BIS - MT · 14/06/2026

Bản Tin AI Hằng Ngày

Cập nhật công nghệ AI mới nhất

“In three words I can sum up everything I've learned about life: it goes on.”

↪ Trong ba chữ tôi có thể tóm tắt tất cả những gì đã học về cuộc sống: nó tiếp tục.

— Robert Frost

Cuộc sống không dừng lại vì bất kỳ điều gì — dù vui hay buồn, tốt hay xấu, hãy tiếp tục bước về phía trước.

TIN TỨC NỔI BẬT

1

Mọi người đều muốn tham gia "vibe coding" — Google cũng không ngoại lệ với Stitch, dự án kế nhiệm Jules

Everyone's looking to get in on vibe coding — and Google is no different with Stitch, its follow-up to Jules

Venturebeat Đọc bài viết →

> Google đang tham gia vào xu hướng "lập trình cảm giác" với việc phát hành Stitch, dự án tiếp theo sau Jules. Thuật ngữ "lập trình cảm giác" đề cập đến sự quan tâm ngày càng tăng trong việc tạo ra các công cụ lập trình cung cấp trải nghiệm□□ và tương tác hơn cho các nhà phát triển. Mặc dù các chi tiết cụ thể về Stitch vẫn chưa rõ ràng, nhưng nó được định vị là người kế thừa của Jules, một dự án nhằm đơn giản hóa quá trình xây dựng và triển khai các model học máy. Với Stitch, Google có khả năng xây dựng trên nền tảng được đặt ra bởi Jules, có khả năng cung cấp các tính năng và khả năng mới giúp nâng cao trải nghiệm của nhà phát triển. Động thái này là một phần của xu hướng rộng lớn hơn trong ngành công nghệ, nơi các công ty đang đầu tư vào các công cụ và công nghệ giúp làm cho việc lập trình trở nên dễ tiếp cận và thú vị hơn. Khi nhu cầu về các nhà phát triển có kỹ năng tiếp tục tăng, các công ty đang tìm cách làm cho quá trình lập trình trở nên hấp dẫn và hiệu quả hơn.

2

Hướng dẫn đầy đủ về các file bộ nhớ của AI Agent (CLAUDE.md, AGENTS.md và hơn thế nữa)

The Complete Guide to AI Agent Memory Files (CLAUDE.md, AGENTS.md, and Beyond)

HackerNoon Đọc bài viết →

Bài viết này cung cấp một hướng dẫn chi tiết về các tệp tin bộ nhớ của tác nhân AI, tập trung cụ thể vào CLAUDE.md và AGENTS.md. Những tệp tin này là các thành phần quan trọng của hệ thống AI, lưu trữ thông tin về kiến thức, mục tiêu và tương tác của tác nhân. CLAUDE.md là một tệp tin siêu dữ liệu chứa thông tin về bộ nhớ của tác nhân, chẳng hạn như đồ thị kiến thức và khả năng suy luận của nó. AGENTS.md, mặt khác, là một tệp tin cấu hình định nghĩa hành vi và tương tác của tác nhân với môi trường. Bài viết giải thích cách những tệp tin này được sử dụng trong hệ thống AI, bao gồm vai trò của chúng trong việc xây dựng đồ thị kiến thức, suy luận và ra quyết định. Nó cũng thảo luận về tầm quan trọng của những tệp tin này trong việc đảm bảo tính nhất quán và tính hợp lý trong hành động và quyết định của tác nhân. Hướng dẫn cung cấp thông tin về cấu trúc và nội dung của những tệp tin này, làm cho nó trở thành một tài nguyên quý giá cho các nhà phát triển và nhà nghiên cứu làm việc với tác nhân AI. Bằng cách hiểu CLAUDE.md và AGENTS.md, các nhà phát triển có thể thiết kế và triển khai hệ thống AI hiệu quả, hiệu lực và đáng tin cậy hơn.

3

AWS open-source MCP server cho Bedrock AgentCore nhằm 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 thực hiện một bước tiến quan trọng trong lĩnh vực trí tuệ nhân tạo (AI) bằng cách mở nguồn một máy chủ MCP (Lập kế hoạch đa tiêu chí) cho Bedrock AgentCore. Phát triển này nhằm mục đích đơn giản hóa quá trình tạo ra các tác nhân AI, là các thành phần quan trọng trong nhiều ứng dụng như robot, xe tự hành và nhà thông minh. Máy chủ MCP được thiết kế để hoạt động liền mạch với Bedrock AgentCore, một framework cho phép các nhà phát triển xây dựng, đào tạo và triển khai các tác nhân AI một cách hiệu quả. Bằng cách mở nguồn máy chủ MCP, AWS đang cung cấp cho cộng đồng nhà phát triển một tài nguyên quý giá có thể được sử dụng để đẩy nhanh quá trình phát triển tác nhân AI. Máy chủ MCP dự kiến

sẽ đơn giản hóa quá trình tạo ra các tác nhân AI bằng cách cung cấp một giải pháp tiêu chuẩn hóa và có thể mở rộng cho việc lập kế hoạch đa tiêu chí. Điều này, đến lượt, có thể dẫn đến việc phát triển và triển khai các ứng dụng được hỗ trợ bởi AI nhanh hơn, cuối cùng thúc đẩy sự đổi mới trong nhiều ngành công nghiệp. Việc mở nguồn máy chủ MCP đánh dấu một bước tiến quan trọng trong nỗ lực của AWS nhằm thúc đẩy sự phát triển và áp dụng AI.

4

Box AI đã xây dựng các enterprise content agent bằng Deep Agents như thế nào

How Box AI built enterprise content agents with Deep Agents

LangChain Blog Đọc bài viết →

Box, một nền tảng quản lý nội dung thông minh, đã phát triển các đại lý nội dung doanh nghiệp với Deep Agents, một công nghệ cho phép tìm kiếm trên toàn bộ thư viện nội dung của doanh nghiệp và tổng hợp kết quả trên hàng nghìn tài liệu. Box Agent, một phần của Box AI, cho phép người dùng đặt câu hỏi phức tạp và nhận báo cáo cũng như phân tích trong khi vẫn tôn trọng các bảo mật và quyền truy cập hiện có. Ban đầu, Box Agent chỉ có thể tìm kiếm trong một tài liệu duy nhất, nhưng nó đã phát triển để xử lý các truy vấn phức tạp trên các lĩnh vực khác nhau. Để đạt được điều này, Box cần một kiến trúc đại lý vượt qua các câu hỏi và trả lời tiêu chuẩn, dẫn họ đến việc chọn Deep Agents cho lớp trừu tượng hóa model và khung đại lý mở. Kiến trúc của Box Agent sử dụng mô hình cha/con, nơi cha (Global Agent) nhận yêu cầu, phân loại ý định và quyết định xem có xử lý trực tiếp hay tạo ra các đại lý con để phân phối công việc. Thiết kế này cho phép xử lý hiệu quả các nhiệm vụ phức tạp và tạo ra các đại lý con động, cho phép hệ thống xử lý các nhiệm vụ mà chưa được thiết kế rõ ràng.

5

Nghiên cứu bảo mật của Amazon được cho là nguyên nhân khiến Nhà Trắng cấm Anthropic Fable

Amazon security research reportedly led to the White House's Anthropic Fable ban

The Verge AI Đọc bài viết →

Nghiên cứu an ninh mạng của Amazon đã được cho là đã góp phần vào quyết định của Nhà Trắng cấm Anthropic's Fable 5 và Mythos 5 được truy cập bởi người nước ngoài. Theo Wall Street Journal, nghiên cứu của Amazon đã phát hiện ra rằng Fable 5 có thể bị khai thác để cung

cấp thông tin có thể được sử dụng trong các cuộc tấn công mạng. CEO Andy Jassy đã chia sẻ những phát hiện này với Nhà Trắng, dẫn đến chỉ thị kiểm soát xuất khẩu. Anthropic đã tranh cãi về việc mô tả vấn đề này là một "jailbreak", cho rằng các lỗ hổng tương tự có thể được phát hiện bằng cách sử dụng các model công khai khác. Việc cấm này đã gây ra sự phức tạp cho các nhà nghiên cứu sinh ra ở nước ngoài của Anthropic, những người bị cấm truy cập vào sản phẩm của chính họ. Quyết định này đã gây ra tranh luận, với một số nhà nghiên cứu bảo mật ủng hộ cách giải thích của Anthropic và những người khác suy đoán rằng sự không thích của Nhà Trắng đối với công ty có thể đã ảnh hưởng đến quyết định.

6

Preply kết hợp AI và gia sư người thật để cá nhân hóa việc học như thế nào

How Preply combines AI and human tutors to personalize learning

OpenAI Blog Đọc bài viết →

Preply, một nền tảng học ngôn ngữ, đã tích hợp công nghệ OpenAI để nâng cao trải nghiệm học tập của mình. Công ty đã phát triển các bản tóm tắt bài học được tạo bởi AI, cung cấp phản hồi cá nhân hóa và các bài tập học ngôn ngữ. Cách tiếp cận đổi mới này nhằm cung cấp trải nghiệm học tập được tùy chỉnh hơn cho người dùng. Bằng cách tận dụng OpenAI, hệ thống AI của Preply có thể phân tích nhu cầu học tập cá nhân và tạo ra nội dung được tùy chỉnh để hỗ trợ phát triển ngôn ngữ. Các bản tóm tắt và bài tập được tạo bởi AI được thiết kế để bổ sung cho hướng dẫn của các gia sư người thật, cho phép học sinh nhận được cả phản hồi tự động và của con người. Sự kết hợp giữa AI và chuyên môn của con người dự kiến sẽ cải thiện hiệu quả của việc học ngôn ngữ, làm cho nó trở nên hấp dẫn và hiệu quả hơn. Việc tích hợp công nghệ OpenAI là một bước phát triển quan trọng cho Preply, đặt nền tảng này vào vị trí hàng đầu trong lĩnh vực đổi mới học ngôn ngữ.

7

The Download: "Tái lập trình" lão hóa và giác quan ẩn interoception

The Download: “reprogramming” aging, and the hidden sense of interoception

MIT Tech Review Đọc bài viết →

Trong phiên bản hôm nay của The Download, một công ty công nghệ sinh học có tên Life Biosciences đã cho bệnh nhân đầu tiên sử dụng

một phương pháp điều trị thử nghiệm nhằm mục đích đảo ngược các bệnh liên quan đến tuổi tác. Phương pháp điều trị này bao gồm việc tiêm một chất vào nhãn cầu để tái tạo các dây thần kinh khỏe mạnh và có khả năng đảo ngược bệnh glaucôm. Nếu thành công, các phương pháp điều trị tương tự có thể đảo ngược các bệnh khác liên quan đến lão hóa, và thậm chí đảo ngược quá trình lão hóa hoàn toàn, bằng cách "lập trình lại" các tế bào để trở về trạng thái trẻ hơn. Cách tiếp cận này là một trong nhiều cách được các công ty công nghệ sinh học khám phá để làm chậm và đảo ngược quá trình lão hóa. Trong khi đó, các nhà nghiên cứu đang làm việc để hiểu rõ hơn về khái niệm cảm nhận nội tại, hoặc cách chúng ta cảm nhận bản thân từ bên trong. Giải thưởng Nobel năm 2021 và các công cụ mới đã dẫn đến sự gia tăng nghiên cứu, với những ý nghĩa đối với việc điều trị các tình trạng như béo phì, đau mãn tính và lo lắng. Ngoài ra, nhiều câu chuyện về công nghệ đang làm tiêu đề, bao gồm cả việc IPO kỷ lục của SpaceX, startup AI công nghiệp mới của Jeff Bezos và việc tăng cường thực thi công nghệ của các nhà quản lý Trung Quốc. Các chủ đề khác bao gồm vụ kiện của Google chống lại Gemini về các trò lừa đảo dựa trên AI và tiềm năng của AI trong việc thống nhất mạng lưới chiến trường trong chiến tranh, cũng như các chủ đề khác liên quan đến AI, API, LLM, model, token, developer, framework, v.v.

8

Anthropic chặn mọi truy cập công khai vào Claude Fable 5, Mythos 5 theo lệnh của chính phủ Mỹ — các enterprise nên làm gì

Anthropic blocks all public access to Claude Fable 5, Mythos 5 following US government order — what enterprises should do

VentureBeat Đọc bài viết →

Chính phủ Mỹ đã ban hành một chỉ thị kiểm soát xuất khẩu chưa từng có, yêu cầu Anthropic đình chỉ truy cập vào các mô hình AI hàng đầu của mình, Claude Fable 5 và Claude Mythos 5, đối với người nước ngoài. Để đáp lại, Anthropic đã chặn tất cả truy cập công khai vào các mô hình này, ảnh hưởng đến cả khách hàng doanh nghiệp trả phí và người dùng nội bộ. Chỉ thị này được đưa ra chỉ ba ngày sau khi phát hành công khai Fable/Mythos 5 và được cho là liên quan đến việc một người dùng có tên "Pliny the Liberator" đã jailbreak mô hình. Hành động của chính phủ này служ như một cảnh báo cho lĩnh vực doanh nghiệp về rủi ro khi phụ thuộc vào các mô hình AI tập trung, dựa trên đám mây, có thể bị kiểm soát và tuân thủ của chính phủ và nhà cung cấp. Anthropic đã xin lỗi khách hàng của mình và tuyên bố rằng họ đang làm việc để khôi phục truy cập càng sớm càng tốt. Tuy nhiên,

> công ty lưu ý rằng các khả năng được phát hiện bởi jailbreak là "có sẵn rộng rãi" trong các mô hình công khai khác, bao gồm cả mô hình GPT-5.5 của đối thủ OpenAI. Sự mất điện đột ngột của các mô hình AI mới nhất của Anthropic làm nổi bật sự cần thiết của sự dư thừa và đa dạng hóa AI trong doanh nghiệp, vì việc phụ thuộc vào một mô hình AI hoặc nhà cung cấp duy nhất tạo ra một điểm thất bại duy nhất, giòn. Sự việc này đã gây ra một cuộc tranh luận về sự đánh đổi giữa việc chạy các mô hình trọng lượng mở cục bộ trên phần cứng chủ quyền và việc áp dụng các mô hình AI tập trung tiên tiến. Trong khi các mô hình cục bộ cung cấp quyền kiểm soát tuyệt đối và miễn dịch với các biện pháp kiểm soát xuất khẩu của chính phủ, chúng hy sinh các khả năng suy luận tiên tiến và khả năng của các mô hình tiền phong. Con đường tiến bộ vững chắc nhất là kiến trúc dự phòng hoạt động, nơi các doanh nghiệp thiết kế hệ thống của mình để trở nên độc lập với mô hình và có thể chuyển đổi động giữa các mô hình hoặc nhà cung cấp khác nhau trong trường hợp mất điện hoặc cấm theo quy định.

TIPS & TRICKS CHO DEV

Tối ưu hóa Retrieval-Augmented Generation

Vấn đề: Model RAG không thể tìm kiếm thông tin liên quan hiệu quả.

Cách làm: Sử dụng thư viện Hugging Face để tinh chỉnh mô hình, ví dụ: `pipeline = pipeline("question-answering")`.

Đánh giá: Hiệu quả khi cần tìm kiếm thông tin cụ thể, nhưng có thể mất thời gian.

Tạo Embeddings cho Semantic Search

Vấn đề: Dữ liệu không có đặc trưng phù hợp cho tìm kiếm ngữ nghĩa.

Cách làm: Sử dụng thư viện sentence-transformers để tạo embeddings, ví dụ: `from sentence_transformers import SentenceTransformer`.

Đánh giá: Hiệu quả khi cần tìm kiếm ngữ nghĩa, nhưng yêu cầu dữ liệu chất lượng.

Áp dụng Semantic Search trong Ứng dụng

Vấn đề: Cần tìm kiếm thông tin liên quan trong dữ liệu lớn.

Cách làm: Sử dụng thư viện FAISS để tìm kiếm nhanh, ví dụ: `import faiss`.

Đánh giá: Hiệu quả khi cần tìm kiếm nhanh, nhưng yêu cầu cấu hình phù hợp.

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, cho phép phát triển các ứng dụng thông minh hơn. Điều này giúp các nhà

phát triển cải thiện trải nghiệm người dùng và tăng hiệu suất công việc. Việc tích hợp AI API cũng giúp giảm thiểu thời gian và công sức phát triển.

3. Ví dụ, khi xây dựng một ứng dụng chatbot, bạn có thể tích hợp AI API như Dialogflow hoặc Microsoft Bot Framework để xử lý ngôn ngữ tự nhiên và trả lời các câu hỏi của người dùng.

4. Tip hoặc bước tiếp theo: Để bắt đầu tích hợp AI API, hãy nghiên cứu các thư viện và framework hỗ trợ như TensorFlow hoặc PyTorch, và tìm hiểu cách deploy mô hình AI lên cloud hoặc edge device.