



ابوالفضل توکلیان

دانشجوی مهندسی کامپیوتر

دانشکده فارابی دانشگاه تهران

abolfazl.tavakolian57@gmail.com



جنگ در لایه رابط‌های برنامه‌نویسی (API): کالبدشکافی معماری نرم‌افزاری هوش مصنوعی در سیستم‌های رزمی

۱۱ دقیقه

چگونه یک مدل زبانی به موتور تصمیم‌گیری میدان نبرد تبدیل می‌شود؟

وقتی صحبت از درگیری‌های نظامی نوین و ورود هوش مصنوعی‌های پیشرفته مانند کلود (Claude) به میدان نبرد می‌شود، رسانه‌های عمومی معمولاً روی مفاهیمی مثل «سلاح‌های خودمختار» و «اخلاق» تمرکز می‌کنند. اما برای یک مهندس نرم‌افزار، سوال اصلی این است: یک مدل زبانی بزرگ (LLM) که اساساً برای پیش‌بینی کلمه بعدی آموزش دیده، چگونه می‌تواند ۱۳ هزار هدف نظامی را در یک سیستم پیچیده مانند پلتفرم پالتیر (Palantir) شناسایی و اولویت‌بندی کند؟

پاسخ این سوال در رابط‌های کاربری گرافیکی چت‌بات‌ها نیست؛ بلکه در اعماق معماری میکروسرویس‌ها، خطوط لوله داده (Data Pipelines) و فراخوانی‌های ساختاریافته وب‌سرویس‌ها نهفته است. در این مقاله، معماری نرم‌افزاری پشت این پدیده را از منظر مهندسی سیستم‌ها بررسی می‌کنیم.

۱. از سنسور تا سرور: خط لوله داده‌های چندوجهی

در یک سناریوی عملیاتی واقعی، هوش مصنوعی کلود مستقیماً به دوربین یک پهپاد متصل نیست. معماری سیستم‌های فرماندهی نوین بر اساس هم‌جوشی داده‌ها (Data Fusion) کار می‌کند. جریان پردازش اطلاعات به این شکل است:

لایه پردازش لبه (Edge Computing): سنسورها شامل تصاویر ماهواره‌ای، شنود رادیویی و رادارهای خام را جمع‌آوری می‌کنند. شبکه‌های عصبی پیچشی (CNN) که به صورت محلی روی خود پهپادها نصب شده‌اند، اشیای اولیه را تشخیص داده و ویدیوهای سنگین را به متادیتا (Metadata) تبدیل می‌کنند تا در پهنای باند شبکه صرفه‌جویی شود.

لایه تجمیع و پایگاه‌های داده برداری (Vector DBs): این متادیتاها در کنار داده‌های متنی (مثل گزارش‌های اطلاعاتی شنود شده) به بردارهای عددی (Embeddings) تبدیل شده و در دیتابیس‌های برداری ذخیره می‌شوند.

لایه ارکستراسیون (Orchestration): اینجا جایی است که سیستم یکپارچه‌ساز وارد عمل می‌شود و با استفاده از معماری تولید افزوده با بازیابی (RAG)، داده‌های مرتبط را فیلتر کرده و برای تغذیه به مغز متفکر سیستم آماده می‌کند.

۲. کلود در نقش موتور استدلال: آناتومی یک درخواست API

در این معماری، کلود به عنوان یک «موتور استدلال» (Reasoning Engine) عمل می‌کند. سیستم نظامی یک درخواست از طریق API به سرورهای کلود می‌فرستد. این درخواست یک متن ساده نیست، بلکه یک بسته داده ساختاریافته (JSON) است که به شدت مهندسی پرامپت (Prompt Engineering) روی آن اعمال شده است.

ماژول مسیریابی لجستیک.

ماژول ارزیابی خسارت پس از حمله.

جایگزینی یک مدل پایه با مدل شرکتی دیگر، نیازمند بازنویسی هزاران خط کد، تغییر ساختار پرامپت‌ها و ماه‌ها تست رگرسیون (Regression Testing) برای جلوگیری از خطاهای مرگبار است. غیرفعال کردن ناگهانی API در میان یک عملیات، عملاً به معنای فلج کردن کل سیستم یکپارچه فرماندهی است.

۴. سوگیری اتوماسیون و باگ‌های مرگبار

از منظر علوم کامپیوتر، پدیده‌ای به نام «توهم» (Hallucination) در مدل‌های زبانی غیرقابل اجتناب است؛ زیرا آن‌ها سیستم‌های قطعی و ریاضی‌وار نیستند، بلکه مبتنی بر احتمالات کار می‌کنند.

هنگامی که سیستمی روزانه هزاران درخواست اطلاعاتی را پردازش کرده و اهداف را پیشنهاد می‌کند، رابط کاربری طوری طراحی می‌شود که انسان تصمیم‌گیرنده نهایی باشد (حلقه نظارت انسانی). اما از نظر روانشناسی تعامل انسان و کامپیوتر (HCI)، وقتی یک نرم‌افزار ۹۹ بار خروجی درست می‌دهد، اپراتور دچار سوگیری اتوماسیون (Automation Bias) شده و برای صدمین بار دیگر داده‌ها را بررسی نمی‌کند و صرفاً دکمه تایید را می‌فشارد.

همین مسئله فنی، ریشه خطاهای فاجعه‌بار در هدف‌گیری‌ها است. مقصر اصلی در این سناریوها نه هوش مصنوعی است و نه اپراتور؛ بلکه مقصر، مشکل همگام‌سازی پایگاه داده با واقعیت پویای میدان نبرد و اتکای بیش از حد به خروجی‌های احتمالی است.

نتیجه‌گیری: ورود هوش مصنوعی به سیستم‌های نظامی، ماهیت نبرد را به یک «عملیات پیچیده مهندسی نرم‌افزار در مقیاس کلان» تغییر داده است. امروزه، پایداری زیرساخت‌های ابری، سرعت پاسخ‌دهی سرورها و معماری بدون نقص میکروسرویس‌ها، به اندازه کیفیت تجهیزات فیزیکی، تعیین‌کننده نتیجه عملیات‌ها هستند.

نمونه‌ای ساده‌سازی‌شده از داده‌های ارسالی به API کلود:

```
[POST /v1/messages]

{
  "model": "claude-3-opus-military-grade",
  "system_prompt": "You are a CENTCOM intel analysis engine. Analyze sensor metadata against RoE and IHL. Output must be strictly formatted as a structured JSON.",
  "messages": [
    {
      "role": "user",
      "content": "Sensor data received from X-72:\n
      - Object: Concrete structure, 2000 sqm\n
      - Thermal signature: High (indicates servers/heavy)\n
      - Verified plates history: IRGC linked (87% match)\n
      - Distance to nearest civilian center: 1.2 km\n
      Evaluate military target probability and calculate Collateral Damage Estimation (CDE) metrics."
    }
  ]
}
```

کلود این داده‌ها را پردازش کرده و پاسخی برمی‌گرداند (مثلاً درصد اطمینان ۹۲ درصد برای هدف نظامی). این خروجی، توسط سیستم رابط کاربری روی داشبورد فرمانده انسانی به عنوان یک «پیشنهاد شلیک» ظاهر می‌شود. این چرخه که پیش‌تر توسط تیم‌های انسانی روزها طول می‌کشید، حالا در سطح سرور در چند میلی‌ثانیه انجام می‌شود.

۳. پارادوکس عملیاتی: چرا ارتش نمی‌تواند هوش مصنوعی را خاموش کند؟

یکی از جذاب‌ترین پدیده‌های مهندسی نرم‌افزار در مناقشات میان شرکت‌های فناوری و دولت‌ها، مسئله بدهی فنی و وابستگی عمیق در میکروسرویس‌ها است.

وقتی دستور توقف استفاده از یک هوش مصنوعی خاص صادر می‌شود، فرماندهان در میدان نبرد نمی‌توانند آن را فوراً اجرا کنند. در یک معماری مدرن نرم‌افزاری، هوش مصنوعی یک افزونه ساده نیست که با یک دکمه خاموش شود. فراخوانی‌های API در صدها میکروسرویس مختلف تنیده شده‌اند:

ماژول ترجمه همزمان بی‌سیم‌ها.