm soát rủi ro, đảm bảo an toàn và bảo mật trong toàn bộ quá trình cung cấp dịch vụ thanh toán không dùng tiền mặt. Quy định này nhằm tăng cường tính minh bạch và bảo vệ người dùng trong bối cảnh các giao dịch điện tử ngày càng phổ biến (Thông tư 15/2024/TT-NHNN, trích từ Thư viện Pháp luật, 2024).

Trong bối cảnh số hóa mạnh mẽ của ngành tài chính – ngân hàng, học máy (machine learning) được xem là một công cụ hữu hiệu giúp các tổ chức tín dụng phát hiện sớm và chủ động xử lý các rủi ro tiềm ẩn, đặc biệt là trong lĩnh vực phát hiện giao dịch bất thường và gian lận tài chính. Theo Hiệp hội Ngân hàng Việt Nam, nhiều ngân hàng trong nước đã từng bước ứng dụng các thuật toán học máy trong phân tích hành vi khách hàng và xây dựng hệ thống cảnh báo sớm, góp phần nâng cao hiệu quả quản trị rủi ro và đảm bảo an toàn hệ thống (Hiệp hội Ngân hàng Việt Nam, 2023). Một số thuật toán học máy thường được sử dụng bao gồm: Decision Tree, Random Forest, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Logistic Regression, Naive Bayes, và Neural Networks. Những thuật toán này có khả năng phát hiện mẫu hành vi bất thường thông qua việc học từ dữ liệu lịch sử, từ đó hỗ trợ hệ thống ngân hàng nhận diện và ngăn chặn các giao dịch có dấu hiệu gian lận một cách kịp thời và chính xác.

2.2.Thực trạng về các phương pháp bảo mật trong giao dịch Mobile Banking

Trong bối cảnh ngân hàng số phát triển mạnh mẽ trên toàn cầu, dịch vụ ngân hàng di động (Mobile Banking) đã trở thành một trong những kênh giao dịch phổ biến nhất đối với người tiêu dùng và doanh nghiệp. Tuy nhiên, song hành với sự tiện lợi là những nguy cơ bảo mật ngày càng gia tăng, đặt ra yêu cầu cấp thiết đối với các tổ chức tài chính trong việc triển khai các biện pháp bảo mật hiệu quả và phù hợp. Trên thế giới, các quốc gia đã và đang áp dụng nhiều phương pháp bảo mật khác nhau nhằm bảo vệ hệ thống, tài khoản và dữ liệu khách hàng trước sự tấn công ngày càng tinh vi của tội phạm mạng.

2.2.1. Các ngân hàng trên thế giới

Ấn Độ

Với dân số vượt qua con số 1.3 tỷ người, Ấn Độ đứng trong số các quốc gia có dân số lớn nhất trên thế giới, tạo nên một nhu cầu không thể phủ nhận cho các dịch vụ tài chính. Mặc dù đã có sự gia tăng trong việc tiếp cận các dịch vụ ngân hàng trong những năm qua, vẫn còn một phần của dân số, đặc biệt là ở các vùng nông thôn và miền núi, vẫn gặp phải những thách thức các dịch vụ tài chính, đặc biệt là Mobile Banking.

Một trong những phương pháp xác thực được sử dụng trong Mobile banking là phương pháp đăng nhập. Tuy nhiên, phương pháp xác thực PINS là một phương pháp cũ và gặp nhiều vấn đề bảo mật như mật khẩu và đánh cắp ID đã được phát hiện trong phương pháp này. Trong những trường họp như vậy, bí mật có thể bị tiết lộ và điều này dẫn đến việc khách hàng không tin tưởng vào các tổ chức tài chính. Các ngân hàng ở Ấn Độ đã tuân theo một số cơ chế bảo mật trong Mobile banking, cơ chế bảo mật này được thực hiện bằng cách xác định số điện thoại, số thẻ SIM, mã PIN của khách hàng, ...Nhưng nếu thiết bị đăng nhập bị đánh cắp thì kẻ cắp cũng có thể tìm thấy mật khẩu từ các tệp nhật kí hoặc các tệp nháp đã lưu vì có rất nhiều khách hàng lưu mật khẩu của họ trong điện thoại di động hoặc họ có thể lưu mật khẩu trong cài đặt tự động của biểu mẫu. Lỗ hổng này có thể dễ dàng bị kẻ xấu khai thác.

Mỹ

Với vị thế là một trong những quốc gia đi đầu về khoa học công nghệ thì các ngân hàng ở Mỹ đã áp dụng phổ biến phương pháp xác định đa yếu tố (MFA) để bảo mật trong Mobliek banking. Tại đây, theo hướng dẫn của Hội đồng kiểm tra các tổ chức tài chính liên bang (FFIEC), xác thực đơn yếu tố đã không còn được coi là đủ an toàn, đặc biệt đối với các giao dịch có giá trị cao hoặc có mức độ rủi ro lớn. Các ngân hàng như Bank of America, Wells Fargo hay JPMorgan Chase đã tích hợp MFA bằng cách kết hợp mật khẩu, mã OTP và sinh trắc học. Ngoài ra còn triển khai hệ thống học máy để phân tích hành vi người dùng theo thời gian thực nhằm phát hiện các giao dịch bất thường, ngăn chặn gian lận trước khi xảy ra. Ví dụ như Bank of America triển khai hệ thống SafePass, cung cấp mã xác thực một lần (OTP) qua tin nhắn SMS hoặc thẻ phần cứng (SafePass Card) để xác minh các giao dịch nhạy cảm. Ngoài ra, ngân hàng còn hỗ trợ xác thực sinh trắc học như vân tay và nhận diện khuôn mặt trên ứng dụng di động.

Nhật Bản

Tại Nhật Bản, một trong những quốc gia có hệ thống tài chính – ngân hàng phát triển hàng đầu châu Á, các tổ chức tài chính đã chủ động ứng dụng các công nghệ bảo mật hiện đại nhằm đảm bảo an toàn cho người dùng trong quá trình giao dịch ngân hàng di động (Mobile Banking).

MUFG – ngân hàng lớn nhất Nhật Bản đang áp dụng công nghệ xác thực tiên tiến nhằm nâng cao bảo mật cho khách hàng sử dụng Mobile Banking. Một trong những công nghệ nổi bật là nhận diện khuôn mặt bằng trí tuệ nhân tạo (AI facial recognition), cho phép so sánh hình ảnh khuôn mặt người dùng được ghi lại qua camera điện thoại với dữ liệu sinh trắc học đã đăng ký từ trước. Bên cạnh đó, MUFG còn triển khai xác thực bằng mã OTP qua SMS để xác minh các giao dịch tài chính. Tất cả thông tin giao dịch và dữ liệu người dùng đều được bảo vệ bằng mã hóa dữ liệu kết hợp kết nối bảo mật SSL, giúp đảm bảo an toàn trong quá trình truyền tải thông tin.

Ngân hàng Mizuho đầu tư mạnh mẽ vào xác thực sinh trắc học bằng cách triển khai cảm biến vân tay tích hợp dưới màn hình điện thoại, cho phép khách hàng đăng nhập và xác nhận giao dịch một cách thuận tiện và an toàn. Ngoài ra, ngân hàng cũng tích cực sử dụng các hệ thống phân tích dữ liệu lớn và trí tuệ nhân tạo nhằm phát hiện các hành vi bất thường có thể là dấu hiệu của gian lận tài chính. Để tăng cường tính linh hoạt và phòng ngừa các cuộc tấn công mạng, Mizuho duy trì chính sách cập nhật thường xuyên các phần mềm và hệ thống bảo mật trên nền tảng ngân hàng di động.

Shinsei Bank nổi bật với việc ứng dụng mã xác thực thời gian thực (real-time authentication) dựa trên nền tảng blockchain cho Mobile Banking. Phương pháp này cho phép xác nhận danh tính và giao dịch một cách chính xác gần như ngay lập tức, giảm thiểu tối đa khả năng bị tấn công trung gian (man-in-the-middle). Ngoài ra, ngân hàng còn triển khai hệ thống tường lửa chuyên dụng cho Mobile Banking và sử dụng công nghệ AI để phân tích lưu lượng mạng, phát hiện mã độc và các hành vi bất thường, từ đó tăng cường năng lực phòng vệ chủ động trước các cuộc tấn công mạng.

Nhìn chung, các ngân hàng lớn tại Nhật Bản đang tích cực đầu tư và đổi mới công nghệ bảo mật trong lĩnh vực Mobile Banking. Việc kết hợp nhiều lớp bảo mật – từ sinh trắc học, OTP, AI, mã hóa đến blockchain – không chỉ giúp gia tăng độ an toàn cho người dùng mà còn thể hiện nỗ lực mạnh mẽ của ngành tài chính Nhật Bản trong việc đối phó với các rủi ro an ninh mạng ngày càng phức tạp. Mô hình bảo mật đa tầng và liên tục cập nhật như tại Nhật Bản có thể được coi là hình mẫu đáng tham khảo cho các quốc gia đang phát triển trong quá trình chuyển đổi số ngân hàng.

2.2.2.Các ngân hàng Việt Nam

Theo thống kê từ Vụ Thanh toán - Ngân hàng Nhà nước Việt Nam (NHNN), năm 2022 chứng kiến sự gia tăng đáng kể trong việc sử dụng các dịch vụ ngân hàng qua Internet Banking và Mobile Banking. Số liệu cho thấy, số lượng giao dịch qua Internet Banking đã tăng gần 48% so với năm trước, và giá trị giao dịch tăng mạnh đến 1.328%, từ 811.717 tỷ đồng lên 10.868.458 tỷ đồng. Đồng thời, kênh Mobile Banking cũng ghi nhận mức tăng trưởng lên đến 100% về cả số lượng và giá trị giao dịch. Đây là kết quả của quá trình chuyển đổi số trong ngành ngân hàng, làm thay đổi thói quen sử dụng dịch vụ của khách hàng và đẩy mạnh quá trình số hóa hệ thống ngân hàng.

Tuy nhiên, cùng với sự gia tăng nhu cầu sử dụng ngân hàng số, vấn đề bảo mật thông tin của khách hàng trở thành một mối quan tâm hàng đầu đối với cả ngân hàng và người dùng. Sự phát triển của tội phạm công nghệ cao với những phương thức tấn công ngày càng tinh vi khiến cho hệ thống bảo mật ngân hàng đứng trước nhiều thử thách. Các nguy cơ như lộ thông tin qua SMS, OTP, việc tài khoản bị giả mạo hay tội phạm lợi dụng giấy tờ, thông tin giả để mở tài khoản đang là những rủi ro phổ biến. Thêm vào đó, một đặc điểm nổi bật của tội phạm công nghệ cao trong ngành ngân hàng là chúng không bị giới hạn về thời gian, không gian, và phương thức tấn công, từ việc gây gián đoạn dịch vụ đến việc chiếm đoạt tiền và đánh cắp thông tin của khách hàng.

Trong bối cảnh gia tăng các hình thức lừa đảo tinh vi và tội phạm công nghệ cao, nhiều ngân hàng thương mại tại Việt Nam đã chủ động triển khai các công nghệ xác thực và cảnh báo rủi ro để bảo vệ khách hàng. Ngân hàng TMCP Đầu tư và Phát triển Việt Nam (BIDV) đã triển khai tính năng Smart Alert trên ứng dụng BIDV SmartBanking. Tính năng này cho phép hệ thống tự động dò quét và so sánh số tài khoản người nhận với cơ sở dữ liệu các tài khoản có dấu hiệu gian lận do cơ quan chức năng cung cấp (như Bộ Công an, NHNN). Khi phát hiện dấu hiệu bất thường, ứng dụng sẽ lập tức gửi cảnh báo đến người dùng nhằm ngăn chặn các giao dịch rủi ro.

Tương tự thế, Ngân hàng TMCP Việt Nam Thịnh Vượng (VPBank) cũng đã tích hợp tính năng cảnh báo bảo mật trên ứng dụng VPBank NEO. Hệ thống sẽ tự động kiểm tra thiết bị của người dùng, phát hiện và cảnh báo nếu thiết bị đang bật quyền truy cập rủi ro (như cấp quyền trợ năng cho ứng dụng lạ hoặc có dấu hiệu bị điều khiển từ xa). Đồng thời, ứng dụng có khả năng chặn các giao dịch đến các tài khoản nằm trong danh sách nghi vấn gian lận.

Ngân hàng TMCP Quân đội (MB) cũng là một đơn vị tiên phong trong việc ứng dụng công nghệ để nhận diện các tài khoản có dấu hiệu lừa đảo. Khi thực hiện thao tác chuyển tiền trên ứng dụng MBBank, khách hàng sẽ được cảnh báo nếu tài khoản người nhận có liên quan đến hành vi gian lận. Bên cạnh đó, MB còn áp dụng các công nghệ phát hiện phần mềm độc hại và bảo vệ thiết bị khỏi bị chiếm quyền truy cập. Các lớp bảo mật như D-OTP, xác thực sinh trắc học, mật khẩu mạnh và cảnh báo tài khoản rủi ro từ Cục A05 cũng được tích hợp đồng bộ trong ứng dụng.

Mặc dù các ngân hàng hiện nay đã triển khai nhiều hình thức bảo mật, như quét vân tay, nhận diện khuôn mặt, hay gửi OTP qua SMS, tuy nhiên, việc bảo vệ thông tin khách hàng vẫn chưa hoàn toàn chắc chắn. Các đối tượng lừa đảo vẫn có thể đánh cắp thông tin qua những cách thức tinh vi như gửi tin nhắn SMS, email hoặc thậm chí sử dụng phần mềm chat để mời gọi khách hàng cung cấp các thông tin bảo mật quan trọng như mật khẩu, số thẻ, hoặc mã OTP. Các vụ tấn công mạng đã xảy ra tại Việt Nam, với việc các nhóm tội phạm từ nước ngoài xâm nhập vào hệ thống ngân hàng để chiếm đoạt tiền từ tài khoản của khách hàng, càng làm tăng mối lo ngại về an toàn bảo mật.

TIỂU KẾT CHƯƠNG II

Chương II nói về thực trạng công tác phát hiện gian lận hiện nay và thực trạng về các phương pháp sử dụng để bảo mật trong Mobile banking ở trên thế giới và tại Việt Nam giúp người đọc hiểu hơn về việc sử dụng học máy phát hiện gian lận và sử dụng các phương pháp xác thực thông minh để bảo mật trong Mobile banking giúp củng cố niềm tin ở khách hàng đồng thời nâng cao trải nghiệm của khách hàng.

Chương III. MÔ HÌNH PHÁT HIỆN GIAN LẬN VÀ XÁC THỰC THÔNMINH TRONG GIAO DỊCH MOBILE BANKING

3.1 .Mô hình nghiên cứu GCD-GNN

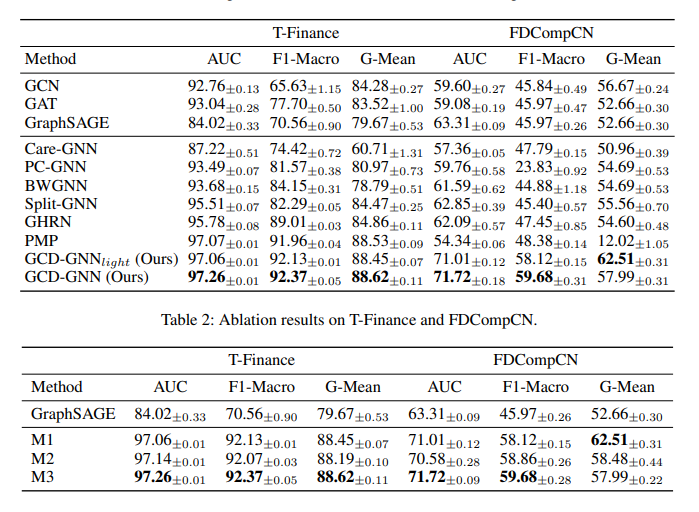
Mạng nơ-ron đồ thị (GNN) được sử dụng rộng rãi trong phát hiện gian lận tài chính nhờ khả năng xử lý dữ liệu có cấu trúc đồ thị và mô hình hóa các kết nối nhiều lớp thông qua việc tổng hợp thông tin từ các nút lân cận. Tuy nhiên, các phương pháp dựa trên GNN hiện tại chủ yếu tập trung vào việc khai thác thông tin ở cấp độ lân cận mà bỏ qua góc nhìn toàn cục

Mô hình GCD-GNN được thiết kế để phát hiện gian lận tài chính bằng cách kết hợp thông tin toàn cục và cục bộ trong mạng nơ-ron đồ thị. Mô hình này bao gồm ba thành phần chính:

1. Biến đổi đặc trưng: Sử dụng một mạng perceptron nhiều lớp (MLP) để biến đổi đặc trưng ban đầu của các nút, giúp loại bỏ thông tin không cần thiết và tăng khả năng phân biệt giữa các nút gian lận và hợp lệ.
2. Tính toán Độ tin cậy toàn cục (GCD): Đánh giá mức độ điển hình của mỗi nút bằng cách so sánh đặc trưng đã biến đổi với một "prototype" đại diện cho lớp của nút đó.
3. Tổng hợp thông tin: Sử dụng GCD để xác định trọng số trong quá trình tổng hợp thông tin từ các nút lân cận, giúp mô hình nhận diện cả các nút điển hình và không điển hình.

Theo nghiên cứu của Liu, Tian và Liu (n.d.), kết quả cho thấy mô hình nhẹ của họ đạt được mức AUC cao trong một khoảng thời gian ngắn. Ngoài ra, mô hình đầy đủ đạt được điểm số cao nhất trong một khoảng thời gian trung bình. Hiệu suất vượt trội của mô hình này đến từ việc các GNN thông thường không xem xét tầm quan trọng của từng mẫu và tổng hợp thông điệp một cách đồng đều. Ngược lại, mô hình của họ sử dụng GCD để đánh giá thông tin từ các nút láng giềng, qua đó cải thiện hiệu suất và tăng tốc độ huấn luyện, đồng thời giảm thiểu sự tiêu thụ tài nguyên tính toán.

Hình 3.3: Hình ảnh kết quả thử nghiệm trên 2 bộ dữ liệu T-Finance và FDCompCN



Nguồn:Tian và Liu (n.d.)

Trong các hệ thống phát hiện gian lận tài chính, dữ liệu thường tồn tại dưới dạng đồ thị, nơi các thực thể như tài khoản, giao dịch, người dùng được biểu diễn bằng các nút (node), còn các tương tác như chuyển khoản hoặc hợp tác được biểu diễn bằng các cạnh (edge). Do đó, biểu diễn dữ liệu dưới dạng đồ thị là một cách tiếp cận hợp lý:

• Node: Tài khoản, giao dịch, người dùng.

• Edge: Giao dịch, hợp tác, liên hệ.

Các phương pháp GNN truyền thống như GCN, GAT, GraphSAGE thường chỉ tận dụng thông tin từ lân cận trực tiếp, bỏ qua cái nhìn toàn cục, dẫn đến việc dễ bị ảnh hưởng bởi thông tin nhiễu từ các node ngụy trang (camouflage nodes).

Thuật toán GCD-GNN (Global Confidence Degree Graph Neural Network) được đề xuất để giải quyết hạn chế này bằng cách kết hợp thông tin toàn cục và cục bộ, cụ thể thông qua khái niệm mới **Global Confidence Degree (GCD)**.

GCD-GNN được đề xuất nhằm kết hợp cả góc nhìn cục bộ và toàn cục bằng cách:

• Tính toán Global Confidence Degree (GCD) giữa mỗi node và lớp mục tiêu.

• Áp dụng Typical Aggregation và Atypical Aggregation từ neighbor.

• Tận dụng đặc trưng toàn cục qua Prototype mỗi lớp.

Biểu diễn dữ liệu - Cho một đồ thị có nhãn G = (V, E, X, Y), trong đó:

* V: tập các node
* E: tập các cạnh giữa các node
* X: ma trận đặc trưng của các node
* Y: tập nhãn {fraud, benign, unlabel}

Để thu được thông tin toàn cục, ta định nghĩa **prototype** cho mỗi lớp  
 , đại diện cho trung bình đặc trưng của tất cả các node thuộc lớp đó:

A mathematical symbols and symbols

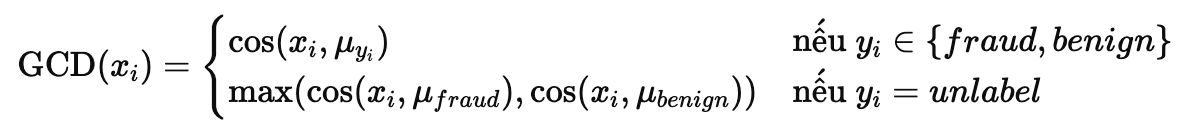
AI-generated content may be incorrect.

Trong đó là tập các node thuộc lớp c, và là đặc trưng của node v.

Để cải thiện khả năng phân biệt, tác giả gốc đề xuất sử dụng một MLP để biến đổi đặc trưng node trước khi tính prototype:

GCD được sử dụng để đo lường mức độ "điển hình" của một node so với lớp dữ liệu.

* Với node có nhãn: GCD là cosine similarity giữa node và prototype lớp tương ứng.
* Với node chưa có nhãn: GCD là giá trị lớn nhất giữa hai cosine similarity với prototype của hai lớp.



Trong đó: : là tập các node được gán nhãn **hợp lệ**.

: là tập các node được gán nhãn **gian lận**.

: là vector đặc trưng của node v.

Đặc trưng node được chuyển sang không gian mới bằng MLP rồi kết hợp với đặc trưng ban đầu:

A close-up of a math problem

AI-generated content may be incorrect.

Tổng hợp thông tin từ lân cận được chia thành hai hướng:

* **Typical Aggregation**: từ các nút có GCD cao (điển hình)
* **Atypical Aggregation**: từ các nút có GCD thấp (khác biệt)

Với mỗi node , ta tính trọng số attention dựa trên GCD của node lân cận j:

A close-up of a word

AI-generated content may be incorrect.

*Với* lần lượt là attention trọng số cho hướng typical và atypical.

Tổng hợp:

*A black text on a white background

AI-generated content may be incorrect.*

Sau khi tổng hợp thông tin, đặc trưng node được cập nhật:

A black math symbol with a white background

AI-generated content may be incorrect.

Trong đó:

• W: ma trận trọng số learnable.

• b: bias learnable.

• σ: hàm kích hoạt LeakyReLU.

GraphNorm được thiết kế để chuẩn hóa embedding của node trên toàn đồ thị:

Trong đó:

• : trung bình embedding các node.

•: phương sai embedding các node.

• γ, β: các tham số learnable.

• ϵ: hằng số nhỏ tránh chia cho 0.

Hàm mất mát chuẩn được dùng để phân loại node:

A black and white symbol

AI-generated content may be incorrect.

Trong đó:

•: nhãn thực tế của node v.

• : xác suất dự đoán node v thuộc lớp.

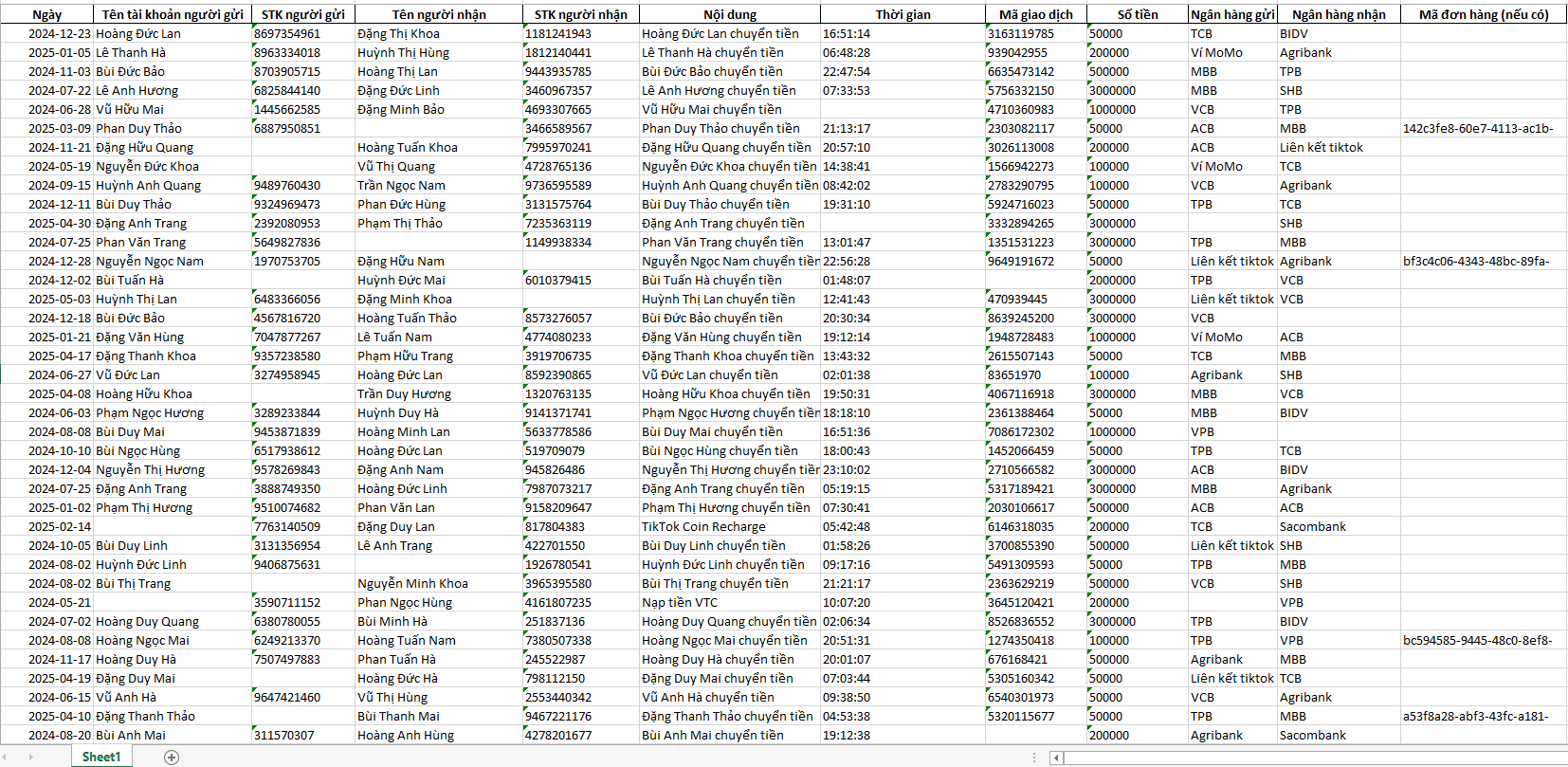
3.2 .Dữ liệu nghiên cứu

**Việc có dữ liệu thực tế từ thế giới thật là yếu tố then chốt quyết định độ tin cậy và độ chính xác của các thuật toán học máy** (Husejinovic, 2020).Bộ dữ liệu được sử dụng trong nghiên cứu này được nhóm tác giả thu thập từ cụm sinh viên đang theo học tại các trường đại học trên địa bàn thành phố Hà Nội. Mục đích của việc thu thập dữ liệu là nhằm mô phỏng các hoạt động giao dịch tài chính thực tế giữa các cá nhân trong cộng đồng sinh viên, từ đó phục vụ cho nghiên cứu các kỹ thuật phát hiện gian lận tài chính thông qua phương pháp phân tích mạng lưới (graph-based analysis).

Tổng cộng, bộ dữ liệu bao gồm **11.068 bản ghi giao dịch**, được tổ chức dưới dạng bảng tính sử dụng công cụ **Microsoft Excel**. Mỗi bản ghi tương ứng với một giao dịch chuyển khoản giữa hai cá nhân, mô tả đầy đủ các trường thông tin cơ bản như: thời gian giao dịch (ngày và giờ), tên và số tài khoản người gửi – người nhận, nội dung giao dịch, mã giao dịch, số tiền được chuyển, ngân hàng gửi – ngân hàng nhận, và mã đơn hàng (nếu có). Nhờ sự chi tiết này, bộ dữ liệu cho phép theo dõi mối quan hệ tài chính giữa các thực thể, đồng thời tạo điều kiện thuận lợi cho việc tiền xử lý và chuyển đổi sang định dạng đồ thị.

Nguồn giao dịch trong bộ dữ liệu thể hiện sự đa dạng về nền tảng giao dịch tài chính trên Mobile Banking, bao gồm các ngân hàng thương mại cổ phần như Vietcombank (VCB), BIDV, MBBank, TPBank, Agribank, ACB và các hình thức thanh toán trung gian như **ví điện tử MoMo**, **liên kết TikTok**, hay **dịch vụ nạp tiền VTC**. Nội dung chuyển tiền được ghi lại dưới dạng các mô tả đơn giản, phản ánh các hành vi chuyển khoản quen thuộc trong đời sống sinh viên, nhưng đồng thời cũng có thể tiềm ẩn các dấu hiệu giao dịch bất thường.

Hình 3.1: Dữ liệu giao dịch của cụm sinh viên



*Nguồn: Nhóm nghiên cứu*

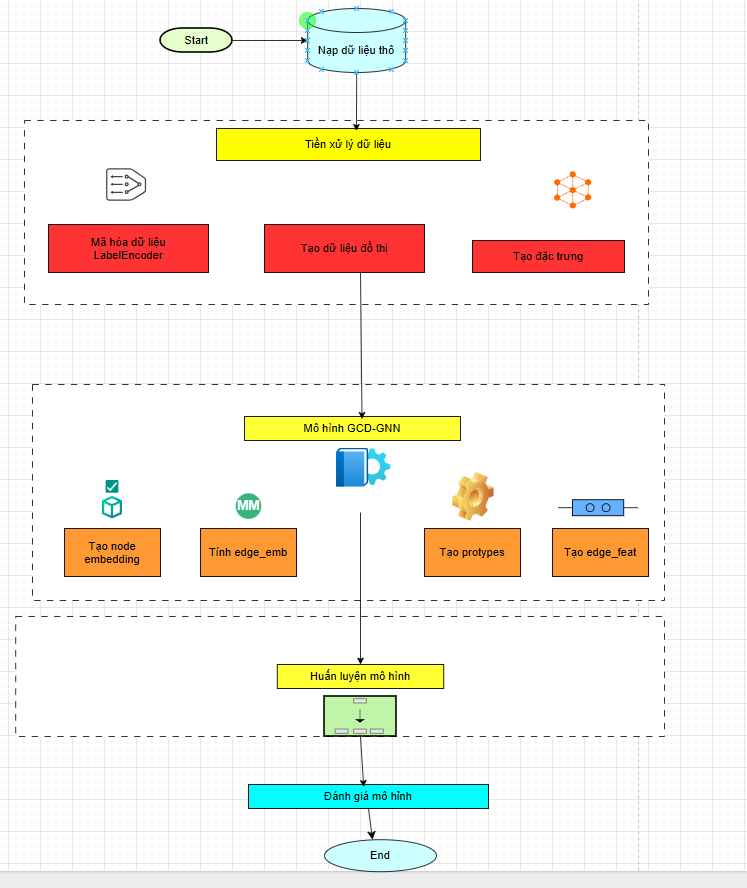
Khác với các hệ thống phát hiện gian lận tài chính truyền thống vốn hướng đến quy mô lớn và đa dạng đối tượng, nghiên cứu này tập trung vào việc xây dựng mô hình dành riêng cho cụm sinh viên – nơi mà hành vi, thói quen giao dịch và tần suất tương tác có sự tương đồng và lặp lại theo chu kỳ (đầu tháng, kỳ học, thời điểm thi, v.v). Bằng cách huấn luyện mô hình cá nhân hóa trên mạng lưới giao dịch nội bộ của sinh viên, hệ thống có khả năng nhận diện tốt hơn các biến thể nhỏ nhưng bất thường trong hành vi tài chính – những đặc điểm mà mô hình tổng quát dễ bỏ qua.

Bộ dữ liệu sẽ được tiền xử lý để chuyển đổi sang định dạng đồ thị, trong đó các đỉnh (nodes) đại diện cho tài khoản người dùng, và các cạnh (edges) là các giao dịch tài chính giữa họ. Với cấu trúc này, các mô hình như GCD-GNN (Graph Contextualized Dynamic Graph Neural Network) có thể được huấn luyện nhằm học biểu diễn động của các tài khoản theo thời gian, đồng thời khai thác thông tin cục bộ (local context) và toàn cục (global structure) trong mạng lưới sinh viên.

Việc huấn luyện mô hình theo hướng cá nhân hóa không chỉ giúp nâng cao độ chính xác trong phát hiện gian lận, mà còn mở ra tiềm năng phát triển các hệ thống cảnh báo gian lận phù hợp với từng nhóm người dùng cụ thể – một hướng tiếp cận hiệu quả trong bối cảnh gian lận tài chính ngày càng tinh vi và mang tính cá nhân hóa cao.

3.3.Quy trình nghiên cứu

Hình 3.2: Quy trình nghiên cứu



*Nguồn: Nhóm tác giả*

3.3.1.Tiền xử lý dữ liệu

Bảng 3.1 : Bảng thuộc tính dữ liệu thực tế

|  |  |
| --- | --- |
| Tên thuộc tính | Mô tả |
| Tên tài khoản người gửi | Tên người chuyển tiền |
| STK người gửi | Số tài khoản người gửi |
| Tên người nhận | Tên người nhận tiền |
| STK người nhận | Số tài khoản người nhận |
| Nội dung | Nội dung chuyển tiền |
| Ngân hàng gửi | Ngân hàng của người gửi |
| Ngân hàng nhận | Ngân hàng của người nhận |
| Số tiền | Số tiền giao dịch |
| Fraud | Nhãn: 1 nếu là giao dịch gian lận, 0 nếu bình thường |

Mỗi **tài khoản** là một node. Mỗi node được mã hóa thành **một chỉ số duy nhất** (ID). Đặc trưng node là **vector one-hot** – mỗi node có một đặc trưng duy nhất.

Mỗi giao dịch là một **cạnh có hướng** (từ người gửi đến người nhận). Giao dịch gồm các thuộc tính: Số tiền, Ngân hàng gửi, Ngân hàng nhận, Nội dung.

Bảng 3.2: Quy trình xử lý dữ liệu

|  |  |  |
| --- | --- | --- |
| **Bước** | **Mục tiêu** | **Chi tiết** |
| 1 | Mã hóa tên tài khoản | Biến tên thành số nguyên (LabelEncoder) để tạo node |
| 2 | |  | | --- | |  |  |  | | --- | | Mã hóa ngân hàng, nội dung | | Biến các văn bản thành số để làm đặc trưng |
| 3 | Chuẩn hóa số tiền | Đưa số tiền về thang đo chuẩn để mô hình học tốt hơn |
| 4 | Tạo edge\_inde | Tạo cặp (sender → receiver) cho mỗi giao dịch |
| 5 | |  | | --- | |  |  |  | | --- | | Tạo edge\_attr | | Tổ hợp đặc trưng giao dịch làm input cho mô hình |
| 6 | Tạo Data object | |  | | --- | |  |  |  | | --- | | Đóng gói dữ liệu thành torch\_geometric.data.Data | |

*Nguồn: Nhóm tác giả*

### **3.3.2. Mô hình GCD-GNN**

Mô hình GCD-GNN (Graph Contrastive Detection using Graph Neural Networks) khai thác cấu trúc của đồ thị để học biểu diễn đặc trưng cho từng cạnh, tương ứng với mỗi giao dịch Mobile Banking:

**GCN layers:**

Các lớp GCN (Graph Convolutional Network) được sử dụng để lan truyền và tổng hợp thông tin giữa các nút trong đồ thị, tương ứng với các tài khoản trong hệ thống giao dịch. Thông qua quá trình lan truyền này, biểu diễn đặc trưng của mỗi nút được cập nhật dựa trên thông tin của các nút lân cận, từ đó nắm bắt được ngữ cảnh toàn cục trong mạng lưới giao dịch. Biểu diễn của các cạnh (giao dịch) sau đó được xây dựng từ các đặc trưng của các nút đầu và cuối của mỗi cạnh, kết hợp với thông tin đặc trưng ban đầu của giao dịch.

**Contrastive Prototype Learning:**

Sau khi thu được biểu diễn đặc trưng cho mỗi giao dịch, mô hình áp dụng cơ chế học tương phản nguyên mẫu (contrastive prototype learning) để tăng cường khả năng phân biệt giữa các loại hành vi giao dịch. Cụ thể, hai prototype – một cho các giao dịch bình thường và một cho các giao dịch gian lận – được học đồng thời trong quá trình huấn luyện. Mục tiêu của bước này là làm cho biểu diễn của các giao dịch cùng loại tiến gần đến prototype tương ứng và cách xa prototype còn lại trong không gian đặc trưng.

**Cosine Similarity:**

Để đo lường mức độ tương đồng giữa một giao dịch cụ thể và hai prototype đã học, mô hình sử dụng hàm cosine similarity. Đây là một chỉ số đo góc giữa hai vector trong không gian đặc trưng, phản ánh mức độ gần gũi về mặt hướng giữa biểu diễn của giao dịch và các prototype. Hai giá trị cosine similarity – tương ứng với prototype của giao dịch bình thường và của giao dịch gian lận – được sử dụng làm đặc trưng đầu vào cho giai đoạn phân loại tiếp theo.

**Classifier:**

Cuối cùng, mô hình sử dụng một bộ phân loại đơn giản, chẳng hạn như một multilayer perceptron (MLP), để dự đoán xác suất một giao dịch là gian lận dựa trên độ tương đồng cosine với hai prototype. Bộ phân loại này được huấn luyện trên các đặc trưng học được, nhằm tối ưu hóa khả năng phân biệt giữa các giao dịch gian lận và hợp lệ. Nhờ vào kiến trúc kết hợp giữa học biểu diễn đồ thị và học tương phản, mô hình đạt được hiệu quả cao trong việc phát hiện các hành vi gian lận trong mạng lưới giao dịch phức tạp.

3.3.3.Huấn luyện

**Mục tiêu huấn luyện:**

Mô hình GCD-GNN được huấn luyện nhằm học cách phân biệt giữa các **giao dịch gian lận (fraud)** và **giao dịch hợp lệ (benign)**. Mỗi cạnh (edge) trong đồ thị đại diện cho một giao dịch và mang nhãn y ∈ {0, 1}:

* 0: giao dịch bình thường (benign)
* 1: giao dịch gian lận (fraud)

**Hàm mất mát (Loss Function):**

Mô hình sử dụng hàm mất mát CrossEntropyLoss – một hàm phổ biến trong bài toán phân loại nhị phân/multi-class. Hàm này đo độ lệch giữa xác suất đầu ra của mô hình và nhãn thật:

Trong đó:

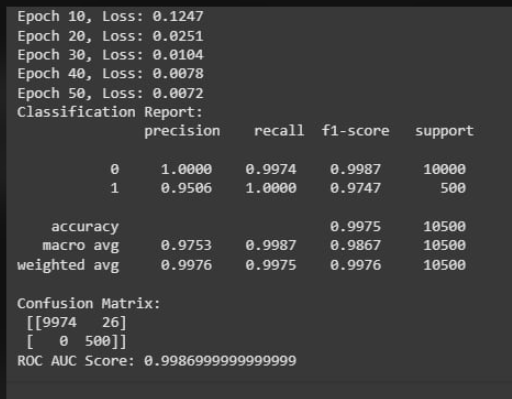
là nhã thật của mẫu thứ 1 (0 hoặc 1)

: là xác suất dự đoán của mô hình cho lớp đó(sau softmax)

Việc tối ưu hóa hàm này giúp mô hình điều chỉnh trọng số để phân loại chính xác hơn.

3.3.4.Đánh giá mô hình

Hình 3.4:Kết quả mô hình phát hiện gian lận



*Nguồn: Nhóm nghiên cứu*

Kết quả mô hình

Mô hình được huấn luyện trên dữ liệu giao dịch với nhãn phân loại gian lận (Fraud) bằng hàm mất mát CrossEntropyLoss, một lựa chọn phổ biến cho các bài toán phân loại nhị phân hoặc đa lớp. Trong quá trình huấn luyện, giá trị loss giảm đều qua các epoch, từ 0.1247 ở epoch 10 xuống còn 0.0072 ở epoch 50. Điều này phản ánh quá trình học của mô hình diễn ra ổn định và hiệu quả, cho thấy mô hình đã học được các đặc trưng phân biệt rõ ràng giữa giao dịch gian lận và hợp lệ.

Kết quả đánh giá mô hình dựa trên nhiều chỉ số khác nhau, bao gồm classification report, confusion matrix và ROC AUC score. Báo cáo phân loại (classification report) cho thấy độ chính xác (precision) của mô hình đối với lớp gian lận đạt 95.06%, trong khi độ hồi tưởng (recall) đạt tuyệt đối 100%. Điều này có nghĩa là mô hình đã dự đoán đúng toàn bộ các giao dịch gian lận trong tập kiểm tra mà không bỏ sót trường hợp nào. Độ đo F1 (F1-score), chỉ số tổng hợp giữa precision và recall, đạt 0.9747 đối với lớp gian lận và 0.9987 đối với lớp bình thường, thể hiện sự cân bằng tốt giữa hai yếu tố. Độ chính xác tổng thể (accuracy) của mô hình đạt 99.75%, phản ánh khả năng phân loại chính xác của mô hình trên toàn bộ tập dữ liệu.

Ma trận nhầm lẫn (confusion matrix) cung cấp cái nhìn trực quan hơn về kết quả phân loại. Trong số 10.500 giao dịch kiểm tra, chỉ có 26 giao dịch hợp lệ bị dự đoán nhầm là gian lận, trong khi tất cả 500 giao dịch gian lận đều được nhận diện chính xác. Điều này cho thấy mô hình có tỷ lệ false positive (cảnh báo nhầm) rất thấp và không có false negative (bỏ sót gian lận), điều rất quan trọng trong các ứng dụng thực tế, đặc biệt trong lĩnh vực tài chính và chống gian lận.

Cuối cùng, chỉ số ROC AUC (Receiver Operating Characteristic - Area Under Curve) đạt 0.9986, gần như tiệm cận với giá trị tối đa 1.0. Chỉ số này phản ánh năng lực tổng thể của mô hình trong việc phân biệt hai lớp ở các ngưỡng phân loại khác nhau. Một AUC cao như vậy chứng minh rằng mô hình duy trì hiệu suất phân biệt tốt giữa giao dịch hợp lệ và gian lận, ngay cả khi ngưỡng phân loại thay đổi.

Tổng hợp lại, các chỉ số đánh giá đều cho thấy mô hình phát hiện gian lận giao dịch dựa trên GCD-GNN không chỉ đạt hiệu suất rất cao mà còn đáng tin cậy trong môi trường thực tế, nơi yêu cầu phát hiện chính xác và kịp thời các hành vi bất thường. Bạn có muốn mình giúp viết phần kết luận hoặc gợi ý hướng mở rộng tiếp theo không?

3.4.Mô hình cá nhân hóa cho sinh viên

Mô hình được kế thừa từ mô hình tổng quan tận dụng các ngưỡng từ FraudGuard-General để cải thiện hiệu quả trên tập dữ liệu mới, đồng thời điều chỉnh mô hình phù hợp với hành vi giao dịch đặc trưng của sinh viên.

**Việc có dữ liệu thực tế từ thế giới thật là yếu tố then chốt quyết định độ tin cậy và độ chính xác của các thuật toán học máy** (Husejinovic, 2020).

TIỂU KẾT CHƯƠNG III

Chương III đã trình bày chi tiết quy trình nghiên cứu từ khâu thu thập dữ liệu đến xây dựng và huấn luyện mô hình phát hiện gian lận giao dịch cá nhân hóa. Bộ dữ liệu được thu thập từ các giao dịch thực tế của sinh viên tại Hà Nội, với hơn 11.000 bản ghi mô tả đầy đủ các thông tin tài chính. Dữ liệu này được tiền xử lý và chuyển đổi thành cấu trúc đồ thị, nơi các tài khoản là các nút và giao dịch là các cạnh có hướng. Mô hình GCD-GNN được lựa chọn nhờ khả năng kết hợp thông tin cục bộ và toàn cục trong mạng lưới giao dịch. Mô hình sử dụng nhiều kỹ thuật như học biểu diễn đồ thị, học tương phản nguyên mẫu và độ tương đồng cosine để tăng độ chính xác. Quá trình huấn luyện cho thấy mô hình đạt độ chính xác rất cao, với recall 100% và AUC gần 1.0. Việc đánh giá qua classification report và confusion matrix khẳng định hiệu suất phát hiện gian lận mạnh mẽ của hệ thống. Ngoài ra, mô hình được điều chỉnh theo hướng cá nhân hóa nhằm thích ứng tốt hơn với hành vi tài chính của nhóm người dùng cụ thể là sinh viên. Cách tiếp cận này giúp phát hiện hiệu quả các hành vi bất thường tinh vi mà mô hình tổng quát dễ bỏ sót. Nhìn chung, chương III đã đặt nền móng quan trọng cho việc triển khai mô hình trong môi trường thực tế.

CHƯƠNG IV. MÔ HÌNH BẢO MẬT TRONG MOBILE BANKING

4.1.Tổng quan mô hình bảo mật trong MOBILE BANKING

Mô hình bảo mật được đề xuất trong nghiên cứu này tập trung vào việc tích hợp các phương pháp xác thực đa tầng, sử dụng các công nghệ hiện đại như mã định danh thiết bị (IMEI), xác thực qua thẻ căn cước công dân gắn chip (CCCD), và ứng dụng VneID và kết hợp với xác thực truyền thống(mã PIN, smart OTP). Các phương pháp này không chỉ tăng cường độ an toàn mà còn đảm bảo tính khả thi trong việc triển khai thực tế.

**Smart OTP** (One-Time Password thông minh) là một phương thức xác thực tiên tiến, trong đó mã OTP được tạo ngẫu nhiên ngay trên thiết bị của người dùng thông qua các thuật toán mã hóa, không phụ thuộc vào kết nối mạng hoặc tin nhắn SMS. Phương pháp này nâng cao tính bảo mật và giảm thiểu rủi ro bị đánh cắp mã OTP qua các hình thức tấn công như phishing hoặc SIM swapping. Theo nghiên cứu của Homoliak và cộng sự (2018), Smart OTP sử dụng cấu trúc cây Merkle và chuỗi băm để tạo ra các mã OTP ngắn, cho phép xác thực hai yếu tố mà không cần kết nối mạng, đồng thời tăng cường khả năng chống lại các cuộc tấn công mạng.

**Mã PIN (Personal Identification Number)** là một chuỗi số được sử dụng rộng rãi như một phương thức xác thực trong các hệ thống bảo mật, bao gồm rút tiền tại máy ATM, mở khóa thiết bị di động và truy cập vào các dịch vụ ngân hàng trực tuyến. Theo tiêu chuẩn ISO 9564, mã PIN phải được quản lý và bảo vệ nghiêm ngặt, bao gồm việc mã hóa trong quá trình truyền tải và lưu trữ, nhằm đảm bảo tính bảo mật và ngăn chặn truy cập trái phép.

**IMEI (International Mobile Equipment Identity)** là một mã số định danh duy nhất gồm 15 chữ số được gán cho mỗi thiết bị di động, đóng vai trò quan trọng trong việc xác thực và bảo mật thiết bị trong các hệ thống ngân hàng số. Sử dụng IMEI trong xác thực người dùng giúp đảm bảo rằng các giao dịch tài chính chỉ được thực hiện từ các thiết bị đã được đăng ký trước đó, từ đó giảm thiểu nguy cơ gian lận và truy cập trái phép.Theo nghiên cứu của Hammood và cộng sự (2020), việc tích hợp IMEI vào mô hình xác thực người dùng trong hệ thống ngân hàng trực tuyến mang lại một lớp bảo mật bổ sung, đặc biệt hữu ích trong việc ngăn chặn các cuộc tấn công như giả mạo thiết bị hoặc sao chép SIM. Tuy nhiên, nghiên cứu cũng chỉ ra rằng hầu hết các mô hình xác thực hiện tại vẫn chưa tận dụng đầy đủ tiềm năng của IMEI trong việc tăng cường bảo mật.

**Căn cước công dân gắn chip (CCCD gắn chip)** là một loại thẻ định danh điện tử hiện đại, tích hợp chip lưu trữ thông tin cá nhân và dữ liệu sinh trắc học như vân tay, khuôn mặt. Trong lĩnh vực ngân hàng, CCCD gắn chip được sử dụng như một phương thức xác thực mạnh mẽ, giúp nâng cao độ chính xác và an toàn trong các giao dịch tài chính

Theo Công văn số 7262/NHNN-TT của Ngân hàng Nhà nước Việt Nam, các tổ chức tín dụng được khuyến khích tích hợp thư viện nhúng (SDK) vào ứng dụng ngân hàng di động để đối chiếu, xác thực thông tin lưu trữ trên CCCD gắn chip với dữ liệu khách hàng. Ngoài ra, việc sử dụng thiết bị chuyên dụng đọc dữ liệu CCCD gắn chip tại quầy giao dịch và kết nối với nền tảng Cơ sở dữ liệu quốc gia về dân cư (CSDLQGvDC) cũng được đề xuất nhằm xác thực khách hàng một cách chính xác và nhanh chóng.

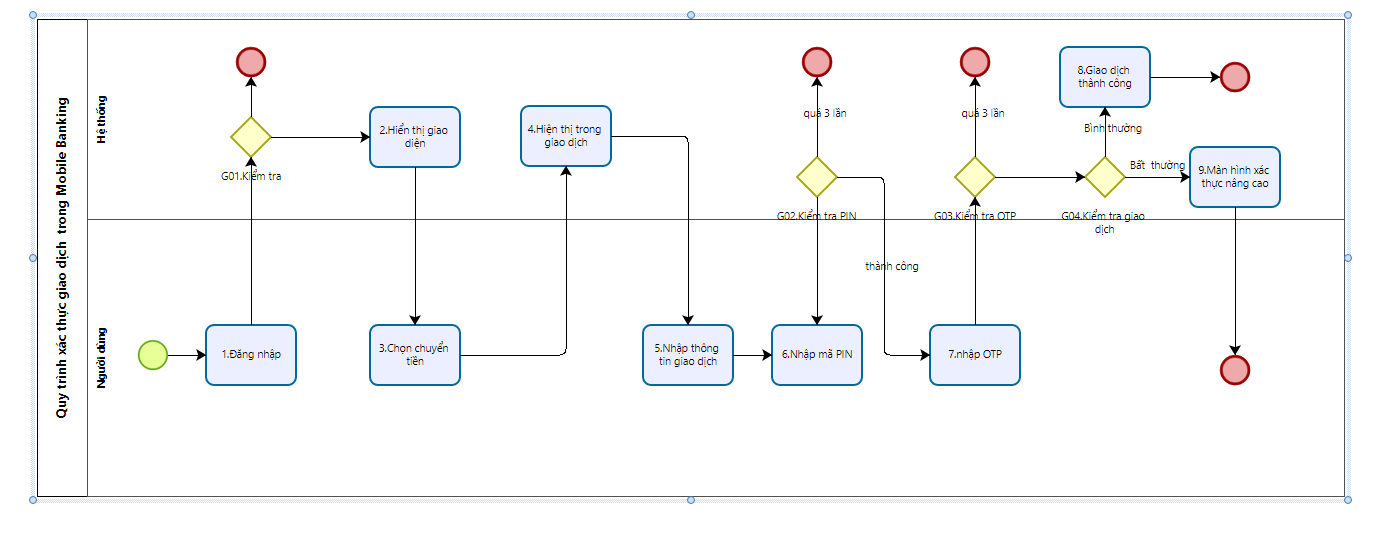
Thực tế, nhiều ngân hàng tại Việt Nam đã triển khai xác thực khách hàng thông qua CCCD gắn chip. Theo báo cáo, đến thời điểm hiện tại, đã có 60 tổ chức tín dụng triển khai xác thực khách hàng thông qua CCCD gắn chip tại quầy, 49 tổ chức tín dụng thực hiện xác thực CCCD gắn chip qua ứng dụng trên thiết bị di động, và 22 đơn vị tham gia triển khai ứng dụng Định danh và xác thực điện tử công dân (VNeID).

Việc sử dụng CCCD gắn chip trong giao dịch ngân hàng không chỉ giúp xác thực danh tính khách hàng một cách chính xác mà còn góp phần giảm thiểu rủi ro gian lận, lừa đảo trong các giao dịch tài chính. Đồng thời, nó cũng tạo điều kiện thuận lợi cho khách hàng trong việc thực hiện các giao dịch trực tuyến một cách an toàn và tiện lợi hơn.

**VNeID** là ứng dụng định danh điện tử quốc gia do Trung tâm Dữ liệu quốc gia về dân cư – Bộ Công an Việt Nam phát triển. Ứng dụng này được xây dựng trên nền tảng cơ sở dữ liệu về định danh, dân cư và xác thực điện tử, nhằm cung cấp các tiện ích phát triển công dân số, chính phủ số và xã hội số.

4.2. Quy trình giao dịch trên Mobile Banking

Hình 4.1: Quy trình giao dịch trong Mobile Banking



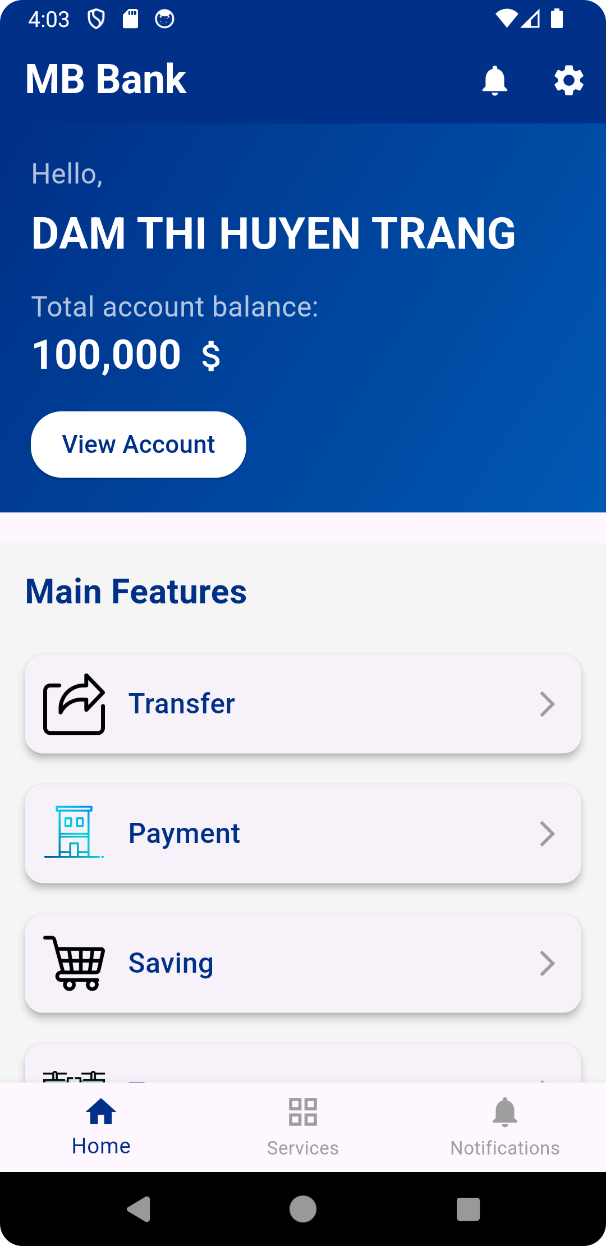
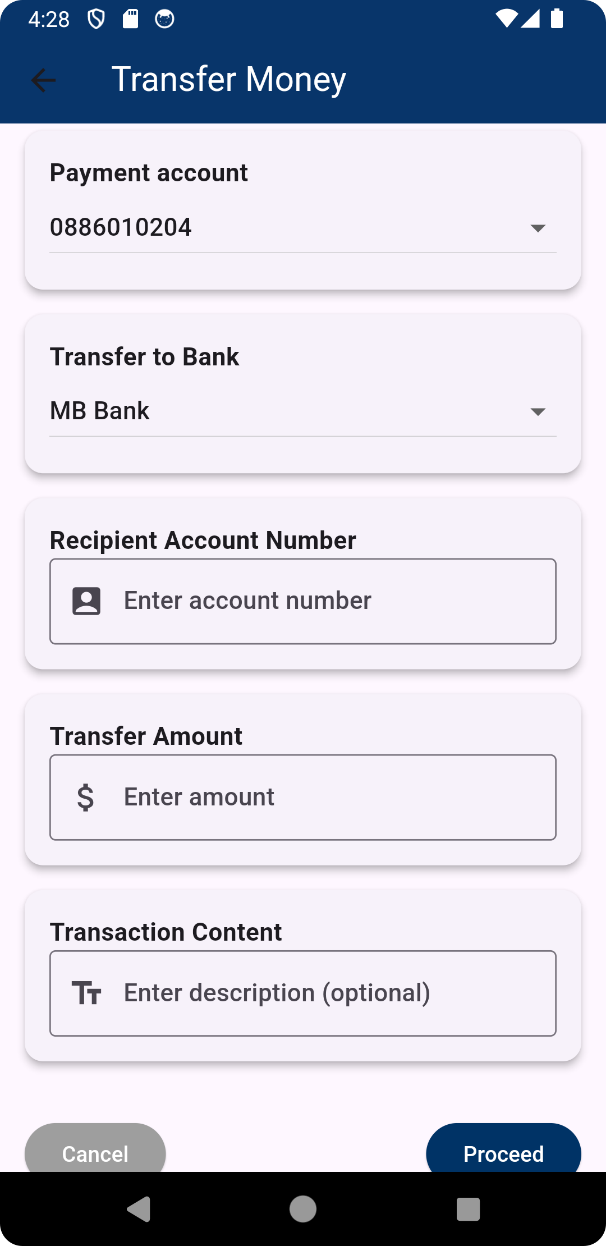
*Nguồn: Nhóm nghiên cứu*

Bảng 4.1: Bảng quy trình xác thực giao dịch trong Mobile Banking

|  |  |  |
| --- | --- | --- |
| **STT** | **Nghiệp vụ** | **Mô tả nghiệp vụ** |
| 1 | Đăng nhập | Người dùng đăng nhập vào ứng dụng Mobile Banking. |
| 2 | Hiển thị giao diện | Hệ thống kiểm tra và hiển thị giao diện chính nếu đăng nhập hợp lệ. |
| 3 | Chọn chuyển tiền | Người dùng chọn chức năng chuyển tiền trong giao diện. |
| 4 | Hiển thị trong giao dịch | Hệ thống hiển thị giao diện thực hiện giao dịch. |
| 5 | Nhập thông tin giao dịch | Người dùng điền thông tin người nhận và số tiền chuyển. |
| 6 | Nhập mã PIN | Người dùng nhập mã PIN để xác nhận giao dịch. |
| 7 | Nhập OTP | Sau khi xác thực PIN thành công, người dùng nhập mã OTP được gửi đến. |
| 8 | Giao dịch thành công | Nếu xác thực OTP hợp lệ và giao dịch bình thường, giao dịch hoàn tất. |
| 9 | Màn hình xác thực nâng cao | Nếu giao dịch bất thường, chuyển sang bước xác thực nâng cao. |
| 10 | Kết thúc | Quy trình kết thúc với trạng thái thành công hoặc thất bại. |

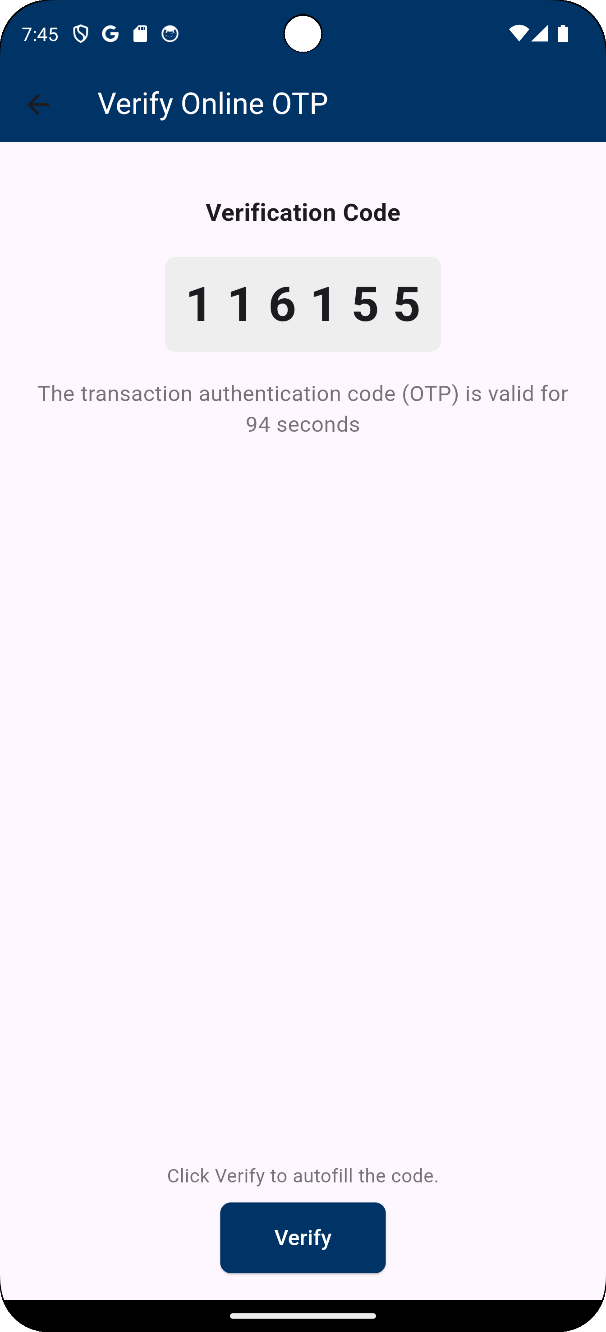
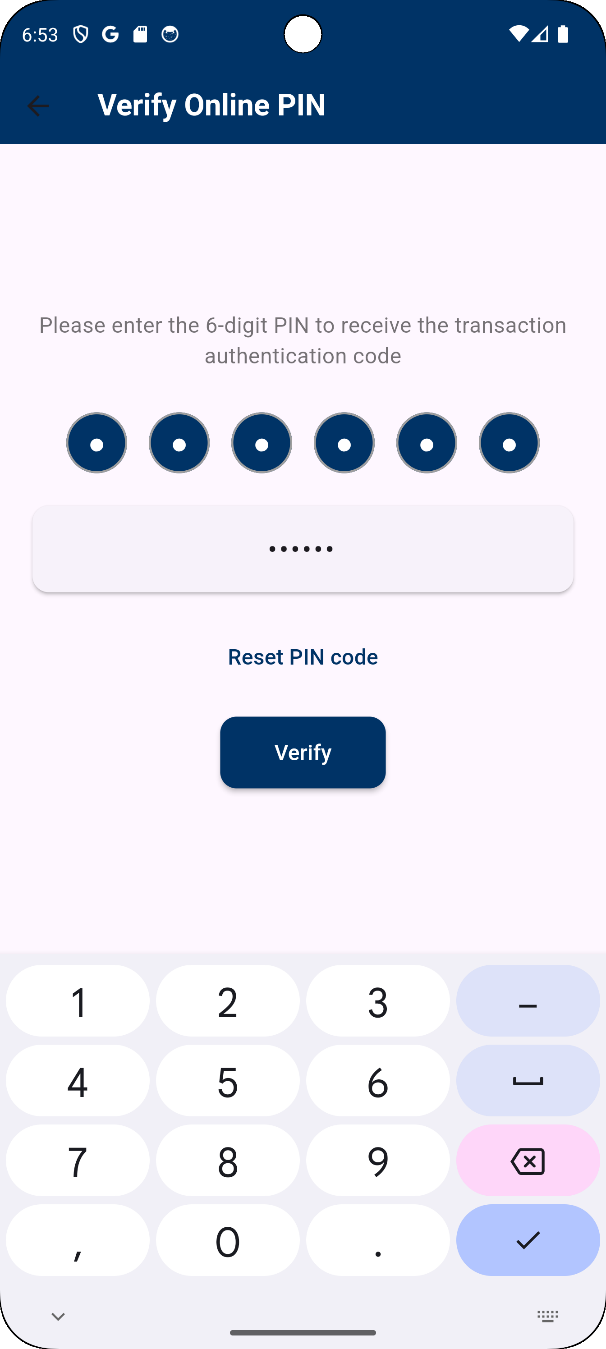
Đây là quy trình nghiệp vụ được xây dựng dựa trên việc tổng hợp từ các quy trình thực tế đang được áp dụng tại nhiều ngân hàng ở Việt Nam, kết hợp với những cải tiến do nhóm nghiên cứu đề xuất. Mục tiêu của việc xây dựng quy trình này là nhằm nâng cao trải nghiệm người dùng, đảm bảo tính chính xác và bảo mật trong từng bước thực hiện giao dịch trên ứng dụng Mobile Banking, đồng thời tăng khả năng phát hiện và ngăn chặn các hành vi gian lận phát sinh trong quá trình sử dụng.

Hình 4.2: Trang chủ và màn hình giao dịch

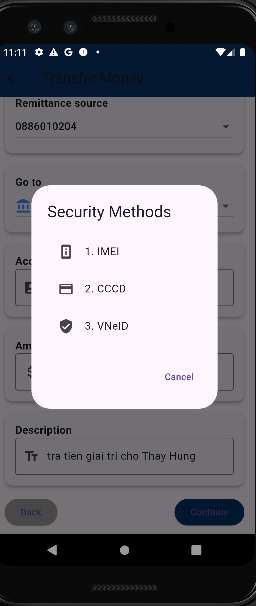
*Nguồn:Nhóm nghiên cứu*

Hình 4.3: Xác thực mã pin và otp



*Nguồn: Nhóm nghiên cứu*

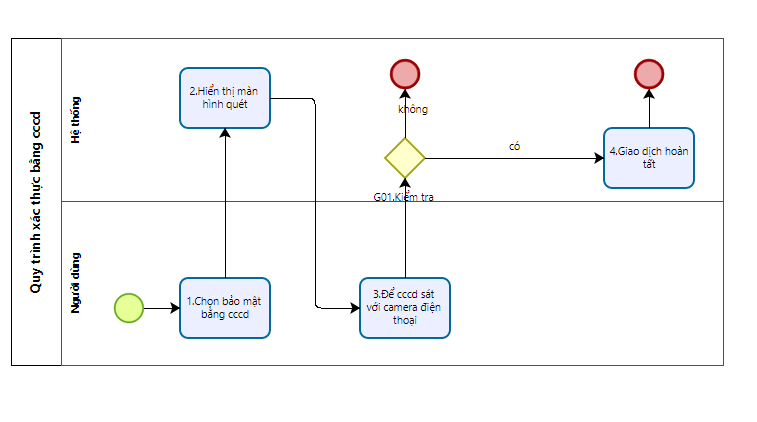
Mô hình xác thực thông minh tích hợp nhiều lớp bảo mật như mã PIN, mã OTP và các công nghệ học máy để tự động nhận diện hành vi bất thường trong giao dịch. Mô hình không chỉ đảm bảo độ an toàn cao mà còn tối ưu trải nghiệm người dùng trong quá trình xác thực trên nền tảng Mobile Banking.



Hình 4.4: Màn hình lựa chọn xác thực khi có giao dịch bất thường

### ***4.2.1.Quy trình xác thực bằng CCCD***

Hình 4.5: Quy trình xác thực bằng cccd

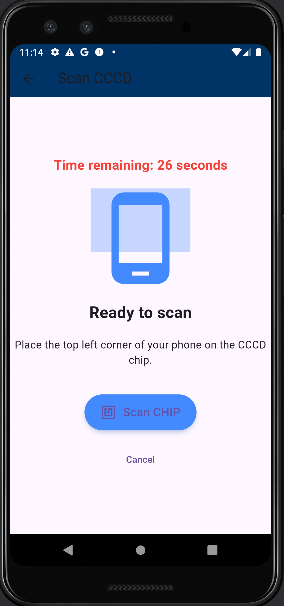


*Nguồn: Nhóm nghiên cứu*

Bảng 4.2 :Bảng Quy trình xác thực bằng cccd

|  |  |  |
| --- | --- | --- |
| **STT** | **Nghiệp vụ** | **Mô tả nghiệp vụ** |
| 1 | Chọn bảo mật bằng CCCD | Người dùng chọn phương thức bảo mật bằng CCCD. |
| 2 | Hiển thị màn hình quét | Hệ thống hiển thị giao diện cho phép quét CCCD. |
| 3 | Để CCCD sát với camera điện thoại | Người dùng đưa CCCD lại gần camera điện thoại để quét. |
| 4 | Kiểm tra | Hệ thống kiểm tra dữ liệu từ CCCD. |
| 5 | Giao dịch hoàn tất | Nếu CCCD hợp lệ, hệ thống xác thực và hoàn tất giao dịch. |
| 6 | Kết thúc | Kết thúc quy trình (thành công hoặc thất bại tùy kết quả kiểm tra). |

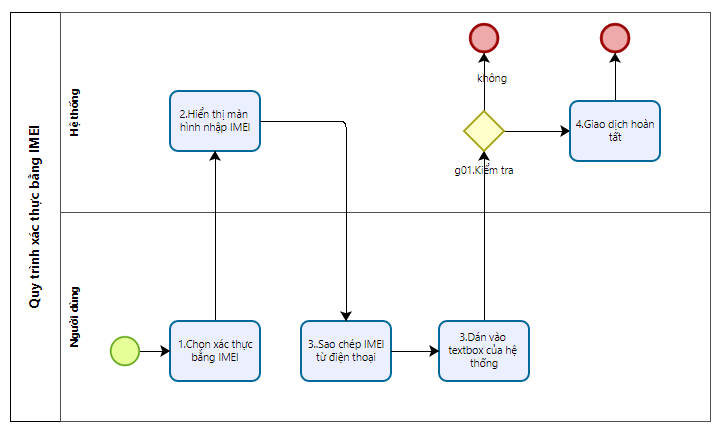
Giao diện hiển thị trên thiết bị di động là màn hình xác thực bằng CCCD gắn chip. Màn hình hiển thị thông báo “Ready to scan” kèm theo hướng dẫn cụ thể: người dùng cần đặt góc trên bên trái của điện thoại lên vị trí chip trên thẻ CCCD để hệ thống bắt đầu quá trình quét dữ liệu. Phía trên giao diện có đồng hồ đếm ngược thời gian còn lại (Time remaining), giúp người dùng chủ động trong thao tác. Nút chức năng chính “Scan CHIP” được bố trí nổi bật ở giữa màn hình, bên dưới là nút “Cancel” cho phép người dùng huỷ thao tác nếu cần thiết. Thiết kế giao diện đơn giản, trực quan và thân thiện với người dùng, đảm bảo hỗ trợ hiệu quả cho quá trình xác thực sinh trắc học bằng CCCD.



Hình 4.6: Màn hình xác thực cccd

4.2.2.Quy trình xác thực bằng IMEI

Hình 4.7: Quy trình xác thực bằng IMEI

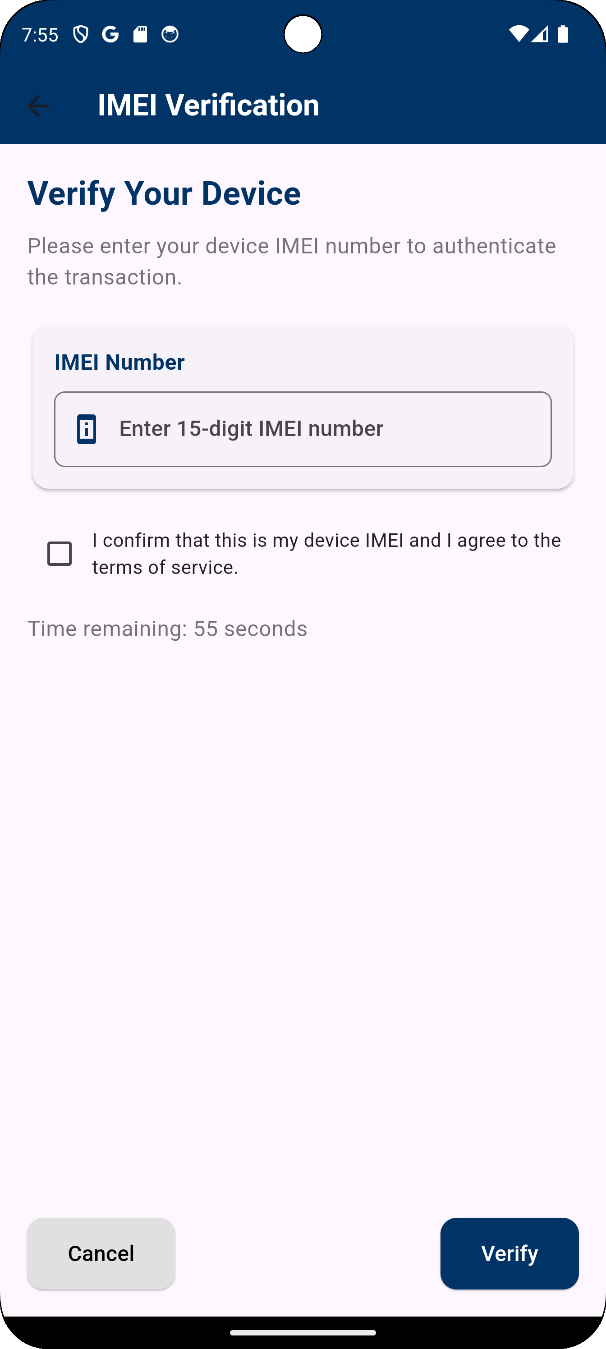


*Nguồn: Nhóm nghiên cứu*

Bảng 4.3:Bảng Quy trình xác thực bằng IMB

|  |  |  |
| --- | --- | --- |
| STT | Nghiệp vụ | Mô tả nghiệp vụ |
| 1 | Chọn xác thực bằng IMEI | Người dùng chọn phương thức xác thực bằng IMEI. |
| 2 | Hiển thị màn hình nhập IMEI | Hệ thống hiển thị giao diện để người dùng nhập IMEI. |
| 3 | Sao chép IMEI từ điện thoại | Người dùng sao chép IMEI từ thiết bị của mình. |
| 4 | Dán vào textbox của hệ thống | Người dùng dán IMEI đã sao chép vào ô nhập của hệ thống. |
| 5 | Kiểm tra | Hệ thống kiểm tra tính hợp lệ của IMEI. |
| 6 | Giao dịch hoàn tất | Nếu IMEI hợp lệ, hệ thống hoàn tất quá trình xác thực. |
| 7 | Kết thúc | Kết thúc quy trình (có thể là thành công hoặc không thành công). |

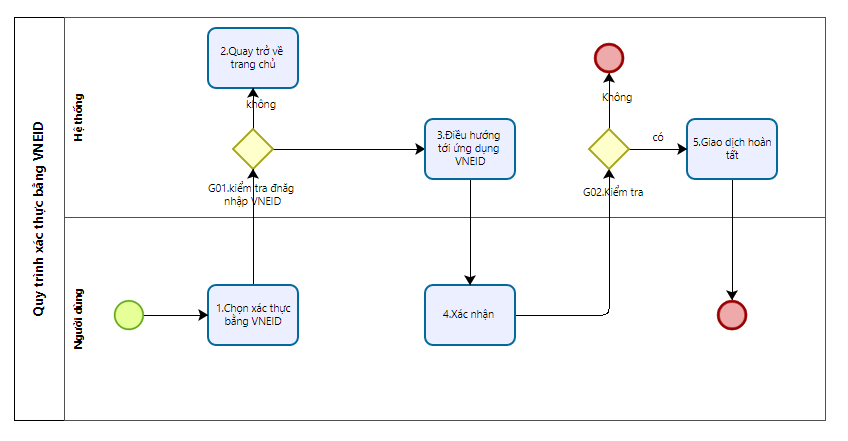
Giao diện thể hiện bước xác thực thiết bị thông qua số IMEI nhằm tăng cường độ tin cậy cho giao dịch tài chính. Trên màn hình, người dùng được yêu cầu nhập số IMEI gồm 15 chữ số vào khung nhập liệu có biểu tượng minh họa bên trái. Bên dưới, có một hộp kiểm xác nhận rằng người dùng đồng ý với điều khoản dịch vụ và xác nhận đây là thiết bị của họ. Đồng thời, hệ thống hiển thị thời gian đếm ngược còn lại (Time remaining) để hoàn tất bước xác thực, tạo cảm giác cấp bách nhưng kiểm soát được. Hai nút chức năng “Cancel” và “Verify” được bố trí rõ ràng ở cuối màn hình, giúp người dùng dễ dàng thao tác. Giao diện được thiết kế đơn giản, trực quan, giúp đảm bảo an toàn giao dịch mà không gây khó khăn cho người sử dụng.



Hình 4.8: Màn hình xác thực imei

4.2.3.Quy trình xác thực bằng VNEID

Hình 4.9: Quy trình xác thực bằng VNEID

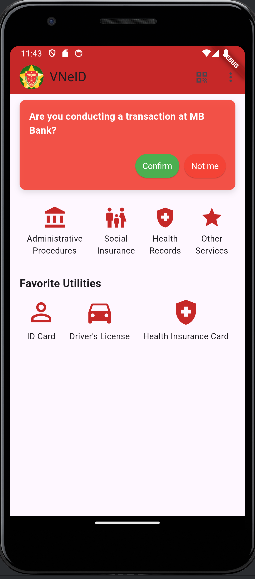


*Nguồn: Nhóm nghiên cứu*

Bảng 4.4: Bảng quy trình xác thực bằng VNEID

|  |  |  |
| --- | --- | --- |
| STT | Nghiệp vụ | Mô tả nghiệp vụ |
| 1 | Chọn xác thực bằng VNEID | Người dùng chọn phương thức xác thực bằng ứng dụng VNEID. |
| 2 | Quay trở về trang chủ | Nếu không đăng nhập VNEID, hệ thống sẽ quay về trang chủ. |
| 3 | Điều hướng tới ứng dụng VNEID | Hệ thống chuyển hướng người dùng đến ứng dụng VNEID. |
| 4 | Xác nhận | Người dùng thực hiện xác nhận trong ứng dụng VNEID. |
| 5 | Kiểm tra | Hệ thống kiểm tra kết quả xác thực từ VNEID. |
| 6 | Giao dịch hoàn tất | Nếu xác thực thành công, hệ thống hoàn tất giao dịch. |
| 7 | Kết thúc | Kết thúc quy trình (thành công hoặc thất bại). |

Giao diện ứng dụng VNeID hiển thị thông báo xác thực giao dịch khi có yêu cầu thực hiện từ hệ thống ngân hàng. Ở phần trên màn hình, một hộp thoại nổi bật với câu hỏi **“Are you conducting a transaction at MB Bank?”** được hiển thị, kèm hai lựa chọn: **“Confirm”** (xác nhận) và **“Not me”** (không phải tôi). Đây là bước xác minh chủ động nhằm đảm bảo rằng chính người dùng đang thực hiện giao dịch, giúp ngăn chặn các hành vi truy cập trái phép.



Hình 4.10: Màn hình xác thực bằng VNEID

4.3. Đánh giá mô hình bảo mật

4.3.1.Đánh giá hiệu quả bảo mật

**Ưu điểm**

**Tăng cường bảo mật đa tầng**: Việc yêu cầu xác thực bổ sung ngoài PIN và OTP tạo ra một lớp bảo vệ thứ ba, làm tăng độ khó cho các hành vi gian lận. Các phương pháp như CCCD gắn chip và VNeID sử dụng dữ liệu sinh trắc học, vốn có độ an toàn cao và khó giả mạo. Các hệ thống bảo mật đa tầng giúp nâng cao khả năng bảo vệ dữ liệu nhờ vào việc kết hợp nhiều yếu tố xác thực khác nhau. Theo một nghiên cứu của Bonneau et al. (2012), bảo mật đa yếu tố (MFA) mang lại sự bảo vệ mạnh mẽ hơn so với các phương pháp xác thực đơn giản như chỉ sử dụng mật khẩu hoặc OTP, đặc biệt là khi các yếu tố bổ sung có tính sinh trắc học (ví dụ: vân tay, nhận diện khuôn mặt) (Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F., 2012).

**Phát hiện và ngăn chặn giao dịch bất thường**: Mô hình tập trung vào các giao dịch bất thường (ví dụ: giá trị giao dịch cao bất thường, tài khoản thụ hưởng lạ), giúp giảm thiểu rủi ro từ các hành vi đánh cắp tài khoản hoặc sử dụng thiết bị không đáng tin cậy. Việc phát hiện các giao dịch bất thường là một phần quan trọng trong hệ thống bảo mật tài chính. Theo một nghiên cứu của Bhattacharyya et al. (2011), các mô hình học máy có thể phát hiện các hành vi gian lận trong các giao dịch ngân hàng, bằng cách phân tích các đặc điểm giao dịch bất thường như số tiền giao dịch cao bất thường hoặc các tài khoản thụ hưởng không rõ ràng. Các phương pháp này làm giảm khả năng bị tấn công và bảo vệ người dùng khỏi các rủi ro tài chính (Bhattacharyya, S., Jha, S., & Ravi, S., 2011).

**Linh hoạt trong xác thực**: Cho phép người dùng chọn một trong ba phương pháp (CCCD, VNeID, IMEI) giúp đảm bảo rằng mô hình vẫn hiệu quả ngay cả khi người dùng không có đầy đủ điều kiện cho một phương pháp cụ thể (ví dụ: thiếu thiết bị hỗ trợ NFC). Việc cho phép người dùng lựa chọn phương pháp xác thực có thể giúp hệ thống bảo mật linh hoạt hơn và dễ tiếp cận hơn đối với nhiều người dùng khác nhau. Theo một nghiên cứu của Arora et al. (2014), việc sử dụng nhiều phương pháp xác thực có thể giúp nâng cao khả năng sử dụng của hệ thống và giảm thiểu rủi ro cho người dùng trong các trường hợp họ không có đầy đủ thiết bị hỗ trợ cho một phương thức cụ thể (Arora, A., Doshi, D., & Patel, P., 2014).

**Hạn chế**

**Phụ thuộc vào thiết bị và hạ tầng**: Việc xác thực qua CCCD yêu cầu thiết bị hỗ trợ NFC – một tính năng chưa phổ biến ở một số dòng smartphone giá rẻ hoặc đời cũ. Ngoài ra, ứng dụng VNeID yêu cầu người dùng phải cài đặt và kích hoạt thành công, trong khi điều này có thể bị cản trở bởi vấn đề hạ tầng, kiến thức kỹ thuật, hoặc khu vực mạng yếu. Theo nghiên cứu của Bhargav-Spantzel et al. (2007), hệ thống xác thực dựa trên phần cứng thường đối mặt với thách thức về khả năng tiếp cận người dùng do sự phụ thuộc vào thiết bị đầu cuối và tính đồng nhất của hạ tầng.

**Rủi ro từ phương pháp IMEI**: IMEI, mặc dù là mã định danh duy nhất của thiết bị, có thể bị giả mạo bởi các công cụ phần mềm trên thiết bị đã root hoặc bị nhiễm mã độc. Theo một nghiên cứu của Conti et al. (2016), các phương pháp xác thực dựa vào thông tin phần cứng như IMEI dễ bị tấn công nếu thiết bị bị root hoặc cài đặt phần mềm độc hại, khiến tin tặc có thể thay đổi hoặc giả mạo thông tin xác thực.

**Khả năng bypass xác thực**: Nếu một tin tặc đã chiếm được quyền kiểm soát toàn phần thiết bị (ví dụ: thông qua phần mềm độc hại hoặc tấn công phishing), thì ngay cả các phương pháp xác thực nâng cao như CCCD gắn chip hay VNeID cũng có thể bị vượt qua. Theo nghiên cứu của Alasmary et al. (2020), các cuộc tấn công nâng cao như *device takeover* hoặc *credential stuffing* có thể làm mất hiệu lực của các lớp bảo mật nếu không có cơ chế xác minh hành vi hoặc thiết bị đáng tin cậy.

4.3.2.Đánh giá tính khả thi triển khai

**Ưu điểm**

**Tận dụng hạ tầng sẵn có**: Tại Việt Nam, việc triển khai đồng bộ CCCD gắn chip và ứng dụng VNeID bởi Bộ Công an đã tạo nền tảng pháp lý và kỹ thuật để tích hợp các phương pháp xác thực vào dịch vụ ngân hàng số. Điều này giúp tiết kiệm chi phí triển khai và nâng cao khả năng ứng dụng thực tế. Theo báo cáo của UNDP (2023), các hệ thống định danh quốc gia số giúp cải thiện hiệu quả trong việc cung cấp dịch vụ công và tài chính, nhất là tại các nước đang phát triển nơi chính phủ có vai trò chủ đạo trong quản lý dữ liệu định danh.

**Khả năng mở rộng**: Việc sử dụng API để kết nối với hệ thống định danh như VNeID hoặc cơ sở dữ liệu CCCD là xu hướng phổ biến nhằm mở rộng quy mô xác thực an toàn. Nghiên cứu của Patel et al. (2021) chỉ ra rằng hệ thống xác thực có thể mở rộng tốt nếu được xây dựng trên kiến trúc dịch vụ (API-first), từ đó dễ dàng tích hợp vào các nền tảng Mobile Banking hiện có..

**Tính linh hoạt**: Việc cho phép người dùng chọn một trong ba phương pháp giúp mô hình phù hợp với nhiều đối tượng khách hàng, từ những người sử dụng thiết bị cơ bản đến những người sở hữu điện thoại thông minh cao cấp.

**Hạn chế**

**Chi phí phát triển và bảo trì**: Việc phát triển hệ thống xác thực tích hợp nhiều phương thức yêu cầu ngân hàng đầu tư đáng kể vào kỹ thuật phần mềm, bảo mật hệ thống, tích hợp với hệ thống công của nhà nước (như VNeID, cơ sở dữ liệu CCCD). Theo báo cáo của World Bank (2019), các hệ thống định danh số và xác thực đa yếu tố thường đòi hỏi ngân sách lớn để đảm bảo tính liên kết, bảo mật, cũng như duy trì hoạt động liên tục.

**Hạn chế về thiết bị**: Không phải tất cả người dùng đều có thiết bị hỗ trợ NFC (để quét CCCD) hoặc đã kích hoạt VNeID. Điều này có thể làm giảm khả năng tiếp cận của mô hình, đặc biệt ở các khu vực nông thôn hoặc với người dùng lớn tuổi. Theo nghiên cứu của GSMA (2022), tỷ lệ phổ cập smartphone hỗ trợ công nghệ mới ở các quốc gia đang phát triển còn thấp, đặc biệt ở nhóm người dùng thu nhập thấp hoặc người cao tuổi.

**Thời gian xử lý giao dịch**: Việc bổ sung một lớp xác thực có thể làm tăng thời gian hoàn thành giao dịch, đặc biệt nếu người dùng chọn phương pháp phức tạp như quét CCCD hoặc xác thực qua VNeID. . Theo Li & Xue (2019), hệ thống xác thực phức tạp có thể làm giảm sự hài lòng của người dùng nếu không được tối ưu hóa tốt về tốc độ xử lý và giao diện thân thiện.

4.4.Giải pháp

**Đào tạo và tuyên truyền**: Tổ chức các chương trình hướng dẫn người dùng về cách sử dụng CCCD gắn chip và VNeID trong Mobile Banking. Cung cấp video hướng dẫn hoặc hỗ trợ trực tiếp tại các chi nhánh ngân hàng.

Việc cung cấp tài liệu hướng dẫn và hỗ trợ trực tiếp giúp người dùng tiếp cận dễ dàng hơn với công nghệ xác thực mới. Theo nghiên cứu của Kumar et al. (2020), thành công của các hệ thống công nghệ trong dịch vụ công phụ thuộc lớn vào khả năng phổ biến kiến thức kỹ thuật tới người dùng, đặc biệt là nhóm không quen thuộc với công nghệ.

**Phương án dự phòng**: Đối với người dùng không thể sử dụng CCCD hoặc VNeID, hệ thống có thể cung cấp các phương pháp xác thực thay thế, như câu hỏi bảo mật hoặc OTP qua SMS, để đảm bảo tính bao quát. Theo nghiên cứu của Aloul (2009), hệ thống xác thực hiệu quả cần kết hợp giữa bảo mật và tính tiện dụng, đặc biệt đối với người dùng có hạn chế thiết bị hoặc vùng phủ sóng yếu.

**Tăng cường bảo mật thiết bị**: Khuyến khích người dùng cài đặt phần mềm bảo mật trên thiết bị và sử dụng các biện pháp bảo vệ như khóa sinh trắc học để giảm nguy cơ xâm phạm. Nghiên cứu của Das et al. (2018) cho thấy việc kết hợp các phương pháp bảo vệ thiết bị với xác thực người dùng sẽ làm giảm đáng kể khả năng tấn công trung gian hoặc giả mạo.

**Hợp tác với cơ quan nhà nước**: Làm việc chặt chẽ với Bộ Công an để đơn giản hóa việc tích hợp VNeID và cơ sở dữ liệu CCCD, đồng thời tối ưu hóa chi phí triển khai.

TIỂU KẾT CHƯƠNG IV

Chương IV đã trình bày mô hình bảo mật đa lớp trong Mobile Banking, kết hợp các yếu tố xác thực mạnh như CCCD gắn chip, VNeID, mã IMEI, mã PIN và Smart OTP nhằm nâng cao độ an toàn cho người dùng. Mô hình này không chỉ đáp ứng yêu cầu bảo mật nghiêm ngặt mà còn đảm bảo tính khả thi khi triển khai trong thực tế, góp phần giảm thiểu rủi ro gian lận và bảo vệ tài sản khách hàng một cách hiệu quả. Từ đó nhìn nhận các ưu điểm và hạn chế để đưa ra giải pháp phù hợp nhất.

# KẾT LUẬN

Nghiên cứu đã làm nổi bật vai trò của học máy và xác thực thông minh trong việc bảo vệ giao dịch Mobile Banking trước nguy cơ gian lận ngày càng tinh vi. Mô hình GCD-GNN, với cơ chế tổng hợp thông tin cục bộ và toàn cục, đã chứng minh khả năng phát hiện gian lận vượt trội, đặc biệt trong môi trường dữ liệu nhãn không đầy đủ. Đồng thời, mô hình bảo mật dựa trên các định danh như IMEI, NVMeID và CCCD cung cấp lớp xác thực thông minh, đảm bảo tính an toàn và minh bạch trong quá trình giao dịch. Mặc dù quy mô dữ liệu thử nghiệm còn hạn chế, các kết quả đạt được mở ra triển vọng lớn. Trong tương lai, việc thu thập dữ liệu giao dịch và định danh quy mô lớn, tích hợp thêm công nghệ AI biometrics, xác thực hành vi, cùng với triển khai thực tế vào hệ thống ngân hàng sẽ nâng cao tính ứng dụng, góp phần xây dựng một hệ sinh thái tài chính an toàn và bền vững.

Đề tài đã khẳng định hiệu quả của việc kết hợp mô hình phát hiện gian lận GCD-GNN và mô hình bảo mật dựa trên IMEI, NVMeID, CCCD trong việc đối phó với các mối đe dọa an ninh trong Mobile Banking. Để tối ưu hóa, cần mở rộng quy mô dữ liệu huấn luyện, bao gồm dữ liệu giao dịch đa dạng từ nhiều thị trường và thông tin định danh từ các nguồn đáng tin cậy. Đối với mô hình bảo mật, việc thu thập thêm dữ liệu về hành vi sử dụng thiết bị (IMEI, NVMeID) và xác minh danh tính (CCCD) sẽ tăng cường khả năng xác thực. Kết hợp với các công nghệ xác thực thông minh như phân tích hành vi và sinh trắc học, cả hai mô hình có thể đạt độ chính xác cao hơn và đáp ứng tốt hơn yêu cầu thực tiễn. Những cải tiến này không chỉ hoàn thiện quy trình bảo mật mà còn đặt nền móng cho các nghiên cứu sâu hơn trong lĩnh vực tài chính – ngân hàng.

Mô hình GCD-GNN và hệ thống bảo mật dựa trên IMEI, NVMeID, CCCD đã mang lại giải pháp toàn diện cho bài toán gian lận và an ninh trong giao dịch Mobile Banking. GCD-GNN cải thiện độ chính xác phát hiện gian lận, trong khi mô hình bảo mật cung cấp lớp xác thực thông minh, đảm bảo tính an toàn từ thiết bị đến danh tính người dùng. Tuy nhiên, để đưa các mô hình này vào ứng dụng thực tiễn, cần khắc phục hạn chế về quy mô dữ liệu bằng cách xây dựng cơ sở dữ liệu lớn về hành vi gian lận và thông tin định danh. Việc tích hợp các công nghệ xác thực tiên tiến như AI biometrics, phân tích hành vi, cùng với triển khai hệ thống giám sát giao dịch thời gian thực, sẽ là bước tiến quan trọng. Nghiên cứu không chỉ đóng góp vào việc nâng cao an ninh tài chính mà còn mở ra hướng phát triển mới cho việc ứng dụng học máy và xác thực thông minh trong kỷ nguyên số.

Nghiên cứu đã chứng minh rằng sự kết hợp giữa mô hình phát hiện gian lận GCD-GNN và mô hình bảo mật dựa trên IMEI, NVMeID, CCCD là chìa khóa để đối phó với các mối đe dọa trong Mobile Banking. Mô hình GCD-GNN mang lại khả năng phát hiện gian lận nhanh chóng và chính xác, trong khi hệ thống bảo mật đảm bảo xác thực đa tầng, từ thiết bị đến danh tính người dùng. Để nâng cao hiệu quả, cần tập trung thu thập dữ liệu giao dịch và định danh từ các nguồn thực tế, đồng thời xây dựng cơ sở dữ liệu lớn về các mẫu hành vi gian lận. Các kiến nghị như tích hợp công nghệ xác thực hành vi, AI biometrics và mở rộng triển khai trên hệ thống ngân hàng trực tuyến sẽ giúp hoàn thiện giải pháp. Với những bước tiến này, nghiên cứu hứa hẹn tạo ra tác động sâu rộng, bảo vệ an toàn tài chính và thúc đẩy sự phát triển của ngành ngân hàng số tại Việt Nam và trên thế giới.

Tài liệu tham khảo

Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., … & Eshun, J. (2023). *A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. Decision Analytics Journal,* 6, 100163. <https://doi.org/10.1016/j.dajour.2023.100163>

Alasmary, W., Alhaidari, F., Alshamrani, A., & Park, J. H. (2020). *Survey on authentication methods for mobile banking applications. Electronics*, 9(9), 1370. https://doi.org/10.3390/electronics9091370

Aloul, F. (2009). Two factor authentication using mobile phones. 2019 IEEE/ACS International Conference on Computer Systems and Applications, 641–644. https://doi.org/10.1109/AICCSA.2009.5069385

Alqudah, N., & Yaseen, Q. (2020). *Machine learning for traffic analysis: A review. Procedia Computer Science*, 170, 911–916.

Arora, A., Doshi, D., & Patel, P. (2014). A comparative analysis of multiple biometric authentication systems. Proceedings of the International Conference on Advances in Computer Science and Engineering, 248-254. https://doi.org/10.1109/ICACSE.2014.55

Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). *Feature engineering strategies for credit card fraud detection. Expert Systems with Applications*, 51, 134–142. https://doi.org/10.1016/j.eswa.2015.12.030

Bank of America. (2025). *Lợi ích và tính năng của Mobile và Online Banking*. https://www.bankofamerica.com/.

Bernard, C. (2021). *Supervised vs. Unsupervised vs. Reinforcement Learning: What’s the Difference?* phData.

Bhattacharyya, S., Jha, S., & Ravi, S. (2011). *Credit card fraud detection using hidden Markov models.* Proceedings of the International Conference on Data Mining, 51-58. https://doi.org/10.1109/ICDM.2011.76

Bhargav-Spantzel, A., Squicciarini, A., & Bertino, E. (2007). Privacy preserving multi-factor authentication with biometrics. *Journal of Computer Security*, 15(5), 529-560. https://doi.org/10.3233/JCS-2007-15502

Biometric Update. (2018). *Mizuho Bank taps Fujitsu solution with Nok Nok Labs authentication suite to secure mobile banking*.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2016). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544-546. https://doi.org/10.1016/j.future.2016.07.060

Costa, I. P. de A., Basílio, M. P., Maêda, S. M. do N., Rodrigues, M. V. G., Moreira, M. Â. L., Gomes, C. F. S., & dos Santos, M. (2021). *Algorithm selection for machine learning classification: An application of the MELCHIOR multicriteria method. Frontiers in Artificial Intelligence and Applications*, 341, 154–161.

Das, A., Borisov, N., & Caesar, M. (2018). *Do you hear what I hear? Fingerprinting smart devices through embedded acoustic components.* ACM Transactions on Privacy and Security (TOPS), 21(3), 1–30. https://doi.org/10.1145/3183343

Digital Savings & Checking. (n.d.). *Mobile và Online Banking*. https://www.wellsfargo.com/mobile-online-banking/.

dos Santos, F. B., & dos Santos, M. (2022). *Choice of armored vehicles on wheels for the Brazilian Marine Corps using PrOPPAGA. Procedia Computer Science*, 199, 301–308.

Dutta, P., Roy, A., & Biswas, M. (2023). *Understanding machine learning concepts. In P. Dutta, A. Roy, & M. Biswas (Eds.), Machine learning techniques for smart city applications: Trends and solutions* (pp. 1–22). IGI Global. https://doi.org/10.4018/978-1-6684-7547-2.ch001

EverBank. (2025). *Mobile Banking, Ngân hàng tiện lợi khi di chuyển*. Truy cập từ https://www.everbank.com/.

Federal Trade Commission. (2025). *Consumer Sentinel Network Data Book 2024*.

Global Anti-Scam Alliance. (2023). *Vietnam Scam Report 2023*.

Goyal, D., & Batra, S. (2011). *Mobile banking in India: Practices, challenges and security issues.*

Goyal, D., & Batra, S. (2011). *Mobile banking in India: Practices, challenges and security issues.*

GSMA. (2022). The Mobile Economy Asia Pacific 2022. GSM Association. https://www.gsma.com/mobileeconomy/

Halvaiee, N. S., & Akbari, M. K. (2014). *A novel model for credit card fraud detection using artificial immune systems. Applied Soft Computing*, 24, 40–49.

Hao, X., & Zhang, Y. (2020). *Research on the effect of security and privacy concerns in mobile banking services. Journal of Risk and Financial Management*, 7(2), 76.

Hiệp hội Ngân hàng Việt Nam. (2023). *Chuyển đổi số ngành ngân hàng và vai trò của trí tuệ nhân tạo*.

Homoliak, I., Breitenbacher, D., Hujnak, O., Hartel, P., Binder, A., & Szalachowski, P. (2020, October). SmartOTPs: An air-gapped 2-factor authentication for smart-contract wallets. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies* (pp. 145-162).

iProov. (2023). Phương pháp xác thực tốt nhất là gì?

Kosinski, M. (2024). What is authentication?.

Ku, L. (2019, July 29). *Tencent’s WeBank applying 'federated learning' in A.I. DigFin.*

*Laukkanen*, T. (2017). *Mobile banking. International Journal of Bank Marketing, 35(7)*, 1042–1043. https://doi.org/10.1108/IJBM-10-2017-0218

Kumar, V., Dixit, A., Javalgi, R. G., & Dass, M. (2020). *Digital service adoption: A customer-centric approach for developing economies.* Journal of Business Research, 116, 362–371. https://doi.org/10.1016/j.jbusres.2020.05.045

LexisNexis Risk Solutions. (2023). *True Cost of Fraud Study: Financial Services & Lending Report.* .

Liu, J., Tian, Y., & Liu, G. (2024). *Global Confidence Degree Based Graph Neural Network for Financial Fraud Detection.*

Li, H., & Xue, Y. (2019). A unified model for understanding secure mobile payment adoption in China: Integrating trust transfer theory and the TAM. Electronic Commerce Research and Applications, 38, 100959. https://doi.org/10.1016/j.elerap.2019.100959

MacGregor, S. (2021). *Japan's Shinsei Bank, Nippon Wealth form business alliance with blockchain startup ConsenSys*.

Mas, I. (n.d.). My PIN is 4321.

MoBShield: *A Novel XML Approach for Securing Mobile Banking*. (2025).

Moreira, M. Â. L., Gomes, C. F. S., dos Santos, M., Basílio, M. P., Costa, I. P. de A., Rocha Junior, C. de S., & Jardim, R. R.-A. J. (2022). *Evaluation of drones for public security: A multicriteria approach by the PROMETHEE-SAPEVO-M1 systematic. Procedia Computer Science*, 199, 125–133.

Mudiri, J. (2023). *Fraud in mobile financial services* (Research Paper No. 151).

Mudiri, J. (2024). *Fraud in mobile financial services [PDF].*

Mudiri, J. (2024). Fraud in mobile financial services. https://www.microsave.net/fr/wp-content/uploads/2024/01/RP151\_Fraud\_in\_Mobile\_Financial\_Services\_JMudiri.pdf

Nguyen, T., Pham, H., Bui, T., & Do, H. (2022). *Enhancing Mobile Banking Security: A Machine Learning Approach Combined with Intelligent Authentication Methods. International Journal of Information Security Science*, 11(4), 250–265.

Ngân hàng Nhà nước Việt Nam. (2020). *Bảo mật thông tin khách hàng khi sử dụng dịch vụ ngân hàng số: Thực trạng và một số kiến nghị*.

Ngân hàng Nhà nước Việt Nam. (2023). *Báo cáo thường niên 2023*. https://sbv.gov.vn/webcenter/ShowProperty?nodeId=/UCMServer/SBV621038//idcPrimaryFile&revision=latestreleased

Ngân hàng Nhà nước Việt Nam. (2024). *Thông tư 15/2024/TT-NHNN: Quy định về cung ứng dịch vụ thanh toán không dùng tiền mặt.* https://thuvienphapluat.vn/van-ban/Tien-te-Ngan-hang/Thong-tu-15-2024-TT-NHNN-cung-ung-dich-vu-thanh-toan-khong-dung-tien-mat-615581.aspx

Nhóm tác giả DTSVN. (2025). *AI và sinh trắc học đang thay đổi 'cuộc chơi' Mobile banking.*

Olowookere, T. A., & Adewale, O. S. (2020). *A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach. Scientific African, 8, e00406*. https://doi.org/10.1016/j.scia.IC2020.e00406

Payer, M., Hartmann, T., & Gross, T. R. (2012, May). Safe loading-a foundation for secure execution of untrusted programs. In *2012 IEEE Symposium on Security and Privacy* (pp. 18-32). IEEE.

Patel, P., Pathak, D., & Joshi, H. (2021). *A review on scalable authentication systems in mobile banking.* International Journal of Computer Applications, 182(15), 20-25. https://doi.org/10.5120/ijca2021921120

Porwal, U., & Mukund, S. (2018). *Credit card fraud detection in e-commerce: An outlier detection approach. arXiv*.

Pousttchi, K., & Schurig, M. (2004). *Đánh giá các ứng dụng mobile banking hiện nay từ góc nhìn yêu cầu của khách hàng. Hội nghị quốc tế Hawaii lần thứ 37 về các khoa học hệ thống.*

Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). *Credit card fraud detection using AdaBoost and majority voting. IEEE Access*, 6, 14277–14284.

Seraj, S., Sadiq, A. S., Kaiwartya, O., Aljaidi, M., Konios, A., Ali, M., & Abazeed, M. (2024). MoBShield: A Novel XML Approach for SecuringMobile Banking. *Computers, Materials & Continua*, *79*(2).

Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. (2008). *Credit Card Fraud Detection Using Hidden Markov Model. IEEE Transactions on Dependable and Secure Computing*, 5(1), 37–48. https://doi.org/10.1109/TDSC.2007.70228

StrongDM. (2024). *Bank of America data breach: What happened and what you need to know*.

Sukma, N. A., & Rahadi, R. A. (2024). *Customer perception towards the use of AI in Indonesia's banking industry: Risk, trust, social influence, digital divide, and regulation perspectives. Journal of Open Innovation: Technology, Market, and Complexity*, 10(2), 100305. https://doi.org/10.1016/j.joitmc.2024.100305

Sở Thông tin và Truyền thông Nam Định. (2020, April 10). *Tăng cường hệ thống cảnh báo bảo mật trên ứng dụng ngân hàng số*.

United Nations Development Programme. (2023). Digital Public Infrastructure for an Equitable Recovery. UNDP Digital Strategy Report. https://www.undp.org/publications/digital-public-infrastructure-equitable-recovery

World Bank. (2019). ID4D Practitioner’s Guide: Version 1. <https://id4d.worldbank.org/guide>