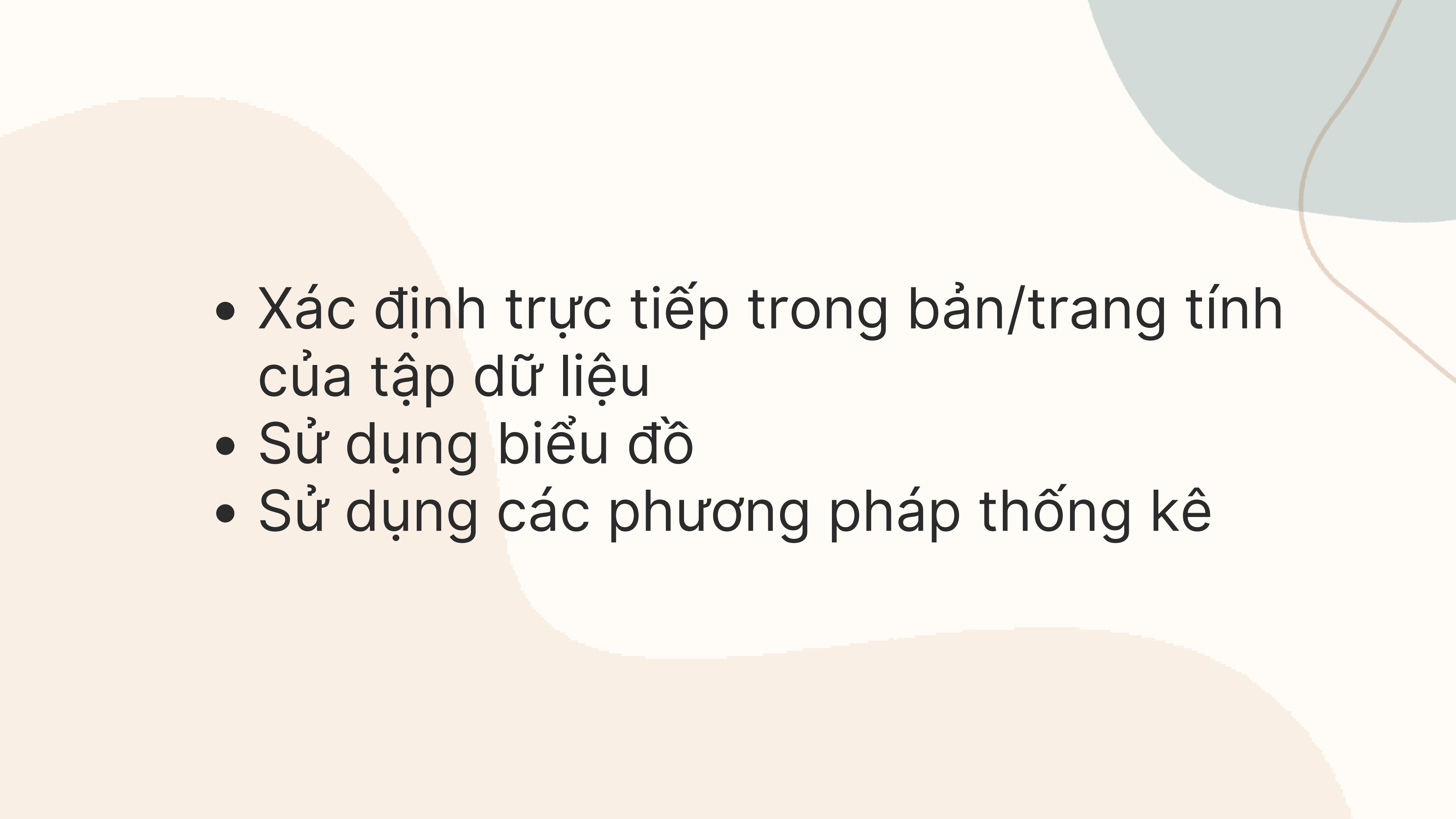


Tổng quan về Machine Learning



Outliner

- Các giá trị không nằm trong miền xác định của dữ liệu. Ví dụ, tuổi, thu nhập hay khoảng cách không thể là số âm.
- Các giá trị có khả năng xảy ra nhưng xác suất rất thấp. Ví dụ, 120 tuổi, thu nhập 1 triệu đô la/tháng. Những giá trị này có khả năng xảy ra nhưng thực sự hiếm có.

- 
- Xác định trực tiếp trong bản/trang tính của tập dữ liệu
 - Sử dụng biểu đồ
 - Sử dụng các phương pháp thống kê

Các phương pháp thống kê

- Tính giá trị trung bình và độ lệch chuẩn
- Sử dụng Z-score
- Sử dụng Interquartile Range
- Sử dụng Hypothesis Test

Machine learning (ML) hay máy học là một nhánh của trí tuệ nhân tạo (AI), nó là một lĩnh vực nghiên cứu cho phép máy tính có khả năng cải thiện chính bản thân chúng dựa trên dữ liệu mẫu (training data) hoặc dựa vào kinh nghiệm (những gì đã được học). Machine learning có thể tự dự đoán hoặc đưa ra quyết định mà không cần được lập trình cụ thể.



Data Variables

- Được định nghĩa là các đặc trưng (features), là thuộc tính đo lường được của điểm dữ liệu, dùng làm đầu vào cho thuật toán học máy
- Chúng có thể là số (như tuổi, diện tích nhà), phân loại (như giới tính, nghề nghiệp), hoặc văn bản. Ví dụ, trong dự đoán giá nhà, đặc trưng có thể là số phòng ngủ, vị trí, hoặc năm xây dựng.

Data Processing

- Là quá trình làm sạch, biến đổi và chuẩn bị dữ liệu để phù hợp cho mô hình ML.
- Bao gồm các bước như xử lý lỗi, điền giá trị thiếu, và chuẩn hóa dữ liệu, đảm bảo dữ liệu thô được chuyển đổi thành định dạng máy có thể đọc được, tối ưu hóa hiệu suất mô hình



Feature Engineering

- Là quá trình biến đổi dữ liệu thô thành thông tin phù hợp cho mô hình học máy
- Nó bao gồm 5 quá trình chính: tạo đặc trưng (feature creation), biến đổi (transformation), trích xuất (extraction), chọn lọc (selection), và chuẩn hóa (scaling).

Phương Pháp Tiền Xử Lý Dữ Liệu

- Chuẩn hóa (Normalization): Đưa dữ liệu về khoảng 0-1, giúp các đặc trưng có cùng mức độ ảnh hưởng.
- Tiêu chuẩn hóa (Scaling): Ví dụ, chuẩn hóa z-score (trung bình=0, độ lệch chuẩn=1) hoặc min-max scaling, đảm bảo dữ liệu đồng nhất.
- Mã hóa (Encoding): Chuyển đổi dữ liệu phân loại thành số, như one-hot encoding (tạo cột nhị phân cho mỗi hạng mục) hoặc label encoding.

- Xử lý dữ liệu thiếu: Có thể xóa hàng thiếu hoặc điền giá trị bằng trung bình, trung vị, hoặc phương pháp tiên tiến hơn.
- Phân nhóm (Binning): Chuyển đổi dữ liệu liên tục thành phân loại, ví dụ: nhóm tuổi 18-25, 26-35, 36-50, 51-80.
- Xử lý văn bản: Loại bỏ từ dừng, stemming, lemmatization, và vector hóa cho dữ liệu văn bản.

Phương Pháp Chọn Đặc Trưng

- Phương pháp lọc (Filter Method): Chọn đặc trưng dựa trên mối quan hệ thống kê, như tương quan cao với mục tiêu.
- Phương pháp bao bọc (Wrapper Method): Đánh giá tập con đặc trưng bằng thuật toán ML, chọn tập cho hiệu suất tốt nhất.
- Phương pháp nhúng (Embedded Method): Tích hợp chọn đặc trưng trong quá trình huấn luyện mô hình.

- Phân tích thành phần chính (Principal Component Analysis): Kết hợp đặc trưng thành các thành phần chính, giữ lại phần lớn phương sai, giảm chiều dữ liệu
- Phân tích phân biệt tuyến tính (Linear Discriminant Analysis) : Tối ưu hóa sự khác biệt giữa các lớp, giữ lại thông tin phân loại

Quá trình huấn luyện mô hình



Huấn luyện mô hình Machine Learning

- là quá trình trong machine learning để giúp một mô hình AI học cách phân tích và đưa ra dự đoán từ dữ liệu.
- Quá trình này bao gồm việc cung cấp cho mô hình các tập dữ liệu huấn luyện (training data) để nó có thể tìm hiểu mối quan hệ, xu hướng hoặc mẫu trong dữ liệu, từ đó tạo ra các dự đoán hoặc phân loại chính xác hơn khi áp dụng vào dữ liệu mới.

Chuẩn bị dữ liệu

- Trước khi tiến hành train model, dữ liệu cần phải được chuẩn bị kỹ càng, bao gồm các bước như làm sạch dữ liệu, chuẩn hóa và phân chia dữ liệu.
- Dữ liệu huấn luyện cần phải đại diện tốt cho các trường hợp mà mô hình sẽ gặp phải sau này.

Chọn Mô Hình Thích Hợp

- Tùy vào bài toán cụ thể, các nhà khoa học dữ liệu sẽ chọn mô hình thích hợp như linear regression, decision tree, neural network, hay support vector machine.
- Lựa chọn mô hình phù hợp sẽ giúp tối ưu hóa kết quả của quá trình train model.

Huấn Luyện Mô Hình

- Trong bước này, dữ liệu huấn luyện được đưa vào mô hình để giúp mô hình học các mẫu và mối quan hệ trong dữ liệu.
- Các thuật toán học máy sẽ liên tục điều chỉnh tham số của mô hình để cải thiện kết quả dự đoán.

Kiểm Tra Và Đánh Giá Mô Hình

- Sau khi hoàn thành quá trình huấn luyện, mô hình sẽ được kiểm tra với tập dữ liệu kiểm tra (testing data) để đánh giá độ chính xác và khả năng tổng quát của mô hình.

Tối Ưu Hóa Mô Hình

- Dựa trên kết quả đánh giá, các nhà khoa học dữ liệu có thể tinh chỉnh mô hình để tăng cường hiệu suất và giảm thiểu sai số.
- Việc tối ưu hóa này có thể bao gồm việc thay đổi cấu trúc của mô hình, điều chỉnh siêu tham số, hoặc thử nghiệm với các thuật toán học máy khác nhau.

Model Evaluation

Confusion Martric(Ma trận nhầm lẫn)

		Actual Values	
		Positive (1)	Negative (0)
Predicted Values	Positive (1)	TP	FP Type 1 Error
	Negative (0)	FN Type 2 Error	TN

TP: True positive (dương tính thật)

FP: False positive (dương tính giả)

TN: True negative (âm tính thật)

FN: False negative (âm tính giả)

Accuracy

- Là độ đo của bài toán phân loại mà đơn giản nhất, tính toán bằng cách lấy số dự đoán đúng chia cho toàn bộ các dự đoán.
- Phép đo độ chính xác đơn giản dễ hiểu nhưng không phù hợp với dữ liệu không cân bằng

$$\text{Accuracy} = \frac{TP+TN}{FP+TN+TP+TN}$$

Precision

- Là độ đo của bài toán phân loại mà đơn giản nhất, tính toán bằng cách lấy số dương tính thật chia cho tổng dương tính dự đoán .
- Sử dụng khi dương tính giả quan trọng hơn âm tính giả

- $$\text{Precision} = \frac{TP}{FP+TP}$$

Recall

- Là một metric quan trọng, tính toán bằng cách lấy số dương tính thật chia cho tổng các dương tính thực tế
- Sử dụng khi giá trị âm tính giả quan trọng hơn dương tính giả

- $$\text{Recall} = \frac{TP}{FN + TP}$$

Recall

- Là một metric quan trọng, tính toán bằng cách lấy số dương tính thật chia cho tổng các dương tính thực tế
- Sử dụng khi giá trị âm tính giả quan trọng hơn dương tính giả

- $$\text{Recall} = \frac{TP}{FN + TP}$$

F1-score

- Là một metric phổ biến đã kết hợp cả Recall và Precision
- Phụ thuộc vào data và vấn đề để dự đoán

- $$\text{F1-score} = \frac{(\text{Recall} * \text{Precision} * 2)}{(\text{Recall} + \text{Precision})}$$



Bias-Variance, overfitting
underfitting

Bias

- là sự khác biệt giữa giá trị dự đoán của mô hình và giá trị thực tế mà mô hình đang cố gắng dự đoán.
- Một mô hình có bias cao thường đơn giản và không thể nắm bắt được sự phức tạp của dữ liệu, dẫn đến việc không đạt được hiệu suất tốt trên cả tập huấn luyện và tập kiểm tra.

Variance

- là sự thay đổi của mô hình với các tập dữ liệu khác nhau.
- Một mô hình có variance cao nhạy cảm với các nhiễu trong dữ liệu, dẫn đến việc nó có thể hoạt động rất tốt trên tập huấn luyện nhưng lại kém khi áp dụng cho dữ liệu mới

Overfitting

- Là trường hợp mô hình quá phức tạp, kết quả rất gần với các training set chứa cả noise và các outlier.
- Một mô hình có thể hoạt động rất tốt trên tập huấn luyện nhưng lại kém khi áp dụng cho dữ liệu mới

Underfitting

- Là trường hợp mô hình quá đơn giản, không nhận ra được mối quan hệ giữa các dữ liệu.
- Mô hình hoạt động rất kém trên dữ huấn luyện và kiểm tra

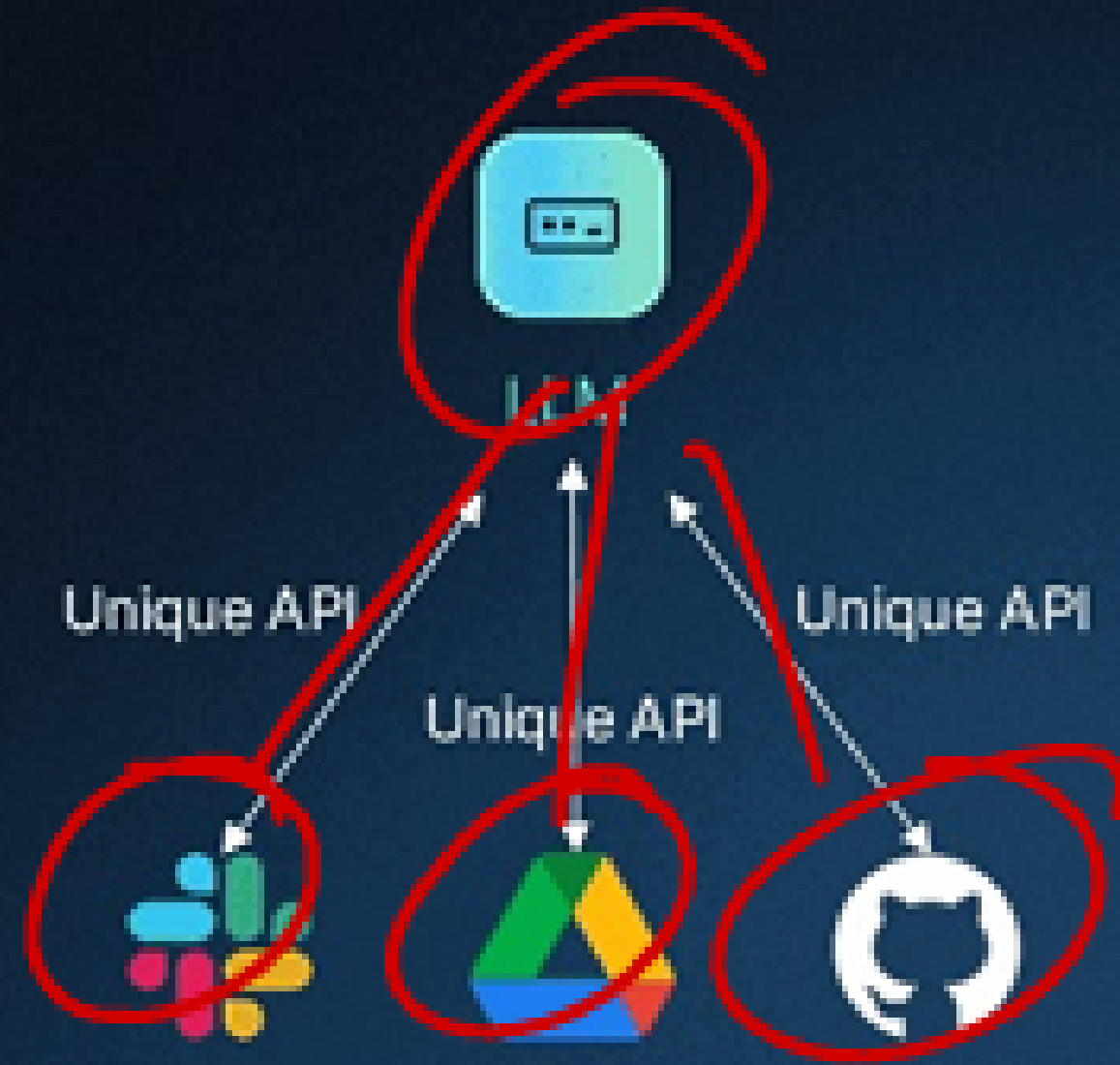


Model context protocol (MCP)

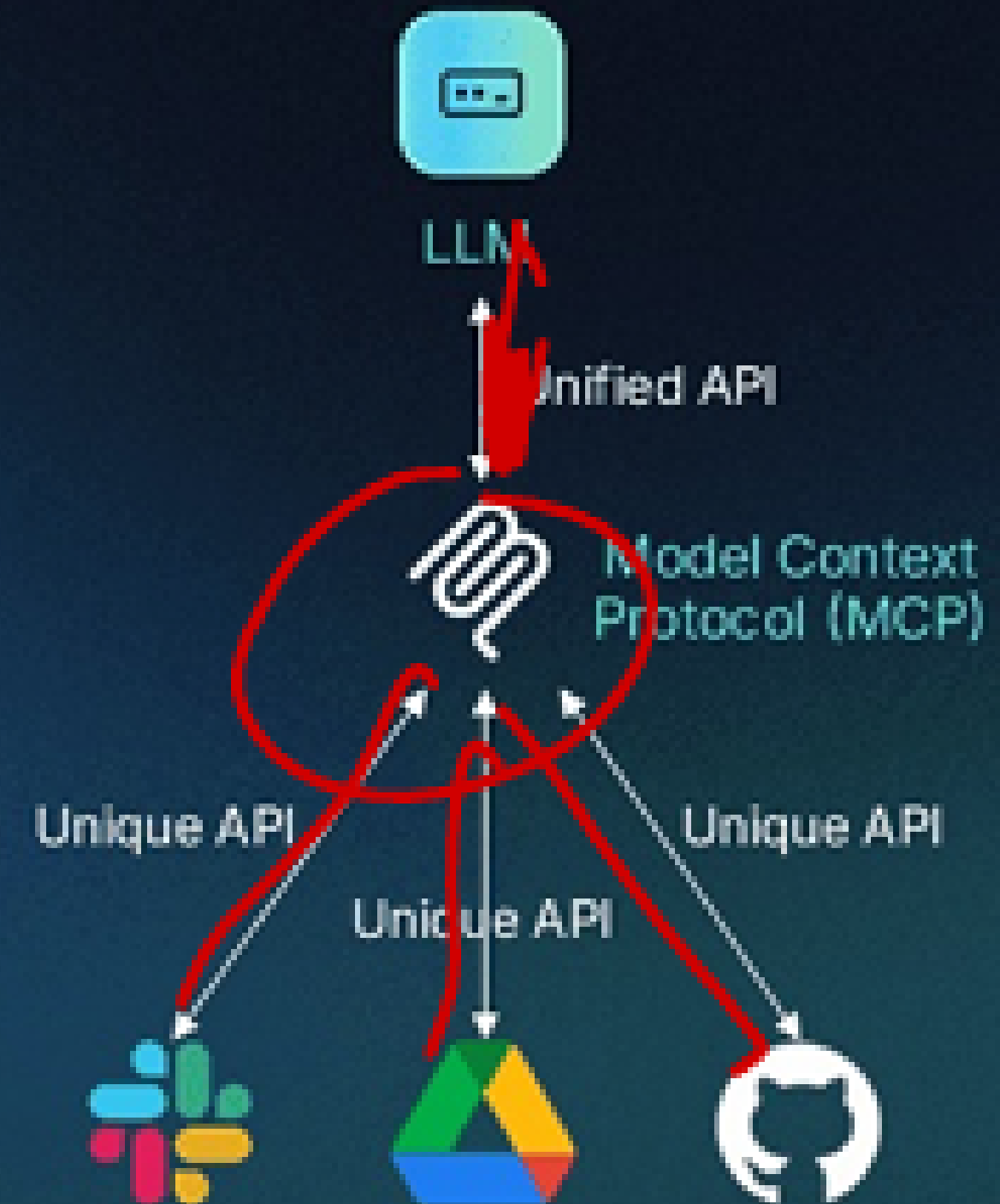
MCP

- Là một tiêu chuẩn mã nguồn mở giúp AI kết nối và tương tác với các nguồn dữ liệu, công cụ và API bên ngoài. Nó hoạt động như một "cổng USB" cho AI, giúp đơn giản hóa việc truy cập dữ liệu theo thời gian thực
- Mục đích chính của MCP là:
 - Hỗ trợ xây dựng các agent AI và quy trình làm việc phức tạp trên LLM.
 - Cung cấp danh sách tích hợp sẵn có, cho phép LLM dễ dàng kết nối với các công cụ và dữ liệu.
 - Đảm bảo khả năng chuyển đổi giữa các nhà cung cấp LLM và công cụ, đồng thời áp dụng các thực hành tốt nhất để bảo mật dữ liệu trong hạ tầng.

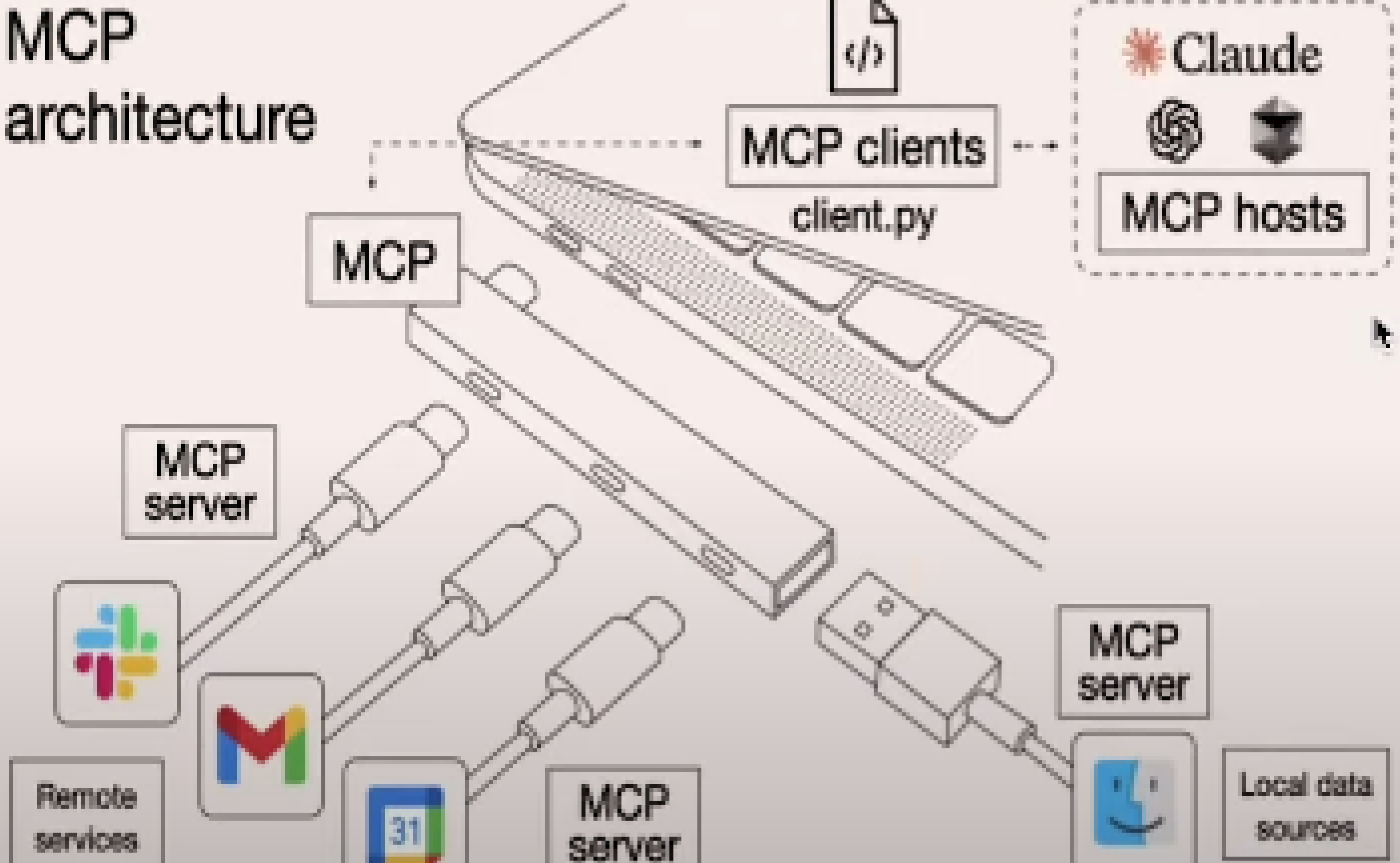
Before MCP



After MCP



MCP architecture



MCP Servers

Currently, the Model Context Protocol defines two
Types of servers

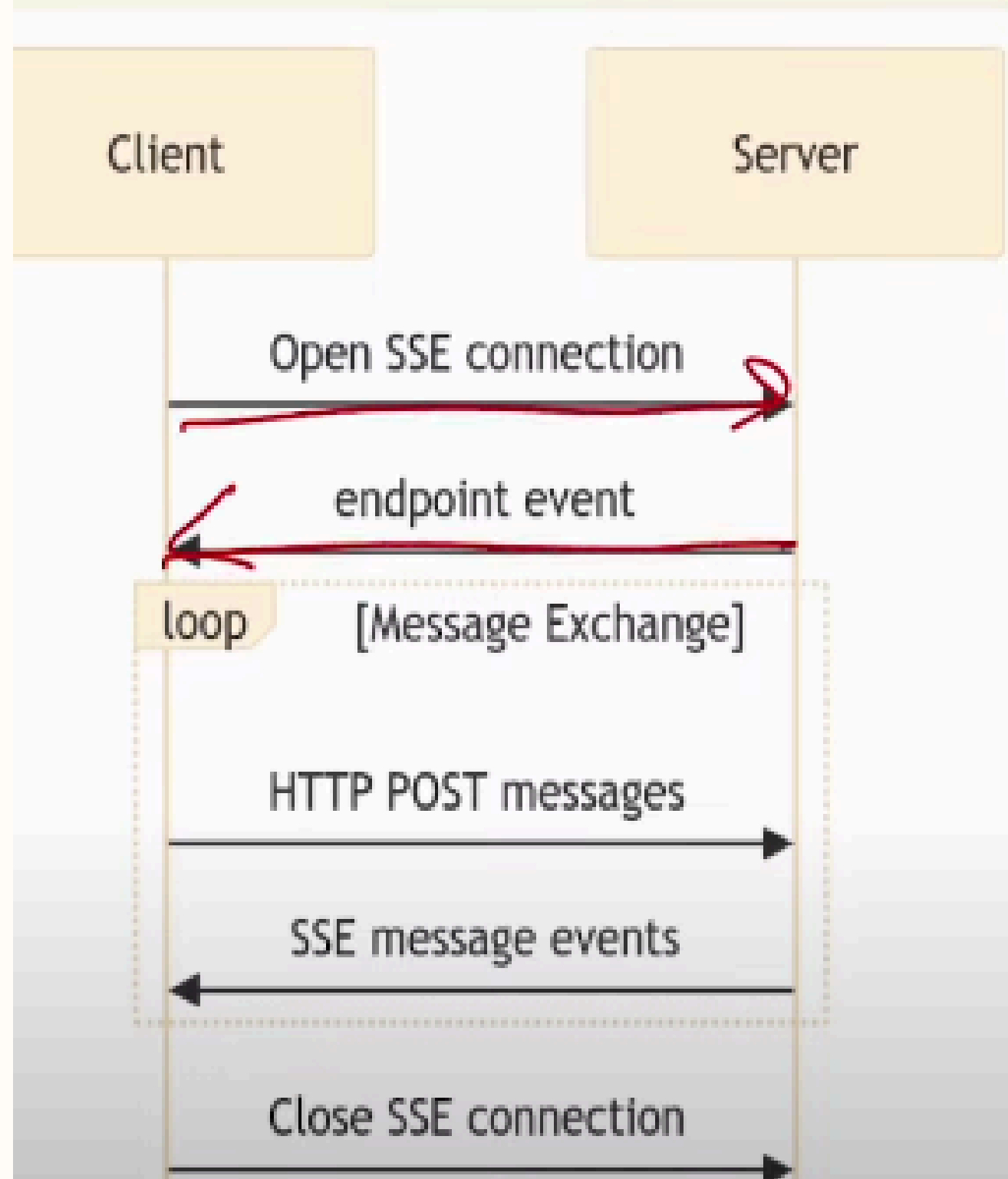
STDIO

Runs as a subprocess
of your AI app

HTTP over SSE

Runs remotely
via a URL

SSE



Stdio

