APJ 7(2):43-50, Summer 2026

Arman Process Journal (APJ)

Arman Process Journal (APJ)

Homepage: https://www.armanprocessjournal.ir

Investigating the Advantages, Disadvantages, and Applications of Common AI Tools in the Field of Information and Communication Technology

A. Soleimani [1*]

[1] Department of Computer Engineering, ShQ.C., Islamic Azad University, Shahr-e Qods, Iran

RESEARCH PAPER

Received: 2026-2-29
Accepted: 2026-7-1

KEYWORDS:
Generative AI,
Large Language Model,
AIOps,
Cybersecurity,
Information and Communication Technology

Corresponding author:
soleimani400@iau.ac.ir

ABSTRACT

The rapid proliferation of generative AI models, large language models, coding assistants, AIOps systems, and intelligent cybersecurity tools has transformed ICT architectures and processes. This research aims to provide a technical and analytical examination of the benefits, drawbacks, risks, and applications of prevalent AI tools across the ICT system lifecycle. Adopting a review-analytical approach grounded in authoritative literature, the study first categorizes these tools into domains such as natural language processing, software engineering, data analysis, networking, cloud computing, IT operations, and cybersecurity. It then compares them based on criteria including accuracy, productivity, security, privacy, cost, scalability, integration capabilities, and the need for human oversight. The results indicate that the value of AI in ICT lies less in mere response generation and more in its capacity to analyze vast datasets, automate repetitive tasks, support decision-making, and establish intelligent feedback loops connecting data, software, and infrastructure. Conversely, challenges such as model hallucinations, the generation of vulnerable code, data leakage, prompt injection attacks, vendor lock-in, and decision-making errors constitute significant barriers to widespread adoption. Finally, the study proposes a multi-criteria framework for AI tool selection and a five-level maturity model for organizational deployment. The key finding is that for critical applications, a "human-in-the-loop" architecture, data governance, access control, continuous model evaluation, and an enterprise AI gateway must be integral architectural requirements.

Copyright © Author(s).

نشریه تخصصی آرمان پردازش، دوره ۷، شماره ۲، تابستان ۱۴۰۵

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

فصلنامه تخصصی فناوری اطلاعات و ارتباطات
شماره مجوز: ۸۷۰۹۰

بررسی مزایا، معایب و کاربردهای ابزارهای هوش مصنوعی رایج در حوزه فناوری اطلاعات و ارتباطات

علیرضا سلیمانی[۱]

۱ گروه مهندسی کامپیوتر، واحد شهر قدس، دانشگاه آزاد اسلامی، شهرقدس، ایران

چکیده

مقاله پژوهشی

واژگان کلیدی:
هوش مصنوعی مولد،
مدل زبانی بزرگ،
AIOps،
امنیت سایبری،
فناوری اطلاعات و ارتباطات

گسترش سریع مدل‌های هوش مصنوعی مولد، مدل‌های زبانی بزرگ، دستیارهای برنامه‌نویسی، سامانه‌های AIOps و ابزارهای هوشمند امنیت سایبری، معماری و فرایندهای فناوری اطلاعات و ارتباطات را دستخوش تغییر کرده است .هدف این پژوهش، بررسی فنی و تحلیلی مزایا، معایب، ریسک‌ها و کاربردهای ابزارهای رایج هوش مصنوعی در چرخه حیات سامانه‌های فناوری اطلاعات و ارتباطات است .پژوهش حاضر با رویکرد مروری ـ تحلیلی و با اتکا بر ادبیات علمی معتبر، ابتدا ابزارها را در حوزه‌های پردازش زبان طبیعی، مهندسی نرم‌افزار، تحلیل داده، شبکه، رایانش ابری، عملیات فناوری اطلاعات و امنیت سایبری طبقه‌بندی می‌کند و سپس آنها را بر اساس معیارهای دقت، بهره‌وری، امنیت، حریم خصوصی، هزینه، مقیاس‌پذیری، قابلیت یکپارچه‌سازی و نیاز به نظارت انسانی مقایسه می‌کند .نتایج نشان می‌دهد که ارزش AI در ICT بیش از آنکه به تولید پاسخ وابسته باشد، به توانایی آن در تحلیل حجم زیاد داده، خودکارسازی وظایف تکراری، پشتیبانی از تصمیم‌گیری و ایجاد حلقه‌های هوشمند میان داده، نرم‌افزار و زیرساخت وابسته است .در مقابل، توهم مدل، تولید کد آسیب‌پذیر، افشای داده، حملات Prompt Injection ، وابستگی به ارائه‌دهنده و خطاهای تصمیم‌گیری از مهم‌ترین موانع استقرار گسترده محسوب می‌شوند .در پایان، یک چارچوب چندمعیاره برای انتخاب ابزار AI و یک مدل بلوغ پنج‌سطحی برای استقرار سازمانی پیشنهاد می‌شود .یافته اصلی آن است که در کاربردهای حساس، معماری Human-in-the-Loop، حاکمیت داده، کنترل دسترسی، ارزیابی مستمر مدل و دروازه هوش مصنوعی سازمانی باید جزء الزامات معماری باشند.

۱ - مقدمه

هوش مصنوعی در سال‌های اخیر از یک فناوری عمدتاً پژوهشی به یک مؤلفه عملیاتی در سامانه‌های فناوری اطلاعات و ارتباطات تبدیل شده است .ظهور مدل‌های بنیادی و مدل‌های زبانی بزرگ امکان انجام وظایفی مانند تولید متن، خلاصه‌سازی، ترجمه، تحلیل اسناد، تولید کد و تعامل طبیعی با سامانه‌های نرم‌افزاری را فراهم کرده است [۱]. معماری Transformer نیز با معرفی سازوکار توجه، زیرساخت بسیاری از مدل‌های زبانی و چندوجهی جدید را فراهم کرد [۲].

درICT ، اهمیت AI صرفاً به چت‌بات‌ها محدود نیست .در مهندسی نرم‌افزار، مدل‌های آموزش‌دیده روی کد می‌توانند دستور زبان طبیعی را به برنامه تبدیل کنند [۳]. در عملیات فناوری اطلاعات، AIOps داده‌های لاگ، متریک، رخداد و ترافیک را برای تشخیص ناهنجاری و تحلیل علت ریشه‌ای ترکیب می‌کند [۴-۵]. در حوزه امنیت سایبری نیز AI برای تشخیص فیشینگ، تحلیل تهدید، اولویت‌بندی هشدارها و کمک به پاسخ‌گویی به رخداد به کار می‌رود [۶].

با وجود این مزایا، افزایش خودکارسازی با افزایش دامنه اثر خطا همراه است [۷]. خروجی یک مدل زبانی ممکن است از نظر زبانی قانع‌کننده اما از نظر واقعیت نادرست باشد؛ کد تولیدی ممکن است اجرا شود اما آسیب‌پذیر باشد؛ و یک عامل هوشمند ممکن است در صورت دسترسی بیش از حد، اقدامی ناخواسته انجام دهد [۸]. بنابراین مسئله اصلی پژوهش حاضر، تعیین جایگاه مناسب ابزارهای AI در معماری ICT و ایجاد توازن میان بهره‌وری و ریسک است.

پرسش اصلی پژوهش این است که ابزارهای رایج هوش مصنوعی در کدام حوزه‌های ICT بیشترین ارزش را ایجاد می‌کنند و تحت چه شرایطی معایب و ریسک‌های آنها می‌تواند بر مزایا غلبه کند؟ پرسش فرعی نیز آن است که سازمان چگونه باید ابزار مناسب را بر اساس یک معیار فنی و چندبعدی انتخاب و استقرار دهد؟

۲ - روش پژوهش

این پژوهش از نوع مروری ـ تحلیلی است .منابع علمی منتخب در حوزه مدل‌های بنیادی،LLM ، تولید کد، امنیتLLM، AIOps ، تشخیص فیشینگ، رایانش ابری و هوش مصنوعی در عملیات ICT بررسی شده‌اند .معیار تحلیل شامل هشت بعد است :دقت و کیفیت خروجی، بهره‌وری، امنیت، حریم خصوصی، هزینه، عملکرد، قابلیت یکپارچه‌سازی و سطح نیاز به نظارت انسانی .به منظور جلوگیری از رتبه‌بندی مطلق ابزارها، تحلیل بر مبنای سناریوی کاربرد انجام شده است. برای تصمیم‌گیری چندمعیاره، امتیاز کلی ابزار به صورت رابطه (1)تعریف می‌شود$Score = \Sigma(w_i\ S_i)$:. که در آن S_i امتیاز ابزار در معیار i و w_i وزن معیار است و .$\Sigma w_i=1$ در کاربردهای حساس امنیتی، وزن امنیت و حریم خصوصی باید نسبت به هزینه افزایش یابد .این مدل، چارچوبی عمومی برای مقایسه ابزارها بدون وابستگی به یک فروشنده خاص ارائه می‌کند.

۳ - تحقیقات مرتبط

Vaswaniو همکاران معماری Transformer را معرفی کردند که با استفاده از توجه خودکار، پردازش توالی را متحول ساخت [۱]. Brownو همکاران نشان دادند که افزایش مقیاس GPT-3 قابلیت انجام وظایف متنوع را با نمونه‌های اندک افزایش می‌دهد [۲]. Bommasaniو همکاران نیز مفهوم مدل‌های بنیادی را تبیین کردند و نشان دادند که یک مدل پایه می‌تواند مبنای طیف وسیعی از کاربردهای پایین‌دستی باشد [۳].

در حوزه LLM ، Zhao و همکاران مروری جامع بر معماری، آموزش و سازگارسازی مدل‌های زبانی بزرگ ارائه کردند [۴]. OpenAI نیز در گزارش فنی GPT-4 بر قابلیت‌های استدلالی و چندوجهی مدل های نسل جدید تأکید کرده است [۵]. این مطالعات مبنای نظری تحلیل ابزارهای عمومی AI در پژوهش حاضر را شکل می‌دهند.

در مهندسی نرم‌افزار، Chen و همکاران Codex را به عنوان مدلی برای تبدیل زبان طبیعی به کد معرفی کردند [۶]. مطالعات تجربی درباره ChatGPT نیز نشان داده‌اند که خروجی کد می‌تواند مفید باشد، اما صحت و کیفیت آن به نوع مسئله و سطح نظارت وابسته است [۱۲]. مرور نظام‌مند امنیت کد تولیدشده توسط LLM ها نیز نشان می‌دهد که استفاده از کد AI بدون آزمون و بازبینی می‌تواند آسیب‌پذیری ایجاد کند [۱۳].

در زمینه امنیت، Ferrag و همکاران کاربردهای LLM و GenAI در امنیت سایبری و آسیب‌پذیری‌های آنها را بررسی کرده‌اند [۸]. مطالعات امنیت LLM نیز تهدیدهایی مانندPrompt Injection ، نشت داده، مسموم‌سازی و سوءاستفاده از مدل را برجسته کرده‌اند [۹-۱۱] در تشخیص فیشینگ نیز پژوهش‌های مروری نشان می‌دهند که مدل‌های AI قابلیت مناسبی دارند، اما تغییر سریع الگوهای حمله، تعمیم‌پذیری را دشوار می‌کند [۱۴].

در حوزه رایانش ابری، پژوهش‌های Fareghzadeh و همکاران بر مدیریت عملکرد، جداسازی عملکرد و معماری پایش در محیط‌های ابری تمرکز داشته‌اند . [۱۵-۱۷] مطالعات دیگر نیز برای تحلیل زیرساخت AI اهمیت دارند، زیرا بارهای کاری هوش مصنوعی به منابع محاسباتی و شبکه‌ای حساس بوده و هم‌زمانی آنها می‌تواند موجب رقابت منابع و افت کیفیت خدمت شود.

درAIOps ، پژوهش‌های جدید حرکت از پایش واکنشی به تحلیل هوشمند، تشخیص علت ریشه‌ای و استفاده ازLLM ها برای تفسیر داده‌های عملیاتی را بررسی کرده‌اند [۱۸-۲۰]. این روند نشان می دهد که AI در حال تبدیل‌شدن از یک ابزار تحلیل به یک لایه تصمیم یار برای عملیات فناوری اطلاعات است.

جدول ۱. دسته‌بندی ابزارهای هوش مصنوعی در ICT

گروه ابزار	نمونه کاربرد	داده ورودی	خروجی
مدل‌های زبانی و مولد	گفت‌وگو، تحلیل سند، تولید محتوا	متن، تصویر، فایل	متن/تحلیل
دستیار برنامه‌نویسی	تولید، تکمیل و بازبینی کد	کد و نیازمندی	کد/تست
تحلیل داده وBI	پیش‌بینی و کشف ناهنجاری	داده ساختاریافته	پیش‌بینی/بینش
AIOps	پایش وRCA	لاگ، متریک،Trace	هشدار/علت احتمالی
امنیت سایبری	تشخیص تهدید و فیشینگ	ترافیک، لاگ،IOC	امتیاز ریسک
Cloud AI	تخصیص و مقیاس‌دهی منابع	متریک زیرساخت	سیاست منابع
Agent	برنامه‌ریزی و اجرای اقدام	هدف + ابزار	اقدام/گزارش

۴ . بررسی فنی ابزارهای مبتنی بر مدل‌های زبانی بزرگ

مدل زبانی بزرگ را می‌توان تابعی احتمالی در نظر گرفت که بر اساس توالی ورودی، توکن بعدی را پیش‌بینی می‌کند .در سطح سامانه، این قابلیت با لایه‌های بازیابی، ابزار و سیاست ترکیب می‌شود .معماری ساده به صورت User→Prompt→LLM→Response است، در حالی که معماری سازمانی بهتر است User→IAM→AI Gateway→RAG/Tools→LLM→Output Filter→User باشد [۲۱-۲۴].

RAGیکی از مهم‌ترین روش‌ها برای استفاده از دانش سازمانی است . در این روش، ابتدا اسناد مرتبط بازیابی و سپس همراه پرسش به مدل داده می‌شوند .به‌صورت مفهومی Answer = LLM(Query + Retrieved Context)است .مزیت اصلی، کاهش اتکا به حافظه ثابت مدل و امکان به‌روزرسانی دانش است؛ با این حال، کیفیت پاسخ همچنان به کیفیت بازیابی و مقاومت سامانه در برابر محتوای مخرب وابسته است [۲۵].

کاربرد در مهندسی نرم‌افزار

چرخه توسعه نرم‌افزار از تحلیل نیازمندی تا نگهداری می‌تواند با AI تقویت شود .در تحلیل نیازمندی، مدل می‌تواند ابهام‌ها و نیازهای استخراج‌نشده را شناسایی کند؛ در طراحی، گزینه‌های معماری پیشنهاد دهد؛ در کدنویسی، قطعات تکراری را تولید کند؛ و در آزمون، Test Caseبسازد [۲۶].

فرآیند ایمن پیشنهادی عبارت است از : Requirement→AI Code Generation→Static Analysis→Unit Test→Security Test→Human Review. این زنجیره اهمیت زیادی دارد، زیرا اجرای مستقیم کد تولیدشده می‌تواند آسیب‌پذیری یا خطای منطقی را وارد محصول کند [۲۷].

در Code Review ، AI می‌تواند الگوهای نامناسب، پیچیدگی، نقص مستندات و برخی آسیب‌پذیری‌ها را برجسته کند .با این حال، نتیجه باید به عنوان پیشنهاد تلقی شود؛ زیرا تشخیص کامل معنا و منطق کسب‌وکار همچنان به تخصص انسانی وابسته است [۱۱-۱۳].

کاربرد در تحلیل داده و تصمیم‌گیری

AIبا تبدیل داده خام به الگو و پیش‌بینی می‌تواند تحلیل داده را تسریع کند .زنجیره کلی Data→Preprocessing→Feature Extraction→Model→Prediction→Decisionاست .

کاربردها شامل طبقه‌بندی، خوشه‌بندی، کشف ناهنجاری، پیش‌بینی سری زمانی و تحلیل رفتار کاربران است.

در سازمان‌ها، ترکیب لاگ، داده شبکه، هویت کاربر و اطلاعات نرم افزار می‌تواند دیدی چندمنبعی ایجاد کند .با این حال، همبستگی آماری الزاماً به معنای رابطه علّی نیست و تصمیم‌های حساس نباید تنها بر اساس یک مدل آماری اتخاذ شوند.

کاربرد در شبکه وAIOps

در مدیریت سنتی شبکه، خرابی پس از وقوع شناسایی و توسط متخصص بررسی می‌شود AIOps .تلاش می‌کند این فرایند را به Monitoring→Correlation→Prediction→Preventive Actionتبدیل کند [۲۸]. داده‌های SNMP، Syslog، NetFlow ، متریک‌های CPU و حافظه، زمان پاسخ سرویس و رخدادهای امنیتی می‌توانند به عنوان ورودی استفاده شوند.

تحلیل علت ریشه‌ای یا RCA یکی از کاربردهای مهم است .در سامانه توزیع‌شده، Root Cause→Service Degradation→Secondary Failures→Alertsرخ می‌دهد؛ بنابراین آخرین هشدار لزوماً علت واقعی نیست AI .باید روابط زمانی، توپولوژی و وابستگی سرویس‌ها را ترکیب کند [۲۹].

در شبکه‌های ارتباطی، AI می‌تواند در سه سطح پایش، پیش‌بینی و کنترل عمل کند .سطح کنترل بیشترین ریسک را دارد، زیرا خروجی

مدل می‌تواند مستقیماً بر پیکربندی شبکه اثر بگذارد .در مرحله استقرار اولیه، حالت Human Approval مناسب‌تر است.

کاربرد در رایانش ابری

AIو Cloud رابطه‌ای دوطرفه دارند Cloud :زیرساخت اجرای مدل است و AI می‌تواند مدیریت منابع ابری را بهینه کند .بارهای کاری مدل‌های بزرگ معمولاً بهCPU، GPU ، حافظه و شبکه قابل‌توجه نیاز دارند .از این رو، مدیریت پویا،Auto Scaling ، زمان‌بندی و کنترل SLA اهمیت پیدا می‌کند [۳۰].

Fareghzadehو همکاران بر ضرورت مدیریت و پایش عملکرد در محیط‌های ابری و توجه هم‌زمان به چند بعد عملکردی تأکید کرده اند . این دیدگاه برای استقرار AI اهمیت دارد، زیرا رقابت میان بارهای کاری می‌تواند باعث افت عملکرد و افزایش هزینه شود.

کاربرد در امنیت سایبری

AIمی‌تواند در SOC برای تحلیل لاگ، همبستگی هشدارها، استخراج شاخص‌های سازش، خلاصه‌سازی رخداد و اولویت‌بندی تهدیدها به کار رود .معماری مفهومی Logs+Traffic+Alerts→AI Analysis→Threat Correlation→Risk Scoring→Responseاست.

با این حال، AI ماهیتی دوگانه دارد .از یک سو توان تحلیل حجم بالای داده را افزایش می‌دهد و از سوی دیگر خود هدف حمله است . Prompt Injection،Data Leakage ، Poisoning و Adversarial Inputsاز مهم‌ترین تهدیدها هستند .بنابراین Human-in-the-Loopبرای رخدادهای حساس توصیه می‌شود.

در تشخیص فیشینگ، مدل می‌تواندURL ، دامنه، محتوای پیام، فرستنده و ویژگی‌های زمانی را ترکیب کند .تغییر سریع تاکتیک مهاجم باعث می‌شود مدل‌های ثابت نیازمند به‌روزرسانی و پایش مستمر باشند.

جدول ۲. تحلیل مزایا و معایب

حوزه	مزیت	عیب/ریسک	سطح نظارت
تولید متن	سرعت و مقیاس	توهم و خطای واقعیت	متوسط
کدنویسی	افزایش بهره‌وری	کد ناامن/منسوخ	بسیار زیاد
تحلیل داده	کشف الگو	سوگیری داده	زیاد
AIOps	تشخیص سریع	RCAنادرست	بسیار زیاد
امنیت	تحلیل داده حجیم	False Positive/Negative	بسیار زیاد
Cloud	بهینه‌سازی منابع	پیچیدگی و هزینه	زیاد
Agent	اتوماسیون	اقدام ناخواسته	بسیار زیاد

لازم به ذکر است، در کاربرد سازمانی، مسیر داده باید از زمان ورود تا حذف مشخص باشد : Data→Encryption→API→Processing→Storage→Rete ntion.سازمان باید بداند داده کجا پردازش می‌شود، چه مدت نگهداری می‌شود، چه کسانی دسترسی دارند و آیا برای آموزش مدل استفاده می‌شود .داده‌های محرمانه نباید بدون سیاست کنترل‌شده به سرویس عمومی ارسال شوند.

در معماری امن، IAM برای احراز هویت و مجوز، AI Gateway برای اعمال سیاست، DLP برای جلوگیری از نشت داده و Logging برای ممیزی به کار می‌روند .جداسازی دستور سیستم، دستور کاربر و محتوای بازیابی‌شده نیز در برابر Prompt Injection اهمیت دارد .

۵ - چارچوب پیشنهادی انتخاب ابزار AI

معماری پیشنهادی برای Agent سازمانی عبارت است از User→Policy Engine→Agent Planner→Tool Gateway→Execution Sandbox→Verification→Human Approval.چنین معماری‌ای دامنه اثر یک تصمیم اشتباه را محدود می‌کند. شکل ۱. چارچوب پیشنهادی و ابعاد آن را نمایش می‌دهد:



شکل ۱. چارچوب پیشنهادی چندمعیاره برای انتخاب، استقرار و پایش ابزارهایAI

شکل بالا چارچوب پیشنهادی انتخاب ابزارهای هوش مصنوعی را در قالب یک فرایند چرخه‌ای و چندمرحله‌ای نشان می‌دهد. در مرحله نخست، نیاز سازمان، اهداف کاربردی، فرایندهای موردنظر و الزامات فنی و غیرعملیاتی مشخص می‌شوند. سپس ابزارها بر اساس معیارهایی شامل دقت و کیفیت خروجی، بهره‌وری، امنیت، حریم خصوصی، هزینه، عملکرد، مقیاس‌پذیری، قابلیت یکپارچه‌سازی و میزان نیاز به نظارت انسانی ارزیابی می‌شوند. در مرحله بعد، ابزارهای متناسب با سناریوی کاربرد، از میان گروه‌هایی مانند مدل‌های زبانی بزرگ، دستیارهای تولید کد، تحلیل داده وAIOps ، امنیت سایبری، رایانش ابری و ابزارهای تخصصی انتخاب می‌شوند. امتیازدهی چندمعیاره امکان مقایسه نظام‌مند گزینه‌ها را فراهم کرده و پس از انتخاب، ابزار باید در معماری سازمانی مناسب و همراه با کنترل‌های امنیتی، سیاست‌های دسترسی، نظارت انسانی و سازوکارهای اعتبارسنجی مستقر شود. در نهایت، پایش مستمر عملکرد و امنیت، ارزیابی دوره‌ای، به‌روزرسانی مدل و مدیریت ریسک، بازخورد لازم را برای اصلاح تصمیم انتخاب و بهبود مستمر فراهم می‌کند. این رویکرد از انتخاب ابزار صرفاً بر مبنای شهرت یا قابلیت‌های عمومی آن جلوگیری کرده و انتخاب AI را به یک فرایند مبتنی بر سناریو، معیارهای فنی و الزامات حاکمیتی تبدیل می‌کند.

انتخاب ابزار باید چندمعیاره باشد .معیارهای پیشنهادی عبارت‌اند از دقت، امنیت، حریم خصوصی، هزینه، سرعت، مقیاس‌پذیری، قابلیت یکپارچه‌سازی و قابلیت اعتماد .امتیاز کلی به صورت $Score=\Sigma(w_iS_i)$محاسبه می‌شود .در سازمان امنیت‌محور، w_Security وw_Privacy باید بزرگ‌تر از w_Cost باشند. جدول زیر مدل بلوغ مرتبط با چارچوب پیشنهادی را نمایش می دهد:

جدول ۳. مدل بلوغ پارچوب پیشنهادی

سناریو	معیار غالب	مدل مناسب	کنترل کلیدی	سطح خودکارسازی
دانشگاه	هزینه/سهولت/حریم خصوصی	مدل عمومی یا سازمانی	سیاست داده	متوسط
شرکت نرم‌افزاری	کیفیت کد/امنیت	دستیار کد	SASTوReview	بالا
مرکز داده	پایداری/عملکرد	AIOps	Human Approval	متوسط
SOC	تشخیص/زمان پاسخ	AI Security	ثبت و تأیید	بالا
زیرساخت حیاتی	ریسک/قابلیت اعتماد	مدل تخصصی	کنترل چندلایه	پایین تا متوسط

براین اساس پنج سطح بلوغ پیشنهاد می‌شود : سطح صفر، بدون استفاده سازمان‌یافته؛ سطح یک، استفاده فردی؛ سطح دو، استفاده کنترل‌شده؛ سطح سه، یکپارچه‌سازی با سامانه‌های داخلی؛ سطح چهار، هوشمندسازی عملیاتی؛ و سطح پنج، عامل‌محوری .با افزایش بلوغ، نیاز به حاکمیتAI ، ارزیابی مدل، مدیریت هویت، ثبت رخداد و نظارت انسانی افزایش می‌یابد.

تحلیل منابع نشان می‌دهد که مزیت اصلی AI در ICT نه جایگزینی کامل نیروی انسانی، بلکه تقویت ظرفیت شناختی و عملیاتی متخصص است AI .می‌تواند حجم زیادی از داده را غربال کند، گزینه های اولیه تولید کند و کارهای تکراری را کاهش دهد؛ اما در وظایف حساس، خروجی آن باید در یک حلقه اعتبارسنجی قرار گیرد.

رابطه میان خودکارسازی و ریسک خطی نیست .افزایش خودکارسازی معمولاً بهره‌وری را بالا می‌برد، اما در سامانه‌های حساس، اثر بالقوه خطا نیز افزایش می‌یابد .بنابراین سطح اختیار AI باید متناسب با پیامد خطا تنظیم شود .این اصل به‌خصوص برای Agentهایی که امکان اجرای عملیات دارند اهمیت دارد.

از منظر اقتصادی نیز صرفه‌جویی زمانی تنها زمانی واقعی است که زمان بازبینی محاسبه شود Net : Saving=T_h−(T_AI+T_Review).بنابراین ادعای کاهش زمان بدون لحاظ کنترل کیفیت می‌تواند بیش‌برآورد ایجاد کند . همچنین هزینه کل مالکیت شاملAPI ، زیرساخت، یکپارچه‌سازی، آموزش، پایش و مدیریت ریسک است.

۶ – نتیجه‌گیری

هوش مصنوعی به یکی از لایه‌های مهم معماری فناوری اطلاعات و ارتباطات تبدیل شده است .ابزارهای مولد، دستیارهای کدنویسی، تحلیل داده،AIOps ، امنیت هوشمند وAgent ها هر یک بخشی از چرخه ICT را دگرگون می‌کنند .نتایج پژوهش نشان می‌دهد که بیشترین ارزش زمانی ایجاد می‌شود که ابزار AI با داده مناسب، فرایند مشخص، کنترل دسترسی، معیار ارزیابی و نظارت انسانی ترکیب شود.

در مهندسی نرم‌افزار، AI می‌تواند سرعت تولید و بازبینی را افزایش دهد، اماSAST ، تست و بازبینی انسانی باید حفظ شود .در شبکه و Cloud، AI برای پیش‌بینی و بهینه‌سازی مفید است، ولی تصمیم های اجرایی باید کنترل‌شده باشند .در امنیت، AI می‌تواند حجم هشدارها را کاهش دهد و تحلیل تهدید را تسریع کند، اما هم‌زمان باید در برابر تهدیدهای اختصاصی LLM محافظت شود.

در نهایت، این پژوهش پیشنهاد می‌کند سازمان‌ها به جای انتخاب یک ابزار بر اساس شهرت، چارچوب چندمعیاره پیشنهادی را به کار گیرند و استقرار را از سطح آزمایشی به سمت یکپارچه‌سازی و سپس خودکارسازی کنترل‌شده توسعه دهند .معماریModel-Agnostic ، AI Gateway، RAG امن،IAM ، ثبت رخداد وHuman-in-the-Loopاز عناصر کلیدی چنین معماری‌ای هستند.

مراجع

[1] A. Vaswani et al., “Attention Is All You Need,” in Proc. NeurIPS, 2017.
[2] T. B. Brown et al., “Language Models are Few-Shot Learners,” in Proc. NeurIPS, 2020.
[3] R. Bommasani et al., “On the Opportunities and Risks of Foundation Models,” arXiv:2108.07258, 2021.
[4] W. Zhao et al., “A Survey of Large Language Models,” arXiv:2303.18223, 2023.
[5] OpenAI, “GPT-4 Technical Report,” arXiv:2303.08774, 2023.
[6] M. Chen et al., “Evaluating Large Language Models Trained on Code,” arXiv:2107.03374, 2021.
[7] L. Zhang et al., “A Survey of AIOps in the Era of Large Language Models,” arXiv:2507.12472, 2025.
[8] M. A. Ferrag et al., “Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities,” Internet of Things and Cyber-Physical Systems, 2025, doi: 10.1016/j.iotcps.2025.01.001.
[9] “The Security of Using Large Language Models: A Survey with Emphasis on ChatGPT,” IEEE/CAA Journal of Automatica Sinica, 2025.
[10] W. Greshake et al., “Not what you’ve signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection,” in Proc. ACM AISec, 2023.
[11] “AI-Powered Code Reviews: Leveraging Large Language Models,” in Proc. SPARC, 2024.
[12] P. Yetistiren, I. Ozsoy, and E. Tuzun, “Assessing the Quality of GitHub Copilot’s Code Generation,” in Proc. ESEM, 2022.

[13] "State of the Art of the Security of Code Generated by LLMs: A Systematic Literature Review," in Proc. IEEE/CONISOFT, 2024.
[14] "Across the Spectrum: In-Depth Review AI-Based Models for Phishing Detection," IEEE Open Journal of the Communications Society, 2024, doi: 10.1109/OJCOMS.2024.3462503.
[15] N. Fareghzadeh et al., "Performance Isolation in Cloud Computing Environments," in Proc. IEEE Int. Conf. Cloud Computing Technology and Science, 2013.
[16] N. Fareghzadeh et al., "A Comprehensive Approach to Performance Management in Cloud Computing," in Proc. IEEE, 2014.
[17] N. Fareghzadeh et al., "A Performance Monitoring Architecture for Cloud Computing," in Proc. IEEE Int. Conf. Cloud Computing and Intelligence Systems, 2014.
[18] "LLM-Based Intelligent Agents for Cybersecurity: A Tutorial and Survey of Automated Vulnerability Discovery," IEEE Access, 2026.
[19] A. Radford et al., "Language Models are Unsupervised Multitask Learners," OpenAI Technical Report, 2019.
[20] T. Brown et al., "Language Models are Few-Shot Learners," arXiv preprint, 2020.
[21] J. Wei et al., "Chain-of-Thought Prompting Elicits Reasoning in Large Language Models," in Proc. NeurIPS, 2022.
[22] Y. Liu et al., "Lost in the Middle: How Language Models Use Long Contexts," Trans. ACL, vol. 12, 2024.
[23] N. Shinn et al., "Reflexion: Language Agents with Verbal Reinforcement Learning," in Proc. NeurIPS, 2023.
[24] P. Lewis et al., "Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks," in Proc. NeurIPS, 2020.
[25] NIST, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," NIST AI 100-1, 2023.
[26] OWASP Foundation, "OWASP Top 10 for Large Language Model Applications," 2025.
[27] N. Carlini et al., "Extracting Training Data from Large Language Models," in Proc. USENIX Security, 2021.
[28] R. Bommasani et al., "On the Opportunities and Risks of Foundation Models," Stanford Center for Research on Foundation Models, 2021.
[29] Y. Dong et al., "Cognitive Deficits of Large Language Models in Reasoning," arXiv preprint, 2023.
[30] "Large Language Model for Vulnerability Detection: Emerging Results and Future Directions," in Proc. IEEE/ACM ICSE-NIER, 2024.