ChatGPT

Model Context Protocol (MCP) Literatür Taraması

Akademik Makaleler

- **Konu Başlığı:** Model Context Protocol (MCP): Landscape, Security Threats, and Future Research Directions
  Kaynak/Kurum & Tarih: arXiv, 2025-03
  Bağlantı: https://arxiv.org/abs/2503.23278
  Türkçe Özet: Bu çalışma, MCP'nin mimari ve güvenlik boyutlarını sistematik olarak inceleyerek protokolün yaşam döngüsünü dört evre ve 16 faaliyet adımında tanımlıyor. Bu temel üzerine, kötü niyetli geliştirici, dış saldırgan, kötü niyetli kullanıcı ve sistem açığı kaynaklı hatalar şeklinde dört saldırgan türüne yayılan 16 senaryoluk bir tehdit taksonomisi sunuyor ve gerçek dünyadan vaka analizleriyle olası saldırı yüzeylerini gösteriyor. Her bir yaşam döngüsü aşaması ve tehdit kategorisi için ince ayarlı, uygulanabilir güvenlik önlemleri öneren makale, MCP'nin mevcut endüstri benimsenmesini ve araç ekosistemini de değerlendirerek güçlü yanlarını ve yaygın kullanımını kısıtlayan eksikleri belirliyor. Son olarak, araca dayalı yapay zekâ sistemlerinin gelişen ekosisteminde MCP'nin standardizasyonunu, güven sınırlarını ve sürdürülebilir büyümesini güçlendirmeye yönelik gelecekteki araştırma yönlerini tartışıyor.

- **Konu Başlığı:** MCP-Universe: Benchmarking Large Language Models with Real-World Model Context Protocol Servers
  Kaynak/Kurum & Tarih: arXiv, 2025-08
  Bağlantı: https://arxiv.org/abs/2508.14704
  Türkçe Özet: Bu makale, mevcut LLM değerlendirme yöntemlerinin gerçekçi uygulama zorluklarını yansıtamadığını öne sürerek *MCP-Universe* adlı kapsamlı bir karşılaştırma paketi sunuyor. *MCP-Universe*, Konum Navigasyonu, Depo Yönetimi, Finansal Analiz, 3D Tasarım, Tarayıcı Otomasyonu ve Web Arama gibi 6 farklı alanda toplam 11 **gerçek MCP sunucusuyla** etkileşimli zorlu görev setleri içeriyor. Yapılan testlerde GPT-5 (%43,7 başarı), Grok-4 (%33,3) ve Claude-4.0-Sonnet (%29,4) gibi en gelişmiş modellerin bile bu gerçekçi senaryolarda belirgin performans kısıtlarına sahip olduğu görülüyor. Bu durum, özellikle ajanların uzun etkileşim adımlarında bağlam pencerelerinin hızla dolması (uzun-bağlam sorunu) ve **tanımadıkları araçlarla karşılaştıklarında** (bilinmeyen araç sorunu) zorlanmalarıyla açıklanıyor. Hatta kurumsal özel ajan örneklerinin dahi standart ReAct yaklaşımlarına üstünlük sağlayamadığı belirtiliyor. Çalışma, araştırmacıların yeni ajanları ve MCP sunucularını kolayca ekleyerek inovasyonu sürdürmeleri için kullanıcı arayüzü desteğiyle birlikte değerlendirici araç setini açık kaynak olarak paylaşıyor.

- **Konu Başlığı:** Automatic Red Teaming LLM-based Agents with Model Context Protocol Tools
  Kaynak/Kurum & Tarih: arXiv, 2025-09
  Bağlantı: https://arxiv.org/abs/2509.21011
  Türkçe Özet: LLM tabanlı ajanlar çeşitli alanlarda hızla yaygınlaşırken, bu ajanların ortamlarıyla etkileşimlerini standartlaştırmak amacıyla **MCP araçları** adeta *de facto* standart haline gelmiştir. Ancak MCP araçlarının kullanımı, bu ajanları **araç zehirleme saldırılarına** karşı savunmasız bırakarak davranış manipülasyonu riskini doğurmuştur. Önceki çalışmalar bu tür güvenlik açıklarını işaret etse de, bunlara yönelik kırmızı ekip (red teaming) testleri genelde kanıt niteliğinde kalmış ve otomatik, sistematik bir yaklaşım geliştirilmemiştir. Bu makalede, LLM ajanlarını kötü niyetli MCP araçları üreterek sınayan otomatik bir kırmızı takım çerçevesi olan **AutoMalTool** öneriliyor. Yapılan kapsamlı deneyler, AutoMalTool'un popüler LLM ajanlarının

davranışlarını gizlice değiştirebilen ve mevcut tespit mekanizmalarından kaçabilen zararlı MCP araçlarını otomatik olarak oluşturabildiğini gösteriyor. Bu bulgular, MCP tabanlı ajan sistemlerinde henüz görülmeyen yeni güvenlik risklerini ortaya koyuyor ve bu risklerle mücadele için daha ileri güvenlik önlemlerine ihtiyaç olduğunu vurguluyor.

- **Konu Başlığı:** Advancing Multi-Agent Systems Through Model Context Protocol: Architecture, Implementation, and Applications
  Kaynak/Kurum & Tarih: arXiv, 2025-04
  Bağlantı: https://arxiv.org/abs/2504.21030
  Türkçe Özet: Çok etmenli yapay zekâ sistemleri (multi-agent systems) karmaşık sorunları çözme potansiyeline sahip olsa da, **bağlam yönetimi**, koordinasyon verimliliği ve ölçeklenebilirlik konularında temel zorluklar yaşamaktadır. Bu çalışma, Model Context Protocol (MCP) ile **standartlaştırılmış bağlam paylaşımı ve ajan koordinasyonu** sağlayarak bu sorunları ele alan kapsamlı bir çerçeve sunuyor. AI ajan mimarileri üzerine önceki çalışmaları genişleterek, birleşik bir teorik temel, gelişmiş bağlam yönetim teknikleri ve ölçeklenebilir koordinasyon desenleri geliştiriliyor. Kurumsal bilgi yönetimi, işbirlikçi araştırma ve dağıtık problem çözme gibi alanlarda gerçekleştirilen ayrıntılı uygulama vakaları, MCP tabanlı yaklaşımın geleneksel yöntemlere kıyasla önemli performans iyileşmeleri sağladığını gösteriyor. Ayrıca makale, multi-agent sistemler için özel olarak tasarlanmış görev ve veri kümeleriyle bir değerlendirme yöntemi sunarak bu iyileşmeleri sistematik olarak ölçüyor. Çalışma, mevcut kısıtlar ve ortaya çıkan araştırma fırsatlarını tartışmanın yanı sıra, MCP'nin endüstrinin farklı kollarında daha **işbirlikçi ve bağlam farkındalığı yüksek** yapay zekâ uygulamalarına zemin hazırlayabileceğine işaret ediyor.

- **Konu Başlığı:** Model Context Protocol (MCP) at First Glance: Studying the Security and Maintainability of MCP Servers
  Kaynak/Kurum & Tarih: arXiv, 2025-06
  Bağlantı: https://arxiv.org/abs/2506.13538
  Türkçe Özet: 2024 sonunda Anthropic tarafından tanıtılan MCP, kısa sürede sekiz milyondan fazla haftalık SDK indirmesiyle **fiili bir standart** haline gelmiştir. Ancak, LLM'lerin karar akışını yönlendiren MCP'nin **öngörülemez ve AI güdümlü** yapısı; sistem sürdürülebilirliği, güvenliği ve bakımı açısından yeni riskler doğurabilir. Bu makale, MCP sunucularının güvenlik ve bakım boyutunu ilk kez geniş ölçekli olarak inceleyerek 1.899 açık kaynak MCP sunucusunu kapsamlı bir yöntemle analiz ediyor. Genel sağlık göstergeleri güçlü bulunmakla birlikte, yalnızca üçü geleneksel yazılım açıklarıyla kesişen **sekiz farklı güvenlik açığı** tespit ediliyor. İncelenen sunucuların %7,2'sinde genel güvenlik zafiyetleri, %5,5'inde ise MCP'ye özgü araç zehirleme riskleri belirleniyor. Bakım tarafında ise projelerin %66'sında kod kokusu (borçları) bulunurken, %14,4'ünde açık kaynak projelerinde sık görülen dokuz hatalı kod kalıbına rastlanıyor. Bu bulgular, MCP ekosistemine özel zafiyet tarama tekniklerinin gerektiğini gösterirken, klasik yazılım analizi ve refaktör uygulamalarının da MCP sunucularının sağlığını iyileştirmede değerini koruduğunu ortaya koyuyor.

- **Konu Başlığı:** MCP-Guard: A Defense Framework for Model Context Protocol Integrity in Large Language Model Applications
  Kaynak/Kurum & Tarih: arXiv, 2025-08
  Bağlantı: https://arxiv.org/abs/2508.10991
  Türkçe Özet: LLM'lerin harici araçlara MCP gibi protokoller aracılığıyla bağlanması, **istem zehirleme, veri sızdırma** gibi ciddi güvenlik zafiyetlerini beraberinde getiriyor. Bu makale, söz konusu açıkları gidermek üzere **MCP-Guard** adını verdikleri çok katmanlı bir savunma mimarisi öneriyor. MCP-Guard, tehditleri tespit etmek için üç aşamalı bir filtreleme kurgusu kullanıyor: İlk aşamada hafif bir statik analiz ile bariz tehditler saptanıyor; ikinci aşamada derin öğrenmeye

dayalı özel bir dedektör, anlam olarak zararlı olabilecek saldırı istemlerini %96 gibi yüksek bir doğrulukla yakalıyor; son aşamada ise hafif bir LLM “hakem” modülü, önceki aşamalardan gelen sinyalleri birleştirerek çok az yanlış alarmla nihai kararı veriyor. Ayrıca çalışma, **MCP-AttackBench** adını verdikleri ve 70 binden fazla örnek içeren bir saldırı senaryoları veri setini tanıtıyor. Bu veri seti, halka açık kaynaklardan toplanan ve GPT-4 ile çeşitlendirilmiş istemler içererek MCP ortamındaki muhtelif saldırı vektörlerini simüle ediyor. Bu sayede araştırmacılar için LLM-araç ekosisteminin güvenliğini sağlama konusunda kapsamlı bir test altyapısı sunulmuş oluyor.

- **Konu Başlığı:** A Survey of the Model Context Protocol (MCP): Standardizing Context to Enhance Large Language Models (LLMs)
  Kaynak/Kurum & Tarih: Preprints.org (derleme), 2025-04
  Bağlantı: https://www.preprints.org/manuscript/202504.0245/v1
  Türkçe Özet: Bu derleme çalışması, Anthropic tarafından 2024 sonunda önerilen Model Context Protocol (MCP)'ün temel mimarisini ve mevcut **parçalı API** çözümlerine kıyasla getirdiği yenilikleri ele alıyor. MCP'nin istemci-sunucu modeli, standartlaştırılmış mesajlaşma formatı, **dinamik araç keşfi** ve güvenlik mekanizmaları gibi unsurları incelenerek, protokolün **ajanik AI** sistemlerinin birlikte çalışabilirliğini ve ölçeklenebilirliğini artırma potansiyeli vurgulanıyor. Ancak, MCP'nin uzun vadeli performans ve etkisine dair verilerin henüz kısıtlı olduğu not ediliyor. Çalışma, MCP tasarımını eleştirel bir gözle değerlendirip finans, sağlık ve müşteri hizmetleri gibi çeşitli alanlardaki olası uygulamalarını tartışıyor ve protokolün karşılaştığı temel zorlukları (ör. güvenlik, standartların olgunluğu, benimsenme engelleri) özetliyor. Amaç, araştırmacıları ve uygulayıcıları MCP'nin **faydaları ve mevcut sınırlamaları** hakkında bilgilendirerek, gelişmekte olan yapay zekâ entegrasyon ekosisteminde bu protokolün rolünü anlamalarına yardımcı olmak.

- **Konu Başlığı:** A Survey of Agent Interoperability Protocols: MCP, ACP, A2A, and ANP
  Kaynak/Kurum & Tarih: arXiv, 2025-05
  Bağlantı: https://arxiv.org/abs/2505.02279
  Türkçe Özet: Bu kapsamlı inceleme, otonom yapay zekâ ajanlarının **birlikte çalışabilirliği** için ortaya çıkan dört yeni protokolü değerlendiriyor: Model Context Protocol (MCP), Agent Communication Protocol (ACP), Agent-to-Agent Protocol (A2A) ve Agent Network Protocol (ANP). Her bir protokol, farklı kullanım senaryolarına yönelik benzersiz yaklaşımlar getiriyor. Örneğin MCP, AI uygulamalarının harici araçları güvenli bir şekilde çağırmasına ve yapılandırılmış veri alışverişi yapmasına imkan veren **JSON-RPC tabanlı istemci–sunucu** arayüzünü tanımlıyor. ACP, çok parçalı mesajlar ve asenkron akış ile **REST benzeri** bir iletişim katmanı sunarak birden çok modlu ajan cevaplarını destekliyor. A2A protokolü, *yetenek kartları* aracılığıyla eşler arası görev devretmeyi mümkün kılarak kurumsal ölçekte ajan işbirliğini kolaylaştırıyor. ANP ise merkeziyetsiz tanımlayıcılar (DID) ve JSON-LD grafikler kullanarak **açık ağ** üzerinde ajan keşfi ve güvenli işbirliği sağlıyor. Makale, bu protokolleri etkileşim biçimleri, keşif mekanizmaları, iletişim modelleri ve güvenlik yaklaşımları açısından karşılaştırarak aralarındaki takasları (trade-off) ortaya koyuyor. Analiz sonucunda, birlikte çalışabilir ajan ekosistemleri için kademeli bir benimseme yol haritası öneriliyor: öncelikle araç çağırma için MCP'nin kullanılması, ardından zengin mesajlaşma için ACP'nin, kurumsal görev orkestrasyonu için A2A'nın ve geniş çaplı açık ajan piyasaları için ANP'nin devreye alınması öngörülüyor. Bu çalışma, LLM destekli otonom ajanlardan oluşan güvenli ve ölçeklenebilir sistemler tasarlamak isteyenler için kapsamlı bir temel sağlıyor.

- **Konu Başlığı:** Model Context Protocols in Adaptive Transport Systems: A Survey
  Kaynak/Kurum & Tarih: arXiv (muhtemel ACM Computing Surveys kabulü), 2025-08
  Bağlantı: https://arxiv.org/abs/2508.19239
  Türkçe Özet: Bu çalışma, **akıllı ulaşım sistemlerindeki** mevcut parçalanmış protokol ve bağlam

yönetimi yaklaşımlarını inceleyerek Model Context Protocol (MCP)'ün bu alanda birleştirici bir rol oynayabileceğini ortaya koyuyor. Otonom araçlar, IoT sensörleri ve dağıtık altyapılar arasında tutarlı bir **bağlamsal veri paylaşımı** olmayışının yarattığı sorunlara dikkat çekilerek, farklı araştırma çabalarının aslında farkında olmadan MCP'ye benzer mimarilere doğru evrildiği tespit ediliyor. Bu bağlamda yazarlar, uyarlanabilir mekanizmalar, bağlam farkındalığı sağlayan çerçeveler, bütünleştirici modeller, entegrasyon stratejileri ve MCP destekli mimariler olmak üzere beş kategori içeren bir taksonomi öneriyor. Analiz sonucunda üç önemli içgörü paylaşılıyor: (1) Geleneksel ağ iletişim protokolleri (ör. TCP/UDP ve özel taşıma protokolleri) izole uyarlamalar açısından sınırlarına ulaşmıştır ve güncel dinamik ortamlarda yetersiz kalmaktadır. (2) MCP'nin istemci-sunucu ve **JSON-RPC** temelli yapısı, farklı sistemler arasında *anlamsal birlikte çalışabilirlik* sağlayarak veri alışverişini ve karar almayı ortak bir zemine oturtabilir. (3) Yapay zekâ destekli otonom ulaşım altyapıları, hızlı değişen çevresel ve operasyonel koşullara uyum sağlamak için MCP'nin sunduğu gibi standartlaştırılmış entegrasyon paradigmalarına ihtiyaç duymaktadır. Makale, MCP'nin geleceğin **uyarlanabilir ve bağlam duyarlı** ulaşım sistemlerinin temel taşlarından biri olabileceğini öngörerek, bu doğrultuda bir araştırma yol haritası sunuyor.

Sektörel Raporlar / Bloglar

- **Konu Başlığı:** Introducing the Model Context Protocol
  Kaynak/Kurum & Tarih: Anthropic (Resmî Duyuru), 2024-11
  Bağlantı: https://www.anthropic.com/news/model-context-protocol
  Türkçe Özet: Anthropic, Kasım 2024'te Model Context Protocol (MCP) adlı yeni bir açık standardı tanıttı. MCP, yapay zekâ asistanları ile **veri kaynaklarının bulunduğu sistemler** arasında güvenli ve çift yönlü bağlantılar kurmayı hedefleyen bir istemci-sunucu protokolüdür. İçerik depoları, kurumsal uygulamalar ve geliştirme ortamları gibi çeşitli kaynaklardaki verileri büyük dil modellerine standart bir arayüzle sunarak her bir veri kaynağı için ayrı ayrı bağlayıcı yazma ihtiyacını ortadan kaldırır. Anthropic'in duyurusunda, MCP spesifikasyonu ve yazılım geliştirme kitlerinin (SDK) **açık kaynak** olarak yayınlandığı; Claude yapay zekâ platformunun masaüstü uygulamasına MCP sunucularına bağlanma desteği geldiği ve Google Drive, Slack, GitHub, Postgres gibi popüler sistemlere erişim sağlayan örnek MCP sunucularının paylaşıldığı belirtiliyor. İlk benimseyen şirketlerin (ör. Block, Apollo) ve geliştirici aracı firmalarının (Zed, Replit, Codeium, Sourcegraph vb.) MCP'yi entegre etmeye başladığı, böylece büyük modellerin ihtiyaç duydukları **güncel ve bağlamsal verilere** daha sade, güvenilir ve ölçeklenebilir bir mimariyle ulaşabildiği vurgulanıyor. Sonuç olarak Anthropic, MCP ile yapay zekâ sistemlerinin farklı araç ve veri setleri arasında tutarlı bir bağlamı koruyarak çalışacağını ve bugün parçalı olan entegrasyon ekosistemini daha sürdürülebilir bir yaklaşımla değiştireceğini ifade ediyor.

- **Konu Başlığı:** Microsoft Build 2025 – The Age of AI Agents and Building the Open Agentic Web (MCP Duyuruları)
  Kaynak/Kurum & Tarih: Microsoft Official Blog, 2025-05
  Bağlantı: https://blogs.microsoft.com/blog/2025/05/19/microsoft-build-2025-the-age-of-ai-agents-and-building-the-open-agentic-web/
  Türkçe Özet: Microsoft, Mayıs 2025'teki Build geliştirici konferansında **"açık ajanik web"** vizyonunu desteklemek için Model Context Protocol (MCP) etrafında kapsamlı adımlar attığını duyurdu. Şirket, GitHub, Copilot Studio, Dynamics 365, Azure AI Foundry, Semantic Kernel ve Windows 11 dahil olmak üzere kendi ajan platformu ve framework'lerinde MCP'yi yerel olarak destekleyeceğini açıkladı. Ayrıca Microsoft ve GitHub, Anthropic liderliğindeki MCP Yürütme Komitesi'ne (Steering Committee) katılarak protokolün güvenli ve ölçekli benimsenmesini hızlandırmayı hedeflediklerini belirttiler. Bu iş birliği kapsamında, **yeni bir yetkilendirme spesifikasyonu** (OAuth 2.1 tabanlı) geliştirildiği ve mevcut kullanıcı kimlik doğrulama yöntemleriyle AI ajanlarına güvenli veri/servis erişimi izni verme standartlarının oluşturulduğu

açıklandı. Ek olarak, herhangi bir kişinin genel veya özel MCP sunucularını kaydedip keşfedebileceği **merkezi bir MCP sunucu dizini** hizmetinin tasarlandığı duyuruldu. Microsoft'un bu girişimleri, geliştiricilerin birden çok özel ajanı orkestra etmesini kolaylaştıran Azure AI Foundry Agent hizmeti ve Entra Agent ID gibi kurumsal güvenlik araçlarıyla birlikte, AI ajan ekosisteminin **açık standartlar** etrafında büyümesini ve kurumsal düzeyde güvenle benimsenmesini teşvik etmeyi amaçlıyor.

- **Konu Başlığı:** Introducing the Data Commons MCP Server: Streamlining Public Data Access for AI Developers
  Kaynak/Kurum & Tarih: Google Developers Blog, 2025-09
  Bağlantı: https://developers.googleblog.com/en/datacommonsmcp/
  Türkçe Özet: Google, Eylül 2025'te Data Commons projesi kapsamında **Model Context Protocol sunucusunu** kullanıma açtığını duyurdu. Bu yeni MCP sunucusu, Google'ın geniş **kamusal veri kümelerini** (istatistiksel veriler, kamu veri setleri vb.) AI geliştiricilerinin ve ajanlarının anında erişimine sunmayı amaçlıyor. MCP sayesinde geliştiriciler, Data Commons'ın kapsamlı verilerini doğrudan ve standart bir arayüzle AI ajanlarına tükettirebilecek ve karmaşık REST API çağrılarını elle yönetmek zorunda kalmayacak. Google, bu yaklaşımın veriyle zenginleştirilmiş **ajan uygulamalarını** çok daha hızlı geliştirmeyi sağladığını ve büyük dil modellerinin güvenilir, kaynak gösterilebilir gerçek verilerle beslenerek hayal ürünü (halüsinasyon) cevaplar üretme olasılığını azalttığını vurguluyor. Blog yazısında sunulan *ONE Data Agent* örneği, MCP sunucusunun küresel sağlık finansmanı gibi dağınık ve çok boyutlu bir veri alanında doğal dil sorgularını anlayıp saniyeler içinde ilgili verileri birçok farklı kaynaktan derleyebildiğini gösteriyor. Bu yenilik sayesinde daha önce ayrı silo'lardaki verilerle elle rapor hazırlamak zorunda kalan kullanıcılar, tek bir AI ajanı aracılığıyla karmaşık sorgulara hızlı ve etkileşimli cevaplar alabiliyor. Google, Data Commons MCP sunucusunun Gemini CLI gibi araçlarla ve Google Cloud'un Agent Development Kit altyapısıyla entegre şekilde çalışabildiğini; böylece geliştiricilerin güvenilir **veri odaklı AI ajanlarını** kendi ürün ve iş akışlarına zahmetsizce dahil edebileceğini belirtiyor.

- **Konu Başlığı:** A New Frontier for Network Engineers: Agentic AI That Understands Your Network
  Kaynak/Kurum & Tarih: Cisco Blogs, 2025-05
  Bağlantı: https://blogs.cisco.com/learning/a-new-frontier-for-network-engineers-agentic-ai-that-understands-your-network
  Türkçe Özet: Cisco'nun Mayıs 2025 tarihli teknik blog yazısı, Model Context Protocol (MCP)'ün ağ mühendisliği alanında devrim yaratabilecek bir araç olduğunun altını çiziyor. MCP'nin özünde, büyük dil modellerine **çalışma zamanında yapılandırılmış ağ bilgisini** (ör. topoloji, ağ cihaz envanteri, kullanılan protokoller, güvenlik politikaları) otomatik ve programatik olarak enjekte etmek olduğu belirtiliyor. Bu sayede, bir LLM tabanlı ağ asistanı, yalnızca genel eğitim verisine dayalı "ortalama" cevaplar üretmek yerine, işletmenin **kendi ağına özgü koşulları** bilen ve onlara uygun çözümler sunan bir yardımcıya dönüşebiliyor. Örneğin, MCP kullanılmadan önce bir yapay zekâ destekli asistan ağ yapılandırması önerirken yanlış veya kurumda kullanılmayan protokoller önerebilir (örn. kurum OSPF kullanıyorken asistanın RIP önermesi gibi). MCP uygulandığında ise asistan, ilgili kurumdaki tüm çekirdek ve uç cihazları, tercih edilen yönlendirme protokollerini (OSPF, BGP vb.), kapsülleme teknolojilerini (VXLAN gibi) ve uyulması gereken güvenlik prensiplerini (ör. "telnet kapalı, SSH zorunlu") **JSON formatlı bir bağlam** olarak LLM'e iletebiliyor. Ardından modelden gelen yanıtlar, kurumun ağına tam uyan, tutarlı ve güvenli yapılandırmalar şeklinde oluyor. Blog, MCP'yi verimli kullanmak için ağ mühendislerinin hâlihazırda bildiği API entegrasyonu, Python ile otomasyon ve temel LLM prompt yönetimi becerilerinin yeterli olacağını belirtiyor. Sonuç olarak MCP'nin, gerçek dünya ağ bilgisini AI sistemlerine öğreterek **ağ tasarımı, sorun giderme ve otomasyon** görevlerinde insan

mühendislere akıllı bir ortak olacağı; bu yetkinliği erkenden edinen ağ profesyonellerinin gelecekteki iş tanımlarında öne çıkacağı vurgulanıyor.

- **Konu Başlığı:** What is Model Context Protocol (MCP)?
  Kaynak/Kurum & Tarih: IBM Think Blog, 2025-05
  Bağlantı: https://www.ibm.com/think/topics/model-context-protocol
  Türkçe Özet: IBM'in 2025 yılında yayınladığı açıklayıcı makale, Model Context Protocol (MCP)'yı yapay zekâ uygulamaları ile harici hizmetler arasında **etkili bir standart katman** olarak tanımlıyor. Yazıda MCP'nin, AI ajanlarını daha **bağlam farkında** hale getirirken, araç ve veri entegrasyonunu ortak bir protokolle düzenlediği; bu yönüyle donanım dünyasında farklı cihazları tek girişte birleştiren *USB-C standardına* benzetilebileceği belirtiliyor. Büyük dil modellerinin tek başına kullanıldığında güncel bilgilere erişememesi ve yalnızca eğitim verisi sınırları içinde yanıt verebilmesi sorununa dikkat çekilerek, MCP sayesinde LLM tabanlı bir ajanın **harici veri tabanları, API'ler veya canlı web kaynaklarına** güvenli erişim sağlayabileceği vurgulanıyor. Makale, LLM'lerin MCP ile metin tamamlama, soru yanıtlama gibi temel becerilerinin ötesine geçerek gerçek zamanlı veri sorgulama, araç kullanarak eylem gerçekleştirme ve kompleks iş akışlarını otomatikleştirme yetileri kazanacağını örneklerle açıklıyor. Örneğin, MCP destekli bir AI asistanının kurumsal bir veritabanına bağlanıp sorgu yapabileceği, bir takvim uygulamasından toplantı bilgisi çekip kullanabileceği veya bir bulut hizmetine API üzerinden erişip işlem gerçekleştirebileceği anlatılıyor. Anthropic'in MCP'yi 2024'te açık kaynak yapmasından bu yana protokolün sektör genelinde hızla benimsenmekte olduğunu belirten IBM, MCP kullanan AI sistemlerinin **daha tutarlı, izlenebilir ve kontrollü** bir şekilde dış dünya ile etkileşim kurduğunu ifade ediyor. Bununla birlikte, yazıda MCP ile gelen yeni güvenlik ve denetim ihtiyaçlarına da değinilerek, protokolün uygulanmasında **politika yönetimi, kimlik doğrulama ve denetim izleri** gibi konuların dikkatle ele alınması gerektiği not ediliyor.

- **Konu Başlığı:** WTF is Model Context Protocol (MCP) and why should publishers care?
  Kaynak/Kurum & Tarih: Digiday (Dijital Medya Analizi), 2025-09
  Bağlantı: https://digiday.com/media/wtf-is-model-context-protocol-mcp-and-why-should-publishers-care/
  Türkçe Özet: Dijital yayıncılık sektörü için kaleme alınan bu makale, **"ajanik web"** çağında Model Context Protocol'ün (MCP) içerik üreticilerine ve yayıncılara etkisini açıklıyor. Uzmanların, gelecekte internetin AI ajanları tarafından kullanıcılar adına gezinilen ve işlem yapılan bir ortama dönüşeceğini öngördükleri belirtilerek, web sitelerinin de bu değişime uyum sağlayıp içeriklerini AI tarafından kolay anlaşılır hale getirmeleri gerekeceği vurgulanıyor. Makale, Anthropic'in Kasım 2024'te açık kaynak olarak yayımladığı MCP'nin yayıncılar için bir anlamda *"AI çağının robots.txt dosyası"* işlevi görebileceğini söylüyor. Yani yayıncılar, sitelerindeki verileri bir MCP sunucusu üzerinden yapılandırarak AI sistemlerine hangi içeriklerinin açılacağını, hangilerinin kapalı kalacağını belirleyebilir. MCP, bir web sitesinin veya veri kümesinin AI ajanlarınca erişilebilir kısmını tanımlamak için standart bir **ara katman (middleware)** ya da API rolü üstlenir. Bu sayede yayıncılar, isterlerse premium veya abonelikle korunan içeriklerini bir MCP sunucusu aracılığıyla AI uygulamalarına lisanslı olarak sunabilir ve yapılan sorgu başına gelir elde edebilirler. Örneğin, *TollBit* adlı bir girişimin yayıncılara kendi MCP sunucularını kurup veri setlerini AI şirketlerine ücretli olarak açma imkanı sunduğu belirtiliyor. Medya özelinde olası kullanım senaryoları henüz gelişme aşamasında olsa da, makale bir AI ajanın birden fazla reklam sunucusuyla MCP üzerinden etkileşime girip bir reklam kampanyası için gerekli verileri hızla derleyebileceği gibi fikirlerin ortaya çıktığını aktarıyor. Özetle, MCP'nin yayıncılara içeriklerini AI ekosistemine **kontrollü ve izlenebilir** şekilde sunma olanağı vererek, hem veri gizliliğini koruma hem de yeni gelir modelleri oluşturma konusunda önemli bir araç haline gelebileceği ifade ediliyor.

Alanlara Göre Yoğunluk Analizi

Model Context Protocol, ortaya atıldığı 2024 sonundan bu yana en yoğun ilgiyi **yapay zekâ ve bilgi teknolojileri** alanlarında görmektedir. Protokol, doğal olarak büyük dil modelleri ve AI ajanlarının yeteneklerini genişletmeye odaklandığı için akademik çalışma ve sektör uygulamalarının büyük kısmı AI altyapısı ve yazılım entegrasyonu üzerinedir. Örneğin, sektörde **bulut ve yazılım devleri** (OpenAI, Anthropic, Microsoft, Google, IBM gibi) MCP'yi benimseyip desteklerken; araştırma camiasında da çok sayıda çalışma protokolün güvenlik, performans ve mimari boyutlarını ele almıştır. **Güvenlik ve siber güvenlik** sektörü özellikle dikkat çekicidir: MCP'nin yaygınlaşmasıyla oluşan yeni saldırı yüzeyleri ve riskler, hem akademide (MCP-Guard, araç zehirleme, vs.) hem de endüstride (Wiz, Bitdefender gibi güvenlik şirketlerinin raporları) detaylı biçimde incelenmektedir. Bunun yanı sıra MCP kavramının, **ağ ve iletişim teknolojileri** (Cisco örneğinde olduğu gibi ağ mühendisliği otomasyonu), **veri bilimi** (Google'ın kamu veri platformunu açması) ve **dijital medya/yayıncılık** (içerik üreticilerinin AI'a içerik sağlama yöntemleri) gibi farklı sektörlere de uzanmaya başladığı görülüyor. **Savunma veya biyoteknoloji** gibi yüksek derecede özel uzmanlık gerektiren alanlarda henüz MCP'ye dair kamuya açık belirgin bir uygulama veya çalışma bulunmasa da, MCP'nin özünde bir entegrasyon standardı olması bu sektörlerde de kapalı kapılar ardında ilgi görmesi muhtemel. Genel resme bakıldığında, MCP şu anda en yoğun etkiyi **yapay zekâ odaklı yazılım geliştirme, veri entegrasyonu ve güvenlik** alanlarında yaratıyor; diğer sektörlerdeki yansıması ise daha başlangıç aşamasında veya dolaylı şekillerde (standartlara uyum, veri paylaşım protokolleri vb. üzerinden) hissedilmeye başlanmış durumda.

Genel Değerlendirme

Model Context Protocol (MCP), yapay zekâ sistemlerini dış dünyaya bağlama sorununa getirdiği standart çözüm ile kısa sürede hem akademik ilgiyi hem de endüstriyel desteği üzerine çekmiştir. Nov 2024'te tanıtılmasından bu yana MCP, başta Anthropic ve OpenAI gibi AI öncüleri ile Microsoft, Google, IBM, Cisco gibi teknoloji devlerinin desteğini alarak fiilen bir *ortak dil* haline gelmeye başlamıştır. Akademide 2025 yılı boyunca MCP etrafında çok sayıda çalışma yayınlanmış olması, protokolün **gerçek bir boşluğu doldurduğunu** ve gelecek vaat ettiğini gösteriyor. Bu çalışmalar, MCP'nin güvenlik açıklarından performans kısıtlarına, çok-etmenli sistemlerde kullanımından farklı protokollerle karşılaştırılmasına dek pek çok boyutu ele alarak protokolün sağlam bir temel üzerinde geliştirilmesine katkı sağlıyor. Sektörel tarafta ise MCP, **ChatGPT, Claude** gibi büyük modellerin araç ve veri hizmetlerine erişimini kolaylaştırarak son kullanıcıya daha zengin ve bağlamsal olarak doğru deneyimler sunmayı mümkün kılıyor. Örneğin, Microsoft ve GitHub'ın MCP'yi destekleyip ortak bir **yürütme komitesi** kurması, yakın gelecekte MCP'nin geniş bir ekosistemde standart haline geleceğine işaret ediyor. Bununla birlikte, MCP'nin yaygınlaşması **yeni güvenlik ve yönetişim zorluklarını** da beraberinde getiriyor; zira AI ajanlarının bir protokol üzerinden pek çok sisteme erişebilmesi, hatalı yapılandırma veya kötüye kullanım durumlarında zincirleme etki yaratabilir. Neyse ki hem araştırmacılar hem de sektör aktörleri bu risklerin farkında olup proaktif çözümler (örn. MCP-Guard, gerçek zamanlı politika denetimleri, yetki sınırları vb.) geliştirmeye başladılar. Sonuç olarak, MCP her ne kadar henüz olgunlaşma sürecinde olan bir standart olsa da, **araçlarla donanmış ve bağlamsal zekâya sahip yapay ajanların** yaygınlaştığı bir geleceğe doğru atılmış önemli bir adım olarak görülüyor. Önümüzdeki yıllarda MCP'nin standardizasyonunun daha da netleşmesi, farklı sektörlerdeki kullanım senaryolarının olgunlaşması ve etrafında bir **açık ekosistem** oluşması beklenebilir. Bu gelişmeler ışığında MCP, yapay zekâ ile gerçek dünya arasındaki etkileşimi *USB-C misali* tek bir arayüzden düzenleyerek, AI çağının altyapı taşıyıcılarından biri olma potansiyeline sahiptir.
