BIS - MT · 07/07/2026

Bản Tin AI Hằng Ngày

Cập nhật công nghệ AI mới nhất

“Chớ thấy sóng cả mà ngã tay chèo.”

— Tục ngữ Việt Nam

Trước khó khăn lớn, đừng bỏ cuộc — giữ vững ý chí và tiếp tục nỗ lực mới là con đường đến thành công.

TIN TỨC NỔI BẬT

1

Chuyên gia bảo mật cảnh báo lỗ hổng trong mã nguồn do AI tạo.

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 đối với bảo mật phần mềm. Vấn đề này phát sinh từ sự phụ thuộc vào các thuật toán học máy, có thể giới thiệu các lỗi và điểm yếu vào mã. Các điểm yếu này có thể bị khai thác bởi các kẻ tấn công, làm tổn hại đến tính toàn vẹn và bảo mật của phần mềm. Các nhà nghiên cứu đã xác định một số vấn đề với mã được tạo ra bởi AI, bao gồm khả năng có backdoor, chức năng không mong muốn và xử lý lỗi kém. Việc sử dụng các model đã được đào tạo trước và thử nghiệm hạn chế cũng có thể dẫn đến các hậu quả không lường trước. Hơn nữa, sự thiếu minh bạch và giải thích trong mã được tạo ra bởi AI làm cho việc xác định và giải quyết các điểm yếu trở nên thách thức. Các phát hiện này nhấn mạnh nhu cầu của các developer phải đánh giá và thử nghiệm cẩn thận mã được tạo ra bởi AI trước khi triển khai. Điều này bao gồm việc thực hiện các thủ tục thử nghiệm và xác thực mạnh mẽ để đảm bảo mã đáp ứng các tiêu chuẩn bảo mật. Cảnh báo của các nhà nghiên cứu đóng vai trò như một lời nhắc nhở về tầm quan trọng của sự giám sát và xem xét của con người trong quá trình phát triển, đặc biệt khi sử dụng mã được tạo ra bởi AI.

2

AWS mã nguồn mở MCP Server cho Bedrock AgentCore để tinh gọn phát triển AI Agent.

AWS Open-Sources an MCP Server for Bedrock AgentCore to Streamline AI Agent Development

MarkTechPost Đọc bài viết →

Amazon Web Services (AWS) đã mở nguồn một máy chủ MCP (Nền tảng Đa đám mây) cho Bedrock AgentCore, một framework được thiết kế để đơn giản hóa việc phát triển các tác nhân AI. Việc này nhằm mục đích đơn giản hóa quá trình tạo và triển khai các tác nhân AI trên nhiều môi trường đám mây khác nhau. Máy chủ MCP là một thành phần quan trọng của Bedrock AgentCore, cho phép các nhà phát triển quản lý và điều phối các tác nhân AI trên nhiều nền tảng đám mây, bao gồm AWS, Azure và Google Cloud. Bằng cách mở nguồn máy chủ MCP, AWS cung cấp một giao diện tiêu chuẩn hóa cho việc phát triển tác nhân AI, giúp các nhà phát triển dễ dàng xây dựng và triển khai các ứng dụng được hỗ trợ bởi AI trên các môi trường đám mây khác nhau. Việc phát hành mã nguồn mở này dự kiến sẽ đẩy nhanh việc phát triển và triển khai tác nhân AI, vì các nhà phát triển hiện có thể tận dụng một nền tảng thống nhất để tạo và quản lý các tác nhân AI trên nhiều nền tảng đám mây. Máy chủ MCP sẽ có sẵn dưới giấy phép Apache 2.0, cho phép các nhà phát triển sửa đổi và mở rộng mã để đáp ứng nhu cầu cụ thể của họ.

3

Các model open-weight hàng đầu Trung Quốc — và những đối thủ mạnh nhất từ Mỹ.

The best Chinese open-weight models — and the strongest US rivals

understandingai.org Đọc bài viết →

Bài viết thảo luận về các mẫu xe điện không giới hạn trọng lượng hàng đầu của Trung Quốc và các đối thủ mạnh nhất của Mỹ. Các mẫu xe không giới hạn trọng lượng đề cập đến xe điện có thiết kế tối giản, thường không có mái cố định hoặc cửa. Các nhà sản xuất Trung Quốc đã đi đầu trong xu hướng này, cung cấp các lựa chọn sáng tạo và thời trang. Một số mẫu xe không giới hạn trọng lượng hàng đầu của Trung Quốc được đề cập bao gồm FAW Hongqi H9, BYD Tang và Geely Geometry A. Những xe này cung cấp sự kết hợp độc đáo giữa hiệu suất, sự thoải mái và phong cách, khiến chúng trở nên phổ biến среди người tiêu dùng. Bài viết cũng nhấn mạnh những đối thủ mạnh nhất của Mỹ đối với các mẫu xe Trung Quốc này. Tuy nhiên, các mẫu xe cụ thể của Mỹ không được cung cấp trong nội dung cho trước. Bài viết kết thúc bằng cách nhấn mạnh sự cạnh tranh ngày càng tăng trong thị

trường không giới hạn trọng lượng, với các nhà sản xuất Trung Quốc đang đẩy ranh giới của sự đổi mới và thiết kế. Bài viết dường như tập trung vào ngành công nghiệp ô tô, đặc biệt là xe điện và các mẫu xe không giới hạn trọng lượng, và cung cấp một so sánh giữa các nhà sản xuất Trung Quốc và Mỹ.

4

VHF Propagation: Những điều mọi RF Engineer cần biết.

VHF Propagation: What Every RF Engineer Should Know

IEEE Spectrum Đọc bài viết →

Sự lan truyền VHF: Hiểu rõ sự phức tạp của tín hiệu tần số vô tuyến Tần số VHF, trải từ 30-300 MHz, được sử dụng cho nhiều ứng dụng khác nhau bao gồm phát sóng, liên lạc giọng nói, dẫn đường hàng không và radar quốc phòng. Tuy nhiên, giả định chung rằng tín hiệu VHF cần một "đường ngắm" để hoạt động là một sự đơn giản hóa quá mức. Trên thực tế, tín hiệu VHF tương tác với khí quyển và các vật thể vật lý, dẫn đến sự khúc xạ, phản xạ và tán xạ. Những hiệu ứng hàng ngày này có thể được bổ sung bởi một số chế độ không phổ biến giúp mở rộng đáng kể phạm vi VHF. Những chế độ này bao gồm ống dẫn troposphere, sự kiện E спорадический, đường mòn ion hóa của sao chổi và liên lạc Trái Đất-Mặt Trăng-Trái Đất. Bài báo này nhằm mục đích giáo dục các kỹ sư và nhà lập kế hoạch về vật lý, đặc điểm và ý nghĩa hoạt động của các chế độ này, cung cấp kiến thức thiết yếu cho thiết kế hệ thống VHF hiệu quả.

5

300 USD cổ phần của gia đình bạn tại OpenAI.

Your family's $300 stake in OpenAI

MIT Tech Review Đọc bài viết →

Giám đốc điều hành OpenAI Sam Altman đã đề xuất một kế hoạch để trao cho chính phủ Mỹ một cổ phần 5% trong công ty, được định giá khoảng 42,6 tỷ USD. Cổ phần này sẽ được phân phối среди các hộ gia đình Mỹ, có thể cung cấp cho mỗi hộ khoảng 320 USD cổ phần. Ý tưởng này dựa trên quan niệm rằng các công ty AI nên bồi thường cho cá nhân về giá trị mà họ tạo ra, vì AI học hỏi từ công việc do con người tạo ra. Điều này có thể phục vụ như một hình thức bồi thường chậm trễ và cung cấp một mạng lưới an toàn cho những người có thể mất việc do tự động hóa AI. Kế hoạch này được cho là đang được thảo luận với Tổng thống Trump, người có lịch sử làm các thỏa thuận công nghệ.

Tuy nhiên, chi tiết của đề xuất vẫn còn hạn chế, và vẫn chưa rõ liệu một kế hoạch cụ thể sẽ được hình thành. Thượng nghị sĩ Bernie Sanders đã đề xuất một kế hoạch tham vọng hơn, trao cho người Mỹ một cổ phần 50% trong các công ty AI hàng đầu. Ý tưởng này có sức hấp dẫn chính trị rộng rãi nhưng vẫn chủ yếu là một câu chuyện chứ không phải là một kế hoạch chính sách.

6

Agentic Batch Changes hiện đã ra mắt public beta.

Agentic Batch Changes is now in public beta

Sourcegraph Blog Đọc bài viết →

Agentic Batch Changes đã bước vào giai đoạn beta công khai, đánh dấu một bước phát triển quan trọng trong việc di chuyển mã tự động. Trình đại lý này được hỗ trợ bởi AI, được thiết kế để tối ưu hóa việc cập nhật mã quy mô lớn trên nhiều kho lưu trữ. Các khả năng của nó bao gồm xác định phạm vi, thực thi và vận chuyển các bản di chuyển mã, cuối cùng đảm bảo rằng tất cả các yêu cầu kéo (PRs) đều có thể hợp nhất. Chức năng chính của trình đại lý này là đơn giản hóa quá trình cập nhật cơ sở mã, một nhiệm vụ có thể tốn thời gian và đòi hỏi nhiều lao động. Bằng cách tự động hóa quá trình này, các nhà phát triển có thể tập trung vào các khía cạnh khác của công việc, chẳng hạn như viết mã mới hoặc giải quyết các vấn đề quan trọng. Phiên bản beta công khai của Agentic Batch Changes cho thấy công nghệ này hiện đã có sẵn để thử nghiệm và đánh giá bởi một đối tượng rộng lớn hơn. Động thái này có thể báo hiệu tiềm năng của trình đại lý này trở thành một công cụ hữu ích cho các nhà phát triển và tổ chức nhằm cải thiện các quy trình quản lý và bảo trì mã của họ.

7

Framework ASPIRE của Nvidia tăng tốc lập trình robot bằng AI tự cải thiện như thế nào.

How Nvidia's ASPIRE framework accelerates robot programming with self-improving AI

BD Tech Talks Đọc bài viết →

Khung ASPIRE của Nvidia là một giải pháp đột phá cho các thách thức lập trình robot truyền thống. Nó sử dụng một phương pháp AI tự cải thiện cho phép các hệ thống trí tuệ nhân tạo viết, thực thi và tinh chỉnh các chương trình điều khiển robot một cách tự động. ASPIRE chẩn đoán các lỗi của chính nó và tích lũy các sửa chữa thành công vào một thư viện kỹ năng có thể tái sử dụng, giảm đáng kể nỗ lực lập

trình, token và gỡ lỗi cần thiết trên các robot vật lý. Khung này phù hợp với xu hướng ngành công nghiệp hướng tới các hệ thống tự cải thiện, có thể thích nghi và triển khai các hệ thống robot trong các môi trường phức tạp. ASPIRE hoạt động như một kỹ sư robot senior, liên tục học hỏi từ kinh nghiệm và tích lũy kiến thức có thể chuyển giao. Không giống như các tác nhân mã hóa robot hiện tại, ASPIRE có thể xác định nguyên nhân gốc rễ của các lỗi và phát triển các chiến lược sửa chữa hiệu quả. Nó cũng có thể nhớ các giải pháp thành công và áp dụng chúng cho các nhiệm vụ trong tương lai, cho phép nó trở nên tốt hơn theo thời gian. Khung ASPIRE có tiềm năng cách mạng hóa lĩnh vực robot bằng cách cho phép robot học hỏi từ kinh nghiệm và cải thiện hiệu suất của chúng một cách tự động. Khả năng tích lũy kiến thức có thể tái sử dụng và thích nghi với các tình huống mới làm cho nó trở thành một phát triển thú vị trong lĩnh vực trí tuệ nhân tạo, đặc biệt là LLM và API, mang lại nhiều cơ hội cho các developer trong việc xây dựng các model và framework mới.

8

Mets gặp khó khăn: Lindor và Stearns nhận trách nhiệm về khởi đầu tệ hại.

Mets' Struggles: Lindor and Stearns Take Responsibility for Dismal Start

Dev.to AI Đọc bài viết →

Đội bóng chày New York Mets đang gặp khó khăn trong mùa giải này, đứng cuối bảng xếp hạng National League East. Trong một diễn biến gần đây, huấn luyện viên Carlos Mendoza đã bị sa thải, khiến ngắnstop Francisco Lindor và chủ tịch vận hành bóng chày David Stearns phải chịu trách nhiệm về hiệu suất kém của đội. Đây là một biểu hiện hiếm thấy về trách nhiệm từ các vận động viên và ban quản lý, khi họ thừa nhận những khó khăn của đội và tự nhận trách nhiệm về hành động của mình. Lindor tuyên bố rằng các cầu thủ đã "thất bại" Mendoza, trong khi Stearns nhấn mạnh rằng mọi người đều phải chịu trách nhiệm về hiệu suất của đội. Sự thay đổi trong thái độ này có thể là một bước ngoặt cho Mets, khi họ bắt đầu tập trung vào việc thực hiện những thay đổi và cải thiện trò chơi của mình. Với Mendoza rời đi, đội sẽ cần tìm một huấn luyện viên mới để dẫn dắt họ thoát khỏi tình trạng này. Mets sẽ cần tái tập hợp và tái tập trung, giải quyết các vấn đề như tấn công yếu kém và phòng thủ lỏng lẻo. Nếu đội sẵn sàng làm việc, họ có thể đang trên con đường trở lại.

TIPS & TRICKS CHO DEV

Sử dụng LangSmith

Vấn đề: Khó theo dõi hiệu suất mô hình AI.

Cách làm: Sử dụng LangSmith để theo dõi và phân tích hiệu suất mô hình. Ví dụ, lệnh `langsmith monitor` giúp theo dõi tiến trình đào tạo.

Đánh giá: Hiệu quả cao trong việc tối ưu hóa mô hình, đặc biệt khi đào tạo mô hình lớn.

Tích hợp Langfuse

Vấn đề: Chi phí đào tạo mô hình AI cao.

Cách làm: Tích hợp Langfuse để giảm chi phí đào tạo mô hình. Ví dụ, lệnh `langfuse optimize` giúp giảm thiểu tài nguyên cần thiết.

Đánh giá: Giúp giảm chi phí đào tạo mô hình, đặc biệt khi sử dụng tài nguyên điện toán đám mây.

Triển khai Arize Phoenix

Vấn đề: Khó kiểm soát và theo dõi mô hình AI trong sản xuất.

Cách làm: Triển khai Arize Phoenix để giám sát và kiểm soát mô hình AI trong sản xuất. Ví dụ, lệnh `arize phoenix deploy` giúp triển khai mô hình nhanh chóng.

Đánh giá: Hiệu quả cao trong việc đảm bảo mô hình AI hoạt động ổn định và đáng tin cậy trong sản xuất.

BÀI HỌC AI HÔM NAY CHO DEV

1. **Tích hợp AI API vào ứng dụng**
2. Tích hợp AI API vào ứng dụng giúp tăng cường khả năng xử lý và phân tích dữ liệu, từ đó cải thiện trải nghiệm người dùng. Điều này cho phép các nhà phát triển tạo ra các ứng dụng thông minh hơn, có thể tự động hóa các nhiệm vụ và đưa ra quyết định dựa trên dữ liệu. Việc tích hợp AI API cũng giúp giảm thiểu thời gian và công sức phát triển.
3. Ví dụ, một ứng dụng có thể sử dụng API của Google Cloud Vision để phân tích hình ảnh và nhận diện đối tượng, hoặc sử dụng API của IBM Watson để phân tích ngôn ngữ tự nhiên và trả lời câu hỏi của người dùng.
4. Tip hoặc bước tiếp theo: Để bắt đầu tích hợp AI API vào ứng dụng, các nhà phát triển nên nghiên cứu các dịch vụ AI API hiện có và chọn dịch vụ phù hợp với nhu cầu của ứng dụng, sau đó đọc tài liệu và thực hiện các bước tích hợp theo hướng dẫn.