Model Bağlam Protokolü (MCP): LLM Entegrasyonu, Ajans Sistemleri ve Araç Kullanımı Standartlaştırmasında Rolünün Uzman Analizi

1. Giriş: Otonom Yapay Zeka için Temel Katman Olarak MCP

Büyük Dil Modeli (LLM) yeteneklerinin hızlı genişlemesi, akademik merakı pratik uygulamaya dönüştürmüştür. Ancak bu geçiş, kritik bir mimari boşluğu ortaya çıkarmıştır: LLM'lerin harici kaynaklar ve özel araçlarla dinamik olarak arayüz oluşturması için standartlaştırılmış, güvenilir bir yöntemin olmaması. **Model Bağlam Protokolü (MCP)**, bu zorluğa kesin bir yanıt olarak ortaya çıkmış ve kendisini AI modelleri ile harici kaynaklar veya araçlar arasında birleşik, çift yönlü bir iletişim katmanı tanımlayan temel bir açık standart olarak konumlandırmıştır.

MCP'nin temel amacı, heterojen AI ekosistemleri arasında temel olarak birlikte çalışabilirliği geliştirmek ve birçok erken dönem araç destekli sistemin karakteristik özelliği olan parçalanmayı önemli ölçüde azaltmaktır. MCP, LLM'lerin yalnızca mevcut araçların temel açıklamalarına dayandığı basit işlev çağrısından, protokol odaklı bir bağlam sunma yöntemine doğru bir mimari dönüşümü temsil eder. Bu yöntem, web hizmeti uç noktalarını bilimsel kavramlar, operasyonel şemalar ve ayrıntılı meta verilerle açıkça ilişkilendiren, standartlaştırılmış, makine tarafından işlenebilir bir katman getirerek pasif araç açıklamalarını aktif bağlam kaynaklarına dönüştürür.

Etkili akademik çalışmaların incelenmesi, MCP ile ilgili temel araştırmaların (tanımı, güvenlik analizi, performans karşılaştırmaları ve ilk alan uygulamaları dahil) 2025 zaman diliminde yoğunlaştığını göstermektedir.[1] Bu eşzamanlı ortaya çıkış, MCP'nin kademeli bir akademik evrimin ürünü olmadığını, aksine kritik mimari sınırlamalara karşı gerekli ve acil bir endüstri tepkisi olduğunu göstermektedir. Erken dönem ajans sistemleri, karmaşık, çok adımlı görevlerle karşılaştıklarında, uzun bağlamları yönettiklerinde ve geniş bir araç envanteriyle etkileşime girdiklerinde hızla ölçeklendirme eksiklikleri ortaya koydu. MCP'nin sunduğu standardizasyon,

gerekli mimari olgunluğu sağlayarak bu ihtiyacı doğrudan karşılıyor.

2. Mimari Gereklilik: Dağıtım Modelleri ve Gelişmiş Sistem Entegrasyonu

MCP'nin etkili bir şekilde entegrasyonu, sunucu uygulaması ve yönetimi için titiz ve tanımlı bir yaklaşım gerektirir. Tipik durum bilgisi olmayan API'lerden farklı olarak, MCP birleşik, çift yönlü bir iletişim protokolünü yönetir ve tam yaşam döngüsü yönetimi gerektirir. Araştırmalar, MCP sunucu yaşam döngüsünü dört ayrı aşamadan oluştuğunu belirlemiştir: oluşturma, dağıtım, işletim ve bakım. Bu aşamalar, 16 temel faaliyete ayrılmıştır ve MCP'nin sadece arayüz tanımının ötesine geçerek sistem mimarisi tanımının yapısal bir gerekliliği haline geldiğini doğrulamaktadır.

Ölçeklenebilirlik ve Verimlilik için FaaS Tarafından Barındırılan MCP Hizmetleri

Ölçeklenebilir MCP dağıtımı için önerilen önemli bir teknik yenilik, MCP sunucularını barındırmak için bulut İşlevleri Hizmet Olarak (FaaS) kullanılmasıdır. *AgentX: FaaS tarafından barındırılan MCP Hizmetleri ile Sağlam Ajan İş Akışı Kalıplarını Düzenlemeye Doğru* başlıklı makale, yerel MCP sunucu dağıtımlarına kıyasla FaaS alternatifleriyle ilişkili başarı oranını, gecikmeyi ve maliyeti deneysel olarak değerlendirmiştir. FaaS ve MCP arasındaki mimari uyum açıktır: ajan araç kullanımı, özellikle üretim ortamlarında, sporadik olma eğilimindedir ve yüksek patlama kullanım modelleriyle karakterize edilir. FaaS, bu iş yükü profilini doğal olarak barındırır ve maliyet optimizasyonu, sorunsuz ölçeklendirme ve büyük ölçekli üretim ajan sistemleri için vazgeçilmez olan kalıcı sunucu altyapısı bakımının ortadan kaldırılması açısından önemli avantajlar sunar.

Uzman Karışımı (MoE) Mimarilerinde MCP

Model Bağlam Protokolü, özellikle son derece uzmanlaşmış ve kritik alanlarda, Uzman Karışımı (MoE) gibi sofistike mimari modellerin uygulanmasında çok önemli bir rol oynar. Kritik Altyapı içindeki varlık keşfi bağlamında, MoE mimarisi, farklı operasyonel aşamalar için özel, ince ayarlı

hafif modelleri koordine eder. Burada MCP, LLM odaklı MoE'yi harici, gerçek zamanlı tehdit istihbaratı kaynaklarına bağlayarak önemli **Model Bağlamı** enjekte etmek için bir mekanizma görevi görür.

Özellikle, MCP, Endüstriyel Kontrol Sistemleri (ICS) çerçevesini kullanarak düşmanca davranışların haritalanmasını destekleyen MITRE ATT&CK, gerçek zamanlı gösterge alımı için MISP ve risk değerlendirmesini bilgilendiren CVE güvenlik açığı veritabanı gibi platformlardan gelen tehdit istihbaratı beslemelerinin entegrasyonunu kolaylaştırır. LLM tabanlı MoE'yi sürekli güncellenen bu harici bilgi grafiklerine bağlayarak, MCP semantik bağlam farkındalığını kolaylaştırır. Bu, sistemin katı, önceden belirlenmiş taksonomilere veya önsel veri sınıflandırmasına dayanmadan heterojen veri kaynaklarını ve çeşitli protokolleri dinamik olarak yorumlamasına olanak tanır, böylece uzman yönlendirme kararlarını iyileştirir ve kapsamlı varlık risk değerlendirmelerini zenginleştirir. MCP, bu nedenle, dinamik yönlendirme ve bağlamsallaştırma katmanı olarak işlev görür ve AI sistemlerini karmaşık, gerçek zamanlı endüstriyel ortamlara uyarlamak için gerekli olduğunu kanıtlar.

2025 yılında temel makalelerin eşzamanlı olarak yayınlanması, araştırma camiasının ölçeklenebilir ajanların mimari taleplerine verdiği ani tepkiyi göstermektedir:

Tablo 1: Temel MCP Araştırması: Zaman Çizelgesi ve Odak Noktası (2025 Kümesi)

Kağıt (Ref.)	**Yayın Tarihi (Yaklaşık)**	**Birincil Tema**	**Ana Mimari Konsept**
Model Bağlam Protokolü (MCP)...	Mart 2025	Temel Tanım ve Güvenlik	Tam Sunucu Yaşam Döngüsü, Tehdit Sınıflandırması
MCPmed: MCP özellikli... için çağrı	Temmuz 2025	Alan Uzmanlığı	Makine Tarafından İşlenebilir Katman (FAIR İlkeleri)
Yardım mı, engel mi? Modeli yeniden düşünmek...	Ağustos 2025	Ampirik Değerlendirme	MCPGAUGE (Proaktiflik, Genel Gider Analizi)
Üretken Yapay Zeka ve... [6]	Ağustos 2025	Ajan Entegrasyonu	Bağlam Duyarlı Otonom Ajanlar
AgentX:	Eylül 2025	İş Akışı Düzenleme	FaaS Tarafından

Orkestrasyon Yolunda...			Barındırılan MCP Hizmetleri, AgentX Modeli

3. Yörünge I: Proaktif Güvenlik Tasarımı ve Tehdit Sınıflandırması

Model Context Protocol araştırmasının belirleyici bir özelliği, güvenlik etkilerinin proaktif ve anında tanımlanmasıdır. Protokolün tanımıyla eşzamanlı olarak yayınlanan temel makale, MCP sunucusunun tüm yaşam döngüsü boyunca güvenlik ve gizlilik risklerini haritalayan kapsamlı bir tehdit sınıflandırması oluşturmuştur. Bu mimari olgunluk, AI modelleri ile harici yürütme ortamları arasında çift yönlü iletişimi mümkün kılmanın, doğası gereği önemli yeni saldırı yüzeyleri yarattığına dair bir anlayışı göstermektedir.

Güvenlik sınıflandırması, dört ana saldırgan türüne göre risklerin kapsamlı bir sınıflandırmasını oluşturur: **kötü niyetli geliştiriciler, dış saldırganlar, kötü niyetli kullanıcılar ve güvenlik açıkları**. Bu analiz, 16 farklı tehdit senaryosunu kapsar ve mevcut MCP uygulamaları içindeki potansiyel saldırı yüzeylerini ve güvenlik açıklarını doğrulamak için gerçek dünya vaka çalışmalarını kullanır. Bu kapsamlı tehdit modellemesine dayalı olarak, araştırma bir dizi ayrıntılı ve uygulanabilir güvenlik önlemi önermektedir. Bu önlemler, her yaşam döngüsü aşamasına (oluşturma, dağıtım, işletim, bakım) ve ilgili tehdit kategorisine özgü riskleri ele almak için açıkça uyarlanmıştır ve kurumsal ortamlarda MCP'nin güvenli bir şekilde benimsenmesi için pratik rehberlik sunmaktadır.

Bağlamsal Güvenlik Geliştirme ve Risk Dengesi

MCP'nin benimsenmesi, artan işlevsellik ile genişleyen tehdit maruziyeti arasında kritik bir denge sunar. Protokol, tanımlanmış 16 tehdit senaryosuna karşı güvenli hale getirilmelidir, ancak aynı zamanda mimarisi kritik operasyonel alanlarda güvenliği *güçlendirmek* için kullanılır. Örneğin, Kritik Altyapıda MCP, keşfedilen varlıkları harici tehdit istihbaratına bağlayarak varlık keşif sistemlerinin gerçek zamanlı, bağlam farkında risk değerlendirmeleri gerçekleştirmesini sağlar. Protokol, cihaz profilinin CVE verileri ve MITRE ATT&CK eşlemesi ile anında zenginleştirilmesine olanak tanır, bu da geleneksel, bağlantısız araçlarla imkansızdır.

Bu ikilik, protokolün istismar edilebilecek yeni, tanımlanmış bir vektör (örneğin, kötü amaçlı

araç oluşturma veya veri zehirleme yoluyla) getirirken, aynı zamanda bağlamsal olarak bilgilendirilmiş güvenlik ajanları oluşturmak için gerekli mekanizmayı da sağladığını vurgulamaktadır. MCP'yi benimseyen kuruluşlar, protokolün, tehdit taksonomisinde ayrıntılı olarak açıklanan önerilen güvenlik önlemlerine sürekli izleme ve uyum gerektiren bir güven sınırı tanımladığını kabul etmelidir.[1]

4. Yörünge II: Performans Doğrulama ve Araç Kullanımının "Engeli"

Model Bağlam Protokolünün etkinliği, yalnızca sağlam mimari tanımıyla değil, aynı zamanda LLM'lerin yeteneklerinden yararlanırken sergiledikleri ampirik performansla da belirlenir. *Yardım mı, Engel mi? Model Bağlam Protokolü ile Güçlendirilmiş Büyük Dil Modellerini Yeniden Düşünmek* başlıklı makale, LLM–MCP etkileşimlerini incelemek için özel olarak tasarlanmış ilk kapsamlı değerlendirme çerçevesi olan **MCPGAUGE**'yi tanıttı.

MCPGAUGE Çerçevesi

MCPGAUGE, pratik uygulama zorluklarını titizlikle test ederek teorik faydaların ötesine geçmek için geliştirilmiş bir benchmark paketidir. Çerçeve, bilgi kavrama, genel muhakeme ve kod üretimi gibi kritik alanları kapsayan kapsamlı bir 160 komut istemi paketi ve 25 farklı veri seti içerir. Değerlendirmenin kapsamı çok genişti; yaklaşık 20.000 API çağrısı, altı ticari LLM'nin test edilmesi ve 30 farklı MCP araç paketinin kullanılmasıyla, önemli bir hesaplama yatırımı (6.000 ABD dolarının üzerinde) gerektirdi.

Çerçeve, araç destekli ajan dağıtımı için kritik öneme sahip dört temel boyutta performansı ölçer:

1. **Proaktiflik:** LLM'nin açık bir talimat olmadan kendi kendine başlattığı, uygun araç kullanım kapasitesini ölçmek.
2. **Uyumluluk:** LLM'nin tanımlanmış araç kullanım talimatlarına ve MCP şemasına uygunluğunun ölçülmesi.
3. **Etkinlik:** MCP aracını entegre ettikten sonra elde edilen genel görev performansı ve doğruluğu değerlendirmek.
4. **Genel gider:** MCP etkileşimi nedeniyle ortaya çıkan hesaplama maliyeti ve gecikmeyi değerlendirme.

Yaygın Varsayımlara Meydan Okumak

Performans çalışmasının kışkırtıcı başlığı —*Yardım mı, Engel mi?*— önemli bir analitik bulguyu vurgulamaktadır: MCP entegrasyonu, mimari açıdan sağlam olsa da, *evrensel olarak* performans artışını garanti etmemektedir. Kapsamlı çalışma, MCP entegrasyonunun doğasında var olan etkinliği hakkındaki yaygın varsayımları doğrudan sorgulayan dört önemli bulgu ortaya koymuştur.

Veriler, protokolün iletişim katmanını başarıyla standartlaştırmasına rağmen, mevcut LLM'lerin bağlamı etkili bir şekilde kullanmak için gereken karmaşık *meta-akıl yürütme* ile sık sık zorlandığını göstermektedir. Araç talimatlarına uyumun zayıf olması ve proaktifliğin düşük olması gibi sorunlar, modellerin MCP tarafından tanımlanan özel kaynakları *ne zaman* ve *nasıl* çağırmak gerektiğini anlamak için en uygun şekilde ayarlanmadığını göstermektedir. Ayrıca, MCP etkileşimi sırasında ortaya çıkan önemli hesaplama yükü, özellikle gecikmeye duyarlı uygulamalarda protokolün pratik yararını azaltabilir. Bu mimari sınırlama, gelecekteki araştırmaların MCP uyumluluğunu iyileştirmek, etkileşim maliyetlerini azaltmak ve modellerin karmaşık bağlam kullanımını güvenilir bir şekilde öğrenmesini sağlamak için LLM eğitimini ve ince ayarını optimize etmeye öncelik vermesi gerektiğini ima etmektedir.

Bu performans ve güvenlik faktörlerinin bir araya gelmesi, MCP benimseme gereksinimlerine ilişkin dengeli bir bakış açısı oluşturur:

Tablo 2: MCP Entegrasyonu: Avantajlar, Riskler ve Performans Boyutları

Kategori	**Gözlemlenen Fayda**	**Tespit Edilen Risk/Sınırlama**	**MCPGAUGE Boyut**
Mimari	Birleştirilmiş, dinamik araç keşfi, FaaS ölçeklenebilirliği, MoE entegrasyonu [1]	Tam yaşam döngüsü yönetimi gerektirir (16 faaliyet)	Etkinlik
İşlevsel	Anlamsal bağlam farkındalığı, dinamik veri yorumlama, Özerklik [6]	LLM uyumluluğunun yetersizliği ve araç kullanımında	Proaktiflik, Uyum

		proaktif olmama	
Operasyonel	Geliştirilmiş tekrarlanabilirlik, müdahalesiz varlık yönetimi [2]	Önemli hesaplama maliyeti/ek yükü	Genel giderler
Güvenlik	Dış tehdit istihbaratının entegrasyonu (MITRE ATT&CK, CVE)	16 farklı tehdit senaryosuna maruz kalma (örneğin, kötü niyetli geliştiriciler)	Yok

5. Yörünge III: Gelişmiş Ajan İş Akışı Düzenleme

MCP'nin kullanışlılığı, sağlam, yeni nesil ajansal iş akışlarının tasarımında en belirgin şekilde ortaya çıkmaktadır. Çağdaş ajansal AI sistemleri, halüsinasyonları azaltmak için büyük araç setlerinde gezinme, karmaşık, çok adımlı işlemleri yürütme ve uzun bağlam geçmişini sürdürme ile ilgili sık sık darboğazlarla karşılaşmaktadır. Chain-of-Thought (CoT) ve ReAct gibi teknikler kısmi çözümler sunarken, sistemik güvenilirlik için MCP gibi protokol düzeyinde bir çözüm gereklidir.

AgentX Modeli ve FaaS Entegrasyonu

Bu ölçeklendirme zorluklarına yanıt olarak, araştırmacılar **AgentX** olarak bilinen yeni bir ajan iş akışı modeli tanımladılar. Bu iş akışı yapısal olarak üç özel bileşenden oluşur: sahne tasarımcısı, planlayıcı ve yürütücü ajan. AgentX modeli, araç etkileşimlerini yönetmek için FaaS tarafından barındırılan MCP hizmetlerini entegre ederek, ReAct ve Magentic One dahil olmak üzere mevcut en gelişmiş modellerle rekabet edebilecek veya bunlardan daha üstün bir performans elde etmesini sağlar. Ampirik değerlendirmeler, FaaS tarafından barındırılan MCP araçlarının kullanılmasıyla pratik uygulamalar için başarı oranı, gecikme süresi ve maliyetle ilgili önemli operasyonel avantajlar sağlandığını doğruladı ve böylece esnek ajans sistemlerini koordine etmek için bir plan oluşturdu.

Bağlam Duyarlı Otonomi için Birleşik Çerçeve

Belirli iş akışı modellerinin ötesinde, MCP, Generative AI, Model Context Protocol ve Applied Machine Learning (ML) birleştiren önerilen birleşik çerçevenin merkezi bileşeni olarak tanımlanmaktadır.[6] Bu sinerjik kombinasyon, otonom karar verme ve zaman içinde sürekli kendini geliştirme için tasarlanmış gelişmiş ajansal AI sistemlerini güçlendirmek için gerekli araçları sağlar.[6]

Bu birleşik vizyonda, Üretken Yapay Zeka yeni verilerin ve içgörülerinin oluşturulmasını kolaylaştırır. Ancak, Model Bağlam Protokolü, yapay zeka modellerinin **bağlamsal farkındalığa sahip** olmasını ve çeşitli, dinamik ortamlar ve koşullarda işlevsel bütünlüğünü koruyabilmesini garanti eden vazgeçilmez bir unsurdur. [6] Uygulamalı Makine Öğrenimi, gerçek dünyadaki dağıtım ve öğrenmenin gerekli bileşenine katkıda bulunarak, ajanların anında uyum sağlamasına ve akıllı kararlar almasına olanak tanır. MCP'nin üretilen zekayı uygulamalı gerçekçilikle birleştirdiği bu entegre çerçeve, uyarlanabilir karar verme sürecinin temel bir operasyonel gereklilik olduğu sağlık, finans ve robotik gibi yüksek riskli alanlar için çok önemlidir.[6]

6. Yörünge IV: Alanlar Arası Uzmanlaşma ve Standardizasyon

MCP'nin çok yönlülüğü ve mimari bütünlüğü, yaşam bilimlerinden kritik altyapı siber güvenliğine kadar çok farklı alanlarda uzmanlaşmış olmasıyla açıkça görülmektedir.

MCPmed: Biyomedikal Araştırmada FAIR İlkelerinin Uygulanması

Biyoinformatikte, geleneksel web sunucuları (örneğin GEO, STRING, UCSC Cell Browser) öncelikle insan kullanıcılar için tasarlanmıştır, bu da LLM'lerin ve derin araştırma ajanlarının bunları özerk bir şekilde okumalarını ve kullanmalarını zorlaştırmaktadır. Bu insan merkezli tasarım, otomatik bilimsel keşiflerin potansiyelini sınırlamaktadır. Bu sınırlamayı aşmak için, **MCPmed** olarak bilinen topluluk çabası, MCP'yi biyoinformatik web sunucusu arka uçlarına uyarlamayı önermektedir.

MCPmed'i uygulayarak, web hizmetleri, hizmet uç noktalarını bilimsel kavramlar ve bunların

ayrıntılı meta verileriyle açıkça ilişkilendiren standartlaştırılmış, makine tarafından işlenebilir bir katman kazanır. Bu yapılandırılmış geçiş, otomasyonu önemli ölçüde geliştirir, tekrarlanabilirliği artırır ve birlikte çalışabilirliği sağlar. Temel olarak, MCP'nin biyoinformatik alanındaki adaptasyonu, AI sistemleri için **FAIR (Bulunabilir, Erişilebilir, Birlikte Çalışabilir, Yeniden Kullanılabilir) ilkelerini** işlevsel hale getirir. LLM odaklı araştırma keşifleri, yapılandırılmış verilere otomatik erişime bağlıdır ve MCP, eski altyapıyı yeni nesil araştırma ajanları için erişilebilir veri kaynaklarına dönüştürmek için gerekli mimari zorunluluğu sağlar.[2]

Kritik Altyapı Varlık Keşfinde MCP

Model Bağlam Protokolü, kritik altyapı (CI) siber güvenliği gibi yüksek riskli alanlarda eşdeğer bir değer sunar. Endüstriyel Kontrol Sistemlerinde (ICS) varlık keşfi, derin bağlamsal muhakeme gerektirir, çünkü geleneksel metodolojiler sabit parmak izi stratejileri kullanan deterministik araçlara dayanır ve genellikle modern CI sistemlerinin heterojen, dinamik mimarilerine uyum sağlayamaz.

Uzman Karışımı (MoE) temelli gelişmiş bir mimari, LLM'leri kullanarak çoklu protokol iletişimlerini yorumlar ve kodunu çözer, ayrıca heterojen veri kaynaklarını birbiriyle ilişkilendirir. Bu mimari içinde MCP, harici tehdit istihbaratı beslemelerinin (MITRE ATT&CK, MISP, CVE) entegrasyonunu kolaylaştırarak sistemin bağlam farkındalığı kapasitesini garanti eder. Bu bağlamsal bağlantı, LLM'nin keşif sonuçları için açıklamalar oluşturmasına ve yeni cihazlar için uyarlanabilir keşif sorguları üretmesine olanak tanır, böylece müdahaleci olmayan varlık yönetimi çözümlerinin geliştirilmesini destekler ve kritik altyapı sistemlerinin siber güvenlik duruşunu önemli ölçüde güçlendirir.

Tablo 3: Alan Spesifik Zorluklarda MCP'nin Rolü

Etki alanı	**MCP Öncesi Sınırlama**	**MCP Çözümü/Çerçeves i**	**Temel MCP İşlevi**
Biyoinformatik/Ar aştırma	LLM okunabilirliğini sınırlayan insan merkezli web sunucuları	MCPmed topluluk çabası, hafif ekmek kırıntıları	**Birlikte çalışabilirlik:** Bilimsel verilere makine tarafından işlenebilir erişim [7]
Kritik Altyapı	Varlık kimliği için	MCP aracılığıyla	**Bağlam**

(ICS)	bağlamsal muhakeme yeteneğinden yoksun deterministik araçlar	tehdit istihbaratını entegre eden LLM tabanlı MoE	**Enjeksiyonu:** Gerçek zamanlı tehdit verilerini (MISP, CVE) operasyonel varlıklara bağlama

7. Google Scholar Özet Koleksiyonu: Markdown'da Model Bağlam Protokolü (MCP)

Aşağıdaki koleksiyon, Model Bağlam Protokolü ile ilgili yüksek etkili akademik özetleri sunar ve LLM entegrasyonu, ajans sistemleri ve araç kullanımı alanlarındaki rolünü ele alır. Özetler, gerekli olduğu şekilde Markdown formatında düzenlenmiştir.

Model Bağlam Protokolü (MCP): Genel Durum, Güvenlik Tehditleri ve Gelecekteki Araştırma YönelimleriYazar(lar): XINYI HOU, YANJIE ZHAO, SHENAO WANG, HAOYU WANG

Özet:

Model Bağlam Protokolü (MCP), birleşik, çift yönlü...kaynak

AgentX: FaaS tarafından barındırılan MCP Hizmetleri ile Sağlam Ajan İş Akışı Kalıplarını Düzenlemeye DoğruYazar(lar): Shiva Sai Krishna Anand Tokal, Vaibhav Jha, Anand Eswaran, Praveen Jayachandran, Yogesh Simmhan

---

Özet:

Üretken Yapay Zeka (GenAI), çeşitli alanları hızla dönüştürmüştür...kaynak ajans iş akışları.

Yardım mı, engel mi? Model Bağlam Protokolü ile Güçlendirilmiş Büyük Dil Modellerini Yeniden DüşünmekYazar(lar): Wei Song, Haonan Zhong, Ziqi Ding, Jingling Xue, Yuekang Li

---

Özet:

Model Bağlam Protokolü (MCP), büyük dil modellerinin (LLM'ler) erişimini sağlar...kaynak araçlarla güçlendirilmiş LLM'ler.

MCPmed: LLM Odaklı Keşif için MCP Destekli Biyoinformatik Web Hizmetleri ÇağrısıYazar(lar): Matthias Flotho, Ian Ferenc Diks, Philipp Flotho, Leidy-Alejandra G. Molano, Pascal Hirsch, Andreas Keller

---

Özet:

Biyoinformatik web sunucuları, modern biyomedikal araştırmalarda kritik öneme sahip kaynaklardır ve zengin görselleştirme özelliklerine sahip özel olarak tasarlanmış arayüzler aracılığıyla veri kümelerinin etkileşimli olarak keşfedilmesini kolaylaştırır. Ancak, bu insan merkezli tasarım, büyük dil modelleri (LLM'ler) ve derin araştırma ajanları için makine okunabilirliğini sınırlamaktadır. Bu boşluğu, Model Context Protocol (MCP) protokolünü biyoinformatik web sunucusu arka uçlarına uyarlayarak kapatıyoruz. MCP, web hizmeti uç noktalarını bilimsel kavramlar ve ayrıntılı meta verilerle açıkça ilişkilendiren, standartlaştırılmış, makine tarafından işlenebilir bir katmandır. Yaygın olarak kullanılan veritabanlarında (GEO, STRING, UCSC Cell Browser) yaptığımız uygulamalar, MCP özellikli LLM'ler aracılığıyla gelişmiş keşif yeteneklerini göstermektedir. Benimsemeyi hızlandırmak için, henüz tam olarak MCP özellikli olmayan hizmetler için hafif ekmek kırıntıları ve yeni sunucular kurmak için şablonlarla desteklenen bir topluluk çabası olan MCPmed'i öneriyoruz. Bu yapılandırılmış geçiş, otomasyonu, tekrarlanabilirliği ve birlikte çalışabilirliği önemli ölçüde artırarak biyoinformatik web hizmetlerini yeni

nesil araştırma ajanları için hazırlamaktadır.

Gelişmiş Ajansel Yapay Zeka Sistemleri için Uygulamalı Makine Öğrenimi ile Üretken Yapay Zeka ve Model Bağlam Protokolü (MCP) EntegrasyonuYazar(lar): Nilesh Bhandarwar

---

Özet:

Üretken Yapay Zeka, Model Bağlam Protokolü (MCP) ve Uygulamalı Makine Öğrenimi...kaynak önemlidir.

---

8. Araştırma Bulgularının Sentezi ve Gelecekteki Standardizasyon Zorlukları

Analiz, Model Bağlam Protokolünün, araçlarla desteklenen AI sistemlerinin güvenilir ve ölçeklendirilmiş bir şekilde uygulanması için gerekli olan önemli bir mimari değişimi temsil ettiğini doğrulamaktadır. 2025 yılında temel makalelerin hızlı ve eşzamanlı olarak ortaya çıkması, MCP'nin birinci nesil ajan sistemlerinin sınırlarını, özellikle de karmaşık çok adımlı görevlerle mücadelelerini ve uzun bağlam geçmişini sürdürme konusundaki zorluklarını aşmak için acil ve pratik bir gereklilik olduğunu göstermektedir.

MCP, LLM aracı etkileşimini resmileştiren standardı tanımlar ve basit API çağrılarının ötesine geçerek, AgentX iş akışı modeli ve MoE çerçeveleri gibi sağlam, dağıtılabilir sistemler için gerekli olan yapılandırılmış, çift yönlü bir protokole geçer. [3] Ayrıca, FaaS dağıtımını anında dikkate almasıyla kanıtlanan MCP'nin mimari tasarımı, protokolün kurumsal ölçeklenebilirlik, maliyet optimizasyonu ve mikro hizmet entegrasyonu temel gereksinimleri göz önünde bulundurularak geliştirildiğini göstermektedir.

MCP'nin uzun vadeli sürdürülebilirliği, birbiriyle bağlantılı iki önemli zorluğun başarıyla aşılmasına bağlıdır:

İkili Zorunluluklar: Güvenlik ve Verimlilik

1. **Güvenlik Riski Yönetimi:** MCP'nin temel belgeleri, proaktif olarak kapsamlı bir tehdit sınıflandırması oluşturmuştur. Bu analiz, güvenlik ve gizlilik risklerini 16 farklı senaryo ve dört saldırgan türüne göre sınıflandırmış ve MCP'nin benimsenmesi için sunucu yaşam döngüsünün her aşamasına özel güvenlik önlemlerinin titizlikle uygulanmasını zorunlu kılmıştır. Protokol, genişletilmiş bir saldırı yüzeyi sunar ve güvenli bir şekilde uygulanması için kuruluşların harici yürütme ortamlarında bulunan güven sınırlarını titizlikle yönetmesi gerekir.
2. **Verimlilik ve Model Uyumluluğu:** MCPGAUGE tarafından sağlanan ampirik veriler, protokolün teorik faydalarının genellikle pratik performans sınırlamaları nedeniyle azaldığını göstermektedir. Yüksek hesaplama yükü ve LLM proaktifliği ve uyumluluğundaki eksiklikler, etkili araç destekli yapay zekanın önündeki temel engelin yalnızca iletişim standardının kendisi değil, LLM'leri harici bağlamı doğru ve verimli bir şekilde kullanmak için ayarlamanın zorluğu olduğunu ortaya koymaktadır. Bu, geliştiricilerin hesaplama maliyetini azaltmak ve doğru araç çağrısını sağlamak için MCP uyumluluğuna özgü model eğitiminin optimizasyonuna yoğun bir şekilde odaklanmaları gerektiğini ima etmektedir.

Sürdürülebilir Büyümeye Giden Yol

Biyoinformatik alanındaki MCPmed ve kritik altyapı siber güvenliğinde MoE entegrasyonu gibi alanlara özgü uygulamaların başarısı, protokolün uyarlanabilirliğini teyit etmektedir. Biyoinformatik alanındaki uygulama özellikle önemlidir, çünkü MCP, eski, insan merkezli veri altyapısı içinde LLM keşfini mümkün kılan teknik standart olarak etkili bir şekilde işlev görerek, AI sistemleri için FAIR ilkelerini işlevsel hale getirmektedir.[2]

Gelecekteki araştırma ve geliştirme çabaları, MCP'nin çeşitli uygulamalar genelinde standardizasyonunu güçlendirmeye, yürütme ortamları içindeki güven sınırlarını iyileştirmeye ve MCPGAUGE tarafından belirlenen uyumluluk ve ek yük sorunlarını ele almak için LLM performansını optimize etme yöntemlerine yoğun bir şekilde odaklanmaya devam etmelidir. Araçlarla desteklenen yapay zekanın sürdürülebilir büyümesi, Model Bağlam Protokolünün olgunluğu ve sağlamlığı ile doğrudan ilişkilidir.

Alıntılanan çalışmalar

1. Model Bağlam Protokolü (MCP): Manzara, Güvenlik Tehditleri ... - arXiv, erişim tarihi Ekim 13, 2025, https://arxiv.org/abs/2503.23278
2. MCPmed: A Call for MCP-Enabled Bioinformatics Web ... - arXiv, erişim tarihi Ekim 13, 2025, https://arxiv.org/abs/2507.08055
3. AgentX: Sağlam Ajan İş Akışını Düzenlemeye Doğru ... - arXiv, erişim tarihi Ekim 13, 2025, https://arxiv.org/abs/2509.07595

4. Yardım mı, Engel mi? Model Bağlam Protokolü ile Güçlendirilmiş ...'yi Yeniden Düşünmek, erişim tarihi Ekim 13, 2025, https://arxiv.org/abs/2508.12566
5. Kritik Altyapılarda Varlık Keşfi: LLM Tabanlı Bir Yaklaşım - MDPI, erişim tarihi Ekim 13, 2025, https://www.mdpi.com/2079-9292/14/16/3267
6. Üretken Yapay Zeka ve Model Bağlamını Entegre Etmek ... - ResearchGate, erişim tarihi Ekim 13, 2025, https://www.researchgate.net/profile/Nilesh-Bhandarwar/publication/395238999_Integrating_Generative_AI_and_Model_Context_Protocol_MCP_with_Applied_Machine_Learning_for_Advanced_Agentic_AI_Systems/links/68b895e1d9261f6f51b124fa/Integrating-Generative-AI-and-Model-Context-Protocol-MCP-with-Applied-Machine-Learning-for-Advanced-Agentic-AI-Systems.pdf
7. MCPmed: LLM Odaklı Keşif için MCP Destekli Biyoinformatik Web Hizmetleri Çağrısı, erişim tarihi Ekim 13, 2025, https://arxiv.org/html/2507.08055v1
8. Dr. Luigi Coppolino | Yazar | Parthenope Üniversitesi, 80133 Napoli, İtalya - SciProfiles, erişim tarihi Ekim 13, 2025, https://sciprofiles.com/profile/1411308?utm_source=mdpi.com&utm_medium=website&utm_campaign=avatar_name