Model Context Protocol 기술동향 및 발전방향 고찰에 관한 연구

오준영, 전중양*, 임현진**

정보통신기획평가원, *충남대학교, **과학기술정보통신부

sechs11@iitp.kr, *mislab@cnu.ac.kr, **hyunjin0@korea.kr

A Study on the trend and development direction of the Model Context Protocol

Oh Jun Young, *Jeon Joong Yang, **Im Hyun Jin

Institute of Information & communications Technology Planning & Evaluation, *Chungnam National Univ., **Ministry of Science and ICT

요 약

본 논문은 생성형 AI의 외부 데이터 및 도구 활용을 표준화하는 Model Context Protocol(MCP)의 등장 배경과 구조, 기술 동향을 고찰하고, 기존 RAG 방식과의 차별성을 분석한다. MCP는 AI 모델의 자율성과 도구 연동성을 높여 다양한 산업에 적용 가능성을 확대하지만, 보안 취약성, 컨텍스트 관리의 어려움, LLM 성능 의존 등의 한계를 지닌다. 이에 따라 보안 프레임워크 강화, 다단계 워크플로우 오류 복구, 통신 효율 개선, 다양한 플랫폼과의 상호운용성 확보 등 기술 발전 방향을 제시한다. MCP는 향후 AI 생태계의 핵심기술로 자리잡을 것이며 다양한 산업 분야에서 새로운 AI 기반 서비스 및 애플리케이션 창출을 가능하게 할 것으로 기대된다.

Ⅰ. 서 론

우리는 모두 인공지능(AI) 시대에 살고 있다. AI 분야 중에서도 특히 LLM의 놀라운 발전은 상호작용이 가능하고 지능적인 시스템의 새로운 패러다임을 열었다.[1] 2022년 11월, OpenAI에서 챗GPT 서비스를 출시한 이후 AI기술은 더욱 더 빠른 속도로 발전해 왔으며 기술 뿐 아니라 정치, 경제, 사회 등 우리 인류의 모든 영역에 큰 영향을 미치기 시작했다. 챗GPT 뿐 아니라, 제미나이, 클로드, DeepSeek 등 새로운 LLM들이 출현하고 있으며 비약적인 발전을 거듭하고 있다. 이에 따라 AI모델이 외부의 다양한 데이터 및 도구와 효과적으로 연동되어 활용될 필요성이 점차 증대되고 있다. 기존의 AI 시스템 통합 방식은 특정 목적에 따라 개별적 맞춤형 코딩 및 플러그인 개발에 의존하는 경우가 많아 시스템 비효율성을 야기하고 확장이 제한되는 경우가 많았다. 이러한 문제점을 해결하고 AI모델과 외부 환경 간의 안전하고 표준화된 통신을 가능하게 하는 새로운 접근방식으로 MCP가 주목받고 있다. LLM의 발전은 더욱 정교하고 복잡한 작업을 수행하는 방향으로 발전하고 있지만 여전히 학습 데이터에 의존하는 등 한계점을 보이고 있다. 실세계의 문제 해결을 위해서 최신 정보에 대한 접근과 외부 도구 활용이 필수적이며 기존의 임시 방편적 통합 방식으로는 신뢰할 수 있는 AI모델을 구현하기 어렵다. MCP는 AI 애플리케이션과 다양한 외부 시스템 간의 연결을 표준화함으로써 개발과정을 단순화하고 다양한 서비스와의 호환성을 높여 AI 기술의 활용 범위를 획기적으로 확장할 수 있는 잠재력을 가지고 있다.[2] 이러한 기술 잠재력을 주목하여 빅테크 기업들은 MCP를 적극적으로 활용하고 발전시킬 수 있는 방안들을 강구하고 있다.

본 논문에서는 MCP의 등장배경 및 개념, 기본구조·작동방식을 살펴보고 기존 기술과의 비교, 최신산업·기술동향, 적용사례를 고찰하고자 한다. 이러한 내용을 바탕으로 MCP의 문제점 및 한계, 기술발전 방향을 제언한다.

Ⅱ. 본론

1. MCP의 등장배경 및 개념

최근 LLM 등 생성형 AI를 비롯한 챗봇 서비스가 급속하게 발전하면서 더욱 복잡한 상황에서 Hallucination 없이 사용자의 질문에 대해 정확하고 맥락에 맞는 응답을 제공하기 위한 컨텍스트 관리의 중요성이 부각되었으며 이러한 배경 하에 MCP가 등장하게 되었다. 기존의 생성형 AI 모델은 학습데이터에 지나치게 의존하거나 제한적인 방식으로 외부 데이터에 접근하는데 그쳐 정보의 고립이라는 근본적인 문제점을 갖고 있었다. 그리고 새로운 데이터 소스를 AI 시스템에 통합하기 위해서는 각 소스마다 맞춤형 구현이 필수적이었으며 이는 연결된 시스템의 확장성을 저해하는 요인으로 작용하였다. 또한 AI 애플리케이션마다 외부 시스템과의 연결 방식을 개별적으로 개발해야 하는 상황은 개발의 비효율성을 초래하여 개발 및 유지보수 비용을 증가시키는 단점을 초래하였다. 다양한 데이터소스와 AI 시스템을 통합하는 단일의 표준화된 표준 프로토콜을 제공함으로써 개별적인 시스템 통합을 간소화하고 데이터의 신뢰성을 높이는데 기여한다. AI 에이전트의 기능은 다양한 외부와의 원활한 연결과 통합을 통해 크게 강화될 수 있으며 이러한 시스템 통합에서 MCP와 같은 표준화된 프로토콜은 핵심적인 기능을 담당한다. 특히 MCP는 전문적인 코딩 역량이 없어도 비개발자가 AI 에이전트 기능을 쉽게 확장할 수 있도록 지원하며 이는 AI 기술의 접근성을 높이고 다양한 분야에서의 활용 가능성을 확대하는데 큰 의미를 가진다.[3] 이러한 MCP의 등장으로 AI 에이전트와 에이전틱 워크플로우의 급속한 발전을 이루고 있으며, 이는 휴머노이드, AI반도체, 차세대 보안, 디지털 헬스케어 등 다양한 산업 도메인에서 더욱 더 큰 파급효과를 지닐 전망이다. 다음으로 MCP의 개념에 대해 살펴보자. MCP는 AI 모델이 데이터베이스 등 외부 데이터 소스 및 도구와 효과적으로 상호작용할 수 있

도록 설계된 표준 통신규약으로써 Anthropic에서 개발하여 2024년 11월 오픈소스로 공개하였다.[4][5] MCP는 AI 모델의 확장성과 활용성 향상을 목표로 하고 있으며 최근 AI 에이전트와 에이전틱 워크플로우의 발전으로 MCP에 대한 산업계의 관심이 급증하고 있다. 또한 OpenAI 등 글로벌 빅테크 기업 및 오픈소스 커뮤니티에서 표준으로 채택되어 급속히 증가하고 있다.

2. MCP의 기본구조 및 작동방식

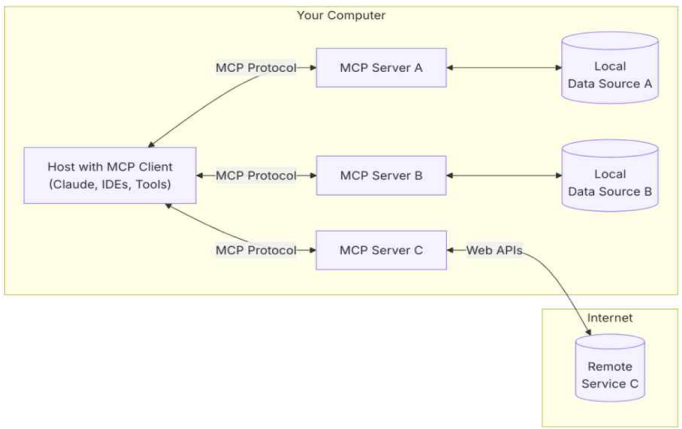
MCP는 클라이언트-서버 아키텍처를 기반으로 설계되었으며, MCP 호스트, MCP 클라이언트, MCP 서버의 세 가지 핵심적 구성요소로 이루어져 있다.[6]

·MCP호스트 : AI 애플리케이션의 컨테이너 역할을 하며 클라이언트 연결을 관리하고 AI/LLM 통합을 조정한다. 예시:클로드 앱, IDEs, AI도구 등

·MCP클라이언드 : MCP 호스트에 의해 생성되며 서버와의 독립적인 연결을 유지하며 프로토콜 메시지를 양방향으로 라우팅한다. 각 클라이언트는 일반적으로 서버 당 하나의 연결을 유지하며, 호스트와 서버 간의 통신을 중개하는 통역사와 같은 역할을 수행한다.

·MCP서버 : 특정 컨텍스트트와 기능을 제공하며 리소스, 도구 및 프롬프트를 노출한다. 로컬 프로세스 또는 원격 서비스일 수 있으며 하나의 호스트는 동시에 여러개의 서버와 연결하여 다양한 기능을 통합적으로 사용할 수 있는 유연성을 제공한다.

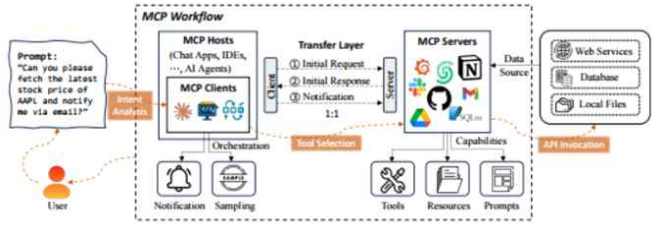
<그림1, MCP의 기본구조>



<출처 : MCP 기본가이드, https://modelcontextprotocol.io/introduction>

MCP의 일반적인 작동방식은 다음과 같다. 먼저 외부 클라이언트로부터 요청이 수신되면 해당 요청을 처리하기 위한 컨텍스트가 생성된다. 이 컨텍스트는 요청과 관련된 데이터, 사용 가능한 도구 및 리소스 정보 등을 포함할 수 있다. 다음으로 AI모델은 생성된 컨텍스트를 참조하여 요청된 데이터를 처리하거나, 필요한 경우 연결된 MCP 서버를 통해 외부 도구를 호출하여 작업을 수행한다. 마지막으로 처리된 결과는 다시 컨텍스트에 저장된 후 클라이언트에게 반환된다.[7]

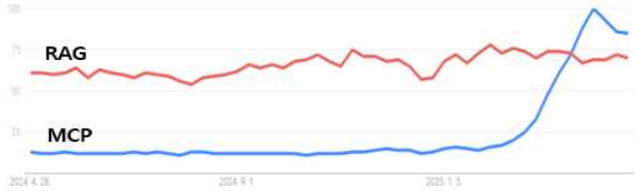
<그림2, MCP 워크플로우>



3. MCP와 기존 기술과의 비교

MCP 이전에 외부정보를 활용할 수 있도록 지원하는 대표적인 기술로 RAG을 들 수 있겠다. RAG(Retrieval-Augmented Generation, 검색증강생성)이란 사전에 저장된 지식 기반(Knowledge Base) 또는 외부 문서 저장소에서 현재 입력과 관련된 정보를 검색하여 AI모델 답변에 포함하는 방식으로 이는 컨텍스트 윈도우의 한계를 보완하며 최신 정보 반영에도 유용한 기술이다.[8] 최근 AI모델의 최신 정보 반영 및 환각현상 최소화에 RAG가 유용하게 사용되었으나, 2025년 3월 이후 OpenAI가 MCP 표준을 지원한다고 발표한 후 기술업계의 MCP에 대한 관심은 RAG을 뛰어넘고 있다.

<그림3, RAG & MCP 구글 트렌드분석>



MCP와 RAG 모두 LLM이 외부 정보를 활용할 수 있도록 지원하지만 양방향성, LLM의 자율성 등에서 MCP가 기술적 이점을 가진다.

<표1, MCP와 RAG 비교분석>

구분	MCP	RAG
정보흐름	**양방향**(LLM이 필요한 정보를 요청하고 받음)	**단방향**(사전 검색된 정보를 프롬프트에 삽입)
맥락제어	LLM이 많은 자율성 보유	개발자가 제어
맥락창 활용	필요한 정보만 선택적으로 요청하여 효율적 활용	검색된 모든 정보가 맥락창을 차지
검색시점	대화 중 동적으로 필요할 때	사용자 쿼리 시점에 고정
구현복잡성	양방향 프로토콜 구현 필요	상대적으로 단순

4. MCP 최신산업·기술 동향

Anthropic에서 MCP를 오픈소스로 공개한 이후 MCP는 다양한 LLM모델이 여러 데이터 소스와 도구에 표준화된 방식으로 연결되도록 지원하고 있으며, 이는 개발자들이 AI 애플리케이션을 용이하게 구현할 수 있도록 확대되고 있으며 많은 기업들이 MCP를 새로운 기술 표준으로 채택하고 있다. 그중 Anthtopic의 경쟁사인 OpenAI가 MCP를 공식적으로 지원하기로 결정('25.3월)한 이후 국내를 비롯한 전 세계 업계 전반으로 확산되는 추세이다. 또한 Microsoft는 자사의 브라우저 자동화 기술 래퍼인 Playwright-MCP를 출시('25.4월)하였고 Google은 MCP 표준 참여를 검토하하고 있다. 최근 Anthropic에서는 integration기능을 업데이트했는데, 이를 통해 개발자들은 자체 앱 서버를 구축해 연결 기능을 확대할 수 있으며 사용자는 해당 기능을 클로드에서 직접 검색하고 연결할 수 있다. 주요 빅테크 기업들은 MCP 기술 고도화에 박차를 가하고 있으며 다음과 같은 특징적 경향을 보이고 있다.

·OpenAIGPT-4Turbo : 128K 토큰 길이의 context window를 제공함으로써 방대한 문서를 입력하고 받아들이고 일관된 응답을 생성할 수 있다. 이와 함께 Function Calling, Tool Use 등의 기능을 통해 대화 흐름내 도구 활용까지 결과에 반영하고 있다.

·AnthropicClaude3 : 'Constitutional AI' 개념에 기반하여 컨텍스트를 윤리적, 논리적으로 정제하는 방식을 채택하였다. 이 모델은 장기 메모리 기능을 통해 사용자의 대화내역을 요약하고 지속적 학습이 가능한 방향을 제시하고 있다.

·Langchain,LiamaIndex 등 : 컨텍스트 저장, 요약, 재사용 기능을

표준화하여 애플리케이션 개발자의 활용을 제고하고 있다.

MCP의 주요 기술동향을 살펴보면 다음과 같다. MCP는 표준화된 프로토콜을 통해 서로 다른 환경에서 개발된 AI에이전트와 도구간의 상호 운용성을 강화하는데 중점을 두고 있다. 또한 클라이언트와 서버 간 통신을 표준화함으로써 특정 AI모델에 종속되지 않고 다양한 프레임워크를 활용할 수 있는 유연성을 가지고 있다. 이러한 유연성은 개발자들이 특정 플랫폼, 기술에 종속되지 않고 자신의 프로젝트에 최적화된 도구와 기술을 선택하고 통합할 수 있도록 지원하고 있다.

MCP는 AI 에이전트가 실시간 데이터 스트림, 로컬 파일 시스템, 다양한 외부 시스템 등 광범위한 정보 소스에 더욱 쉽고 빠르게 접근하고 활용될 수 있도록 빠르게 개발되고 있다. 이는 AI 에이전트의 접근성을 획기적으로 높여 단순히 학습된 데이터에 의존하는 것이 아니라 실세계의 최신 정보를 실시간으로 반영하여 정확한 답변을 제공하도록 지원한다.[9] 마지막으로 MCP 기술발전이 가속화되고 많은 개발자들이 쉽게 접근할 수 있도록 다양한 개발 도구 및 생태계가 활발하게 조성되고 있다. 예를 들어 Quick-start Auto MCP는 사용자들이 복잡한 단계 없이 클로드 Desktop이나 Cursor와 같은 환경에서 기능을 즉시 활용할 수 있도록 지원하여 개발 편의성을 크게 높이고 있다. 또한, LangChain이나 Dify와 같이 널리 사용되는 AI 에이전트 구축 프레임워크와의 연동이 강화되면서, MCP를 활용한 다양한 애플리케이션 개발이 증가하고 있으며, 이는 MCP 기반 AI 서비스 개발 생태계 전반을 더욱 활성화시키는 중요한 요인이 된다.

5. MCP 적용사례

MCP는 다양한 산업 분야에서 AI 에이전트의 활용 가능성을 넓히고 혁신적인 서비스를 창출하는 데 기여하고 있다. 고객 서비스 분야에서 MCP는 챗봇 성능을 획기적으로 향상시키는 데 활용된다. MCP를 통해 챗봇은 고객의 문의 내용을 보다 정확하게 이해하고, 관련된 내부 지식 베이스나 외부 정보를 실시간으로 검색하여 고객의 상황에 맞는 맞춤형 답변을 빠르게 제공한다. 또한 챗봇이 고객의 감정을 분석하고 적절한 어조로 응대하며, 해결 과정을 안내하는 등 더욱 인간과 유사한 상호작용을 가능하게 하여 고객 만족도를 높이고 상담원의 업무 부담을 줄여준다. 챗봇이 단순히 미리 정의된 스크립트에 따라 응답하는 수준을 넘어 대화의 맥락을 깊이 있게 파악하고 실시간 정보를 융합하여 더욱 지능화된 고객 응대를 제공하여 고객 서비스 품질을 향상시키고 운영 효율성을 극대화한다..

교육 분야에서 MCP를 활용하여 개인 맞춤형 학습 플랫폼을 구축하는 사례가 늘고 있다. MCP 기반 AI 튜터는 학생 개개인의 학습 스타일, 현재 수준, 관심사를 정확하게 파악하여, 각 학생에게 최적화된 교육 콘텐츠를 제공하고 학습 진도를 맞춤형 학습진도 관리가 가능하다. 또한 학습 과정에서의 어려움이나 감정 상태를 분석하여 학습 동기를 부여하고, 질문에 즉각적으로 답변하며, 학습 효과를 극대화하는 데 필요한 다양한 기능을 제공한다. 이러한 개인 맞춤형 학습 경험은 개인 학습 능력을 향상시키고, 교육 격차를 해소하며, 교육환경 조성에 효과적이다.

금융 분야에서는 MCP가 AI 기반 위험 관리 시스템 구축에 중요하게 작용한다..AI 모델은 방대한 양의 금융 시장 데이터, 거래 기록, 뉴스를 실시간으로 분석하여 잠재적 위험 요소를 신속하게 감지하고 투자 결정을 지원하는 데 활용된다. MCP는 AI 모델이 비정상적인 거래 패턴을 분석하여 사기 행위를 탐지하고, 자금 세탁과 같은 불법적인 금융 활동을 방지하며, 금융 거래의 전반적인 안전성을 높이는 데 필요기능을 제공한다. 이는 금융 기관이 잠재적인 손실을 줄이고, 규제 준수를 강화하며, 더욱 안전하고 투명한 금융 시스템을 구축하는 데 크게 기여한다.

소프트웨어 개발 자동화에서도 MCP가 활발하게 활용된다. LLM과 MCP를 결합하여 요구사항 분석부터 코드 작성, 테스트 생성, 코드 리뷰, 기술문서 작성,최종 배포 스크립트 자동화까지 전체 개발 프로세스 자동화가 가능하다. 특히 MCP를 통해 LLM 기반 DevOps 파이프라인을 구성함으로써, 지속적인 통합 및 배포 프로세스를 자동화하여 SW개발 효율성을 대폭 향상시킨다. MCP는 AI 에이전트들이 다양한 개발 도구 및 관련 정보에 효율적으로 접근하고 협업할 수 있도록 지원함으로써, 소프트웨어 개발의 생산성과 최종 결과물의 품질을 동시에 높이는 데 중요한 역할을 한다.

또 다른 주요 적용 사례는 파일 시스템 및 외부 서비스와의 연동이다. MCP 서버를 활용하면 AI 에이전트가 로컬 컴퓨터의 파일 시스템이나 클라우드 저장소에 직접 접근하여 파일을 검색, 정리, 생성, 업로드하는 등 작업을 자동화할 수 있다. 외부 API와의 연동을 통해 실시간 날씨 정보, 주식 데이터, 개인 일정 관리 등 외부 정보를 AI에이전트가 필요에 따라 가져와 활용할 수 있다. 외부 정보 통합능력은 AI 에이전트의 활용 범위를 대폭 확장시키고, 실제 환경에서의 작업 수행 능력을 크게 향상시킨다.

한편, MCP를 활용한 AI 서비스 개발 및 적용 과정에서 개인 정보 보호는 중요한 고려사항으로 부각되고 있다. MCP를 통해 AI 에이전트가 접근할 수 있는 컨텍스트 데이터에는 사용자가 입력한 민감한 개인 정보가 포함될 위험이 존재하며, AI 서비스 제공자에 의한 개인 정보 오남용, 그리고 프롬프트나 결과물을 통한 개인 정보 유출 및 재식별 가능성에 대한 충분한 인식이 필요하다. 따라서 MCP 기반 AI 서비스를 설계하고 개발할 때에는 차등적 프라이버시 기법 적용, 엄격한 접근 권한 관리, 그리고 모든 활동에 대한 상세 로그 기록 관리 등 다양한 보안 및 개인 정보 보호 기술을 적극적으로 도입하고 적용하는 것이 강조된다.

Ⅲ. 결론

1. MCP의 문제점 및 한계

MCP는 AI생태계에 많은 가능성과 이점을 제공하지만 아직 초기 단계로 다음과 같은 문제점과 한계를 가지고 있다.

가장 큰 문제는 보안 취약점이다. MCP 서버는 여러 서비스에 대한 인증 토큰을 저장하므로 공격자에게 취약한 공격대상이 된다. 서버가 손상될 경우 연결된 모든 서비스에 대한 접근 권한이 노출될 수 있으며, OAuth 토큰 탈취, 악성 프롬프트 주입 공격, 과도한 권한 설정 등의 보안 위협이 발생할 수 있다. 특히 사용자 인증 및 보안 문제 해결이 중요한 과제이며 여러 도구가 연결되는 환경에서 데이터 유출이나 악성 도구 연결 등의 보안 리스크에 노출될 수 있다. MCP 생태계는 보안 집중식 보안 감독의 부재로 인해 보안관리의 불일치가 발생할 수 있다. MCP 서버는 개별 개발자에 의해 관리되므로 각 서버의 보안 수준이 다를 수 있으며 MCP 서버의 보안을 감사하고 검증할 수 있는 중앙 플랫폼이 없어 일관된 보안 유지가 어렵다.[10]

다단계 시스템 간 워크플로우에서 일관성을 유지하는 것 또한 MCP의 주요 한계이다. 분산시스템의 특성상, 여러 단계로 이루어진 워크플로우에서 연속적인 도구 상호작용 간에 일관된 컨텍스트를 유지하는 것은 어렵다.. 효과적인 상태 관리 및 오류 복구 체계가 부족하면 오류가 전파되거나 중간 결과가 손실될 위험이 있으며, 이는 불완전하거나 일관성 없는 워크플로우를 초래할 수 있다. 다양한 플랫폼 간의 동적 조정 과정에서 지연이나 충돌이 발생할 수 있으며, 이는 MCP 환경 내에서 워크플로우의 원활한 실행을 더욱 복잡하게 만든다.

다음으로 LLM 자체의 한계를 들 수 있다. MCP 통합의 효과는 개별 LLM 자체의 성능에 크게 의존한다. LLM의 신뢰성이 낮으면 MCP를 통해 연결된 도구를 정확하게 활용할 수 없으며 이는 잘못된 정보 제공이나

오작동으로 이어질 수 있다. 또한 LLM은 제공된 모든 데이터를 처리하는데 어려움을 겪을 수 있으며 이는 응답시간 지연, 성능 저하로 이어질 수 있다.

마지막으로 컨텍스트 관리의 어려움이다. MCP는 다양한 데이터 소스와 연결을 지원하지만 높은 처리량 환경에서 컨텍스트를 효율적으로 관리하는데 어려움을 겪을 수 있다. AI 에이전트가 여러 데이터 소스를 넘나들 때 일관성을 유지하고 관련된 모든 정보를 정확하게 추적하는 것은 여전히 해결해야할 문제이다.

2. MCP 기술발전 방향

MCP는 이러한 문제점과 한계를 보완하며 확대해 나갈 것이다.

먼저 MCP 보안 강화이다. MCP 생태계의 신뢰성을 높이기 위해서 표준화된 인증 및 권한 부여 프레임워크 개발이 필요하다. 클라이언트와 서버 간의 안전한 ID 확인 및 접근 제어를 위한 통합 메커니즘을 마련하고 다양한 환경에서 일관된 보안 정책을 적용할 수 있도록 세분화된 권한 관리를 강화해야 한다. 현재 MCP는 클라이언트와 서버 간의 인증 및 권한 부여를 관리하는 통일된 방식이 없어 보안 취약점이 발생하기 쉽다. 표준화된 프레임워크를 개발함으로써 MCP 생태계 전반에 걸쳐 일관된 인증 및 권한 부여 정책을 적용할 수 있게 될 것이다. 데이터 보안 강화를 위해서 향상된 암호화 기술 및 보안 패턴 도입을 고려해야 한다. 전송 계층 보안을 강화하여 데이터의 기밀성을 유지하고 악의적 행위를 방지하기 위한 고급 암호화 기술(예: DPoP) 적용을 검토해야 한다. 또한, MCP 구현자와 채택자를 위해 실행 가능한 보안 패턴을 개발하고 제공함으로써 보다 안전한 MCP 환경을 구축할 수 있을 것이다.

다음으로 MCP 기능개선을 들 수 있다. MCP 기반 시스템의 유지보수와 신뢰도를 높이기 위해서 강력한 디버깅 및 모니터링 도구 개발이 필요하다. 오류 추적, 도구 상호작용 시각화, 시스템 성능 분석 기능을 제공하고 , 표준화된 로깅 메커니즘 및 중앙 집중식 모니터링 시스템을 구축하여 시스템의 상태를 효과적으로 파악하고 문제를 신속하게 해결할 수 있도록 지원해야 한다. 다단계 워크플로우의 안정적 실행을 위해서는 워크플로우 관리 및 오류 복구 메커니즘 개선이 요구된다. 다단계 워크플로우의 상태를 효과적으로 관리하고 오류 발생 시 복구할 수 있는 기능을 강화하여 , 워크플로우 실행의 일관성·안정성을 확보해야 한다. 이는 MCP를 활용한 복잡한 자동화 시스템 구축에 필수적 요소이다. MCP의 활용 범위를 넓히기 위해 다양한 환경 및 플랫폼 지원 확대가 필요하다. 클라우드, 온프레미스, 환경 등 다양한 배포 환경을 지원하고 이기종 장치·시스템과의 원활한 상호운용성을 확보해야 한다. 다양한 환경에서의 호환성은 MCP의 적용 확률을 높일 것이다.

다음으로 MCP의 성능향상을 들 수 있다.. MCP 기반 애플리케이션의 응답성을 향상시키기 위해서 통신 효율성 개선 및 지연 시간 감소가 중요하다. MCP 클라이언트와 서버 간의 통신 프로토콜을 최적화하고 , 특히 낮은 지연 시간이 요구되는 애플리케이션에서의 성능 향상에 집중해야 한다. MCP의 확장성을 위해 효율적인 자원 관리 및 확장성 개선이 필수적이다. 다중 테넌트 환경에서 효율적인 자원 할당 및 격리를 위한 메커니즘을 개발하고 수평적 확장을 용이하게 하는 아키텍처를 연구해야 한다. 이는 MCP가 대규모 사용 및 복잡한 애플리케이션을 지원하는 데 중요한 역할을 할 것이다.

차세대 MCP는 더욱 안전하고 신뢰할 수 있는 프로토콜로 발전할 것으로 기대된다. 강화된 보안 기능과 안정적인 작동을 통해 사용자 신뢰를 확보하고, 잠재적인 보안 위협에 대한 선제적 대응 능력을 갖출 것이다. 또한, 지능적이고 자동화된 워크플로우 지원이 강화될 것이다. AI 기반 컨텍스트 관리 및 도구 선택 자동화를 통해 효율적인 작업 수행을 지원하고, 복잡한 다단계 워크플로우의 원활한 실행 및 관리를 도울 것이다. 더불어, 다양한 AI 모델 및 외부 시스템과의 완벽한 통합을 제공하여 이기종 환경에서의 높은 상호운용성을 보장하고, 새로운 AI 모델 및 기술과의 용이한 통합을 지원할 것이다. 이러한 발전을 통해 차세대 MCP는 이전에는 불가능했던 혁신적인 AI 기반 서비스 및 애플리케이션 창출을 가능하게 하고, 다양한 산업 분야에서 AI 활용의 새로운 혁신을 열 것으로 기대된다. 이러한 MCP의 성능향상과 발전은 휴머노이드의 확산, 일반인공지능(AGI)의 구현에 밑거름이 될 것이다.

3. 종합적 제언

본 연구에서 MCP의 등장배경 및 개념, 기본구조, 산업·기술동향, 발전방향 등에 대해 심층적으로 살펴보았다. MCP는 AI 모델과 외부 데이터 소스 및 다양한 도구를 연결하기 위한 표준화된 개방형 프로토콜로서 기존의 개별적 통합방식이 가지고 있던 여러 한계를 극복하고 AI 애플리케이션 개발의 비효율성을 획기적으로 제고하며 시스템 확장성을 향상시키는 핵심적 기술로 부상하고 있음을 확인하였다. 최신 기술 동향 분석을 통해 MCP가 이미 다양한 산업 도메인에서 활발하게 적용되고 있으며 주요 빅테크 기업들의 적극적인 도입·지원을 통해 그 필요성, 중요성이 부각되고 있음을 알 수 있었다. 또한 MCP의 미래 발전방향 전망을 통해 기술적 개선 뿐 아니라 산업 전반의 각 산업 분야로의 광범위한 확산을 예측할 수 있었다. 특히 사용자 편의성 증대, 보안기능 강화, 다양한 AI모델과의 호환성 향상 등이 향후 MCP 기술 발전에 중요한 요소로 작용할 것으로 기대한다. 본 연구를 통해 MCP 기술의 현재 상황과 미래 잠재력에 대한 깊이 있는 인사이트를 제공하며 관련 산업 및 기술발전에 조금이나마 기여할 수 있었으면 한다. 향후 실제 기업에서 벌어지는 MCP 적용사례에 대한 심층분석, MCP 시스템의 보안 취약점 분석과 해결방안 연구 등으로 확대될 것을 기대한다.

ACKNOWLEDGMENT

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation(IITP) & Korea government(MSIT).

참 고 문 헌

[1] Partha Pratim Ray, “A Survey on Model Context Protocol: Architecture, State-of-the-art, Challenges and Future Directions.” TechRxiv, April 2025.

[2] Felipe Jaramillo, “How Model Context Protocol Is Changing Enterprise AI Integration”, Editorial, April 2025.

[3] goover, “AI시대의 열쇠, Model Conttext Protocol(MCP)의 현재와 미래”, April 2025.

[4] Anthropic Docs, https://www.anthropic.com/news/model-context-protocol, Nov.2024..

[5] Vineeth Sai Narajala and Idan Habler, “Enterprise-Grade Security for the Model Context Protocol (MCP): Frameworks and Mitigation Strategies”, arXiv, April 2025.

[6] MCP 기본가이드, https://modelcontextprotocol.io/introduction

[7] Xinyi Hou, “Model Context Protocol (MCP): Landscape, Security Threats,and Future Research Directions”, arXiv, April 2025.

[8] NIA, “검색증강생성(RAG) 기술의 등장과 발전방향”, Digital Insight 2024.

[9] Jim Liddle, “Why Your Company Should Know About Model Context Protocol”, NASUNI Report, April 2025.

[10] QueryPie, “MCP 보안성 평가: 문헌 조사를 통한 MCP 보안 위협 식별 및 취약점 분석”, White paper, April 2025.