BIS - MT · 19/05/2026

🤖 Bản Tin AI Hằng Ngày

Cập nhật công nghệ AI mới nhất

✨ *"The function of leadership is to produce more leaders, not more followers."*

↪ Chức năng của lãnh đạo là tạo ra nhiều nhà lãnh đạo hơn, không phải nhiều người theo hơn.

— Ralph Nader

💡 *Người lãnh đạo tốt đầu tư vào việc phát triển người khác — tạo ra những nhà lãnh đạo tiếp theo mới là di sản thật sự.*

📰 TIN TỨC NỔI BẬT

1 Các nhà nghiên cứu bảo mật cảnh báo về lỗ hổng trong code do AI tạo ra

🇬🇧 *Security Researchers Sound the Alarm on Vulnerabilities in AI-Generated Code*

📰 Infosecurity Magazine 🔗 Đọc bài viết →

> Các nhà nghiên cứu bảo mật đã bày tỏ mối quan ngại về các điểm yếu trong mã được tạo ra bởi AI, nhấn mạnh các rủi ro tiềm ẩn liên quan đến công nghệ mới nổi này. Mã được tạo ra bởi AI đang trở nên phổ biến ngày càng tăng, đặc biệt là trong việc phát triển phần mềm và ứng dụng. Tuy nhiên, một nghiên cứu gần đây đã tiết lộ rằng loại mã này có thể chứa các lỗi bảo mật và điểm yếu mà các kẻ tấn công có thể khai thác. Các nhà nghiên cứu đã phát hiện ra rằng mã được tạo ra bởi AI có thể dễ bị lỗi và không nhất quán, khiến nó dễ bị tấn công mạng hơn. Điều này đặc biệt đáng lo ngại vì mã được tạo ra bởi AI thường được sử dụng trong các hệ thống và ứng dụng quan trọng, nơi các vi phạm bảo mật có thể có hậu quả nghiêm trọng. Kết quả nghiên cứu nhấn mạnh nhu cầu của các nhà phát triển phải xem xét và kiểm tra kỹ lưỡng mã được tạo ra bởi AI trước khi triển khai nó trong môi trường sản xuất. Điều này bao gồm việc xác minh tính toàn vẹn của mã, xác định các điểm yếu tiềm ẩn và triển khai các biện pháp bảo mật mạnh mẽ để giảm thiểu rủi ro. Khi mã được tạo ra bởi AI trở nên phổ biến hơn, điều quan trọng là các nhà phát triển và tổ chức phải ưu tiên bảo mật và thực hiện các bước chủ động để giải quyết các điểm yếu tiềm ẩn.

2 Cách chạy các AI model cục bộ trên RTX 5060 Ti của bạn — Hướng dẫn từng bước

🇬🇧 *How to Run Local AI Models on Your RTX 5060 Ti — Step-by-Step Guide*

📰 TechnoSports Media Group 🔗 Đọc bài viết →

> Bài viết cung cấp hướng dẫn từng bước về việc chạy các mô hình AI cục bộ trên card đồ họa NVIDIA RTX 5060 Ti. Hướng dẫn này nhằm giúp người dùng tận dụng sức mạnh của card đồ họa để chạy các mô hình AI trên máy cục bộ của họ, loại bỏ nhu cầu sử dụng dịch vụ đám mây. Để bắt đầu, người dùng cần cài đặt phần mềm cần thiết, bao gồm CUDA Toolkit và cuDNN. Những công cụ này cho phép RTX 5060 Ti xử lý các tính toán AI một cách hiệu quả. Tiếp theo, người dùng phải cài đặt một khuôn khổ học sâu như TensorFlow hoặc PyTorch, cung cấp các thư viện và công cụ cần thiết để xây dựng và chạy các mô hình AI. Khi phần mềm đã được cài đặt, người dùng có thể tải xuống và cài đặt

một mô hình AI đã được đào tạo trước, chẳng hạn như mô hình học máy hoặc thị giác máy tính. Bài viết sau đó hướng dẫn người dùng qua quá trình tải mô hình AI vào khuôn khổ đã chọn và chạy nó trên RTX 5060 Ti. Điều này liên quan đến việc thiết lập các biến môi trường cần thiết và cấu hình khuôn khổ để tận dụng khả năng AI của card đồ họa. Bằng cách làm theo hướng dẫn này, người dùng có thể mở khóa toàn bộ tiềm năng của RTX 5060 Ti và chạy các mô hình AI cục bộ một cách dễ dàng.

3

Tối ưu hóa GitHub workflow bằng generative AI với Amazon Bedrock và MCP | Amazon Web Services

🇬🇧 *Streamline GitHub workflows with generative AI using Amazon Bedrock and MCP | Amazon Web Services*

📰 Amazon Web Services (AWS) 🔗 Đọc bài viết →

Amazon Web Services (AWS) đã giới thiệu một tích hợp mới cho phép người dùng tối ưu hóa các quy trình làm việc trên GitHub với sự giúp đỡ của AI tạo sinh. Tích hợp này kết hợp Amazon Bedrock, một dịch vụ model ngôn ngữ lớn (LLM), với MCP, một nền tảng không phụ thuộc vào model cho việc triển khai và quản lý các model AI. Với tích hợp này, các nhà phát triển có thể tận dụng AI tạo sinh để tự động hóa các nhiệm vụ và nâng cao quy trình làm việc trên GitHub của họ. Bằng cách sử dụng Amazon Bedrock và MCP, người dùng có thể tạo các model AI tùy chỉnh có thể thực hiện các nhiệm vụ như tạo mã, sửa lỗi và tài liệu. Điều này có thể giúp giảm thời gian và công sức cần thiết để hoàn thành các nhiệm vụ này, cho phép các nhà phát triển tập trung vào các nhiệm vụ cấp cao hơn. Tích hợp này cung cấp một trải nghiệm liền mạch cho các nhà phát triển, cho phép họ dễ dàng triển khai và quản lý các model AI của mình trên GitHub. Điều này có thể giúp cải thiện hiệu quả và năng suất tổng thể của các đội phát triển, và cho phép họ xây dựng và triển khai phần mềm chất lượng cao hơn một cách nhanh chóng.

4

Top 11 máy cho mèo ăn tự động tốt nhất chúng tôi đã test trong năm 2026

🇬🇧 *These 11 Automatic Cat Feeders Were the Best We Tested in 2026*

📰 Wired 🔗 Đọc bài viết →

Các máy cho ăn mèo tự động đã cách mạng hóa việc chăm sóc thú cưng, mang lại sự yên tâm cho chủ sở hữu và một lối sống tiện lợi hơn.

Các thiết bị này sử dụng Wi-Fi và ứng dụng di động để lên lịch cho ăn, theo dõi thói quen ăn uống và thậm chí phân phát thức ăn theo yêu cầu. Các mẫu mới hơn đã tích hợp các tính năng tiên tiến như máy ảnh được hỗ trợ bởi AI, có thể phân tích thức ăn còn lại và ngăn chặn việc cho ăn quá mức. Petkit YumShare Dual-Hopper 2 Automatic Feeder With Camera là một lựa chọn hàng đầu, với máy ảnh tích hợp có thể nhận dạng lên đến 20 chú mèo và theo dõi thói quen ăn uống cá nhân. Một sản phẩm nổi bật khác là Petlibro Polar Smart Wet Feeder, một tủ lạnh mini giữ thức ăn ướt tươi và cho phép cho ăn và ghi nhật ký tùy chỉnh. Các máy cho ăn tự động này không chỉ có lợi cho mèo mà còn có thể được sử dụng cho chó nhỏ hơn. Chúng cung cấp một loạt các tính năng, bao gồm cuộc gọi bữa ăn tùy chỉnh, âm thanh hai chiều và tầm nhìn ban đêm, khiến chúng trở thành một công cụ quý giá cho chủ sở hữu thú cưng muốn thúc đẩy thói quen ăn uống lành mạnh và theo dõi sức khỏe của thú cưng.

5

SandboxAQ đưa các drug discovery model của mình lên Claude — không cần bằng PhD về computing

🇬🇧 *SandboxAQ brings its drug discovery models to Claude — no PhD in computing required*

📰 TechCrunch AI 🔗 Đọc bài viết →

SandboxAQ, một công ty được thành lập bởi Alphabet như một công ty độc lập, đã hợp tác với Anthropic để tích hợp các mô hình AI khoa học của mình vào Claude, một giao diện trò chuyện. Động thái này nhằm mục đích đưa các công cụ khám phá thuốc và khoa học vật liệu mạnh mẽ đến tay các nhà nghiên cứu mà không cần cơ sở hạ tầng tính toán chuyên dụng. Các mô hình độc quyền của SandboxAQ, được gọi là Mô hình Lượng tính Lớn (LQMs), là "được thiết lập trên cơ sở vật lý" và có thể chạy các tính toán phức tạp, mô phỏng động lực học phân tử và phản ứng hóa học. Những mô hình này đã được đào tạo trên dữ liệu phòng thí nghiệm thực tế và các phương trình khoa học, khiến chúng phù hợp với nền kinh tế lượng tính, bao gồm các ngành công nghiệp như dược phẩm sinh học, dịch vụ tài chính và năng lượng. Tập trung của công ty là đưa những mô hình này đến với khán giả rộng lớn hơn, chứ không chỉ là các nhà khoa học tính toán và nhà nghiên cứu. Với sự tích hợp này, người dùng có thể truy cập và sử dụng LQMs của SandboxAQ bằng ngôn ngữ tự nhiên, có khả năng cách mạng hóa quá trình khám phá thuốc và các ngành công nghiệp khác.

6 Manchester Code giúp các bit hoạt động ổn định

🇬🇧 *Manchester Code Made Bits Behave*

📰 IEEE Spectrum 🔗 Đọc bài viết →

> Vào cuối những năm 1940, một đội kỹ sư tại Đại học Manchester, Anh, đã đối mặt với một thách thức đáng kể trong lĩnh vực tính toán kỹ thuật số: máy móc có thể tạo ra các bit, nhưng chúng không thể đọc lại chúng một cách đáng tin cậy do thời gian tín hiệu không nhất quán. Dưới sự dẫn dắt của Frederic C. Williams, Tom Kilburn và G.E. (Tommy) Thomas, đội đã nghĩ ra một giải pháp được gọi là mã Manchester hoặc mã hóa pha. Đổi mới này mã hóa mỗi bit với một chuyển tiếp ở giữa khoảng thời gian bit, hiệu quả là nhúng thông tin thời gian trực tiếp vào dòng dữ liệu. Tín hiệu tự đồng hồ này cho phép người nhận liên tục giữ thời gian, ngay cả khi tín hiệu bị suy giảm hoặc thời gian trôi đi slightly. Bằng cách loại bỏ nhu cầu về các đồng hồ riêng biệt và giảm thiểu lỗi đồng bộ hóa, mã Manchester đã làm cho việc truyền dữ liệu trở nên mạnh mẽ hơn trên cáp và mạch. Tác động của nó rất đáng kể, mở đường cho các giao thức mạng và truyền thông kỹ thuật số hiện đại. Vào ngày 13 tháng 4 năm 2026, đột phá này đã được vinh danh với một tấm biển IEEE Milestone trong một lễ trao giải tại Đại học Manchester.

7 Sau Orthogonality: Agency đạo đức đức hạnh và AI Alignment

🇬🇧 *After Orthogonality: Virtue-Ethical Agency and AI Alignment*

📰 The Gradient 🔗 Đọc bài viết →

> Trong bài viết này, tác giả cho rằng những người có lý trí không có mục tiêu, mà thay vào đó, họ căn chỉnh hành động của mình với các thực hành, những mạng lưới gồm các hành động, khuynh hướng, tiêu chí đánh giá và tài nguyên. Quan điểm này có những ý nghĩa quan trọng đối với sự phát triển của trí tuệ nhân tạo (AI) có thể hỗ trợ và cộng tác một cách chân chính với khả năng hành động của con người. Tác giả đề xuất rằng sự suy xét của các tác nhân AI nên chia sẻ một "chữ ký loại" với logic dựa trên thực hành được con người sử dụng, thay vì dựa trên mục tiêu hoặc quy tắc. Tác giả khám phá khái niệm eudaimonia, hay sự thịnh vượng, lý trí và năng động của con người, và cho rằng nó chỉ đến một cấu trúc suy xét khác với lý trí hợp lý tiêu chuẩn. Hình thức hoạt động lý trí này, được gọi là lý trí eudaimonic, được xem là một khuôn khổ hữu ích cho khả năng hành động và giá trị của các AI được căn chỉnh với con người. Tác giả tuyên bố rằng lý trí

eudaimonic là ổn định và an toàn hơn so với khả năng hành động deontological và consequentialist, và nó có thể giúp giải quyết các vấn đề và nghịch lý an toàn AI cổ điển. Tác giả cũng giới thiệu khái niệm "khuyến khích x một cách x", nó nắm bắt ý tưởng rằng hoạt động cuộc sống có ý nghĩa của con người và đạo đức thực sự của con người liên quan đến việc khuyến khích các giá trị một cách nhất quán với những giá trị đó. Bài viết kết thúc bằng cách lập luận rằng lý trí eudaimonic là một hình thức khả năng hành động tự nhiên và hiệu quả, và nó nên được xem xét như một khuôn khổ để căn chỉnh AI với sự thịnh vượng của con người.

8 Mòng biển Glaucous-winged, Bồ nông nâu, Diệc tuyết, Ngỗng Canada

🇬🇧 *Glaucous-winged Gull, Brown Pelican, Snowy Egret, Canada Goose*

📰 Simon Willison 🔗 Đọc bài viết →

Một người đam mê công nghệ đã đi dạo buổi sáng gần sự kiện PyCon US để phát hiện một con Bồ câu nâu trước khi về nhà. Trong chuyến đi, họ đã thành công khi phát hiện ra con chim, mặc dù họ không thể chụp được một bức ảnh rõ ràng. Ngoài ra, họ đã quan sát những con vịt con gần hồ thuyền swan. Bài đăng cũng đề cập đến một cơ hội tài trợ cho một bản tóm tắt email được chỉnh sửa của các phát triển Large Language Model (LLM) quan trọng nhất trong tháng với giá 10 đô la mỗi tháng.

⚡ TIPS & TRICKS CHO DEV

⚡ Quản lý context window

Vấn đề: Quản lý context window để tránh mất thông tin quan trọng.

Cách làm: Sử dụng kỹ thuật **windowing** để chia nhỏ văn bản thành các phần nhỏ hơn, như ví dụ: `Claude: Summarize the text into 3 sentences, considering only the last 100 words`.

Đánh giá: Hiệu quả khi xử lý văn bản dài, giúp tránh mất thông tin quan trọng.

⚡ Tối ưu hóa long-context

Vấn đề: Tối ưu hóa long-context để tăng hiệu suất xử lý văn bản dài.

Cách làm: Sử dụng kỹ thuật **caching** để lưu trữ thông tin đã xử lý, như ví dụ: `Transformers: use_cache=True` trong thư viện Hugging Face.

Đánh giá: Hiệu quả khi xử lý văn bản dài, giúp giảm thời gian xử lý.

⚡ Quản lý memory

Vấn đề: Quản lý memory để tránh lỗi tràn bộ nhớ khi xử lý dữ liệu lớn.

Cách làm: Sử dụng kỹ thuật **batching** để chia nhỏ dữ liệu thành các phần nhỏ hơn, như ví dụ: `Batch size=32` trong lệnh□□ mô hình.

Đánh giá: Hiệu quả khi xử lý dữ liệu lớn, giúp tránh lỗi tràn bộ nhớ.

📚 BÀI HỌC AI HÔM NAY CHO DEV

1. **Tối ưu chi phí & hiệu năng LLM**
2. Để giảm thiểu chi phí và tăng hiệu năng của mô hình ngôn ngữ lớn (LLM), các nhà phát triển cần biết cách tối ưu hóa chúng. Điều này giúp cải thiện hiệu suất và giảm thiểu chi phí tính toán. Việc tối ưu hóa LLM cũng giúp tăng cường bảo mật và giảm thiểu rủi ro.
3. Ví dụ, có thể sử dụng kỹ thuật fine-tuning và LoRA (Low-Rank Adaptation) để tối ưu hóa LLM cho các use case cụ thể. Điều này giúp giảm thiểu số lượng tham số và tăng cường hiệu suất của mô hình.
4. 💡 Tip hoặc bước tiếp theo: Sử dụng các công cụ như Hugging Face Transformers và các thư viện khác để thực hiện fine-tuning và LoRA cho LLM của bạn, và theo dõi hiệu suất của mô hình để đảm bảo rằng nó hoạt động tốt nhất có thể.