एमसीपी 2.0

डी क्यू एल–रेडी डेटा से एआई–रेडी प्रणालियों की ओर

संपादित : **मोहन दास विस्वम्**

कृत्रिमबुद्धिमत्ता (एआई) प्रणालियों—विशेष रूप से एलएलएम—ने मानव भाषा को समझने, उसका विश्लेषण करने तथा उसे उत्पन्न करने की क्षमता में उल्लेखनीय प्रगति की है। वर्तमान में इन मॉडलों का व्यापक उपयोग सूचना प्राप्ति, दस्तावेज़ों का संक्षेपण, निर्णय समर्थन, सामग्री सृजन तथा संवादात्मक उपयोक्ता अंतरफलक जैसे विविध कार्यों में किया जा रहा है। विशाल पाठ्य-संग्रह पर तर्क करने और प्राकृतिक भाषा में उत्तर देने की इनकी क्षमता ने उपभोक्ता एवं व्यावसायिक—दोनों ही परिवेशों में सुगम्यता को उल्लेखनीय रूप से बढ़ाया है।

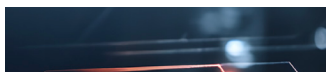
हालाँकि, इन प्रगतियों के बावजूद एलएलएम मूलतः स्वतंत्र एवं पृथक संगणकीय प्रणालियों के रूप में कार्य करते हैं। संरचनात्मक रूप से इनमें बाह्य उपकरणों, सक्रिय (लाइव) डेटाबेसों, उद्यम अनुप्रयोगों, एपीआई अथवा परिचालन कार्यप्रवाहों के साथ प्रत्यक्ष रूप से संवाद करने हेतु कोई अंतर्निहित, मानकीकृत एवं सुरक्षित तंत्र उपलब्ध नहीं होता। परिणामस्वरूप, एलएलएम किसी कार्य की अनुशंसा या उसका वर्णन तो कर सकते हैं, किंतु व्यापक बाह्य अवसंरचना के बिना वास्तविक प्रणालियों में उन कार्यों को विश्वसनीय रूप से निष्पादित नहीं कर पाते।

यह सीमा वास्तविक-विश्व तथा उद्यम परिवेशों में एआई के व्यावहारिक परिनियोजन को गंभीर रूप से सीमित करती है, जहाँ वास्तविक-समय डेटा तक पहुँच, नियंत्रित प्रणाली क्रियाएँ तथा संगठनात्मक नीतियों और गवर्नेंस ढाँचों का अनुपालन अत्यंत आवश्यक होता है। वर्तमान एकीकरण पद्धतियाँ प्रायः कस्टम-निर्मित कनेक्टरों, विशेष मिडलवेयर अथवा एड-हॉक एवं अत्यधिक युग्मित अंतरफलक पर आधारित होती हैं। ऐसी व्यवस्थाएँ प्रायः अस्थिर, बहु-मॉडल अथवा बहु-उपकरण परिवेश में विस्तार के लिए कठिन, अनुरक्षण की दृष्टि से महँगी तथा सुरक्षा, अभिगम नियंत्रण, ऑडिट, और दीर्घकालिक गवर्नेंस से संबंधित जोखिम उत्पन्न करने वाली होती हैं।

निलाद्रि बिहारी मोहंती
वैज्ञानिक–डी
niladri.mohanty@nic.in

निखिल कुमार
वैज्ञानिक अधिकारी
nikhil.kumar27@nic.in

एमसीपी एक खुला और मानकीकृत ढाँचा है, जो एआई मॉडलों को बाहरी टूल्स, डेटा स्रोतों और प्रणालियों से सुरक्षित रूप से जोड़ने में सक्षम बनाता है। जटिल और कस्टम एकीकरणों के स्थान पर एकीकृत क्लाइंट–सर्वर संरचना प्रदान कर, एमसीपी सुरक्षित, स्केलेबल और सुशासित एआई अंतःक्रियाओं को संभव बनाता है। यह एआई को एक स्वतंत्र भाषा मॉडल से आगे बढ़ाकर एंटरप्राइज और मिशन-क्रिटिकल उपयोग के लिए उपयुक्त, भरोसेमंद और कार्य-उन्मुख प्रणाली में परिवर्तित करता है।



एमसीपी इनका समाधान एक खुले, मानकीकृत एवं संरचित संचार ढाँचे के माध्यम से करता है, जो एआई मॉडलों को बाह्य प्रणालियों के साथ सुरक्षित तथा पारस्परिक रूप से संगत संवाद करने में सक्षम बनाता है। एआई मॉडलों और वास्तविक-विश्व के उपकरणों, डेटा स्रोतों तथा कार्यप्रवाहों के बीच एक सामान्य अंतरफलक के रूप में कार्य करते हुए एमसीपी एड-हॉक एकीकरण की आवश्यकता को समाप्त करता है तथा एआई तर्क-प्रक्रिया और प्रणाली निष्पादन के बीच स्पष्ट विभाजन सुनिश्चित करता है। यह स्थापत्य दृष्टिकोण एआई प्रणालियों को केवल निष्क्रिय भाषा-समझ तक सीमित न रखकर उन्हें विश्वसनीय, क्रिया-उन्मुख अनुप्रयोगों में विकसित होने में सक्षम बनाता है—जो उद्यम-स्तरीय सीमाओं के भीतर रहते हुए विश्वास, सुरक्षा, और गवर्नेंस को बनाए रखते हैं।

मुख्य समस्या

N × M एकीकरण चुनौती

एमसीपी के आने से पहले, एआई प्रणालियों को बाहरी टूल्स और सिस्टम्स से जोड़ना एक बड़ी स्केलेबिलिटी समस्या से जुड़ा था, जिसे N* × M* समस्या कहा जाता है। इसमें

- ***N: एआई मॉडलों की संख्या को दर्शाता है (जैसे जीपीटी, क्लॉड, जेमिनी)**
- ***M: बाहरी टूल्स या डेटा स्रोतों की संख्या को दर्शाता है (जैसे एपीआई, डेटाबेस, सीआरएम, फाइल सिस्टम)**

पारंपरिक मॉडल में प्रत्येक एआई मॉडल के लिए हर बाहरी सिस्टम के साथ अलग कस्टम एकीकरण करना पड़ता था। जैसे-जैसे मॉडलों और टूल्स की संख्या बढ़ती गई, एकीकरण की जटिलता भी तेजी से बढ़ती गई।

उदाहरण के लिए, यदि 3 एआई मॉडल और 5 टूल्स हों, तो 15 अलग-अलग एकीकरण करने पड़ते थे। इससे रखरखाव लागत बढ़ती थी, त्रुटियों की संभावना अधिक होती थी तथा सुरक्षा और गवर्नेंस से जुड़े जोखिम भी उत्पन्न होते थे।

एमसीपी का संरचनात्मक समाधान

मॉडल कॉन्टेक्स्ट प्रोटोकॉल (एमसीपी) इस जटिलता को 1 × M या N × 1 संरचना में परिवर्तित करता है। इसमें बाहरी टूल्स और सिस्टम्स को केवल एक बार एमसीपी के अनुरूप बनाना होता है, जिसके बाद कोई भी एमसीपी-संगत एआई मॉडल उन्हें सुरक्षित रूप से उपयोग कर सकता है। यह दृष्टिकोण एकीकरण को सरल बनाता है, रखरखाव को आसान करता है और सुरक्षा को सुदृढ़ करता है।

एमसीपी क्या है?

एमसीपी एक खुला, मानकीकृत संचार प्रोटोकॉल है, जो एआई मॉडलों को बाह्य प्रणालियों, उपकरणों तथा डेटा स्रोतों के साथ सुरक्षित रूप से संवाद करने में सक्षम बनाता है। जेसन-आरपीसी 2.0 पर आधारित एमसीपी एक सुसंगत क्लाइंट–सर्वर ढाँचा परिभाषित करता है, जिसके माध्यम से एआई अनुप्रयोग नियंत्रित और शासित तरीके से बाह्य क्षमताओं की खोज तथा उनका उपयोग कर सकते हैं।

एमसीपी एआई मॉडलों के लिए उपकरणों, डेटा संसाधनों तथा संरचित प्रॉम्प्ट्स को उपलब्ध कराने का एक एकीकृत माध्यम प्रदान करता है, साथ ही एआई की तर्क-प्रक्रिया और प्रणाली निष्पादन के बीच स्पष्ट विभाजन बनाए रखता है। एआई मॉडल प्रत्यक्ष रूप से किसी अवसंरचना या एपीआई तक पहुँच नहीं बनाते; इसके स्थान पर सभी अंतःक्रियाएँ एमसीपी सर्वरों के माध्यम से संचालित होती हैं, जो प्रत्येक अनुरोध का सत्यापन करते हैं तथा उसे गवर्नेंस ढाँचे के अंतर्गत नियंत्रित करते हैं।

एआई मॉडलों को प्रामाणिक, वास्तविक-समय डेटा तथा नियंत्रित क्रियाओं से जोड़कर एमसीपी अविश्वसनीय अथवा

अनियंत्रित परिणामों को कम करने में सहायक होता है और विश्वसनीय, कार्य-उन्मुख एआई व्यवहार को सक्षम बनाता है। यही कारण है कि एमसीपी उन उद्यम एवं सरकारी परिवेशों के लिए विशेष रूप से उपयुक्त है, जहाँ सुरक्षा, ऑडिट-क्षमता तथा विस्तारशीलता अनिवार्य आवश्यकताएँ होती हैं।

एमसीपी संरचना का अवलोकन

एमसीपी क्लाइंट

एमसीपी क्लाइंट मॉडल कॉन्टेक्स्ट प्रोटोकॉल का एआई-उन्मुख घटक है। इसे सामान्यतः किसी एआई अनुप्रयोग, एजेंट फ्रेमवर्क या एलएलएम रनटाइम में एकीकृत किया जाता है और यह एआई मॉडल तथा बाहरी प्रणालियों के बीच होने वाली अंतःक्रियाओं का प्रबंधन करता है।

मानकीकृत जेसन-आरपीसी 2.0 इंटरफेस का उपयोग करते हुए, एमसीपी क्लाइंट टूल्स तक पहुँचने, डेटा प्राप्त करने या पूर्वनिर्धारित क्रियाओं को निष्पादित करने के लिए एमसीपी सर्वरों को संरचित अनुरोध भेजता है। यह उपलब्ध क्षमताओं की डायनेमिक खोज का समर्थन करता है, जिससे एआई अनुप्रयोग रनटाइम के दौरान बिना हार्ड-कोडेड एकीकरणों पर निर्भर हुए स्वयं को अनुकूलित कर सकता है।

महत्वपूर्ण रूप से, एमसीपी क्लाइंट अवसंरचना या बाहरी एपीआई से सीधे अंतःक्रिया नहीं करता। सभी वास्तविक क्रियाएँ एमसीपी सर्वरों को सौंप दी जाती हैं, जिससे एआई की सोच और निष्पादन के बीच स्पष्ट और कड़ा पृथक्करण सुनिश्चित होता है।

एमसीपी सर्वर

एमसीपी सर्वर एआई मॉडलों और वास्तविक प्रणालियों के बीच एक अधिकृत गेटवे के रूप में कार्य करता है। यह अच्छी तरह परिभाषित और खोज-योग्य क्षमताओं को उजागर करता है, जबकि अंतर्निहित अवसंरचना तक सीधे पहुँच को रोकता है।

एमसीपी सर्वर अनुरोधों का सत्यापन करने, अनुमतियों को लागू करने और एआई मॉडलों द्वारा आरंभ की गई स्वीकृत क्रियाओं को निष्पादित करने के लिए उत्तरदायी होता है। यह एपीआई, डेटाबेस, फाइल सिस्टम, व्यावसायिक लॉजिक और आंतरिक सेवाओं सहित विभिन्न बैकएंड प्रणालियों को समाहित कर सकता है और उन्हें मानकीकृत, एआई-रेडी रूप में प्रस्तुत करता है।

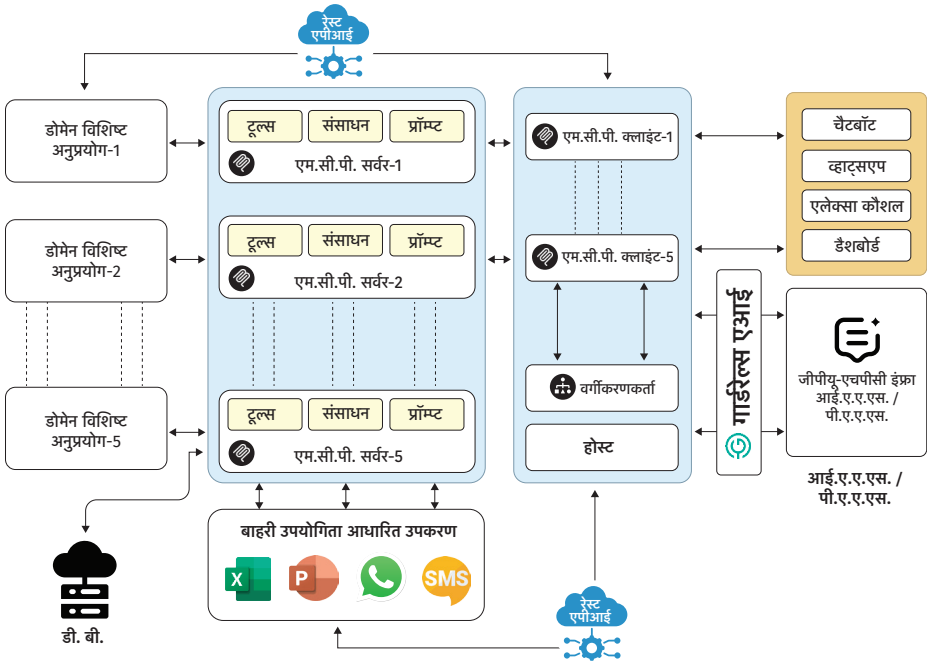
नियंत्रण और निष्पादन को केंद्रीकृत करके, एमसीपी सर्वर संगठनों को मौजूदा संरचनाओं में बिना पुनःडिज़ाइन किए एआई को एकीकृत करने में सक्षम बनाता है, साथ ही मजबूत सुरक्षा, गवर्नेंस और ऑडिटेबिलिटी बनाए रखता है।

संचार परत

संचार परत मॉडल कॉन्टेक्स्ट प्रोटोकॉल की आधारशिला है और यह जेसन-आरपीसी 2.0 पर आधारित है, जो संरचित संचार के लिए एक हल्का और व्यापक रूप से अपनाया गया मानक है।

यह परत एमसीपी क्लाइंट और सर्वर के बीच भाषा-निरपेक्ष तरीके से विश्वसनीय, द्विदिश संचार को सक्षम बनाती है, जिससे विभिन्न प्लेटफॉर्म्स और प्रोग्रामिंग परिवेशों में कार्यान्वयन संभव हो पाता है। इसमें टूल्स, संसाधनों और प्रॉम्प्ट्स के लिए केवल एब्स्ट्रैक्शन प्रदान की गई हैं, जिससे सरलता और शीघ्र अपनाने की सुविधा मिलती है।

अपने मानकीकृत और विस्तारयोग्य डिज़ाइन के माध्यम से, संचार परत एआई–सिस्टम अंतःक्रियाओं के लिए इंटरऑपरेबिलिटी, स्केलेबिलिटी और दीर्घकालिक स्थिरता सुनिश्चित करती है।



▲ चित्र 11.1 एम.सी.पी. आर्किटेक्चर अवलोकन

एमसीपी में सुरक्षा और गवर्नेंस

एमसीपी में सुरक्षा एक मूल सिद्धांत है। इसके प्रमुख प्रावधान हैं:

- भूमिका-आधारित अभिगम नियंत्रण
- क्षमता-आधारित सीमांकन
- एलएलएम द्वारा सीधे सिस्टम एक्सेस का अभाव
- सर्वर-साइड सत्यापन
- ऑडिट योग्य निष्पादन

एमसीपी का भविष्य

एमसीपी अगली पीढ़ी की एआई प्रणालियों के लिए एक मौलिक अवसंरचनात्मक स्तर के रूप में उभर रहा है, जो ऐसे स्वायत्त एआई एजेंटों के विकास को सक्षम बनाता है, जो बहु-चरणीय कार्यों की योजना बना सकते हैं, तर्क कर सकते हैं तथा उनका निष्पादन कर सकते हैं। बाह्य उपकरणों और प्रणालियों के साथ संवाद हेतु एक मानकीकृत एवं शासित अंतरफलक प्रदान करके एमसीपी एआई मॉडलों को पृथक प्रॉम्प्ट्स तक सीमित रहने के बजाय वास्तविक-विश्व परिवेशों में विश्वसनीय रूप से कार्य करने में सक्षम बनाता है।

एमसीपी सुदृढ़ बहु-चरणीय तर्क-प्रणालियों को भी समर्थ बनाता है, जिसके अंतर्गत एआई प्रणालियाँ डेटा, उपकरणों तथा कार्यप्रवाहों के साथ क्रमिक रूप से अंतःक्रिया कर सकती हैं, जबकि तर्क-प्रक्रिया और निष्पादन के बीच कठोर विभाजन बनाए रखा जाता है। यह संरचित दृष्टिकोण प्रामाणिक डेटा तक नियंत्रित अभिगम सुनिश्चित करता है तथा प्रणाली के व्यवहार को पूर्वानुमेय बनाता है।

उद्यम स्तर पर, एमसीपी विस्तारशील, सुरक्षित एवं पारस्परिक रूप से संगत एआई प्लेटफॉर्मों के लिए एक प्रमुख आधारभूत घटक के रूप में कार्य करता है। विखंडित एकीकरणों के स्थान पर एकीकृत प्रोटोकॉल को अपनाकर यह संगठनों को गवर्नेंस या अनुपालन से समझौता किए बिना विभिन्न प्रणालियों और आपूर्तिकर्ताओं के पार एआई के परिनियोजन में सक्षम बनाता है। जैसे-जैसे एआई संवादात्मक चैटबॉट्स से क्रिया-उन्मुख "डू-बॉट्स" की ओर विकसित हो रहा है, एमसीपी बुद्धिमत्ता और निष्पादन को सुरक्षित रूप से जोड़ने हेतु आवश्यक अवसंरचना प्रदान करता है—जिससे एआई वास्तविक-विश्व कार्यप्रवाहों में एक विश्वसनीय एवं क्रिया-सक्षम सहभागी के रूप में परिवर्तित हो जाता है।

निष्कर्ष

एमसीपी इस बात में एक निर्णायक परिवर्तन का प्रतिनिधित्व करता है कि कृत्रिम बुद्धिमत्ता प्रणालियाँ वास्तविक-विश्व के साथ किस प्रकार अंतःक्रिया करती हैं। एकीकरण की जटिलता, सुरक्षा गवर्नेंस तथा विस्तारशीलता से संबंधित दीर्घकालिक चुनौतियों का समाधान करके एमसीपी उस आधारभूत अवसंरचना की स्थापना करता है, जो पृथक भाषा मॉडलों से आगे बढ़ने के लिए आवश्यक है।

एमसीपी एआई को केवल अंतर्दृष्टि प्रदान करने वाले निष्क्रिय साधन से उठाकर एक सुरक्षित, विश्वसनीय एवं क्रिया-सक्षम एजेंट के रूप में विकसित करता है, जो सुव्यवस्थित नियंत्रणों के अंतर्गत सक्रिय प्रणालियों, डेटा तथा कार्यप्रवाहों के साथ अंतःक्रिया करने में सक्षम होता है। जैसे-जैसे एआई का अंगीकरण मिशन-क्रिटिकल क्षेत्रों में विस्तारित हो रहा है, एमसीपी एक प्रमुख सक्षम मानक के रूप में उभरता है—जो बुद्धिमत्ता को विश्वास, सटीकता और वास्तविक-विश्व प्रभाव के साथ कार्य करने की क्षमता प्रदान करता है।

अधिक जानकारी के लिए संपर्क करें

राज्य सूचना विज्ञान अधिकारी
एनआईसी ओडिशा राज्य केंद्र
यूनिट-IV, सचिवालय मार्ग
भुवनेश्वर, ओडिशा-751001
ईमेल: sio-ori@nic.in