Định nghĩa và đặc điểm gian lận

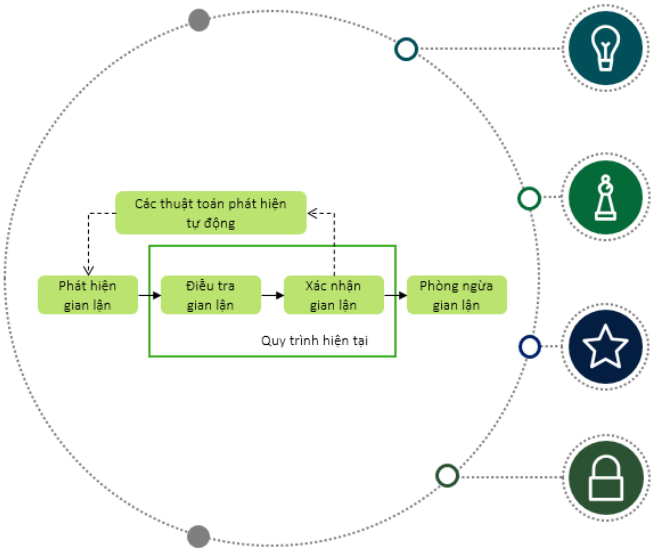
Có nhiều định nghĩa về Gian lận

- **COSO**
  Gian lận là bất kỳ hành động hoặc mưu đồ cố ý nào được tạo ra để lừa dối người khác, dẫn đến việc nạn nhân bị thiệt hại và/hoặc thủ phạm đạt được lợi ích.
- **Ngân hàng Commonwealth**
  Một người thực hiện hành vi gian lận khi họ có bất kỳ hành vi không trung thực nào nhằm: (a) đạt được hoặc cố gắng đạt được lợi ích (tài chính hay phi tài chính); và/hoặc (b) gây ra hoặc cố gắng gây ra bất lợi về tài chính.
- **Van Vlasselaer (Gotcha! Phát hiện gian lận bảo hiểm xã hội dựa trên mạng lưới thông tin) (2015)**
  Gian lận là một việc không phổ biến, được cân nhắc kỹ lưỡng, được che giấu một cách tinh vi, thay đổi theo thời gian và thường được thực hiện một cách có tổ chức dưới nhiều hình thức khác nhau.
- **ACFE**
  Gian lận trong nghề nghiệp bao gồm các hành vi sau: Lợi dụng chức vụ (vị trí làm việc), Cố ý lạm dụng nguồn lực và tài sản của tổ chức, Theo đuổi lợi ích cá nhân

Đặc điểm của gian lận

- Được thực hiện một cách bí mật và có chủ đích
- Hành vi và phương thức thay đổi theo thời gian
- Trực tiếp hay gián tiếp phục vụ mục đích kinh tế cá nhân/tổ chức (một cách bất hợp pháp)
- Ảnh hưởng tiêu cực đến tài sản, doanh thu hoặc/ và giá trị thặng dư cũng như danh tiếng của cá nhân/tổ chức
- Vi phạm nghĩa vụ trung thành với công ty

Vòng đời của gian lận



Phát hiện gian lận: Áp dụng các mô hình phát hiện trên các quan sát mới, chưa từng được quan sát và gán rủi ro gian lận cho mỗi quan sát.

Điều tra gian lận: Một chuyên thường được yêu cầu để điều tra các trường hợp đáng ngờ, hoặc được gắn cờ vì sự tinh vi và phức tạp liên quan.

Xác nhận gian lận: Xác định gán nhãn gian lận cuối cùng, có thể cần thực hiện nghiên cứu thực địa.

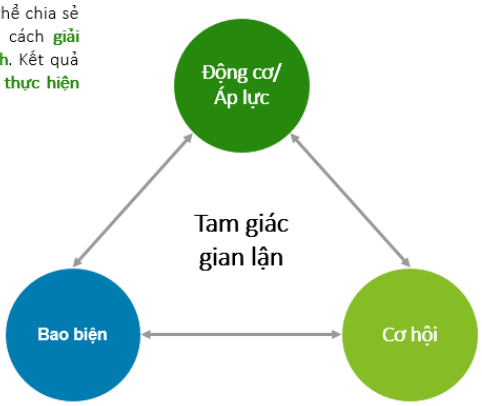
Phòng ngừa gian lận: Ngăn chặn gian lận tái diễn trong tương lai. Điều này thậm chí có thể giúp phát hiện gian lận ngay cả trước khi kẻ gian lận biết mình sẽ thực hiện hành vi gian lận.

Phạm vi của hoạt động xây dựng mô hình gian lận học máy sẽ tập trung vào phát hiện gian lận trong vòng đời của gian lận, nhằm đưa ra những cảnh báo về các hành vi/giao dịch đáng ngờ hoặc có điểm số gian lận cao. Sau đó các hành vi/giao dịch này sẽ được các chuyên gia điều tra gian lận đánh giá, tra soát để xác nhận xem hành vi/giao dịch đó có phải là gian lận hay không

Tam giác Gian lận

Tam giác gian lận giải thích vì sao một người lại thực hiện hành vi gian lận

Khi một cá nhân có vấn đề không thể chia sẻ với người khác, anh/cô ấy sẽ tìm cách **giải quyết một cách bí mật và một mình**. Kết quả là, phát sinh **động cơ hoặc áp lực thực hiện hành vi gian lận**



Khi 3 yếu tố này tồn tại, gian lận có thể xảy ra bất cứ lúc nào hoặc có thể đã thực sự xảy ra

Khi cá nhân biết rằng anh/cô ấy gặp phải vấn đề mà dẫn đến việc **mất mặt/hình phạt nặng** và việc này có thể tránh khỏi nếu thực hiện gian lận, anh/cô ấy **bao biện cho hành vi sai lệch** của mình

Những điều kiện sau tạo **cơ hội cho việc thực hiện hành vi gian lận**: chốt kiểm soát nội bộ yếu kém, khả năng bị phát hiện thấp, hoặc hình phạt khá nhẹ khi bị phát hiện

Phạm vi và mục tiêu trong mô hình mobile banking

Cùng với sự phát triển của nghiệp vụ NHS, các ngân hàng cũng phải đối mặt với nhiều loại hình gian lận, các loại hình gian lận thường gặp đối với nghiệp vụ NHS

Gian lận danh tính

Là việc sử dụng (i) danh tính của một người khác hoặc (ii) sử dụng danh tính tổng hợp từ việc: giả mạo danh tính bằng cách trộn lẫn thông tin từ nhiều người khác nhau, sửa đổi thông tin dựa trên danh tính của người khác hoặc làm giả toàn bộ thông tin về danh tính.

Chiếm đoạt tài khoản

Lừa đảo chiếm đoạt tài khoản là khi kẻ gian truy cập vào tài khoản không thuộc về họ, thay đổi thông tin như thông tin đăng nhập hoặc thông tin cá nhân, sau đó thực hiện các giao dịch trái phép trong tài khoản đó.

Gian lận mở tài khoản

Là việc kẻ gian đăng ký mở tài khoản mới bằng cách sử dụng các thông tin khách hàng từ hoạt động gian lận danh tính[1].

Các hình thức gian lận trên hầu như đều liên quan tới **Đánh cắp danh tính** và sau đó dẫn tới **Gian lận thanh toán**

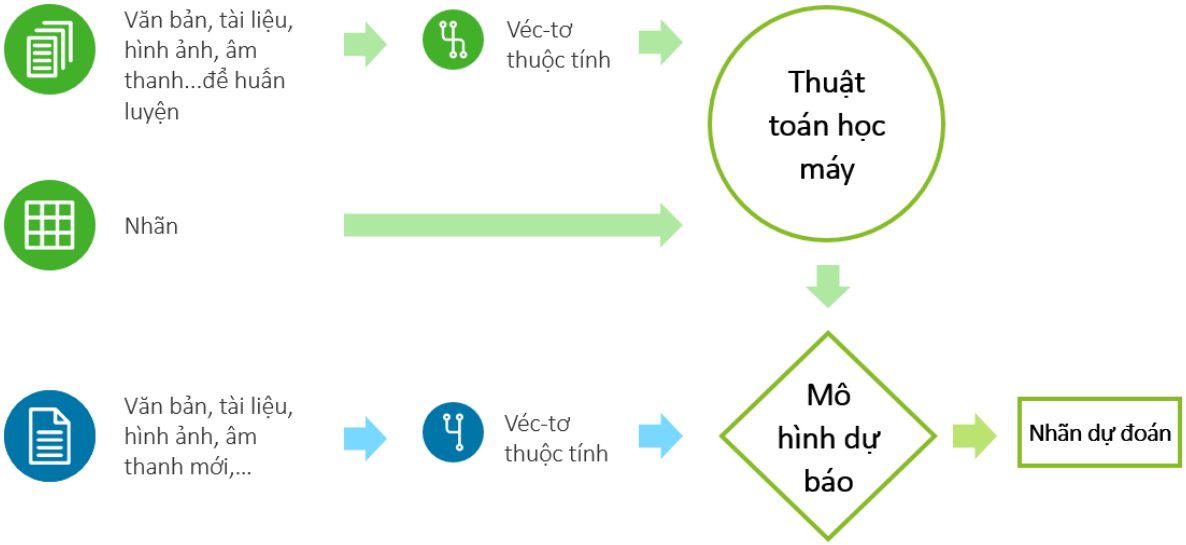
(1) Do hình thức gian lận này rất phổ biến nên mặc dù là một loại gian lận danh tính nhưng vẫn được liệt kê ngang hàng.

Theo khảo sát "The 2020 Faces of Fraud Survey"[2] **03 loại hình gian lận trên đều nằm trong tốp 10 loại hình gian lận mà các TCTC tại Mỹ quan tâm nhất.**

(2) Tham khảo Phụ lục 4 – Tốp 10 loại hình gian lận mà các TCTC tại Mỹ quan tâm nhất

Cấu trúc học máy

Học máy có giám sát



Tổng hợp đặc trưng thủ công

Tổng hợp Đặc trưng thủ công – Chuyên gia nội bộ: Tìm kiếm chuyên gia phù hợp

Những chuyên gia đầu ngành là nguồn tốt nhất cung cấp thông tin về yếu tố nào có khả năng dự đoán gian lận trong điều kiện của Ngân hàng; Quá trình trao đổi và thảo luận với các chuyên gia sẽ giúp xây dựng một danh sách các biến đầy đủ và hoàn thiện.

Những chuyên gia điều tra gian lận (kiểm toán nội bộ, kiểm soát nội bộ): là nguồn rất tốt cung cấp thông tin tại sao lại xảy ra gian lận

Chuyên gia nghiệp vụ, Chuyên gia quản lý rủi ro gian lận: là nguồn cung cấp thông tin tin cậy về các trường hợp gian lận có thể xảy ra

Chuyên gia mô hình rủi ro gian lận: là nguồn cung cấp thông tin về các đặc trưng qua nghiên cứu và kinh nghiệm từ các dự án trước

Tổng hợp đặc trưng thủ công

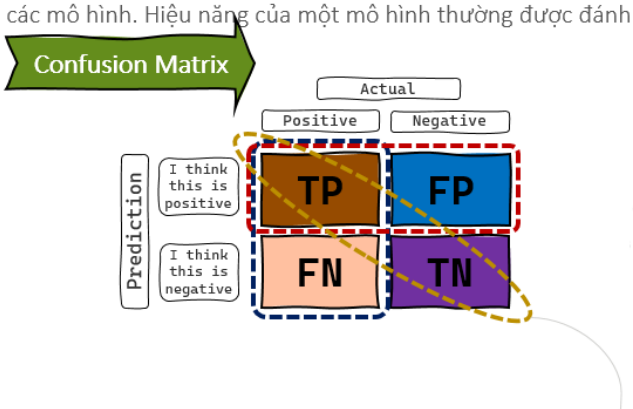
Phân tích hành vi gian lận và kịch bản phát hiện

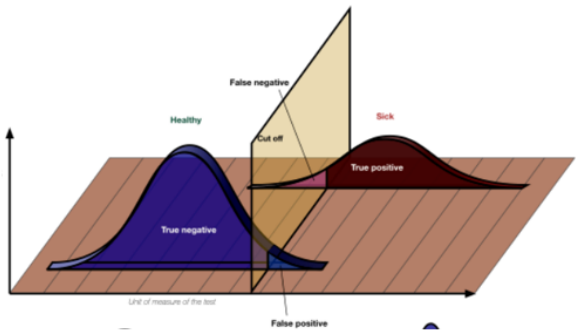
Các trường hợp gian lận → **Các quy tắc phát hiện gian lận** → **Danh sách biến yêu cầu cho từng quy tắc**

Kịch bản	Biến
• Khách hàng thực hiện đăng nhập vào khung giờ nằm ngoài thời gian giao dịch thông thường (giá trị trung bình của thời gian theo phân phối Von Mises +/- 3 sigma) • Khách hàng đăng nhập (thành công hoặc không thành công) sử dụng hơn 03 ISP (Internet service provider) trong 12h qua • Khách hàng trong 3-6 tháng qua luôn đăng nhập thành công ở lần đăng nhập đầu tiên Hoặc Khách hàng luôn đăng nhập thành công ở lần đăng nhập đầu tiên trong 30 lần đăng nhập gần nhất (áp dụng đối với KH mới chưa đủ thời gian giao dịch 3/6 tháng) & Khách hàng đăng nhập không thành công từ 3 lần trở lên • Trình duyệt đang dùng nằm ngoài trình duyệt khách hàng sử dụng trong [xxx] tháng • Khách hàng trong vòng [xxx] giờ sử dụng trình duyệt A, nhưng sau đó lại dùng trình duyệt B ở giao dịch mới	• Thời gian giao dịch • Trung bình thời gian giao dịch theo phân phối Von Mises • Độ lệch chuẩn thời gian giao dịch theo phân phối Von Mises • Internet Service Provider • Cờ chỉ báo KH đăng nhập thành công/không thành công • Số lần đăng nhập không thành công trong 3-6 tháng • Số lần đăng nhập không thành công trong 30 lần gần nhất • Trình duyệt đang sử dụng • Cờ chỉ báo khách hàng sử dụng trình duyệt mới

Chỉ tiêu đánh giá mô hình dự đoán – Ma trận nhầm lẫn (Confusion Matrix)

Khi xây dựng một mô hình máy học, chúng ta cần công cụ để đánh giá khả năng phân lớp của mô hình và để so sánh gii các mô hình. Hiệu năng của một mô hình thường được đánh giá dựa trên tập dữ liệu kiểm thử (test data).





✓ **Precision** = **TP / (TP + FP)**

Precision đo lường tỷ lệ giao dịch gian lận trong các giao dịch được cảnh báo bởi quy tắc. Precision cao đồng nghĩa với tỉ lệ đoán đúng các giao dịch gian lận của quy tắc là cao

✓ **Recall** = TP / (TP + FN)

Recall đo lường tỷ lệ giao dịch gian lận được phát hiện bởi quy tắc. Recall cao đồng nghĩa với tỉ lệ bỏ sót các giao dịch của quy tắc gian lận là thấp

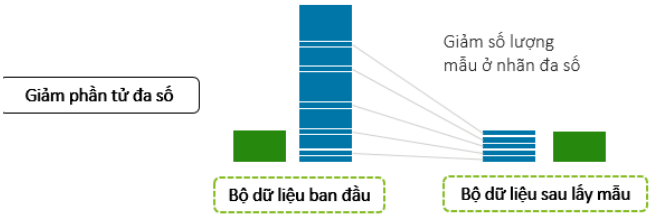
✓ **Accuracy** = (TP + TN) / (TP + FP + FN + TN)

Accuracy đo lường tỷ lệ phán đoán chính xác cho các giao dịch gian lận và không gian lận

Vấn đề mất cân bằng dữ liệu

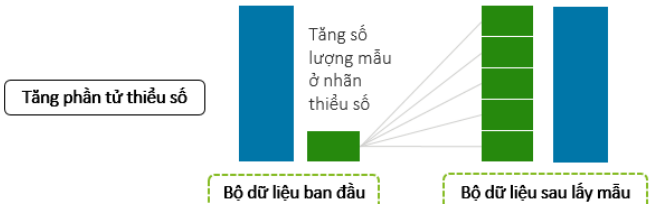
Mất cân bằng dữ liệu là hiện tượng phổ biến đối với bài toán phát hiện gian lận khi số lượng nhãn gian lận thường rất nhỏ so với số lượng nhãn không gian lận. Vấn đề mất cân bằng dữ liệu nghiêm trọng thường dẫn tới dự báo kém chính xác trên nhóm thiểu số, trong khi việc dự báo chính xác nhóm thiểu số lại có tầm quan trọng hơn.

Phương pháp xử lý mất cân bằng dữ liệu: tăng phần tử thiểu số (**Oversampling**), giảm phần tử đa số (**Undersampling**).



Giảm phần tử đa số (Under sampling): Phương pháp này giảm số lượng các quan sát của nhóm đa số để nó trở nên cân bằng với số quan sát của nhóm thiểu số.

Giảm ngẫu nhiên phần tử đa số (Random undersampling) là phương pháp lựa chọn loại bỏ ngẫu nhiên các quan sát của nhóm đa số để trở nên cân bằng với quan sát của nhóm thiểu số hoặc đạt đến một tỷ lệ chấp nhận được.



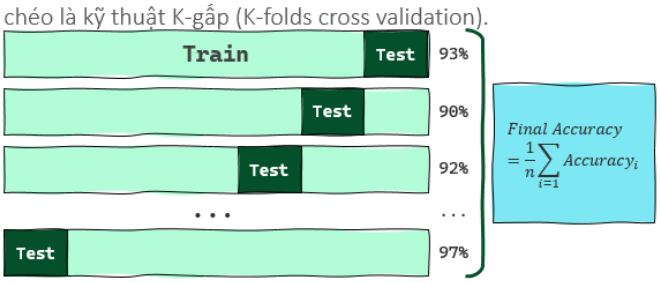
Tăng phần tử thiểu số (Over sampling): Phương pháp giúp giải quyết hiện tượng mất cân bằng mẫu bằng cách gia tăng kích thước mẫu thuộc nhóm thiểu số bằng các kĩ thuật khác nhau.

Có 2 phương pháp chính để thực hiện over sampling đó là:

- ✓ Lựa chọn mẫu có tái lập.
- ✓ Mô phỏng mẫu mới dựa trên tổng hợp của các mẫu cũ.

Huấn luyện mô hình – Kiểm chứng chéo

Kiểm chứng chéo (Cross validation) là một phương pháp được sử dụng để ước lượng hiệu quả của các mô hình máy học. Kiểm định chéo đánh giá được khả năng dự báo đồng thời mức độ ổn định của mô hình. Phương pháp này sử dụng kỹ thuật liên tục lấy mẫu từ chính dữ liệu gốc để kiểm tra chéo lẫn nhau. Kỹ thuật thường được áp dụng trong kiểm chứng chéo là kỹ thuật K-gấp (K-folds cross validation).



K-fold Cross validation: Phương pháp này phân chia dữ liệu thành k tập con có cùng kích thước. Tại mỗi vòng lặp sử dụng k-1 tập con là tập huấn luyện và tập con còn lại là tập kiểm chứng.

Giá trị k thường là = 10. Ta có thể dùng một trong hai cách:

- ✓ Leave-one-out : k=số mẫu trong dữ liệu (dành cho tập dữ liệu nhỏ)
- ✓ Stratified cross-validation : dùng phương pháp lấy mẫu để các lớp trong từng tập con có phân phối tương tự như trên bộ dữ liệu gốc

1. Xáo trộn dữ liệu gốc một cách ngẫu nhiên
2. Chia dữ liệu gốc thành k nhóm

Với mỗi nhóm:

- Sử dụng nhóm hiện tại để đánh giá hiệu quả mô hình
- Các nhóm còn lại được sử dụng để huấn luyện mô hình
- Huấn luyện mô hình
- Đánh giá và sau đó hủy mô hình

3. Đánh giá một cách toàn diện khả năng của mô hình bằng cách tổng hợp và phân tích thống kê các kết quả riêng rẽ

Lưu ý:

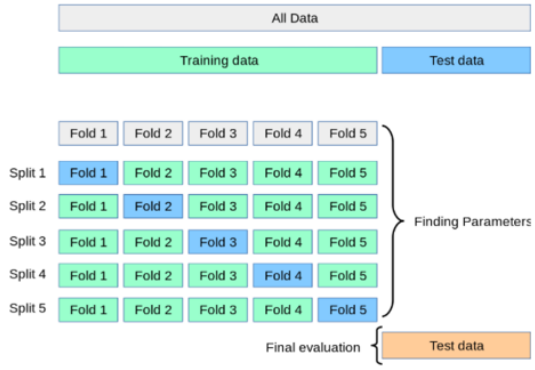
- Kỹ thuật này đặc biệt hiệu quả với bộ dữ liệu nhỏ do không cần quá nhiều quan sát vẫn có thể huấn luyện và kiểm chứng hiệu quả mô hình dự báo
- Mỗi mẫu chỉ được gán cho duy nhất một nhóm và phải ở nguyên trong nhóm đó cho đến hết quá trình
- Kết quả tổng hợp thường là trung bình của các lần đánh giá. Ngoài ra việc bổ sung thông tin về phương sai và độ lệch chuẩn vào kết quả tổng hợp cũng được sử dụng trong thực tế.

Huấn luyện mô hình – Huấn luyện nhiều lần

Thực hiện huấn luyện một lần trên tập dữ liệu huấn luyện và tập dữ liệu kiểm chứng có thể gây ra vấn đề số lượng quan sát có thể sử dụng cho việc mô hình học bị giảm đi và kết quả kiểm chứng có thể bị ảnh hưởng bởi các cặp (huấn luyện, kiểm chứng) ngẫu nhiên.

Bên cạnh đó, khi thực hiện huấn luyện một lần, mô hình có thể dự đoán tốt kết quả tốt trên tập kiểm chứng, tuy nhiên có thể dự đoán không tốt ở tập kiểm thử hoặc với dữ liệu thực tế. Vì vậy, để đảm báo tính ổn định của mô hình được lựa chọn cần thực hiện huấn luyện mô hình lặp lại nhiều lần với mỗi thuật toán. Khi đó việc phân chia tập huấn luyện và tập kiểm chứng không được thực hiện cố định mà thực hiện lấy mẫu liên tục từ dữ liệu gốc để kiểm tra chéo lẫn nhau. Kỹ thuật này được gọi là kiểm chứng chéo (Cross – validation).

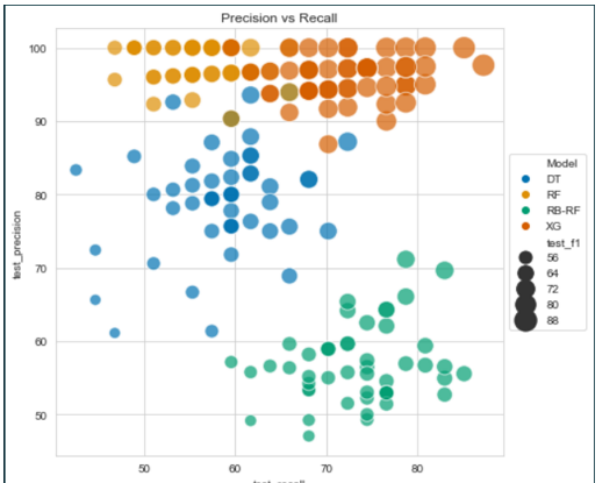
Mỗi lần thực hiện huấn luyện mô hình sẽ nhận được một bộ chỉ tiêu đánh giá kết quả mô hình. Khi đó, các chỉ tiêu đánh giá khả năng dự đoán của mô hình được xác định dựa trên giá trị trung bình của tất cả các lần lấy mẫu.



Lựa chọn mô hình – Phân tích chỉ tiêu Precision và Recall

Thực hiện liên tục lấy mẫu trên tập dữ liệu huấn luyện được tập các chỉ tiêu đánh giá cho mỗi lần thực hiện huấn luyện và trực quan hóa các chỉ tiêu đánh giá.

Trực quan hóa chỉ tiêu đánh giá của mô hình



Trực quan hóa chỉ tiêu Precision và Recall:

- ✓ Trục tung là giá trị Precision và trục hoành là giá trị Recall trên tập kiểm chứng mỗi lần lấy mẫu
- ✓ Mỗi chấm tròn thể hiện kết quả của một cặp giá trị (Precision, Recall) của một lần huấn luyện.
- ✓ Màu sắc của mỗi chấm tròn thể hiện một thuật toán khác nhau.
- ✓ Vị trí của chấm tròn càng về phía góc phần tư thứ nhất của hình càng thể hiện khả năng dự đoán của mô hình.
- ✓ Vị trí của các chấm tròn cùng màu càng gần càng thể hiện tính ổn định của mô hình.
- ✓ Kích thước của chấm tròn thể hiện giá trị F1-score của mô hình, chấm tròn càng to giá trị F1-score càng cao.

Trong hình minh họa, có thể thấy mô hình xGBoost là mô hình có khả năng dự đoán tốt nhất. Chấm tròn của hình xGBoost có giá trị tập trung ở phía góc phần tư thứ nhất, thể hiện mô hình có giá trị Precision và Recall cao và có tính ổn định. Kích thước của chấm tròn mô hình xGBoost thể hiện mô hình có giá trị F1-score cao nhất trong các thuật toán.

Lựa chọn biến

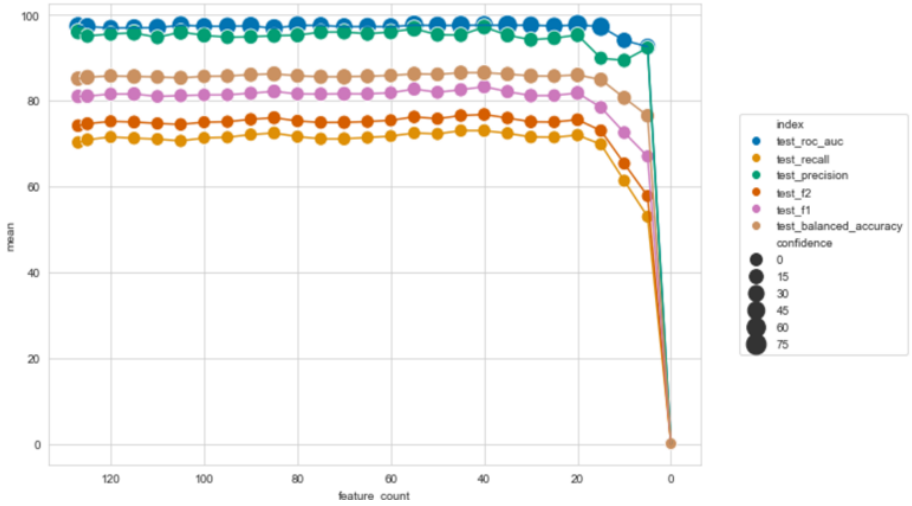
Việc chạy mô hình với số lượng lớn các biến (chẳng hạn như hơn 300 biến) sẽ yêu cầu rất nhiều tài nguyên, nguồn lực và thời gian để xây dựng mô hình cũng như đưa ra dự báo. Vì thế, sau khi đã lựa chọn được mô hình xGBoost với dữ liệu được tăng phần tử thiểu số, thực hiện chọn lọc các biến có ý nghĩa để tăng tốc độ tính toán cho mô hình mà vẫn giữ đư khả năng dự đoán của mô hình

Tiêu chí lựa chọn

- **Hệ số tương quan (correlation)**
- **Điểm số khả năng dự báo (Accuracy, Precision, Recall, AUC, F1)**
- **Tầm quan trọng của đặc trưng (features importances)**

Lựa chọn biến – Loại dần từng biến

Thực hiện loại dần từng biến để lựa chọn ra Top xx biến có khả năng dự báo nhất để sử dụng trong mô hình. Sử dụng các chỉ tiêu đánh giá **Accuracy, Precision, Recall, F1-Score, AUC** sau mỗi lần lọc biến và so sánh với mô hình với đầy đủ các biến để đưa ra quyết định số lượng biến sau khi lọc theo nhóm. Mỗi đường có màu sắc khác nhau thể hiện một chỉ tiêu đánh giá của mô hình sau mỗi lần lọc biến.



Tối ưu siêu tham số

Siêu tham số là các tham số mà các nhà khoa học dữ liệu có thể thiết lập, chỉ định các giá trị cụ thể để kiểm soát cách các thuật toán học máy và cũng để điều chỉnh hiệu suất của mô hình

Khi xây dựng một mô hình học máy, chúng ta thường sẽ phải lựa chọn thiết kế cho mô hình học máy của mình, ví dụ như:

- ✓ Độ sâu tối đa (max depth) cho cây quyết định nên là bao nhiêu?
- ✓ Nên đưa bao nhiêu cây vào mô hình rừng ngẫu nhiên?

Thông thường, trước khi xây dựng một mô hình, chúng ta không thể biết ngay lập tức kiến trúc mô hình tối ưu cho mô hình đó, và vì thế chúng ta muốn thử nghiệm kết quả của mô hình với một loạt các siêu tham số khác nhau (ví dụ như so sánh kết quả mô hình với các lựa chọn max depth là 2, 4, 6, 8, 10, 12, 14).

Trong học máy, lý tưởng nhất là chúng ta sẽ yêu cầu máy thực hiện khám phá so sánh này và tự động chọn kiến trúc mô hình tối ưu nhất. Tối ưu siêu tham số là quá trình lựa chọn các giá trị cho các siêu tham số của mô hình nhằm tối đa hóa độ chính xác của mô hình