# TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA TOÁN – TIN HỌC



# BÁO CÁO FINAL PROJECT

Đề tài: Phát Hiện Tin Giả Dựa Trên Học Máy và Học Sâu

## Thành viên nhóm

Họ và tên	Mã số sinh viên
Lương Thanh Nam	22280056
Lê Trọng Nghĩa	22280059
Phạm Tấn Phước	22280069

Chi t	tiết đề tài	2
Phần	ı 1: Tiền xử lý dữ liệu	3
1.	Đọc và Gộp dữ liệu	3
2.	Làm sạch dữ liệu	3
3.	Kết quả	3
Phần	n 2: Khám phá dữ liệu (EDA)	3
1.	Phân tích cơ bản	3
2.	Trích xuất đặc trưng	3
Phần	n 3: Xây dựng mô hình	4
1.	Mô hình học máy truyền thống	4
2.	Mô hình học sâu	4
Phầr	n 4: Thiết lập siêu tham số	5
1.	Học máy truyền thống	5
2.	Học sâu	5
Phần	n 5: Huấn luyện mô hình	5
1.	Random Forest	5
2.	Decision Tree	8
3.	XGBoost Classifier	10
4.	Logistic Regression	11
5.	RNN với LTSM	12
6.	BERT	13
7.	XLNet	13
Phần	n 6: Kết luận	13
Phần	n 7: Đánh giá điểm mạnh, yếu các mô hình	14
Phần	n 8: Đề xuất cải thiện	18

## Chi tiết đề tài

Việc phát tán rộng rãi tin tức giả và tuyên truyền gây ra những rủi ro nghiêm trọng cho xã hội, bao gồm sự sói mòn lòng tin của công chúng, phân cực chính trị, thao túng bầu cử và lan truyền thông tin sai lệch có hại trong các cuộc khủng hoảng như đại dịch và xung đột. Theo quan điểm của NLP, việc phát hiện tin tức giả mạo đầy rẫy những thách thức. Về mặt ngôn ngữ, tin tức giả mạo bắt chước giọng điệu và cấu trúc của báo chí chính thống, khiến việc phân biệt bằng các tính năng bề mặt trở nên khó khăn. Việc không có các tập dữ liệu được gắn nhãn đáng tin cậy và cập nhật, đặc biệt là trên nhiều ngôn ngữ và khu vực, cản trở hiệu quả của các mô hình học có giám sát. Ngoài ra, bản chất năng động và đối đầu của thông tin sai lệch có nghĩa là những tác nhân độc hại liên tục phát triển ngôn ngữ và chiến lược của chúng để vượt qua các hệ thống phát hiện. Bối cảnh văn hóa, sự mia mai, châm biếm và thành kiến ngầm càng làm phức tạp thêm quá trình phân tích tự động. Hơn nữa, các mô hình NLP có nguy cơ khuyếch đại các thành kiến có trong dữ liệu đào tạo, dẫn đến phân loại không công bằng và khả năng kiểm duyệt nội dung hợp pháp. Những thách thức này nhấn mạnh nhu cầu về các phương pháp tiếp cận thận trọng, có nhận thức về bối cảnh, vì việc không giải quyết chúng có thể vô tình góp phần gây ra thông tin sai lệch, thay vì giảm thiểu nó.

## Bộ dữ liệu

- 1. Bài viết có thật:
- **File**: MisinfoSuperset\_TRUE.csv
- Nguồn: các phương tiện truyền thông có uy tín như Reuters, The New York Times, The Washington Post, ...
- 2. Bài viết giả mạo/ thông tin sai lệch/ tuyên truyền:
- **File:** MisinfoSuperset\_FAKE.csv
- Nguồn: các trang web cực đoan cánh hữu của Mỹ (ví dụ: Redflag Newsdesk, Breitbart, Truth Broadcast Network).

Ahmed, H., Traore, I., & Saad, S. (2017): "Detection of Online Fake News Using N-Gram Analysis and Machine Learning Techniques" (Springer LNCS 10618)

# Phần 1: Tiền xử lý dữ liệu

#### 1. Đọc và Gộp dữ liệu

- Hai tệp CSV được đọc bằng thư viện pandas và gộp thành một DataFrame duy nhất.
- Nhãn được gán: 1 cho bài báo thật, 0 cho bài báo giả.
- Cột không cần thiết (Unnamed: 0) được xóa nếu có.

## 2. Làm sạch dữ liệu

- Loại bỏ trùng lặp: Phát hiện và xóa 10,012 dòng trùng lặp, giảm kích thước dữ liệu từ 78,617 xuống 68,605 dòng.
- Xử lý giá trị thiếu: Xóa các dòng có cột text bị thiếu, giảm còn 68,604 dòng.
- Sao chép dữ liệu: Tạo các bản sao của DataFrame (df\_deeplearning, df\_rnn) để sử dụng cho các mô hình học sâu sau này.

## 3. Kết quả

- DataFrame cuối cùng có 68,604 dòng với hai cột: text (nội dung bài báo) và label (nhãn thật/giả).
- Không còn giá trị thiếu hoặc trùng lặp.

# Phần 2: Khám phá dữ liệu (EDA)

#### 1. Phân tích cơ bản

- Kích thước tập dữ liệu: 68,604 dòng, 2 cột.
- Số bài báo thật: 34,975 (sau khi làm sạch: 34,526).
- Số bài báo giả: 43,642 (sau khi làm sạch: 34,078).
- Phân bố nhãn: Gần cân bằng (50.3% giả, 49.7% thật).

# 2. Trích xuất đặc trưng

Các đặc trưng bổ sung được trính xuất từ văn bản bao gồm:

- num\_words: Số từ trong bài báo.
- num\_chars: Số ký tự.

- avg word len: Độ dài trung bình của từ.
- num\_upper: Số ký tự in hoa.
- num\_punct: Số dấu câu.
- num\_stopwords: Số từ dừng (stopwords).
- 3. Phân tích từ phổ biến dựa trên thống kế

Để hiểu rõ hơn về nội dung văn bản, các từ phổ biến nhất trong mỗi lớp (thật và giả) được thống kê sau khi loại bỏ từ dừng và dấu câu, sử dụng CountVectorizer từ thư viện scikit-learn. Các bước thực hiện bao gồm:

- Tiền xử lý văn bản: Chuyển đổi thành chữ thường, loại bỏ từ dừng và dấu câu.
- Đếm tần suất từ: Lấy 10 từ phổ biến nhất trong bài báo thật và giả.

# Phần 3: Xây dựng mô hình

## 1. Mô hình học máy truyền thống

- Random Forest: Sử dụng tập hợp cây quyết định để phân loại.
- Decision Tree: Một cây quyết định đơn giản.
- XGBoost Classifier: Mô hình gradient boosting mạnh mẽ.
- Logistic Regression: Mô hình tuyến tính dựa trên xác suất.

## 2. Mô hình học sâu

- RNN với LSTM: Mạng nơ-ron hồi quy sử dụng các đơn vị LSTM để xử lý chuỗi văn bản.
- BERT (bert-base-uncased): Mô hình transformer được huấn luyện trước, tinh chỉnh cho bài toán phân loại.
- XLNet (xlnet-base-cased): Mô hình transformer cải tiến, tối ưu hóa cho các nhiệm vụ NLP.

# Phần 4: Thiết lập siêu tham số

## 1. Học máy truyền thống

Sử dụng tìm kiếm lưới (Grid Search) hoặc tìm kiếm ngẫu nhiên (Random Search) để tối ưu hóa siêu tham số như độ sâu cây, số lượng cây (Random Forest), tỷ lệ học (XGBoost), và hệ số điều chuẩn (Logistic Regression).

#### 2. Học sâu

- RNN với LSTM: Tinh chỉnh số lớp ẩn, kích thước embedding, và tỷ lệ dropout.
- BERT và XLNet: Sử dụng các siêu tham số như:
- Số epoch: 3.
- Kích thước batch: 24.
- Chế độ FP16 để tối ưu hóa hiệu suất GPU.
- Tỷ lệ học mặc định của Hugging Face Trainer.

# Phần 5: Huấn luyện mô hình

- Chia dữ liệu: Dữ liệu được chia thành tập huấn luyện (70%), tập xác thực (15%), và tập kiểm tra (15%) dùng cho các mô hình học sâu và huấn luyện (80%) và tập kiểm tra (20%).
- Các mô hình học máy truyền thống được huấn luyện trên các đặc trưng trích xuất từ văn bản (TF-IDF hoặc đặc trưng số).
- Các mô hình học sâu (RNN, BERT, XLNet) được huấn luyện trên văn bản đã mã hóa (tokenized) sử dụng GPU.
- BERT và XLNet được huấn luyện trong 3 epoch, với kết quả được lưu vào thư mục results\_bert và results\_xlnet.

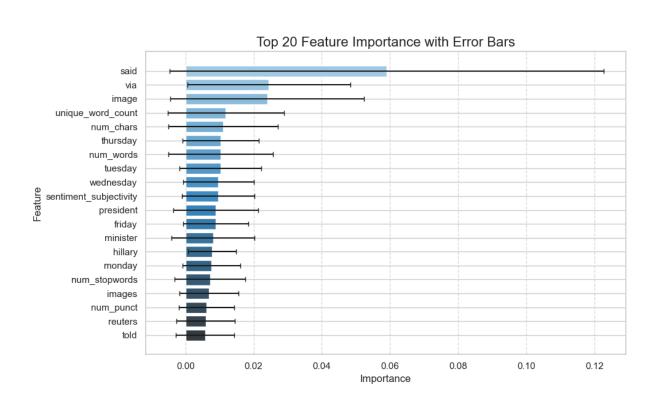
#### 1. Random Forest

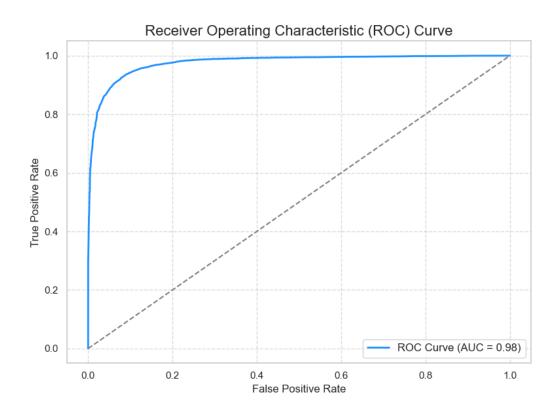
#### Classification Report (Train):

	precision	recall	f1-score	support
0	1.00	1.00	1.00	27262
1	1.00	1.00	1.00	27621
accuracy			1.00	54883
macro avg	1.00	1.00	1.00	54883
weighted avg	1.00	1.00	1.00	54883

Train report saved to reports\rf\_train\_report.txt

	precision	recall	f1-score	support
0	0.93	0.91	0.92	6816
1	0.91	0.94	0.92	6905
accuracy			0.92	13721
macro avg	0.92	0.92	0.92	13721
weighted avg	0.92	0.92	0.92	13721





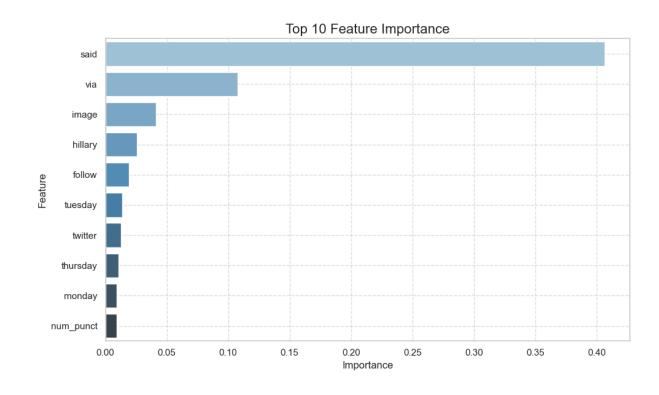
## 2. Decision Tree

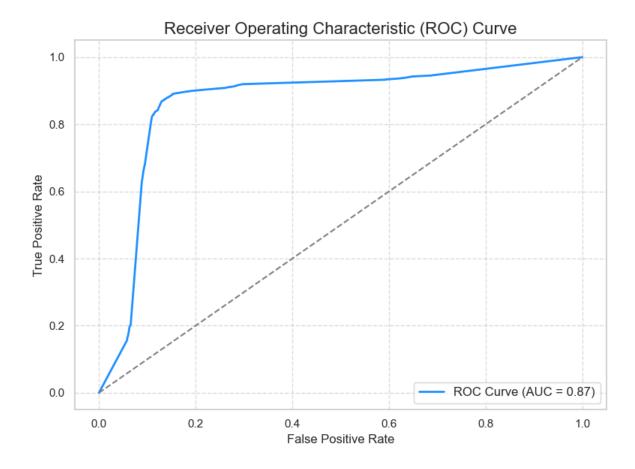
Classification Report (Train):

0 0.96 0.95 0.95 27	262
1 0.95 0.96 0.95 27	621
accuracy 0.95 54	883
macro avg 0.95 0.95 0.95 54	883
weighted avg 0.95 0.95 0.95 54	883

Train report saved to reports\dt\_train\_report.txt

support	f1-score	recall	precision	
6816	0.87	0.86	0.87	0
6905	0.87	0.88	0.87	1
13721	0.87			accuracy
13721	0.87	0.87	0.87	macro avg
13721	0.87	0.87	0.87	weighted avg





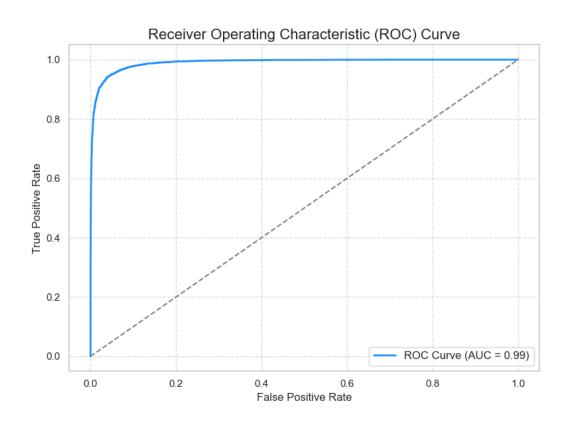
## 3. XGBoost Classifier

Classification Report (Train):

	precision	recall	f1-score	support
0	0.99	1.00	1.00	27262
1	1.00	0.99	1.00	27621
accuracy			1.00	54883
macro avg	1.00	1.00	1.00	54883
weighted avg	1.00	1.00	1.00	54883

Train report saved to 'reports/xgb\_train\_report.txt'

	precision	recall	f1-score	support
0	0.95	0.95	0.95	6816
1	0.95	0.95	0.95	6905
accuracy			0.95	13721
macro avg	0.95	0.95	0.95	13721
weighted avg	0.95	0.95	0.95	13721



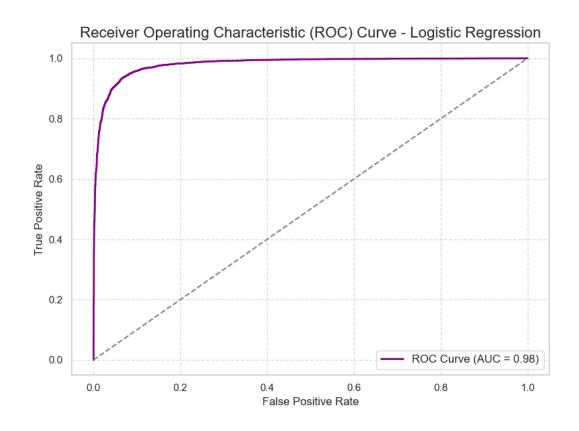
# 4. Logistic Regression

Classification Report (Train):

	precision	récall	f1-score	support
0	0.94	0.95	0.95	27262
1	0.95	0.94	0.95	27621
accuracy			0.95	54883
macro avg	0.95	0.95	0.95	54883
weighted avg	0.95	0.95	0.95	54883

Train report saved to 'reports\lr\_train\_report.txt'

	precision	recall	f1-score	support
0	0.93	0.94	0.93	6816
1	0.94	0.93	0.93	6905
accuracy			0.93	13721
macro avg	0.93	0.93	0.93	13721
weighted avg	0.93	0.93	0.93	13721



#### 5. RNN với LTSM

\_\_\_\_\_

#### MODEL PERFORMANCE METRICS

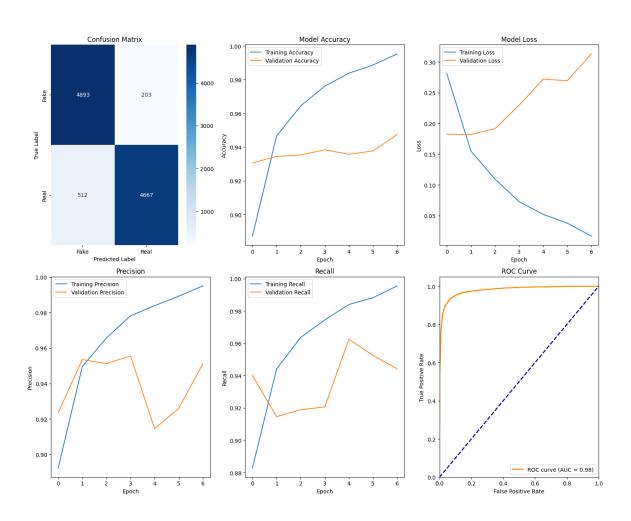
-----

Accuracy: 0.9304 Precision: 0.9583 Recall: 0.9011 F1-Score: 0.9288

#### -----

#### DETAILED CLASSIFICATION REPORT

	precision	recall	f1-score	support
Fake News	0.91	0.96	0.93	5096
Real News	0.96	0.90	0.93	5179
accuracy			0.93	10275
macro avg	0.93	0.93	0.93	10275
weighted avg	0.93	0.93	0.93	10275



#### 6. BERT

Epoch	Training Loss	Validation Loss	Accuracy	F1	Precision	Recall
1	0.101800	0.111401	0.972209	0.972190	0.973213	0.972209
2	0.029200	0.070092	0.982606	0.982605	0.982664	0.982606
3	0.006700	0.082757	0.984744	0.984744	0.984745	0.984744

#### 7. XLNet

Epoch	Training Loss	Validation Loss	Accuracy	F1	Precision	Recall
1	0.087900	0.068309	0.983578	0.983578	0.983584	0.983578
2	0.041000	0.042746	0.986202	0.986200	0.986280	0.986202
3	0.018200	0.040245	0.989408	0.989408	0.989411	0.989408

# Phần 6: Kết luận

- XLNet đạt hiệu suất cao nhất với độ chính xác 99.04% trên tập kiểm tra, vượt trội hơn BERT (98.51%).
- Các mô hình học máy truyền thống và RNN với LSTM có khả năng thấp hơn trong việc xử lý các bài báo phức tạp.
- Tiền xử lý dữ liệu: Dữ liệu được làm sạch hiệu quả, loại bỏ trùng lặp và giá trị thiếu,
   đảm bảo chất lượng đầu vào cho các mô hình.
- EDA cho thấy tập dữ liệu với 68,604 bài báo có phân bố nhãn gần cân bằng (50.3% giả, 49.7% thật), hỗ trợ lựa chọn mô hình và chia dữ liệu hợp lý. Các đặc trưng văn bản như số từ, ký tự, và từ dừng được trích xuất, làm sáng tỏ sự khác biệt ngôn ngữ giữa tin thật và giả, định hướng trích xuất đặc trưng hiệu quả. Những phát hiện này giúp tối ưu hóa tiền xử lý và huấn luyện, đặc biệt cho các mô hình học sâu như BERT và XLNet.
- Huấn luyện và suy diễn: Các mô hình transformer (BERT, XLNet) hoạt động tốt, đặc biệt là XLNet với khả năng học ngữ cảnh hai chiều.

# Phần 7: Đánh giá điểm mạnh, yếu các mô hình

## 1. Random Forest

Điểm mạnh	Điểm yếu
<ul> <li>Khả năng chống overfitting: Sử dụng tập hợp nhiều cây quyết định, giảm thiểu nguy cơ quá khớp so với một cây quyết định đơn lẻ.</li> <li>Xử lý dữ liệu không cân bằng: Có</li> </ul>	<ul> <li>Hiệu suất hạn chế với văn bản:         Không tận dụng được ngữ cảnh chuỗi dài trong dữ liệu văn bản, phụ thuộc nhiều vào đặc trưng trích xuất (như TF-IDF).     </li> </ul>
thể hoạt động tốt trên tập dữ liệu với nhãn không cân bằng nhờ cơ chế lấy mẫu ngẫu nhiên.	<ul> <li>Tốn tài nguyên: Với số lượng cây lớn và dữ liệu lớn (68,604 dòng), thời gian huấn luyện và suy diễn có thể chậm.</li> </ul>
<ul> <li>Dễ sử dụng: Yêu cầu ít tiền xử lý dữ liệu (không cần chuẩn hóa) và dễ tinh chỉnh siêu tham số.</li> <li>Khả năng giải thích: Cung cấp mức</li> </ul>	Khó xử lý ngữ nghĩa phức tạp:  Không hiệu quả trong việc phát hiện các mẫu tin giả sử dụng châm biếm, giễu nhại hoặc ngữ cảnh văn hóa.
độ quan trọng của các đặc trưng, hỗ trợ phân tích các yếu tố ảnh hưởng đến dự đoán.	

## 2. Decision Tree

Điểm mạnh	Điểm yếu		
Dễ hiểu và trực quan: Cấu trúc cây quyết định dễ hình dung, giúp giải thích các quyết định của mô hình.	Dễ overfitting: Một cây quyết định đơn lẻ dễ bị quá khớp, đặc biệt với dữ liệu văn bản phức tạp.		

- Nhanh chóng: Thời gian huấn luyện và suy diễn nhanh trên tập dữ liệu vừa và nhỏ.
- Không cần chuẩn hóa dữ liệu: Có thể xử lý các đặc trung không đồng nhất mà không cần tiền xử lý phức tạp.
- Hiệu suất thấp: So với các mô hình phức tạp hơn, Decision Tree thường có độ chính xác thấp hơn trên bài toán NLP.
- Không tận dụng ngữ cảnh: Không thể nắm bắt được mối quan hệ ngữ nghĩa giữa các từ trong bài báo.

#### 3. XGBoost Classifier

# Điểm mạnh

- Hiệu suất cao: Là một trong những mô hình học máy mạnh mẽ nhất nhờ sử dụng gradient boosting.
- Tối ưu hóa tốc độ: Được tối ưu cho hiệu suất tính toán, phù hợp với tập dữ liêu lớn.
- Khả năng tinh chỉnh: Hỗ trợ nhiều siêu tham số (tỷ lệ học, độ sâu cây, điều chuẩn) để cải thiện hiệu suất.
- Xử lý dữ liệu không cân bằng: Có các tham số như scale\_pos\_weight để xử lý tốt dữ liệu không cân bằng.

## Điểm yếu

- Phụ thuộc vào đặc trưng: Hiệu quả phụ thuộc nhiều vào chất lượng đặc trưng trích xuất (TF-IDF, đặc trưng số).
- Khó giải thích: Mô hình phức tạp hơn Random Forest, khó cung cấp giải thích trực quan cho dự đoán.
- Tốn thời gian tinh chỉnh: Yêu cầu tìm kiếm siêu tham số kỹ lưỡng để đạt hiệu suất tối ưu.

#### 4. Logistic Regression

Điểm mạnh	Điểm yếu		
Đơn giản và hiệu quả: Là mô hình tuyến tính, dễ triển khai và huấn luyện nhanh trên dữ liệu lớn.	Hạn chế với dữ liệu phi tuyến:  Không thể nắm bắt các mối quan hệ  phức tạp trong văn bản.		
<ul> <li>Khả năng giải thích: Hệ số của các đặc trưng có thể được phân tích để hiểu mức độ ảnh hưởng.</li> </ul>	Phụ thuộc vào đặc trưng: Cần trích xuất đặc trưng chất lượng cao (như TF-IDF) để đạt hiệu suất tốt.		
• Tốt cho bài toán nhị phân: Phù hợp với bài toán phân loại thật/giả nhờ đầu ra xác suất.	Không xử lý ngữ cảnh: Không thể hiểu ngữ nghĩa hoặc mối quan hệ chuỗi trong văn bản.		
Ít nhạy cảm với nhiễu: Hoạt động tốt			

## 5. RNN với LSTM

khi đặc trưng được tiền xử lý tốt.

Ðiểm mạnh	Điểm yếu
<ul> <li>Xử lý chuỗi: LSTM có khả năng nắm bắt mối quan hệ tuần tự trong văn bản, phù hợp với bài toán NLP.</li> <li>Học ngữ cảnh dài: Có thể ghi nhớ thông tin từ các từ trước đó, cải thiện việc hiểu ngữ nghĩa.</li> <li>Linh hoạt: Có thể tùy chỉnh kiến trúc (số lớp, kích thước embedding, dropout) để tối ưu hóa.</li> </ul>	<ul> <li>Hiệu suất thấp hơn transformer: So với BERT và XLNet, RNN với LSTM kém hiệu quả trong việc xử lý ngữ cảnh hai chiều.</li> <li>Thời gian huấn luyện lâu: Yêu cầu nhiều thời gian và tài nguyên tính toán, đặc biệt với tập dữ liệu lớn.</li> </ul>

•	Khó tinh chỉnh: Siêu tham số như số
	lớp ẩn, tỷ lệ dropout cần được điều
	chỉnh cẩn thận để tránh overfitting.

 Hạn chế với văn bản dài: LSTM gặp khó khăn khi xử lý các bài báo dài do vấn đề vanishing gradient.

#### 6. BERT (bert-base-uncased)

#### Điểm mạnh Điểm yếu Hiểu ngữ cảnh hai chiều: BERT Tốn tài nguyên: Yêu cầu GPU mạnh được huấn luyện trước trên dữ liệu và RAM lớn để huấn luyện và suy lớn, nắm bắt ngữ nghĩa và mối quan diễn trên tập dữ liệu lớn. hệ ngữ cảnh tốt. Thời gian huấn luyện dài: Mặc dù Hiệu suất cao: Đạt độ chính xác chỉ huấn luyện 3 epoch, thời gian vẫn 98.51% trên tập kiểm tra, phù hợp cho đáng kể (19 phút). bài toán phân loại tin giả. Khó giải thích: Là mô hình black-Khả năng tổng quát: Có thể tinh box, khó phân tích lý do đưa ra dự chỉnh cho nhiều bài toán NLP khác đoán cu thể. nhau. Hạn chế với châm biếm: Có thể gặp Hỗ trợ cộng đồng mạnh: Thư viện khó khăn khi phân biệt tin giả sử dụng Hugging Face cung cấp công cụ dễ sử ngôn ngữ phức tạp hoặc châm biếm.

#### 7. XLNet (xlnet-base-cased)

dụng để huấn luyện và suy diễn.

Điểm mạnh				
Á,	A. D. 40 17	1		

- Hiệu suất vượt trội: Đạt độ chính xác cao nhất (99.04%) nhờ cơ chế học ngữ cảnh hai chiều cải tiến.
- Xử lý chuỗi dài tốt hơn: So với
  BERT, XLNet tối ưu hơn trong việc
  nắm bắt mối quan hệ giữa các từ xa
  nhau.
- Tổng quát hóa tốt: Được huấn luyện trước trên dữ liệu lớn, phù hợp cho nhiều bài toán NLP.
- Khả năng phân biệt ngữ nghĩa phức tạp: Hiệu quả hơn BERT trong việc xử lý các bài báo có ngữ cảnh tinh vi.

# Điểm yếu

- Tốn tài nguyên hơn BERT: Thời gian huấn luyện lâu hơn (29 phút) và yêu cầu bộ nhớ lớn.
- Khó giải thích: Tương tự BERT, là mô hình black-box, khó cung cấp giải thích trực quan.
- Phức tạp trong triển khai: Yêu cầu hiểu biết sâu về transformer và thư viện Hugging Face để tinh chỉnh.
- Hạn chế với dữ liệu đa ngôn ngữ:
   Chỉ hiệu quả trên dữ liệu tiếng Anh,
   cần tinh chỉnh thêm cho các ngôn ngữ
   khác.

# Phần 8: Đề xuất cải thiện

- Mở rộng dữ liệu: Thu thập thêm dữ liệu từ nhiều ngôn ngữ, khu vực, và nguồn để tăng tính tổng quát.
- **Tăng cường đặc trưng**: Kết hợp các đặc trưng bên ngoài như nguồn bài báo, ngày xuất bản, hoặc tín hiệu xã hội (lượt chia sẻ, bình luận).
- Tối ưu hóa mô hình truyền thống: Thực hiện tìm kiếm siêu tham số kỹ lưỡng hơn cho Random Forest, XGBoost, và Logistic Regression.
- Xử lý ngữ cảnh phức tạp: Áp dụng các kỹ thuật như phân tích cảm xúc hoặc phát hiện châm biếm để cải thiện khả năng phân biệt.
- Triển khai thực tế: Xây dựng API hoặc giao diện người dùng để tích hợp mô hình vào các nền tảng kiểm duyệt nội dung.