Supreme National Defense University Quarterly Journal of National Security

https://ns.sndu.ac.ir E-ISSN: 2980-8251

Vol. 16, No. 1, Issue. 59, Spring 2026 **Received:** 2025/07/24 **Accepted:** 2025/11/02

Research paper

A Strategic Model of Big Data Cognitive Computing for Enhancing Cybersecurity in the Islamic Republic of Iran

Seyyed Hamidreza Aarabi
PhD Student in Strategic Cyberspace Management, Cybersecurity, Supreme National Defense University, Tehran, Iran (Corresponding Author).
Email: hr.aarabi99@sndu.ac.ir
Mohammadreza Movahedi Sefat
Associate Professor, Supreme National Defense University, Tehran, Iran
Email: movahedi@sndu.ac.ir
Seyed Alireza Hashemi Golpayegani
Assistant Professor, Amirkabir University of Technology, Tehran, Iran
Email: sa.hashemi@aut.ac.ir
Mohammad Hassan Entezari
Professor, Supreme National Defense University, Tehran, Iran
Email: entezari@irost.org

Abstract

Cognitive computing, which integrates cognitive science and artificial intelligence, has emerged with the aim of supporting and enhancing human decision-making through computer-based systems. In the complex and uncertain cyber ecosystem, this technology leverages big data to provide capabilities for the analysis, prediction, and prevention of cyber threats. Through capabilities such as natural language processing, deep learning, computer vision, and ontology-based knowledge representation, cognitive computing can play an effective role in detecting suspicious behavior and identifying covert cyberattacks. The present study aimed to develop a strategic model of big data cognitive computing for enhancing cybersecurity in the Islamic Republic of Iran. A mixed-methods research design was employed, comprising qualitative analysis of documents and scientific literature, in-depth field interviews with experts, and quantitative data analysis using structural equation modeling. A comparative study of selected countries was also conducted. The findings resulted in the development of a strategic model comprising five main dimensions: cybersecurity big data, including data storage infrastructure, data collection, and data integration; data preprocessing, including natural language processing, deep learning, computer vision, ontology, and threat classification; the cognitive core, encompassing human and environmental interaction, hypothesis generation, modeling, reinforcement learning, and a knowledge base; security, comprising confidentiality, integrity, and availability; and governance, encompassing privacy protection, regulation, management, data governance, and command and control. These components were validated using a census approach involving 53 experts in fields relevant to the study. By adopting a preventive approach, the proposed model can assist organizations in the early detection of cyber threats and in protecting the data and critical infrastructures of the Islamic Republic of Iran. The model is applicable within national executive organizations and can contribute to strengthening cybersecurity resilience in the Islamic Republic of Iran.

Keywords: Cognitive Computing; Big Data; Cybersecurity; Strategic Model

فصلنامه امنیت ملی

سال شانزدهم، شماره اول (پیاپی ۵۹)، بهار ۱۴۰۵، صص. ۹-۴۸
تاریخ دریافت: ۱۴۰۴/۰۵/۰۲ ـ تاریخ پذیرش: ۱۴۰۴/۰۸/۱۱

مقاله پژوهشی

الگوی راهبردی رایانش شناختی کلان‌داده‌ها به‌منظور ارتقای امنیت سایبری جمهوری اسلامی ایران

سید حمیدرضا اعرابی
دانشجوی دکترا مدیریت راهبردی فضای سایبر، امنیت سایبری، دانشگاه عالی دفاعی ملی، تهران، ایران (نویسنده مسئول)
Email: hr.aarabi99@sndu.ac.ir

محمدرضا موحدی صفت
دانشیار دانشگاه عالی دفاع ملی، تهران، ایران
Email: movahedi@sndu.ac.ir

سید علیرضا هاشمی گلپایگانی
استادیار دانشگاه صنعتی امیرکبیر، تهران، ایران
Email: sa.hashemi@aut.ac.ir

محمدحسن انتظاری
استاد دانشگاه عالی دفاع ملی، تهران، ایران
Email: entezari@irost.org

چکیده

رایانش شناختی، تلفیقی از علوم شناختی و هوش مصنوعی، با هدف ارتقای تصمیم‌سازی انسانی از طریق سیستم‌های کامپیوتری شکل گرفته است. در زیست‌بوم پیچیده و نامطمئن سایبری، این فناوری با بهره‌گیری از کلان‌داده‌ها، توان تحلیل، پیش‌بینی و پیشگیری از تهدیدات سایبری را فراهم می‌سازد. رایانش شناختی با قابلیت‌هایی چون پردازش زبان طبیعی، یادگیری عمیق، بینایی ماشین و هستان‌شناسی، در شناسایی رفتارهای مشکوک و حملات پنهان نقش مؤثری دارد. پژوهش حاضر با هدف طراحی الگوی راهبردی رایانش شناختی کلان‌داده‌ها برای ارتقای امنیت سایبری جمهوری اسلامی ایران انجام شده است. روش تحقیق از نوع آمیخته بوده و شامل تحلیل کیفی اسناد، منابع علمی و مصاحبه‌های عمیق میدانی با خبرگان و تحلیل کمی داده‌ها با استفاده از مدل‌سازی معادلات ساختاری است. همچنین مطالعه‌ای تطبیقی از وضعیت کشورهای منتخب در این حوزه صورت گرفته است. یافته‌های پژوهش منجر به تدوین الگویی راهبردی در پنج بُعد اصلی شامل کلان‌داده امنیت سایبری (زیرساخت ذخیره‌سازی، جمع‌آوری و یکپارچه‌سازی داده‌ها)، پیش‌پردازش داده‌ها (پردازش زبان طبیعی، یادگیری عمیق، بینایی ماشین، هستان‌شناسی و طبقه‌بندی تهدیدها)، هسته‌شناختی (تعامل با محیط و انسان، فرضیه‌سازی، مدل‌سازی، یادگیری تقویتی و پایگاه دانش)، امنیت (محرمانگی، یکپارچگی و دسترس‌پذیری) و حکمرانی (حفظ حریم خصوصی، تنظیم‌گری، مدیریت، داده و فرماندهی و کنترل) گردید. این مؤلفه‌ها با تأیید ۵۳ نفر از خبرگان حوزه مرتبط با پژوهش به‌صورت تمام‌شمار اعتبارسنجی شده‌اند. الگوی پیشنهادی با اتخاذ رویکردی پیشگیرانه، سازمان‌ها را در شناسایی زودهنگام تهدیدات سایبری و حفاظت از داده‌ها و زیرساخت‌های حیاتی جمهوری اسلامی ایران یاری می‌دهد. این الگو قابلیت پیاده‌سازی در نهادهای اجرایی کشور را داشته و زمینه‌ساز ارتقای سطح تاب‌آوری سایبری در جمهوری اسلامی ایران خواهد بود.

کلیدواژه‌ها: رایانش شناختی، کلان‌داده‌ها، امنیت سایبری، الگوی راهبردی

https://ns.sndu.ac.ir/ E-ISSN: 2980-8251

صحت مطالب بر عهده نویسنده مقاله است و بیانگر دیدگاه دانشگاه عالی دفاع ملی نیست.

مقدمه

علوم شناختی شاخه‌ای میان‌رشته‌ای است که از ادغام و هم‌افزایی رشته‌های مختلفی مانند روان‌شناسی، فلسفه ذهن، عصب‌شناسی، زبان‌شناسی، انسان‌شناسی، علوم رایانه و هوش مصنوعی تشکیل شده است. این علم به بررسی ماهیت فعالیت‌های ذهنی مانند تفکر، طبقه‌بندی و فرایندهایی که انجام این فعالیت‌ها را ممکن می‌کند می‌پردازد. به‌صورت مشخص‌تر ازجمله اهداف اصلی این رشته پژوهش در زمینهٔ ادراک و بازشناسی، توجه، حافظه و یادگیری، زبان، استدلال و تفکر، قضاوت، برنامه‌ریزی، تصمیم‌گیری است. با توجه به رشد فزاینده تهدیدات سایبری و پیچیدگی روزافزون زیست‌بوم دیجیتال، دیگر نمی‌توان با رویکردهای سنتی به مقابله با مخاطرات امنیتی پرداخت. رایانش شناختی، با توانایی درک، استدلال و تصمیم‌گیری مشابه انسان، می‌تواند تحولی بنیادین در مدیریت امنیت سایبری ایجاد کند. ترکیب این فناوری کلان‌داده‌ها، بستری فراهم می‌آورد تا تهدیدات پنهان شناسایی، رفتارهای مشکوک پیش‌بینی و حملات سایبری پیش از وقوع خنثی شوند.

هدف رایانش شناختی افزایش قدرت تصمیم‌سازی از طریق تولید دستیار هوشمند است. رایانش شناختی می‌تواند در پیشگیری از حملات سایبری کاربرد داشته باشد. در زمینهٔ امنیت سایبری می‌توان از قدرت خودکارسازی فرایندها با استفاده از الگوریتم‌های پیشرفته رایانش شناختی، به شناسایی الگوی رفتارهای مشکوک شبکه ارتباطی، پیش‌بینی رفتارهای ناهنجار در سیستم‌های کامپیوتری و تشخیص حملات سایبری بهره برد. سیستم‌های شناختی قادر به پذیرش انواع مختلفی از داده‌ها از منابع مختلف بوده و نیز توانایی درک، ارزیابی و یادگیری از داده‌هایی را دارند که می‌توانند دریچه‌های جدیدی را به روی انسان بگشایند. سیستم‌های شناختی، نظیر IBM Watson و Darktrace قادر به یادگیری از طریق ورودی کاربر بوده و می‌توانند توسط متخصصین مربوطه آموزش داده شوند.

براساس گزارش «اتحادیه بین‌المللی مخابرات»[1] وابسته به سازمان ملل متحد در ارزیابی امنیت سایبری از ۱۹۴ کشور جهان، کشور جمهوری اسلامی ایران به ترتیب در سال‌های

1. International Telecommunication Union

۲۰۱۵، ۲۰۱۸، ۲۰۲۱ و ۲۰۲۴ به ترتیب در ردیف‌های ۸۰، ۶۰، ۵۴ و ۵۵ قرار داشته است. براساس آخرین گزارش ارزیابی اتحادیه بین‌المللی مخابرات شاخص اقدامات فنی کشور ایران از وضعیت مطلوبی برخوردار نیست. ازاین‌رو الگوی راهبردی رایانش شناختی کلان داده‌های امنیت سایبری به‌منظور خودکارسازی فرایند شناسایی سریع تهدیدات سایبری در دستیابی به آگاهی وضعیتی امنیت سایبری ملی نقش اساسی داشته و فقدان خودآگاهی سایبر شناختی تحیُّر در تصمیم‌گیری را به‌همراه خواهد داشت.

برای دستیابی به آگاهی وضعیتی امنیت سایبری داشتن ساختار و سازمان‌دِهی مناسب کلان‌داده‌های امنیت سایبری ملی امری ضروری و اجتناب‌ناپذیر است و بهبود ساختار و سازمان‌دِهی کلان‌داده‌های امنیت سایبری درنتیجه پیاده‌سازی الگوی راهبردی رایانش شناختی کلان‌داده‌ها منجر به تجزیه‌وتحلیل، استدلال و شناسایی زودهنگام و همچنین پاسخ به‌موقع به حملات سایبری خاص را در پی داشته و از همه مهم‌تر از تصمیم‌گیری‌های سلیقه‌ای و اقدامات مقطعی امنیت سایبری ملی جلوگیری و درنتیجه منجر به بهبود آن در سطح راهبردی می‌گردد.

با استفاده از رایانش شناختی کلان‌داده‌های امنیت سایبری و شناسایی الگوهای رفتاری حملات سایبری، امکان وضع مقررات جدیدی متناسب با این الگوها فراهم خواهد شد. همچنین، با توجه به یکپارچه‌سازی داده‌های امنیت سایبری سازمان‌ها و دستگاه‌های مختلف، تنظیم‌گری مقررات مناسب به‌منظور حفظ یکپارچگی و حریم خصوصی این داده‌ها امری ضروری و اجتناب‌ناپذیر خواهد بود.

با طراحی الگوی راهبردی رایانش شناختی کلان‌داده‌ها و همچنین اشتراک‌گذاری داده‌های امنیت سایبری به‌عنوان بخشی از این الگو امکان تشخیص سریع‌تر و پاسخ‌گویی به حملات سایبری خاص‌منظوره و همکاری بین سازمان‌ها از قبیل انرژی، صداوسیما، فرودگاه‌ها و غیره بهبود می‌یابد. همچنین تحلیل داده‌های امنیت سایبری، تعاملات و اشتراک‌گذاری این داده‌ها بین سازمان‌های مختلف، به بهبود همکاری و تسهیل ارتباطات بین سازمان‌ها کمک خواهد کرد.

۱. مبانی نظری پژوهش

۱-۱. فلسفه و چیستی رایانش شناختی

فلسفه رایانش شناختی به‌عنوان یک حوزه تحقیقاتی میان‌رشته‌ای، به بررسی مسائل فلسفی مرتبط با رایانش شناختی، اصول و مفاهیم بنیادین و نقش آن در بهبود فرایندها، بررسی رفتارهای شناختی، عملیات ذهنی و ارتباط آن‌ها با عملیات رایانشی می‌پردازد. رایانش شناختی به دنبال بهره‌برداری از تئوری‌های شناختی برای حل مسائل شناختی و استفاده از روش‌های رایانشی برای تقلید رفتارهای شناختی انسان است. این حوزه با تقلید از فرایندهای پردازش اطلاعات در مغز انسان، سعی در افزایش کارایی و بهبود عملکرد سیستم‌های هوشمند دارد. این فلسفه بر چندین اصل استوار است ازجمله: تعامل بین انسان و سامانه‌های هوشمند، انعطاف‌پذیری، شفافیت، حریم خصوصی، قابلیت اعتماد و امنیت (Helm,2025).

۱-۲. زیست‌بوم رایانش شناختی

زیست‌بوم رایانش شناختی به مجموعه‌ای از مؤلفه‌های سخت‌افزاری و نرم‌افزاری، شامل شبکه‌ای از سازمان‌ها و نهادها (شرکت‌های فناوری، مؤسسات تحقیقاتی، دانشگاه‌ها و نهادهای حکومتی)، افراد (شامل توسعه‌دهندگان، محققان، سیاست‌گذاران، سرمایه‌گذاران و کاربران نهایی)، فناوری‌ها (شامل هوش مصنوعی، پردازش زبان طبیعی و دیگر فناوری‌های پیشرفته)، منابع کلان‌داده‌ها (مجموعه‌های بزرگی از داده‌ها که برای آموزش و بهبود سیستم‌های شناختی استفاده می‌شوند) و پلتفرم‌ها (سیستم‌ها و ابزارهایی که زیرساخت‌های لازم برای توسعه و بهره‌برداری از رایانش شناختی فراهم می‌کنند اعم از پیام‌رسان‌ها و شبکه‌های اجتماعی) اطلاق می‌شود که در توسعه، استقرار و استفاده از سیستم‌های رایانش شناختی دخیل هستند. این زیست‌بوم یک سامانه بسیار پیچیده و درعینِ‌حال منعطف و پویا شامل طیف گسترده‌ای از بازیگران است که همگی برای پیشبرد و بهره‌برداری از رایانش شناختی با هم تعامل دارند. زیست‌بوم رایانش شناختی باهدف بهبود تصمیم‌گیری‌ها، خودکارسازی فرایندها، ارائه راه‌حل‌های هوشمندانه با افراد و سازمان‌ها شکل‌گرفته و همواره

در حال تحول و پیشرفت است (Cicirelli et al., 2019).

۱-۳. ویژگی‌های رایانش شناختی

کنسرسیوم رایانش شناختی به‌منظور کاربست رایانش شناختی در کاربردهای تجاری و گسترده، ویژگی‌های زیر را برای سیستم‌های رایانشی توصیه کرده است:

۱. «خودتطبیقی»[1]: رایانش شناختی به‌خوبی براساس اطلاعات جدید و تغییرات در محیط، کار می‌کند. سیستم‌های رایانش شناختی توانایی یادگیری از تجربیات گذشته و بهبود عملکرد در طول زمان را دارند. این ویژگی باعث می‌شود سیستم‌های شناختی مؤثرتر و کارآمدتر باشند و پاسخ‌های بهینه‌تری در مواجهه با مسائل مختلف ارائه دهند.

۲. «تعاملی»[2]: رایانش شناختی از مکانیسم‌های تعاملی پیشرفته برای برقراری ارتباط با کاربران، سیستم‌ها و دیگر عناصر محیط استفاده می‌کند. این تعامل می‌تواند از طریق گفتار، نوشتار، تصویر و حتی ژست‌ها و نشانه‌های غیرکلامی انجام شود. سیستم‌های رایانش شناختی به‌طور فعال با کاربران همکاری می‌کنند تا بهترین نتیجه را کسب کنند.

۳. «تکراری»[3]: رایانش شناختی به‌خوبی با انجام مراحل مکرر در طی یک فرایند کار می‌کند. این فرایند شامل بررسی داده‌ها، اعمال الگوریتم‌های یادگیری ماشین و ارزیابی نتایج به‌صورت پیوسته است. با تکرار این مراحل، سیستم‌های رایانش شناختی به‌تدریج به نتیجه بهینه‌تری می‌رسند.

۴. «حافظه‌دار»[4]: رایانش شناختی توانایی ذخیره اطلاعات درباره وضعیت فعلی سامانه و تاریخچه تعاملات گذشته را دارد. این امکان به سیستم‌های رایانش شناختی اجازه می‌دهد تا براساس اطلاعات گذشته و تجربیات کاربران عملکرد بهتری داشته باشند. به‌عنوان مثال، یک سامانه پیشنهادگر محتوا می‌تواند براساس تاریخچه مشاهده‌های کاربر پیشنهادات مناسب‌تری ارائه دهد.

1. Adaptive
2. Interactive
3. Iterative
4. Stateful

۵. «زمینه‌محور»[1]: سیستم‌های رایانش شناختی توانایی درک مفاهیم و ارتباطات در زمینه‌های مختلف را دارند. این سیستم‌ها می‌توانند اطلاعات مربوط به موضوع، کاربر، موقعیت زمانی و مکانی و دیگر عوامل مرتبط را در نظر بگیرند تا پاسخ‌ها و تصمیم‌گیری‌های مناسب‌تری ارائه کنند. به‌عنوان مثال، یک سامانه پاسخ‌گویی به سؤالات می‌تواند درک کند که یک سؤال در مورد محصولی خاص یا در یک بخش خاص از دانش مورد نیاز است و پاسخ‌های مناسب‌تری براساس این زمینه ارائه دهد.

۱-۴. مزایای رایانش شناختی

رایانش شناختی مزایای گسترده‌ای را ارائه می‌دهد که در زمینه‌های مختلف تأثیرات چشمگیری دارد. این فناوری باعث ارتقای تصمیم‌گیری انسانی، افزایش کارایی، «شخصی‌سازی»[2]، «مقیاس‌پذیری»[3] و «صرفه‌جویی در هزینه»[4] در صنایع گوناگون می‌شود.

۱-۵. چهارچوب رایانش شناختی

چهارچوب رایانش انسان‌محور با برتری شناختی در فضای ابری شامل ماشین‌ها، سرور و انسان است. ماشین به معنای تمام دستگاه‌های سخت‌افزاری مانند رایانه، دستگاه ارتباطی، ربات‌ها و غیره است. سرور ابری به معنای فضایی است که شامل تمام مجموعه‌های تاریخی داده‌های گذشته ذخیره شده در شبکه‌های مجازی است. این پارادایم به ما امکان می‌دهد با استفاده از الگوریتم‌های عمیق با ماشین و رابط کاربری دستگاه‌ها و انسان‌ها تعامل داشته باشیم. رایانش شناختی مسیر کارآمدی را در اختیار ماشین‌ها قرار می‌دهد تا به مجموعه‌داده‌های داخلی نگاه کنند تا خدمات هوشمند یا شناختی را به کاربر ارائه دهند. سه رکن اصلی رایانش شناختی؛ کلان‌داده، شامل تمام داده‌های ساخت‌یافته، داده‌های

1. Contextual
2. Personalization
3. Scalability
4. Affordable

نیمه‌ساختاریافته و بدون ساختار است؛ فناوری، شامل هوش مصنوعی، پردازش زبان طبیعی، الگوریتم‌های یادگیری عمیق، تجزیه‌وتحلیل پیشرفته، تجسم و ... است و فرایند، شامل پاسخ به تمام توصیه‌ها، الگوها و پیش‌بینی‌های مجموعه داده‌ها است (Saksono et al.,2024).

۱-۶. «معماری رایانش شناختی»[1]

هدف رایانش شناختی ساخت ماشین‌های شناختی با منابع پردازشی کم است که در زمان واقعی پاسخ می‌دهند. بااین‌حال، ادبیات علمی حوزه‌های تحقیقاتی متفاوت و تفاسیر مختلفی از آن را نشان می‌دهد. این امر مستلزم یک معماری منسجم است که ماهیت رایانش شناختی را مشخص می‌کند. این معماری‌ها عبارت‌اند از:

الف: «معماری‌های شناختی هیبریدی»[2]: این معماری‌ها ترکیبی از تکنیک‌های مختلف هوش مصنوعی مانند شبکه‌های عصبی، الگوریتم‌های یادگیری و سیستم‌های مبتنی بر قوانین را برای ایجاد سیستمی قوی‌تر و قابل تطبیق‌تر استفاده می‌کنند.

ب: «معماری‌های نوروسمبولیک»[3]: این معماری‌ها شبکه‌های عصبی را با استدلال سمبولیک ادغام می‌کنند و امکان پردازش داده‌های غیرساختاریافته (مانند تصاویر و متون) و داده‌های ساخت‌یافته (مانند پایگاه‌های داده) را فراهم می‌کنند. معماری نوروسمبولیک یک رویکرد ترکیبی در حوزه هوش مصنوعی است که تلاش می‌کند تا بهترین ویژگی‌های دو روش اصلی یادگیری ماشین و سیستم‌های سمبولیک را با هم ترکیب کند. این معماری به دنبال ایجاد سیستم‌های هوش مصنوعی است که توانایی یادگیری داده‌های پیچیده و همچنین استدلال منطقی و تفسیری را داشته باشند (Yang X. et al., 2023).

پ: «معماری‌های شناختی پویا»[4]: این معماری‌ها برای تطبیق با محیط‌های تغییرپذیر و اطلاعات جدید طراحی شده‌اند و بسیار انعطاف‌پذیر و پاسخ‌گو هستند (Hilal et al., 2023).

1. Cognitive Computing Architecture
2. Hybrid cognitive architectures
3. Neurosymbolic architectures
4. Dynamic Cognitive Architecture

ت: «معماری‌های الهام‌گرفته از مغز»[1]: این معماری‌ها از اصول علوم عصبی برای ایجاد سیستم‌های کارآمدتر و سریع‌تر، به‌ویژه در تشخیص و پاسخ به تهدیدات استفاده می‌کنند (Wang et al.,2020).

۱-۷. فناوری‌های رایانش شناختی

رایانش شناختی از ترکیبی از فناوری‌های پیشرفته استفاده می‌کند که هرکدام به توانایی سامانه برای تقلید از فرایندهای فکری انسان و افزایش قابلیت‌های تصمیم‌گیری کمک می‌کنند. این فناوری‌ها عبارت‌اند از: هوش مصنوعی، یادگیری ماشینی، پردازش زبان طبیعی، بینایی ماشین و «اتوماسیون فرایند رباتیک»[2] (Baltieri et al., 2023).

۱-۸. هم‌افزایی هوش مصنوعی و رایانش شناختی

هوش مصنوعی را می‌توان به‌عنوان پایه و اساس کار رایانش شناختی در نظر گرفت. سیستم‌های هوش مصنوعی به‌منظور خودکارسازی فرایند تجزیه‌وتحلیل و تبدیل داده‌ها به اطلاعات و سپس دانش، طراحی شده‌اند. این سیستم‌ها با به‌کارگیری دانش حاصل، قادر به شبیه‌سازی وظایف شناختی؛ مانند شناسایی الگوها، پیش‌بینی، تصمیم‌گیری و انجام تحقیقات در حوزه‌های موضوعی مختلف هستند. به‌عبارت‌دیگر، هوش مصنوعی به دنبال ایجاد ماشین‌هایی است که بتوانند وظایفی را که به‌طور معمول به هوش انسانی نیاز دارند، انجام دهند. درواقع، هوش مصنوعی ابزاری برای پیاده‌سازی رایانش شناختی محسوب می‌شود. رایانش شناختی با استفاده از تکنیک‌های هوش مصنوعی، به دنبال ایجاد سیستم‌هایی است که بتوانند؛ مانند انسان یاد بگیرند، استدلال کنند و تصمیم بگیرند. سیستم‌های هوش مصنوعی می‌توانند قابلیت‌های شناختی انسان را در فرایند درک و پردازش اطلاعات به‌طور قابل‌توجهی افزایش دهند. ازاین‌رو، می‌توان از هم‌افزایی آن‌ها در هر زمینه‌ای که انسان از هوش طبیعی

1. Architectures Inspired by The Brain
2. Robotic Process Automation

خود استفاده می‌کند، بهره برد. به‌طور خاص، سیستم‌های هوش مصنوعی پتانسیل خودکارسازی فرایندهای شناختی در تمامی حوزه‌های علمی را دارند. بااین‌حال، باید توجه داشت که هوش مصنوعی با وجود پیشرفت‌های چشمگیر، هنوز محدودیت‌هایی دارد (Veniaminovich , 2024).

۱-۹. تمایز رایانش شناختی و هوش مصنوعی

رایانش شناختی و هوش مصنوعی دو حوزه مرتبط در علوم کامپیوتر هستند که هدف آن‌ها ایجاد سیستم‌های هوشمند است. بااین‌حال، این دو حوزه در رویکرد و اهداف خود تفاوت‌های اساسی دارند هوش مصنوعی به‌طورکلی بر توسعه الگوریتم‌هایی تمرکز دارد که می‌توانند وظایف خاصی را به‌طور خودکار انجام دهند.

این الگوریتم‌ها براساس مجموعه‌ای از قوانین از پیش تعریف شده عمل می‌کنند و برای حل مسائل با ساختار مشخص و داده‌های از پیش تعیین شده مناسب هستند. به‌عبارت‌دیگر، هوش مصنوعی بر «محاسبه» برای حل مسائل تأکید دارد. رایانش شناختی بر «شناخت» و «درک» برای حل مسائل تأکید دارد (Kelly et al., 2013) یکی از تفاوت‌های کلیدی بین هوش مصنوعی و رایانش شناختی در نحوه پردازش اطلاعات است. در هوش مصنوعی، اطلاعات ورودی براساس الگوریتم‌های از پیش تعریف شده پردازش می‌شود و کل فرایند تحت کنترل سامانه باقی می‌ماند. در رایانش شناختی، سامانه به‌عنوان یک دستیار عمل می‌کند و به انسان در درک داده‌ها و تصمیم‌گیری کمک می‌کند (Guerrero et al., 2023).

۱-۱۰. هم‌گرایی رایانش کوانتومی و ابری در رایانش شناختی

هم‌گرایی رایانش کوانتومی و ابری می‌تواند تحولات شگرفی در حوزه رایانش شناختی ایجاد کند. با استفاده از قدرت پردازشی کوانتومی، می‌توان الگوریتم‌های یادگیری ماشین و هوش مصنوعی را به‌طور چشمگیری بهبود بخشید و سیستم‌های شناختی قدرتمندتری را برای حل مسائل پیچیده؛ مانند کشف آسیب‌پذیری، تشخیص زودهنگام تهدیدات سایبری، تحلیل

کلان‌داده‌ها و پیش‌بینی حملات سایبری توسعه داد. هم‌گرایی این سه حوزه، یک زیست‌بوم قدرتمند برای رایانش شناختی ایجاد می‌کند:

۱. ابر به‌عنوان بستر: ابر زیرساخت لازم برای ذخیره‌سازی داده‌ها، دسترسی به منابع رایانشی و استقرار برنامه‌های کاربردی را فراهم می‌کند.
۲. کوانتوم به‌عنوان شتاب‌دهنده: رایانش کوانتومی می‌توانند وظایف خاصی را که برای رایانش شناختی حیاتی هستند، مانند یادگیری ماشین و بهینه‌سازی، تسریع کنند.
۳. رایانش شناختی به‌عنوان مغز: الگوریتم‌ها و مدل‌های شناختی از داده‌ها و قدرت رایانشی فراهم شده توسط ابر و کوانتوم برای حل مسائل پیچیده و ارائه بینش استفاده می‌کنند.

ترکیب قابلیت‌های منحصربه‌فرد رایانش کوانتومی با انعطاف‌پذیری و مقیاس‌پذیری رایانش ابری می‌تواند تحولی اساسی در حوزه پردازش اطلاعات و سیستم‌های هوشمند ایجاد کند. ادغام قابلیت‌های رایانش کوانتومی با مزایای مقیاس‌پذیری و انعطاف‌پذیری رایانش ابری می‌تواند منجر به پیشرفت‌های قابل‌توجهی در زیست‌بوم رایانش شناختی شود. همچنین، این هم‌گرایی می‌تواند به بهبود کارایی، اثربخشی و بهره‌وری در زیرساخت‌های رایانش شناختی منجر شود. (اعرابی و همکاران، ۱۴۰۳ الف)

۱-۱۱. مزایای هم‌گرایی فناوری رایانش ابری و کوانتومی در رایانش شناختی

هم‌گرایی این دو فناوری در رایانش شناختی مزایای متعددی را به ارمغان می‌آورد، در جدول (۱)، به برخی از مزایای حاصل از کاربست فناوری رایانش ابری و کوانتومی در رایانش شناختی اشاره شده است (اعرابی و همکاران، ۱۴۰۳ الف).

جدول ۱: مزایای هم‌گرایی فناوری رایانش ابری و کوانتومی در رایانش شناختی

ردیف	عنوان	توضیحات
۱	افزایش سرعت و کارایی در تحلیل داده‌های پیچیده	رایانش کوانتومی می‌تواند سرعت پردازش داده‌های پیچیده را در الگوریتم‌های یادگیری ماشین و هوش مصنوعی به‌طور قابل‌توجهی افزایش دهد. این امر به رایانش شناختی کمک

ردیف	عنوان	توضیحات
		می‌کند تا وظایف پیچیده را سریع‌تر و کارآمدتر انجام دهد.
۲	حل مسائل پیچیده‌تر	رایانش کوانتومی می‌تواند به حل مسائل پیچیده‌ای که برای رایانه‌های کلاسیک دشوار یا غیرممکن هستند، مانند پردازش زبان طبیعی و درک تصاویر، کمک کند.
۳	دسترسی آسان به منابع رایانشی	رایانش ابری امکان دسترسی آسان به منابع رایانشی کوانتومی را برای محققان و توسعه‌دهندگان فراهم و همین امر به تسریع روند توسعه و نوآوری در رایانش شناختی نیز کمک می‌کند.
۴	مقیاس‌پذیری و انعطاف‌پذیری	رایانش ابری به کاربران اجازه می‌دهد تا منابع رایانشی خود را براساس نیاز خود مقیاس‌بندی کنند. این امر به رایانش شناختی کمک می‌کند تا با حجم داده‌های روبه‌رشد و پیچیدگی وظایف، سازگار شود. رایانش ابری قدرت پردازشی مورد نیاز برای اجرای مدل‌های شناختی را به‌صورت مقیاس‌پذیر و براساس تقاضا فراهم می‌کند.
۵	کاهش هزینه‌های عملیاتی	استفاده از خدمات ابری هزینه‌های مرتبط با زیرساخت سخت‌افزاری و نگهداری را کاهش می‌دهد.

هم‌گرایی رایانش ابری و کوانتومی در زیست‌بوم رایانش شناختی، بهبود معناداری در شاخص‌های عملکردی ایجاد می‌کند و موجب کاهش زمان تشخیص ناهنجاری‌های امنیتی و افزایش دقت پیش‌بینی حملات می‌شود. ادغام رمزنگاری کوانتومی، نرخ شناسایی حملات پیشرفته را تا حد زیادی نسبت به سیستم‌های مبتنی بر روش‌های کلاسیک افزایش می‌دهد. این بهبود عمدتاً ناشی از قابلیت پردازش هم‌زمان داده‌های چند منبعی و شناسایی الگوهای پنهان با استفاده از الگوریتم‌های شناختی – کوانتومی است. بااین‌حال، چالش‌های فنی یکپارچه‌سازی سخت‌افزار کوانتومی با مراکز داده ابری، هزینه عملیاتی را تا حدی نسبت به سیستم‌های مرسوم افزایش می‌دهد؛ بنابراین، هم‌گرایی این فناوری‌ها موجب کاهش زمان تشخیص ناهنجاری‌ها، افزایش دقت پیش‌بینی حملات و بهینه‌سازی مصرف منابع رایانشی می‌شود (اعرابی و همکاران، ۱۴۰۴).

۱-۱۲. رایانش شناختی در امنیت سایبری

امروزه، امنیت سایبری به یکی از مهم‌ترین چالش‌های جهانی تبدیل‌شده است، به‌طوری‌که سیستم‌های دولتی و اطلاعات حساس پیوسته در معرض تهدیدات و حملات سایبری قرار دارند. رایانش شناختی کلان‌داده‌ها می‌تواند با خودکارسازی فرایندها و تقویت تحلیل‌های انسانی، تصمیم‌گیری‌ها را بهبود بخشد. رایانش شناختی با بهره‌گیری از الگوریتم‌های پیشرفته یادگیری ماشین و پردازش زبان طبیعی، توانایی شبیه‌سازی فرایندهای شناختی مغز انسان نظیر یادگیری، استدلال و حل مسئله را دارد. این قابلیت‌ها به رایانش شناختی امکان می‌دهد تا با تحلیل پیشرفته کلان‌داده‌های فضای سایبر، الگوهای پنهان و رفتارهای مشکوک را شناسایی کرده و با پیش‌بینی حملات سایبری، به مقابله به‌موقع با آن‌ها کمک کند. رایانش شناختی به‌طور قابل‌توجهی می‌تواند آگاهی وضعیتی امنیت سایبری را ارتقا داده و کارایی سیستم‌های امنیتی را بهبود بخشد. (اعرابی و همکاران، ۱۴۰۳ ب) رایانش شناختی می‌تواند در موارد ذیل به‌عنوان یک نیروی محرک در ارتقای امنیت سایبری عمل کرده و به سازمان‌ها کمک کند تا در برابر تهدیدات سایبری پیچیده و پیشرفته، دفاعی قوی‌تر و مؤثرتر داشته باشند:

پیشرفت در کشف تهدیدها: رایانش شناختی با استفاده از الگوریتم‌های پیشرفته یادگیری ماشین، می‌تواند تهدیدات سایبری جدید و ناشناخته را با سرعت و دقت بیشتری نسبت به روش‌های سنتی شناسایی کند. این سیستم‌ها به‌طور مداوم از داده‌ها و حملات گذشته یاد می‌گیرند و می‌توانند به‌سرعت الگوهای جدید تهدیدات را شناسایی کنند، ازجمله حملات روز صفر و «تهدیدات پیشرفته مداوم»[1].

واکنش سریع‌تر و خودکار: ازآنجاکه زمان تشخیص و پاسخ به حملات سایبری بسیار حیاتی است، رایانش شناختی می‌تواند این فرایندها را تسریع کرده و به‌صورت خودکار اقدامات مناسبی را برای متوقف کردن یا محدود کردن تأثیرات حملات انجام دهد. این ویژگی به‌ویژه در شرایطی که سرعت پاسخ‌گویی برای جلوگیری از گسترش حمله حیاتی

1. Advanced Persistent Threat

است، اهمیت دارد.

تحلیل و پیش‌بینی تهدیدهای آینده: رایانش شناختی با تحلیل الگوهای تهدیدات سایبری و رفتارهای غیرعادی در شبکه‌ها و سیستم‌ها می‌تواند به پیش‌بینی تهدیدات آینده کمک کند. این قابلیت به سازمان‌ها امکان می‌دهد تا پیش از وقوع حملات، اقدامات پیشگیرانه‌ای انجام دهند و استراتژی‌های امنیتی خود را براساس تهدیدات بالقوه تنظیم کنند.

بهبود مدیریت حوادث امنیتی: رایانش شناختی می‌تواند از طریق تحلیل خودکار و سریع داده‌های مربوط به حوادث امنیتی، به گروه‌های امنیت سایبری کمک کند تا حوادث را اولویت‌بندی کرده و به‌سرعت به آن‌ها پاسخ دهند. این سیستم‌ها با تجزیه‌وتحلیل حجم بالایی از اطلاعات، می‌توانند به شناسایی منبع و نوع حمله کمک کرده و بهترین راهکارهای مقابله‌ای را پیشنهاد دهند.

کاهش هزینه‌های عملیاتی: با خودکارسازی فرایندهای امنیتی و کاهش نیاز به دخالت انسانی در بسیاری از مراحل، رایانش شناختی می‌تواند هزینه‌های عملیاتی را کاهش دهد. علاوه بر این، با جلوگیری از حملات سایبری و کاهش تأثیرات آن‌ها، هزینه‌های ناشی از مقابله با حوادث امنیتی و بازیابی سیستم‌ها نیز کاهش می‌یابد.

تطبیق‌پذیری و انعطاف‌پذیری بالا: رایانش شناختی با قابلیت یادگیری مداوم و تطبیق با تهدیدات جدید، به سازمان‌ها کمک می‌کند تا دفاع‌های خود را به‌طور پیوسته بهبود ببخشند. این فناوری می‌تواند به‌سرعت با تغییرات محیطی و ظهور تهدیدات جدید سازگار شده و راهکارهای جدیدی را برای مقابله با تهدیدات ارائه دهد.

افزایش دقت و کارایی: سیستم‌های رایانش شناختی می‌توانند با تحلیل حجم عظیمی از داده‌ها، تهدیدها را بادقت و کارایی بیشتری نسبت به روش‌های سنتی شناسایی کنند.

کاهش زمان پاسخ به تهدیدات: سیستم‌های رایانش شناختی می‌توانند به‌طور خودکار به تهدیدات پاسخ داده و زمان لازم برای مقابله با آن‌ها را کاهش دهند.

شناسایی تهدیدات جدید: سیستم‌های رایانش شناختی می‌توانند با یادگیری مداوم، تهدیدات جدید و ناشناخته را شناسایی کرده و از سازمان‌ها در برابر آن‌ها محافظت کنند.

ایجاد مرکز عملیات امنیت شناختی: رایانش شناختی می‌تواند با تحلیل کلان‌داده‌ها و ایجاد قابلیت آگاهی وضعیتی در «مرکز عملیات امنیت شناختی»[1]، سطح امنیت را به‌طور قابل‌توجهی ارتقا دهد. این امر از طریق دو مکانیزه اصلی محقق می‌شود: نخست، تحلیل هم‌زمان حجم عظیمی از داده‌ها که امکان شناسایی تهدیدات امنیتی را در زمان واقعی فراهم می‌آورد. دوم، پاسخ سریع و خودکار به حوادث امنیتی با بهره‌گیری از مؤلفه‌های رایانش شناختی برای مقابله مؤثر با تهدیدها (Agilandeswari et al., 2024).

۱-۱۳. تأثیر رایانش شناختی بر ارکان امنیت سایبری

امنیت سایبری بر سه رکن اساسی «محرمانگی»[2]، «جامعیت»[3] و «دسترس‌پذیری»[4] استوار است. رایانش شناختی با ارائه راهکارهای نوآورانه می‌تواند به تقویت هر یک از این ارکان کمک کند.

تأثیر رایانش شناختی بر ارتقای محرمانگی: در دنیای امروز، سازمان‌ها با حجم عظیمی از داده‌های حساس مواجه هستند که باید از آن‌ها در برابر تهدیدات سایبری محافظت کنند. چالش‌های موجود در حفظ محرمانگی شامل حملات فیشینگ، بدافزارها، نفوذ به شبکه‌ها و سرقت داده‌ها است. رایانش شناختی با ارائه مؤلفه‌هایی مانند یادگیری ماشین، پردازش زبان طبیعی و بینایی کامپیوتر، می‌تواند به سازمان‌ها در ارتقای محرمانگی کمک کند (Xu et al., 2020). یکی از کاربردهای یادگیری ماشین در حفظ محرمانگی، تشخیص ناهنجاری‌ها در الگوهای دسترسی به داده‌ها است. با استفاده از الگوریتم‌های یادگیری ماشین، می‌توان رفتار عادی کاربران را مدل‌سازی کرد و هرگونه انحراف از این الگو را به‌عنوان یک تهدید بالقوه شناسایی کرد (Anderson et al., 2019).

تأثیر رایانش شناختی بر حفظ جامعیت داده‌ها: جامعیت به معنای تضمین صحت و عدم تغییر داده‌ها است. چالش‌های موجود در حفظ جامعیت داده‌ها و سیستم‌ها شامل حملات

1. Cognitive SOC
2. Confidentiality
3. Integirity
4. Avalaiblity

تزریق کد، دست‌کاری داده‌ها و حملات سایبری پیچیده است. رایانش شناختی با کاربست فناوری بلاک‌چین، می‌تواند به سازمان‌ها در تضمین جامعیت داده‌ها کمک کند (Yampolskiy, 2018). بلاک‌چین به‌عنوان یک فناوری دفتر کل توزیع‌شده، امکان ثبت تراکنش‌ها به‌صورت امن و غیرقابل‌تغییر را فراهم می‌کند. با استفاده از بلاک‌چین، می‌توان از صحت داده‌ها و جلوگیری از دست‌کاری آن‌ها اطمینان حاصل کرد (Kshetri, 2018). برای مثال، اگر در یک سامانه مالی، تراکنش‌های غیرمعمول و مشکوک مشاهده شود، سامانه می‌تواند این تراکنش‌ها را به‌عنوان دست‌کاری داده‌ها شناسایی کرده و اقدامات لازم را برای جلوگیری از آن‌ها انجام دهد (Narayanan et al., 2016).

تأثیر رایانش شناختی بر بهبود دسترس‌پذیری: دسترس‌پذیری به معنای اطمینان از دسترسی کاربران مجاز به داده‌ها و سیستم‌ها در زمان نیاز است. رایانش شناختی با استفاده از یادگیری ماشین، می‌تواند به سازمان‌ها در افزایش دسترس‌پذیری کمک کند. با استفاده از الگوریتم‌های یادگیری ماشین، می‌توان الگوهای ترافیک شبکه را تجزیه‌وتحلیل نمود و حملات DDoS را به‌طور پیشگیرانه شناسایی و مسدود کرد. علاوه بر این، با تجزیه‌وتحلیل داده‌های مربوط به عملکرد سیستم‌ها، می‌توان الگوهای خرابی را شناسایی کرد و اقدامات پیشگیرانه را برای جلوگیری از اختلال در دسترس‌پذیری انجام داد (Wang et al., 2019).

۱-۱۴. شناسایی تأثیر فناوری‌های حوزه کلان‌داده بر رایانش شناختی

کلان‌داده و رایانش شناختی دو حوزه مهم و تحولی در فناوری‌های نوین هستند که با یکدیگر هم‌افزایی دارند. (Sechin Matoori et al., 2021) کلان‌داده به مدیریت و تحلیل حجم عظیمی از داده‌ها می‌پردازد، درحالی‌که رایانش شناختی تلاش می‌کند هوش مصنوعی را با الگوبرداری از عملکرد مغز انسان توسعه دهد. فناوری‌های کلان‌داده تأثیرات گسترده‌ای بر پیشرفت رایانش شناختی داشته‌اند و این دو حوزه در بسیاری از جنبه‌ها به یکدیگر وابسته‌اند (Guan et al., 2021). رایانش شناختی باهدف شبیه‌سازی فرایندهای شناختی انسان، مانند درک زبان، یادگیری، تصمیم‌گیری و حل مسائل پیچیده، به داده‌های گسترده و متنوع نیاز دارد (Sreedevi

et al., 2022). تحولات شتابان فناوری‌های نوظهور در فضای سایبری، به‌ویژه در زمینهٔ تحلیل کلان‌داده و هوشمندی مبتنی بر داده، نقش تعیین‌کننده‌ای در ارتقای امنیت ملی ایفا می‌کنند. مؤلفه «هوشمندی مبتنی بر داده» بیشترین رابطه مستقیم و مثبت را با امنیت ملی دارد که نشان‌دهنده اهمیت بهره‌گیری از الگوریتم‌های شناختی در شناسایی تهدیدات و فرصت‌های سایبری است. (ترقّی و همکاران،۱۴۰۴) این یافته‌ها با رویکرد رایانش شناختی در کلان‌داده‌ها هم‌راستا بوده و بیانگر آن است که تحلیل‌های پیشرفته رفتاری و الگوریتم‌های یادگیری ماشین می‌توانند به تصمیم‌گیری به‌هنگام و راهبردی در حوزه امنیت سایبری کمک کنند. فناوری کلان‌داده امکان پردازش، ذخیره‌سازی و تحلیل این حجم عظیم از داده‌ها را فراهم می‌کنند؛ بنابراین، کلان‌داده بستری حیاتی برای توسعه سیستم‌های شناختی است. در جدول (۲)، به برخی مؤلفه‌های تأثیرگذار فناوری کلان‌داده بر رایانش شناختی پرداخته شده است (Guan et al., 2021).

جدول ۲: مؤلفه‌های تأثیرگذار فناوری کلان‌داده بر رایانش شناختی

ردیف	عنوان	توضیحات
۱	دسترسی به داده‌های متنوع و گسترده	فناوری‌های کلان‌داده، ازجمله سیستم‌های مدیریت داده‌های حجیم مانند هدوپ و اسپارک، امکان جمع‌آوری و تحلیل داده‌های ساختاریافته، نیمه‌ساختاریافته و غیرساختاریافته را فراهم می‌کنند. این داده‌ها شامل متن، صوت، تصویر، ویدئو و داده‌های حسگرها هستند که برای آموزش و بهینه‌سازی الگوریتم‌های رایانش شناختی ضروری‌اند.
۲	افزایش دقت مدل‌های شناختی	کلان‌داده با ارائه داده‌های متنوع، به سیستم‌های شناختی کمک می‌کند تا الگوهای پیچیده‌تری را شناسایی و تحلیل کنند. این امر باعث بهبود دقت در پیش‌بینی‌ها، تصمیم‌گیری‌ها و یادگیری سیستم‌های شناختی می‌شود. به‌عنوان‌مثال: تحلیل داده‌های پزشکی برای تشخیص بیماری‌ها. پردازش زبان طبیعی برای درک بهتر زبان انسان.
۳	توسعه یادگیری عمیق و هوش مصنوعی	الگوریتم‌های یادگیری عمیق به حجم زیادی از داده‌ها برای آموزش نیاز دارند. فناوری‌های کلان‌داده، این داده‌ها را در مقیاس وسیع فراهم کرده و امکان تحلیل سریع آن‌ها را فراهم می‌کنند. شبکه‌های عصبی عمیق که در قلب رایانش شناختی قرار دارند، به‌شدت از این داده‌ها بهره‌مند می‌شوند.

ردیف	عنوان	توضیحات
۴	«پردازش بلادرنگ»[1]	فناوری‌های کلان‌داده مانند کافکا و استورم امکان پردازش بلادرنگ داده‌ها را فراهم می‌کنند. این ویژگی در بسیاری از کاربردهای رایانش شناختی، مانند تحلیل احساسات یا تشخیص تقلب در سیستم‌های مالی، اهمیت ویژه‌ای دارد.
۵	بهبود شخصی‌سازی و تعامل انسانی	با استفاده از کلان‌داده، سیستم‌های رایانش شناختی قادر به تحلیل عمیق رفتار و ترجیحات کاربران هستند. این مسئله منجر به بهبود تعامل انسان و ماشین و ارائه خدمات شخصی‌سازی‌شده می‌شود. نمونه‌هایی از این کاربردها شامل دستیارهای شخصی هوشمند مانند سیری و الکسا است.

۱-۱۵. اثر کلان‌داده‌های حوزه شناختی بر امنیت سایبری

کلان‌داده‌های حوزه شناختی تأثیرات چشمگیری بر امنیت سایبری دارند. این تأثیرات شامل بهبود شناسایی تهدیدها، ارتقای واکنش به حملات و تقویت پیش‌بینی و پیشگیری از حملات هستند. جدول (۳)، به برخی از این تأثیرات مهم پرداخته می‌شود (اعرابی و همکاران، ۱۴۰۳ب)

جدول ۳: اثر کلان‌داده‌های حوزه شناختی بر امنیت سایبری

ردیف	عنوان	توضیحات
۱	شناسایی تهدیدات پیشرفته	تحلیل الگوهای رفتاری: کلان‌داده‌های شناختی می‌توانند الگوهای رفتاری کاربران و سیستم‌ها را تحلیل کنند و هرگونه رفتار غیرعادی یا مشکوک را شناسایی کنند. این امر به شناسایی تهدیدات ناشناخته و پیچیده کمک می‌کند. یادگیری ماشین و هوش مصنوعی: با استفاده از تکنیک‌های پیشرفته یادگیری ماشین و هوش مصنوعی، سیستم‌ها می‌توانند تهدیدات جدید را بادقت بیشتری شناسایی کند.
۲	ارتقای واکنش به حملات	تشخیص سریع‌تر و دقیق‌تر: با استفاده از کلان‌داده‌ها، سیستم‌ها می‌توانند به‌سرعت اطلاعات مربوط به حملات را جمع‌آوری و تحلیل کنند و به واکنش‌های سریع‌تر و دقیق‌تر منجر شوند. خودکارسازی پاسخ‌ها: تحلیل‌های شناختی می‌توانند به خودکارسازی پاسخ‌ها به تهدیدات کمک کنند، مثلاً با

1. Real-Time Processing

ردیف	عنوان	توضیحات
		ایجاد سیاست‌های امنیتی پویا و تطبیق‌پذیر که به‌صورت خودکار اجرا می‌شوند.
۳	پیش‌بینی و پیشگیری از حملات	پیش‌بینی تهدیدات آینده: با تحلیل داده‌های تاریخی و الگوهای رفتاری، سیستم‌ها می‌توانند تهدیدات آینده را پیش‌بینی کنند و اقدامات پیشگیرانه را انجام دهند. تحلیل روندها و الگوها: کلان‌داده‌ها می‌توانند روندها و الگوهای بلندمدت را شناسایی کنند که ممکن است به حملات سایبری منجر شوند.
۴	افزایش آگاهی و آموزش	آموزش کارمندان: تحلیل داده‌های شناختی می‌تواند نقاط ضعف در رفتارهای امنیتی کارمندان را شناسایی کند و به آموزش‌های هدفمند برای بهبود آگاهی امنیتی منجر شود. ارتباطات و اطلاع‌رسانی: با استفاده از داده‌های شناختی، سازمان‌ها می‌توانند بهبودهای مستمری در روش‌های ارتباطات و اطلاع‌رسانی امنیتی ایجاد کنند.
۵	تقویت سیستم‌های احراز هویت	احراز هویت چندعاملی: استفاده از تحلیل‌های شناختی برای تقویت سیستم‌های احراز هویت چندعاملی می‌تواند از حملات فیشینگ و دسترسی‌های غیرمجاز جلوگیری کند. بیومتریک و تحلیل رفتاری: آن داده‌های شناختی می‌توانند به تحلیل داده‌های بیومتریک و رفتاری برای احراز هویت دقیق‌تر کمک کنند.

۱-۱۶. مدل‌های ارتقای امنیت سایبری متأثر از رایانش شناختی

رایانش شناختی به سیستم‌های کامپیوتری امکان می‌دهد تا مانند انسان فکر کرده و یاد بگیرند. این قابلیت‌ها تأثیر بسزایی در ارتقای امنیت سایبری داشته و مدل‌های جدیدی را برای مقابله با تهدیدات پیچیده امروزی ارائه می‌دهند. در جدول (۴)، به پنج مدل ارتقای امنیت سایبری متأثر از رایانش شناختی اشاره می‌شود (Ihor Sikorsky et al., 2024):

جدول ۴: پنج مدل ارتقای امنیت سایبری متأثر از رایانش شناختی

ردیف	عنوان	توضیحات
۱	شناسایی و پیشگیری از تهدیدات	تشخیص ناهنجاری‌های رفتاری: سیستم‌های رایانش شناختی با تحلیل حجم عظیمی از داده‌های شبکه و سیستم‌ها، می‌توانند الگوهای رفتاری عادی را یاد گرفته و هرگونه انحراف از این الگوها را به‌عنوان ناهنجاری و

ردیف	عنوان	توضیحات
	پیشرفته	تهدید بالقوه شناسایی کنند. این قابلیت به‌ویژه در تشخیص «حملات روز صفر»[1] که هنوز امضای مشخصی ندارند، بسیار مؤثر است. تحلیل تهدیدات چندوجهی: رایانش شناختی می‌تواند اطلاعات را از منابع مختلف مانند لاگ‌های سامانه، ترافیک شبکه، گزارش‌های امنیتی و حتی شبکه‌های اجتماعی جمع‌آوری و تحلیل کند تا دیدگاهی جامع از وضعیت امنیتی ارائه دهد و تهدیدات پیچیده را که از روش‌های مختلفی استفاده می‌کنند، شناسایی کند. پیش‌بینی تهدیدات: تحلیل روندهای حملات گذشته و اطلاعات موجود در مورد آسیب‌پذیری‌ها، سیستم‌های رایانش شناختی می‌توانند احتمال وقوع حملات آینده را پیش‌بینی کرده و اقدامات پیشگیرانه لازم را انجام دهند.
۲	مدیریت هوشمند آسیب‌پذیری	اولویت‌بندی آسیب‌پذیری‌ها: با توجه به حجم بالای آسیب‌پذیری‌های نرم‌افزاری و سخت‌افزاری، سیستم‌های رایانش شناختی می‌توانند با تحلیل میزان خطر، احتمال سوءاستفاده و تأثیر بالقوه هر آسیب‌پذیری، آن‌ها را اولویت‌بندی کرده و به تیم‌های امنیتی کمک کنند تا بر روی مهم‌ترین موارد تمرکز کنند پیشنهاد راه‌حل‌های اصلاحی: سیستم‌های رایانش شناختی می‌توانند با توجه به نوع آسیب‌پذیری و ساختار سامانه، راه‌حل‌های اصلاحی مناسب را پیشنهاد دهند و حتی در مواردی به‌طور خودکار آن‌ها را اعمال کنند. شناسایی آسیب‌پذیری‌های زنجیره‌ای: این سیستم‌ها قادرند آسیب‌پذیری‌هایی را که به‌تنهایی خطرناک نیستند؛ اما در ترکیب با یکدیگر می‌توانند منجر به حملات موفق شوند (آسیب‌پذیری‌های زنجیره‌ای) را شناسایی کنند.
۳	پاسخ خودکار به حوادث امنیتی	تشخیص و پاسخ سریع به حوادث: سیستم‌های رایانش شناختی می‌توانند با تحلیل علائم اولیه حملات، به‌سرعت آن‌ها را شناسایی کرده و اقدامات لازم برای مقابله با آن‌ها را به‌طور خودکار انجام دهند، مانند قرنطینه کردن سیستم‌های آلوده، مسدود کردن ترافیک مشکوک و بازیابی سیستم‌ها تحلیل ریشه علت حوادث: پس از وقوع یک حادثه امنیتی، سیستم‌های رایانش شناختی می‌توانند با تحلیل داده‌های موجود، علت اصلی حادثه را شناسایی کرده و از وقوع مجدد آن جلوگیری کنند یادگیری از حوادث گذشته: این سیستم‌ها می‌توانند از تجربیات حوادث

1. Zero-Day Attacks

ردیف	عنوان	توضیحات
		گذشته برای بهبود عملکرد خود در شناسایی و پاسخ به حوادث آینده استفاده کنند.
۴	احراز هویت و کنترل دسترسی پیشرفته	احراز هویت چندعاملی تطبیقی: سیستم‌های رایانش شناختی می‌توانند با تحلیل رفتار کاربر، موقعیت مکانی، زمان دسترسی و سایر عوامل، سطح ریسک هر درخواست دسترسی را ارزیابی کرده و در صورت نیاز، احراز هویت چندعاملی را درخواست کنند. مدیریت دسترسی مبتنی بر نقش و رفتار: این سیستم‌ها می‌توانند با تحلیل رفتار کاربران و وظایف شغلی آن‌ها، دسترسی‌های لازم را به‌طور خودکار تخصیص داده و از دسترسی‌های غیرمجاز جلوگیری کنند. تشخیص جعل هویت: سیستم‌های رایانش شناختی می‌توانند با تحلیل الگوهای رفتاری کاربران، مانند نحوه تایپ کردن، حرکات ماوس و الگوهای استفاده از سامانه، تلاش‌های جعل هویت را شناسایی کنند.
۵	تحلیل امنیتی داده‌های بزرگ	کشف الگوهای پنهان در داده‌های امنیتی: سیستم‌های رایانش شناختی می‌توانند با تحلیل حجم عظیمی از داده‌های امنیتی، الگوهای پنهانی را که نشان‌دهنده فعالیت‌های مخرب هستند، کشف کنند. این الگوها ممکن است در داده‌های سنتی قابل‌مشاهده نباشند. تجسم داده‌های امنیتی: این سیستم‌ها می‌توانند داده‌های امنیتی پیچیده را به‌صورت بصری نمایش دهند تا تحلیلگران امنیتی بتوانند به‌راحتی آن‌ها را درک کرده و تهدیدات را شناسایی کنند. شناسایی تهدیدات داخلی: با تحلیل رفتار کاربران و الگوهای دسترسی به داده‌ها، سیستم‌های رایانش شناختی می‌توانند تهدیدات داخلی را که توسط کارکنان سازمان یا افراد مجاز انجام می‌شوند، شناسایی کنند.

۱-۱۷. مطالعه چهار کشور آمریکا، چین، هند و آلمان در خصوص رایانش شناختی کلان‌داده‌ها و امنیت سایبری

چهار کشور آمریکا، چین، هند و آلمان که بیشترین توسعه رایانش شناختی در صنایع مختلف را دارند به‌عنوان مطالعه تطبیقی انتخاب شده است.

آمریکا: با رهبری فناوری‌های پیشرفته و زیرساخت‌های قوی، همچنان یکی از قدرت‌های اصلی در امنیت سایبری است. همکاری گسترده بین بخش خصوصی و دولتی، همراه با

سرمایه‌گذاری‌های عظیم در رایانش شناختی و تحلیل کلان‌داده، آمریکا را در خط مقدم مقابله با تهدیدات سایبری قرار داده است (Soni, 2020) (Dobrovolska et al., 2024).

چین: با مدل خاص خود در نظارت دولتی و امنیت سایبری از فناوری‌های کلان‌داده و رایانش شناختی برای تقویت امنیت ملی و اقتصادی بهره می‌برد (Lai, 2019).

هند: به‌عنوان یک کشور درحال‌توسعه با اقتصادی روبه‌رشد در حال سرمایه‌گذاری گسترده در زیرساخت‌های دیجیتال و امنیت سایبری است. رشد سریع استارتاپ‌ها و نوآوری‌ها نویدبخش آینده‌ای روشن برای این کشور است.

آلمان: به‌عنوان یکی از رهبران اروپا و مدافع حریم خصوصی داده‌ها تمرکز خود را بر استقلال سایبری و همکاری‌های بین‌المللی معطوف کرده است (Dörpinghaus, 2019).

جدول (۵)، کاربست رایانش شناختی در امنیت سایبری کشورهای منتخب را نشان می‌دهد.

جدول ۵: بررسی کاربرد رایانش شناختی کلان‌داده در امنیت سایبری کشورهای منتخب

صنعت	ایالات‌متحده	چین	آلمان	هند
امنیت سایبری	در ایالات‌متحده، رایانش شناختی برای شناسایی تهدیدات پیشرفته سایبری، تحلیل الگوهای حملات و ارائه پاسخ‌های سریع‌تر به رخدادهای امنیتی استفاده می‌شود. این فناوری در حفاظت از زیرساخت‌های حیاتی آمریکا نقش کلیدی دارد.	چین از رایانش شناختی برای تقویت دفاع سایبری ملی، تحلیل حملات پیچیده و پیش‌بینی تهدیدات آینده استفاده می‌کند. این فناوری در حفاظت از داده‌های شهروندان و زیرساخت‌های حیاتی بسیار پیشرفته است.	آلمان از رایانش شناختی برای تحلیل رفتارهای غیرعادی در شبکه‌ها، شناسایی تهدیدات سایبری در مراحل اولیه و بهبود امنیت اطلاعات در سازمان‌های دولتی و خصوصی بهره می‌برد.	در هند، از رایانش شناختی برای پیش‌بینی حملات سایبری، شناسایی نقاط ضعف شبکه‌ها و بهبود امنیت سیستم‌های دولتی و شرکت‌های خصوصی استفاده می‌شود. این فناوری به کاهش آسیب‌پذیری‌ها کمک می‌کند.

۲. الگوی مفهومی پژوهش

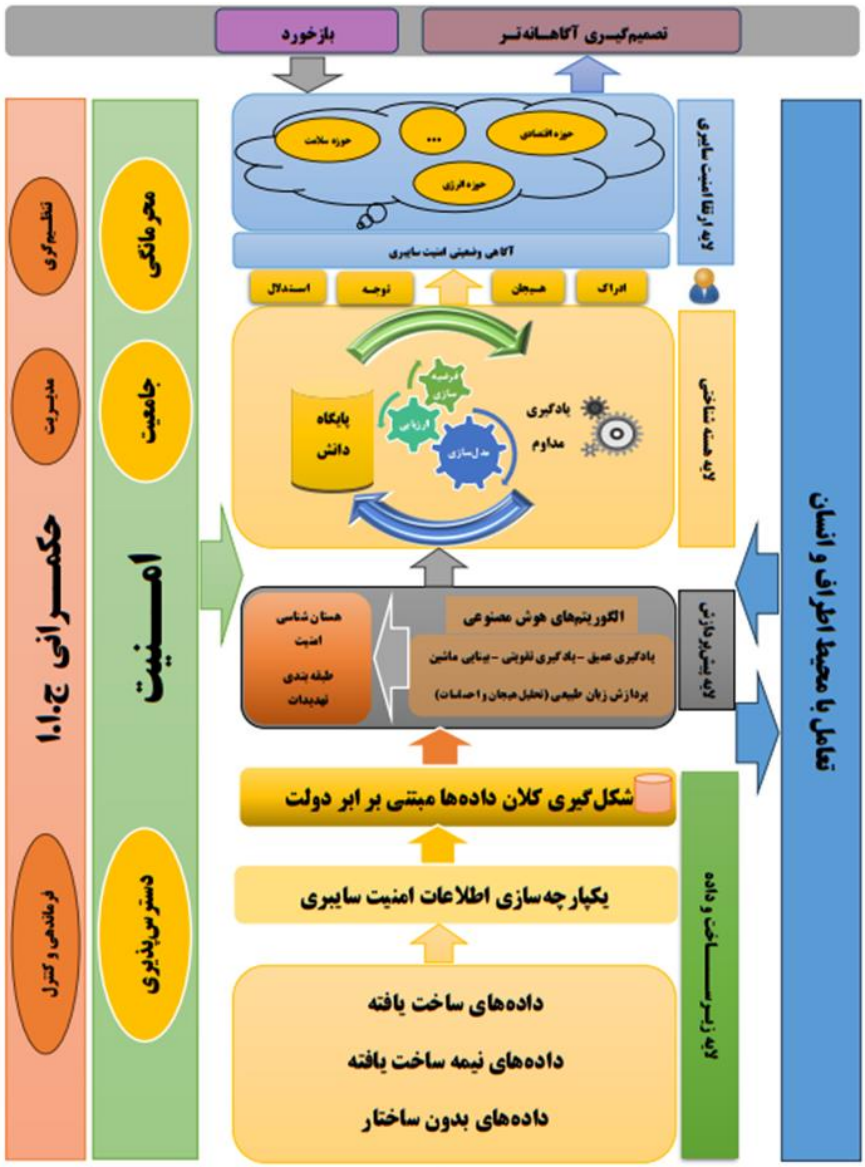
براساس مطالعه اسناد، کتب، رساله‌ها، مقالات و گزارش‌های متعدد در حوزه پژوهش و نتایج حاصل‌شده از انجام مصاحبه عمیق با خبرگان حوزه پژوهش و به‌کارگیری روش تحقیق تحلیل محتوا و عقلایی الگوی مفهومی نمایش داده شده در شکل (۱)، ارائه می‌گردد. این مدل ناظر به ادبیات نظری و تأیید خبرگان است. مدل مفهومی پیشنهادی، از یک معماری لایه‌ای با رویکرد پایین به بالا بهره می‌برد. در پایه‌ترین سطح، لایه زیرساخت و داده قرار دارد که وظیفه یکپارچه‌سازی داده‌های امنیت سایبری و تشکیل یک ابرداده دولتی یکپارچه را بر عهده دارد. خروجی این لایه، به‌عنوان ورودی لایه پیش‌پردازش عمل می‌کند. این لایه متشکل از الگوریتم‌های پیشرفته هوش مصنوعی (شامل یادگیری عمیق، یادگیری تقویتی، بینایی ماشین و پردازش زبان طبیعی)، همراه با هستان‌شناسی‌های امنیت و سیستم‌های طبقه‌بندی تهدیدات سایبری است که داده‌های خام را به اطلاعات معنادار تبدیل می‌کنند. خروجی پردازش‌شده این لایه، لایه هسته‌شناختی را تغذیه می‌کند. این هسته شامل مؤلفه‌های شناختی پیشرفته‌ای همچون موتورهای فرضیه‌سازی، ارزیابی، مدل‌سازی، یادگیری مستمر و یک پایگاه دانش پویا است. علاوه بر این، مؤلفه‌های شناخت انسانی شامل ادراک، هیجان، توجه و استدلال نیز در این لایه ادغام شده‌اند. برهم‌کنش این مؤلفه‌ها منجر به ظهور آگاهی وضعیتی در این زیست‌بوم می‌شود که تصمیم‌گیری در سطوح کلان مدیریتی را تقویت کرده و موجب ارتقای امنیت سایبری در حوزه‌های حیاتی مانند اقتصاد، انرژی و سلامت می‌گردد. سه رکن اساسی این زیست‌بوم، به‌صورت عمودی بر تمامی لایه‌های این مدل سایه افکنده‌اند:

۱. لایه امنیت که اصول سه‌گانه محرمانگی، جامعیت و دسترس‌پذیری را تضمین می‌کند؛

۲. لایه تعامل با محیط اطراف و انسان که به‌عنوان یکی از ویژگی‌های متمایز سیستم‌های رایانش شناختی، ارتباط پویای سامانه با محیط اطراف و کاربران انسانی را ممکن می‌سازد؛

۳. لایه حکمرانی متعالی که براساس اصول و ارزش‌های جمهوری اسلامی ایران طراحی شده و نقش یک چهارچوب فراگیر برای تنظیم‌گری، مدیریت، فرماندهی و کنترل در کل زیست‌بوم رایانش شناختی را ایفا می‌کند. پیاده‌سازی این زیست‌بوم در مقیاس ملی، نه‌تنها به

تصمیم‌گیری‌های آگاهانه‌تر در مواجهه با تهدیدات سایبری منجر خواهد شد، بلکه به‌واسطه مکانیسم‌های یادگیری مستمر و بازخورد سازنده، به‌تدریج از هوشمندی و کارایی بیشتری برخوردار خواهد شد.



شکل ۱: مدل مفهومی پژوهش

۳. روش‌شناسی پژوهش

این تحقیق با رویکرد آمیخته (کمی و کیفی) و به‌صورت توصیفی-تحلیلی و روش موردی-زمینه‌ای انجام‌شده است. پژوهش حاضر ازاین‌جهت توصیفی-تحلیلی است که برای گردآوری اطلاعاتی که مدون نشده به‌کار می‌رود و با توصیف عینی، واقعی و منظم موضوعات انجام می‌گردد و از این منظر موردی - زمینه‌ای است که مطالعه عمیق روی نمونه‌هایی از یک پدیده در محیط واقعی صورت می‌گیرد. با توجه به این‌که این تحقیق درصدد ارائه الگوی راهبردی براساس اسناد، مقالات، منابع و اندیشه‌ها و تجربیات خبرگان حوزه پژوهش بوده و موجب افزایش دانش موجود نسبت به موضوع تحقیق می‌شود، توسعه‌ای است و ازآن‌جهت که نتایج تحقیق برای مرکز رصد و پایش امنیت سایبری کشور کاربرد دارد، از نوع کاربردی است.

گردآوری داده‌ها با به‌کارگیری دو روش تحلیل محتوا و براساس تحقیقات کتابخانه‌ای شامل مقالات معتبر علمی و تخصصی، سایت‌های معتبر اینترنتی همچنین روش عقلایی براساس تحقیقات میدانی شامل مصاحبه عمیق و سپس تنظیم پرسش‌نامه انجام گردید. برای تحلیل داده‌های بخش کمی (داده‌های حاصل از پرسش‌نامه) از روش‌های آمار توصیفی و استنباطی ازجمله معادلات ساختاری، تحلیل واریانس، ضریب هم‌بستگی استفاده‌شده است.

به‌منظور اخذ نظر خبرگان جهت ارائه الگوی اولیه پژوهش، مصاحبه عمیق با نه نفر از مدیران و خبرگان مرتبط با حوزه شناختی، کلان‌داده و امنیت سایبری که دارای مسئولیت در سطوح میانی یا عالی مدیریتی یا اجرایی کشور هستند؛ صورت پذیرفت. سپس به‌منظور ارزیابی الگوی احصا شده، پرسش‌نامه‌ای براساس طیف لیکرت تنظیم گردید و به ۵۳ نفر از مدیران و کارشناسان حوزه تحقیق ارسال شد. پرسش‌نامه به لحاظ روایی ظاهری و محتوا به تأیید جمعی از اساتید رسانده شد و به لحاظ پایایی با استفاده از نرم‌افزار SPSS آلفای کرونباخ پرسش‌نامه ۰/۷۳۳ محاسبه شد که پایایی قابل قبولی محسوب می‌شود. برای محاسبات معادلات ساختاری نیز از نرم‌افزار Smart PLS بهره‌برداری گردید.

۴. تجزیه‌وتحلیل یافته‌ها

جهت بررسی هم‌بستگی داده‌ها، ابتدا باید پارامتری یا ناپارامتری داده‌ها مشخص شود. برای این منظور از آزمون کلموگروف- اسمیرنوف استفاده می‌گردد. براساس اطلاعات به‌دست‌آمده از نتیجه این آزمون، میزان sig متناظر با هر یک از داده‌ها برابر با ۰/۰۰۰ است؛ بنابراین داده‌های پرسش‌نامه از توزیع نرمال برخوردار نبوده و برای تحلیل استنباطی آن‌ها از آمار ناپارامتریک استفاده می‌شود. با توجه به ناپارامتری بودن داده‌ها، برای محاسبه ضریب هم‌بستگی از آزمون اسپیرمن بهره برده می‌شود.

۴-۱. بررسی ارتباط بین مؤلفه‌ها و ابعاد

ارتباط بین مؤلفه‌ها و ابعاد با استفاده از ضریب هم‌بستگی اسپیرمن محاسبه‌شده و نتایج آن به شرح ذیل است.

۴-۱-۱. هم‌بستگی بین ابعاد الگوی راهبردی رایانش شناختی کلان‌داده‌ها به‌منظور ارتقای امنیت سایبری جمهوری اسلامی ایران

جدول ۶: نتایج هم‌بستگی بین ابعاد الگوی راهبردی رایانش شناختی کلان‌داده‌ها

آماره / بُعد		کلان‌داده امنیت سایبری	پیش‌پردازش داده‌ها	هسته‌شناختی	امنیت	حکمرانی
الگوی راهبردی رایانش شناختی کلان‌داده‌ها به‌منظور ارتقای امنیت سایبری ج.ا.ایران	ضریب هم‌بستگی	۰/۴۰۰	۰/۷۴۸	۰/۸۴۵	۰/۳۲۳	۰/۴۷۸
	سطح معناداری	۰/۰۰	۰/۰۰	۰/۰۰	۰/۰۱	۰/۰۰

سطوح معناداری قیدشده در جدول (۶)، نشان می‌دهد که هم‌بستگی بین ابعاد و الگوی راهبردی رایانش شناختی کلان‌داده‌ها به‌منظور ارتقای امنیت سایبری جمهوری اسلامی ایران در تمامی موارد معنادار است که نشان‌دهنده وجود هم‌بستگی قوی بین این ابعاد و الگو است.

۴-۱-۲. هم‌بستگی بین مؤلفه‌های بُعد کلان‌داده امنیت سایبری و بُعد مذکور

جدول ۷: نتایج هم‌بستگی بین مؤلفه‌های بُعد کلان‌داده امنیت سایبری

بُعد / مؤلفه		زیرساخت مناسب برای ذخیره‌سازی	جمع‌آوری داده‌های امنیتی	یکپارچه‌سازی داده‌ها
کلان‌داده امنیت سایبری	ضریب هم‌بستگی	۰/۷۵۸	۰/۸۰۰	۰/۵۸۳
	سطح معناداری	۰/۰۰	۰/۰۰	۰/۰۰

سطوح معناداری در جدول (۷)، نشان می‌دهد که هم‌بستگی بین مؤلفه‌های بُعد کلان‌داده امنیت سایبری با بُعد مربوطه در سطح ۰/۰۰۰ معنادار است که نشان‌دهنده وجود هم‌بستگی معنادار و غیرتصادفی بین مؤلفه‌های مذکور و بُعد کلان‌داده امنیت سایبری است.

۴-۱-۳. هم‌بستگی بین مؤلفه‌های بعد پیش‌پردازش داده‌ها و بُعد مذکور

جدول ۸: نتایج هم‌بستگی بین مؤلفه‌های بُعد پیش‌پردازش داده‌ها

بُعد / مؤلفه		پردازش زبان طبیعی	یادگیری عمیق	بینایی ماشین	هستان‌شناسی و طبقه‌بندی تهدیدات
پیش‌پردازش داده‌ها	ضریب هم‌بستگی	۰/۳۵۸	۰/۶۴۱	۰/۷۱۹	۰/۶۲۹
	سطح معناداری	۰/۰۰	۰/۰۰	۰/۰۰	۰/۰۰

سطوح معناداری در جدول (۸)، نشان می‌دهد که در تمامی موارد، هم‌بستگی بین مؤلفه‌های بُعد پیش‌پردازش داده‌ها با بُعد مربوطه؛ با اطمینان بیش از ۹۹ درصد معنادار است؛ که نشان‌دهنده وجود هم‌بستگی قوی بین این مؤلفه‌ها و بُعد پیش‌پردازش داده‌ها است.

۴-۱-۴. هم‌بستگی بین مؤلفه‌های بُعد هسته‌شناختی و بُعد مذکور

جدول ۹: نتایج هم‌بستگی بین مؤلفه‌های بُعد هسته‌شناختی

بُعد / مؤلفه		تعامل با محیط و انسان	فرضیه‌سازی	مدل‌سازی	یادگیری پیوسته (تقویتی)	پایگاه دانش
هسته‌شناختی	ضریب هم‌بستگی	۰/۷۲۶	۰/۵۶۷	۰/۸۴۵	۰/۷۴۰	۰/۶۷۹
	سطح معناداری	۰/۰۰	۰/۰۰	۰/۰۰	۰/۰۰	۰/۰۰

سطوح معناداری قیدشده در جدول ۹ نشان می‌دهد که در تمامی موارد، هم‌بستگی بین مؤلفه‌های بُعد هسته‌شناختی با بعد مربوطه با اطمینان بیش از 99 درصد معنادار بوده که نشان از وجود هم‌بستگی قوی بین این مؤلفه‌ها و بُعد هسته‌شناختی دارد.

۴-۱-۵. هم‌بستگی بین مؤلفه‌های بعد امنیت و بعد مذکور

جدول ۱۰: نتایج هم‌بستگی بین مؤلفه‌های بُعد امنیت

بُعد / مؤلفه		محرمانگی	یکپارچگی	دسترس‌پذیری
امنیت	ضریب هم‌بستگی	۰/۷۴۳	۰/۶۸۰	۰/۴۲۹
	سطح معناداری	۰/۰۰	۰/۰۰	۰/۰۰

سطوح معناداری در جدول (۱۰)، نشان می‌دهد که در تمامی موارد، هم‌بستگی بین مؤلفه‌های بُعد امنیت با بُعد مربوطه؛ با اطمینان بیش از ۹۹ درصد معنادار است؛ که نشان‌دهنده وجود هم‌بستگی قوی بین این مؤلفه‌ها و بُعد امنیت است.

۴-۱-۶. هم‌بستگی بین مؤلفه‌های بعد حکمرانی و بعد مذکور

جدول ۱۱: نتایج هم‌بستگی بین مؤلفه‌های بُعد حکمرانی

بُعد	مؤلفه	حفظ حریم خصوصی	تنظیم‌گری	مدیریت	داده	فرماندهی و کنترل
حکمرانی	ضریب هم‌بستگی	۰/۵۳۰	۰/۵۳۶	۰/۶۷۸	۰/۶۱۵	۰/۷۶۸
	سطح معناداری	۰/۰۰	۰/۰۰	۰/۰۰	۰/۰۰	۰/۰۰

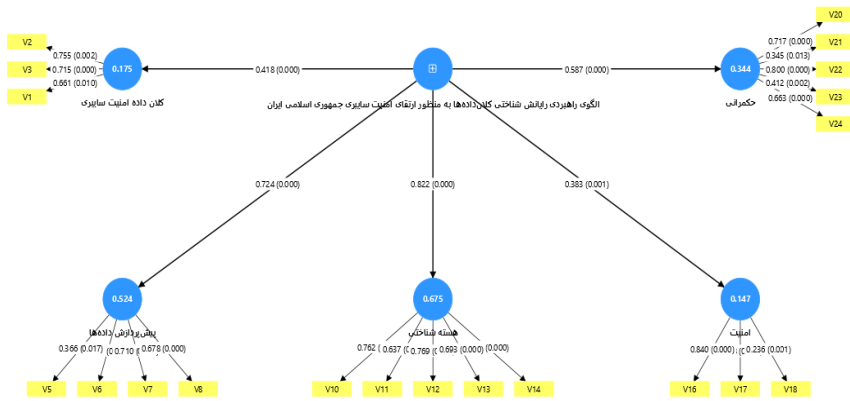
سطوح معناداری قیدشده در جدول (۱۱)، نشان می‌دهد که در تمامی موارد، هم‌بستگی بین مؤلفه‌های بُعد حکمرانی با بُعد مربوطه با اطمینان بیش از ۹۹ درصد معنادار بوده که نشان از وجود هم‌بستگی قوی بین این مؤلفه‌ها و بُعد حکمرانی دارد.

۴-۲. بررسی الگوی تحقیق

بررسی الگو این تحقیق براساس روش آماری «حداقل مربعات جزئی»[1] صورت پذیرفته است. این روش در قالب کلی «مدل معادلات ساختاری»[2] مطرح است. در این پژوهش برای انجام محاسبات فوق‌الذکر از نرم‌افزار Smart PLS استفاده‌شده است.

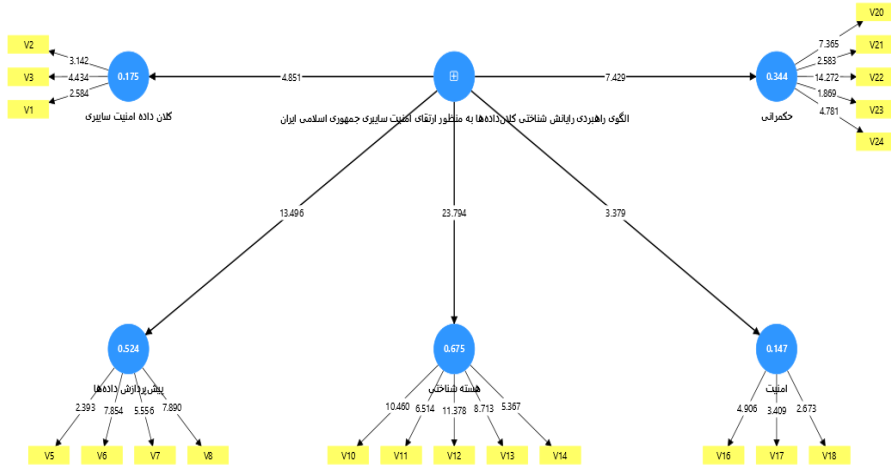
۱. الگوی ساختاری تحقیق: در شکل‌های (۲) و (۳)، الگوی ساختاری تحقیق به‌همراه ضرایب مسیر الگو، مقادیر t الگوی ساختاری و مقدار P ترسیم شده است.

1. Partial Least Squares
2. Structural Equation Modeling



شکل ۲: الگوی ساختاری تحقیق به‌همراه ضرایب مسیر الگو و مقدار P

در الگوی ساختاری شکل (۲)، ابعاد و مؤلفه‌های مورد تأیید نشان داده‌شده‌اند. در این الگو مؤلفه‌ها همان متغیرهای آشکار هستند که در مستطیل‌های زردرنگ به ابعاد مربوط به خود متصل شده‌اند. همچنین مقدار بار عاملی، ضرایب مسیر و مقدار P مربوط به ابعاد و مؤلفه‌ها نیز در الگو مشخص‌شده است. در شکل (۳)، نیز الگوی ساختاری تحقیق به‌همراه ضریب معناداری (آماره t) به تصویر درآمده است. با توجه به این‌که مقدار t برای تمام ابعاد و مؤلفه‌های پژوهش بیشتر از ۱/۹۶ است؛ بنابراین رابطه بین ابعاد و مؤلفه‌ها تأیید می‌شود.



شکل ۳: الگوی ساختاری تحقیق به‌همراه مقادیر t الگوی ساختاری

۴-۳. نتایج الگوی ساختاری

جدول ۱۲: نتایج حاصل از یافته‌های الگوی ساختاری تحقیق

روابط / شاخص	ضریب مسیر	انحراف استاندارد	مقدار t	سطح معناداری	نتیجه
کلان‌داده امنیت سایبری الگوی راهبردی رایانش شناختی کلان‌داده‌ها به‌منظور ارتقای امنیت سایبری جمهوری اسلامی ایران	۰/۵۸۷	۰/۰۸۶	۴/۸۵۱	۰/۰۱	تأیید رابطه
پیش‌پردازش داده‌ها الگوی راهبردی رایانش شناختی کلان‌داده‌ها به‌منظور ارتقای امنیت سایبری جمهوری اسلامی ایران	۰/۳۸۳	۰/۰۵۴	۱۳/۴۹۶	۰/۰۰	تأیید رابطه
هسته‌شناختی الگوی راهبردی رایانش شناختی کلان‌داده‌ها به‌منظور ارتقای امنیت سایبری جمهوری اسلامی ایران	۰/۸۲۲	۰/۰۳۵	۲۳/۷۹۴	۰/۰۰	تأیید رابطه
امنیت الگوی راهبردی رایانش شناختی کلان‌داده‌ها به‌منظور ارتقای امنیت سایبری ج.ا.ایران	۰/۴۱۸	۰/۱۱۳	۳/۳۷۹	۰/۰۰	تأیید رابطه
حکمرانی الگوی راهبردی رایانش شناختی کلان‌داده‌ها به‌منظور ارتقای امنیت سایبری جمهوری اسلامی ایران	۰/۷۲۴	۰/۰۷۹	۷/۴۲۹	۰/۰۰	تأیید رابطه

جدول (۱۲)، نشان می‌دهد که همه ضرایب الگوی ساختاری با سطح اطمینان ۹۹ درصد یا بیشتر به معناداری آماری رسیده‌اند. معناداری ضرایب آماری نشان می‌دهد که الگوی راهبردی رایانش شناختی کلان‌داده‌ها به‌منظور ارتقای امنیت سایبری جمهوری اسلامی ایران از ابعاد کلان‌داده امنیت سایبری، پیش‌پردازش داده‌ها، هسته‌شناختی، امنیت و حکمرانی تشکیل‌شده است. این نتایج، نشان می‌دهد که الگوی راهبردی رایانش شناختی کلان‌داده‌ها به‌منظور ارتقای امنیت سایبری جمهوری اسلامی ایران از استحکام بالایی برخوردار است.

۴-۴. نتایج الگوهای اندازه‌گیری

جدول ۱۳: نتایج حاصل از یافته‌های الگوی اندازه‌گیری تحقیق

روابط / شاخص	ضریب مسیر	انحراف استاندارد	مقدار t	سطح معناداری	نتیجه
زیرساخت مناسب برای ذخیره‌سازی کلان‌داده امنیت سایبری	۰/۶۶۱	۰/۲۵۶	۲/۵۸۴	۰/۰۱	تأیید رابطه
جمع‌آوری داده‌های امنیتی کلان‌داده امنیت سایبری	۰/۷۵۵	۰/۲۴۰	۳/۱۴۲	۰/۰۰	تأیید رابطه
یکپارچه‌سازی داده‌ها کلان‌داده امنیت سایبری	۰/۷۱۵	۰/۱۶۱	۴/۴۳۴	۰/۰۰	تأیید رابطه
پردازش زبان طبیعی پیش‌پردازش داده‌ها	۰/۳۶۶	۰/۱۵۳	۲/۳۹۳	۰/۰۱	تأیید رابطه
یادگیری عمیق پیش‌پردازش داده‌ها	۰/۷۰۱	۰/۰۸۹	۷/۸۵۴	۰/۰۰	تأیید رابطه
بینایی ماشین پیش‌پردازش داده‌ها	۰/۷۱۰	۰/۱۲۸	۵/۵۵۶	۰/۰۰	تأیید رابطه
هستان‌شناسی و طبقه‌بندی تهدیدات→ پیش‌پردازش داده‌ها	۰/۶۷۸	۰/۰۸۶	۷/۸۹۰	۰/۰۰	تأیید رابطه
تعامل با محیط و انسان هسته‌شناختی	۰/۷۶۲	۰/۰۷۳	۱۰/۴۶۰	۰/۰۰	تأیید رابطه
فرضیه‌سازی هسته‌شناختی	۰/۶۳۷	۰/۰۹۸	۶/۵۱۴	۰/۰۰	تأیید رابطه
مدل‌سازی هسته‌شناختی	۰/۷۶۹	۰/۰۶۸	۱۱/۳۷۸	۰/۰۰	تأیید رابطه
یادگیری پیوسته (تقویتی) هسته‌شناختی	۰/۶۹۳	۰/۰۸۰	۸/۷۱۳	۰/۰۰	تأیید رابطه
پایگاه دانش هسته‌شناختی	۰/۶۶۱	۰/۱۲۳	۵/۳۶۷	۰/۰۰	تأیید رابطه
محرمانگی امنیت	۰/۸۴۰	۰/۱۷۱	۴/۹۰۶	۰/۰۰	تأیید رابطه
یکپارچگی امنیت	۰/۷۵۸	۰/۲۲۲	۳/۴۰۹	۰/۰۰	تأیید رابطه
دسترس‌پذیری امنیت	۰/۲۳۶	۰/۳۵۰	۲/۶۷۳	۰/۰۰	تأیید رابطه
حفظ حریم خصوصی حکمرانی	۰/۷۱۷	۰/۰۹۷	۷/۳۶۵	۰/۰۰	تأیید رابطه
تنظیم‌گری حکمرانی	۰/۳۴۵	۰/۲۱۸	۲/۵۸۳	۰/۰۱	تأیید رابطه
مدیریت حکمرانی	۰/۸۰۰	۰/۰۵۶	۱۴/۲۷۲	۰/۰۰	تأیید رابطه
داده حکمرانی	۰/۴۱۲	۰/۲۲۱	۲/۸۶۹	۰/۰۰	تأیید رابطه
فرماندهی و کنترل حکمرانی	۰/۶۶۳	۰/۱۳۹	۴/۷۸۱	۰/۰۰	تأیید رابطه

نتایج جدول (۱۳)، نشان می‌دهد که مؤلفه‌های زیرساخت مناسب برای ذخیره‌سازی، جمع‌آوری داده‌های امنیتی، جمع‌آوری داده‌های امنیتی دارای تأثیر مثبت و معنادار بر بُعد کلان‌داده امنیت سایبری هستند. مؤلفه‌های پردازش زبان طبیعی، یادگیری عمیق، بینایی ماشین، هستان‌شناسی و طبقه‌بندی تهدیدات، دارای تأثیر مثبت و معنادار بر بُعد پیش‌پردازش داده‌ها هستند. مؤلفه‌های تعامل با محیط و انسان، فرضیه‌سازی، مدل‌سازی، یادگیری پیوسته (تقویتی) و پایگاه دانش دارای تأثیر مثبت و معنادار بر بُعد هسته‌شناختی هستند. مؤلفه‌های محرمانگی، یکپارچگی و دسترس‌پذیری دارای تأثیر مثبت و معنادار بر بعد امنیت هستند. مؤلفه‌های حفظ حریم خصوصی، تنظیم‌گری، مدیریت، داده و فرماندهی و کنترل دارای تأثیر مثبت و معنادار بر بعد حکمرانی هستند.

۵. نتیجه‌گیری و پیشنهاد

براساس یافته‌های پژوهش، الگوی راهبردی رایانش شناختی کلان‌داده‌ها به‌منظور ارتقای امنیت سایبری ج.ا.ایران به پنج بُعد و نوزده مؤلفه تقسیم‌بندی گردید. بُعد کلان‌داده امنیت سایبری به سه مؤلفه زیرساخت مناسب برای ذخیره‌سازی، جمع‌آوری داده‌های امنیتی و یکپارچه‌سازی داده‌ها تقسیم می‌گردد. بُعد پیش‌پردازش داده‌ها نیز به چهار مؤلفه پردازش زبان طبیعی، یادگیری عمیق، بینایی ماشین و هستان‌شناسی و طبقه‌بندی تهدیدات بخش‌بندی می‌شود؛ بعد هسته‌شناختی به پنج مؤلفه تعامل با محیط و انسان، فرضیه‌سازی، مدل‌سازی، یادگیری پیوسته (تقویتی) و پایگاه دانش دسته‌بندی می‌شود؛ بُعد امنیت به سه مؤلفه محرمانگی، یکپارچگی و دسترس‌پذیری تقسیم‌بندی می‌گردد و در نهایت بعد حکمرانی نیز به پنج مؤلفه حفظ حریم خصوصی، تنظیم‌گری، مدیریت، داده و فرماندهی و کنترل تقسیم می‌گردد. با توجه به ابعاد، مؤلفه‌ها و شاخص‌های نهایی شده که به تأیید ۵۳ نفر از خبرگان حوزه پژوهش رسیده است؛ الگوی راهبردی به شرح شکل (۴)، ارائه می‌گردد:



شکل ۴: الگوی راهبردی رایانش شناختی کلان‌داده‌ها به‌منظور ارتقای امنیت سایبری جمهوری اسلامی ایران

برای اجرای موفق الگوی راهبردی فوق، مجموعه‌ای از راهکارهای سیاستی، مدیریتی و فناورانه باید به‌صورت هماهنگ و هدفمند به‌کار گرفته شوند.

۵-۱. پیشنهادهای پژوهش

به‌عنوان ادامه پژوهش می‌توان به توسعه الگوهای رایانش شناختی مبتنی بر هوش مصنوعی پرداخت که براساس آن مدل‌های پیشرفته‌تری از رایانش شناختی مبتنی بر شبکه‌های عصبی عمیق و یادگیری تقویتی، در محیط‌های کلان‌داده طراحی و آزمایش می‌شوند تا قابلیت‌های تشخیص خودکار حملات سایبری بهبود یابد؛ همچنین بهینه‌سازی الگوریتم‌های شناختی برای محیط‌های توزیع‌شده و بررسی روش‌های بهینه‌سازی الگوریتم‌های رایانش شناختی در

محیط‌های توزیع‌شده و مرکزی نشده (مانند بلاک‌چین) به‌منظور افزایش مقیاس‌پذیری و کاهش تأخیر در تشخیص تهدیدها می‌تواند زمینه پژوهش‌های آینده قرار گیرد.

فهرست منابع

اعرابی، سید حمیدرضا؛ موحدی صفت، محمدرضا (۱۴۰۴). ***ارائه مدل مفهومی هم‌گرایی فناوری‌های نوظهور در زیست‌بوم رایانش شناختی به‌منظور ارتقای امنیت سایبری***. شناخت پژوهی مطالعات سیاسی، ۲(۱)

اعرابی، سید حمیدرضا؛ موحدی صفت، محمدرضا (۱۴۰۳ الف)، ***بررسی تأثیر هم‌گرایی رایانش ابری و کوانتومی بر زیست‌بوم رایانش شناختی***، نخستین همایش ملی عرصه جنگ‌شناختی: علوم و فناوری، دانشگاه مالک اشتر

اعرابی، سید حمیدرضا؛ موحدی صفت، محمدرضا (۱۴۰۳ ب)، ***نقش رایانش شناختی کلان‌داده‌ها در ارتقای امنیت سایبری***، سومین کنفرانس ملی محاسبات نرم و علوم شناختی، مینودشت.

ترقی، عبدالرضا؛ فیروزآبادی، ابوالحسن؛ بهنام نیا، علی‌اصغر؛ کریمی قهرودی، محمدرضا (۱۴۰۴). ***تأثیر فناوری‌های نوظهور فضای سایبر بر امنیت ملی***. امنیت ملی، ۱۵(۵۵).

References

Agilandeswari, V., Basheer, M., Bagchi, S., Menon, G., & Prasanna, P. M. (2024). *Cognitive computing in respiratory health: Revolutionizing medicine through artificial intelligence (AI) and machine learning (ML)*. International Journal of Advancement in Life Sciences Research, 7(3), 55-64.

Alsamhi, S. H., Kumar, S., Hawbani, A., Shvetsov, A. V., Zhao, L., & Guizani, M. (2024). *Synergy of human-centered AI and cyber-physical-social systems for enhanced cognitive situation awareness: Applications, challenges and opportunities*. Cognitive Computation, 1-21.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganán, C., Moore, T., Vasek, M. (2019). *Measuring the cost of cybercrime*. In R. Böhme, C. Moore, & M. Vasek (Eds.), The economics of information security and privacy (265-300). Springer, Cham.

Baltieri, M., Iizuka, H., Witkowski, O., Sinapayen, L., & Suzuki, K. (2023). *Hybrid life: Integrating biological, artificial, and cognitive systems*. Wiley Interdisciplinary Reviews: Cognitive Science, 14(6), e1662.

Cicirelli, F., Guerrieri, A., Mercuri, A., Spezzano, G., & Vinci, A. (2019). *Itema: A methodological approach for cognitive edge computing iot ecosystems*. Future Generation Computer Systems, 92, 189-197.

Dobrovolska, O., & Rozhkova, M. (2024). *Development of the country's sustainable cyberspace strategy to ensure the country's national security*. SocioEconomic Challenges, 8(2), 197-214.

Dörpinghaus, S. (2019). *Artificial intelligence in the cybersecurity of German small and medium sized enterprises* (Doctoral dissertation).

Guan, Y., & Chen, Q. (2021). *Research on Intelligent Perception and Cognitive Computing of Information Security System Based on Computer Big Data*. Wireless Communications and Mobile Computing, 2021(1), 3281825.

Guerrero, L. E., Castillo, L. F., Arango-Lopez, J., & Moreira, F. (2023). *A systematic review of integrated information theory: a perspective from artificial intelligence and the cognitive sciences*. Neural Computing and Applications, 1-33.

Helm, B. W. (2025). *Cognitivist theories of emotions in philosophy and affective science*. In Emotion theory: The Routledge comprehensive guide (408-428). Routledge.

Hilal, W., Gadsden, S. A., & Yawney, J. (2023). *Cognitive dynamic systems: A review of theory, applications, and recent advances*. Proceedings of the IEEE, 111(6), 575-622.

Ihor Sikorsky, K. P. I. (2024). *Cognitive modeling in cybersecurity: Review, basic cognitive model of cyber threat*. Theoretical and Applied Cybersecurity, 137.

Kelly, J. E., & Hamm, S. (2013). *Smart machines: IBM's Watson and the era of cognitive computing*. Columbia University Press.

Kshetri, N. (2018). *Blockchain's roles in meeting key supply chain management objectives*. International Journal of Information Management.

Lai, L. S. (2019). *The adoption of cognitive computing technology in China*. IT Professional, 21(6), 14-21.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Obi, O. C., Dawodu, S. O., Daraojimba, A. I., Onwusinkwue, S., Akagha, O. V., & Ahmad, I. A. I. (2024). *Review of evolving cloud computing paradigms: security, efficiency, and innovations*. Computer Science & IT Research Journal, 5(2), 270-292.

Saksono, H., & Parker, A. G. (2024). *Socio-cognitive framework for personal informatics: A preliminary framework for socially-enabled health technologies*. ACM Transactions on Computer-Human Interaction, 31(3), 1-41.

Sechin Matoori, S., & Nourafza, N. (2021). *Big data analytics and cognitive computing: A review study*. Journal of Business Data Science Research, 1(1), 23-32.

Soni, V. D. (2020). *Challenges and solution for artificial intelligence in cybersecurity of the USA*. Available at SSRN 3624487.

Sreedevi, A. G., Harshitha, T. N., Sugumaran, V., & Shankar, P. (2022). *Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review*. Information Processing & Management, 59(2), 102888.

Veniaminovich, L. E. (2024). *Artificial intelligence systems as systems for automating the process of scientific cognition and doubling the nomenclature of scientific specialties by using these systems for research in various fields of science*. Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета, (195), 74-110.

Wang, G., Atighehchian, P., Azimi, R., & Shoaran, M. (2019). *Failure prediction in cloud computing using machine learning techniques*. Journal of Cloud Computing, 8(1), 1-16.

Wang, Wenfeng, Deng, Xiangyang, Ding, Liang, Zhang, Limin (2020). *Brain-Inspired Intelligence and Visual Perception* (The Brain and Machine Eyes) || Neural Cognitive Computing Mechanisms. (booksc.org).

Xu, Z., Tian, Y., & Chen, X. (2020). *Anomaly detection based on machine learning: A survey*. IEEE Access.

Yampolskiy, R. V. (2018). *Artificial intelligence safety and security*. CRC Press.

Yang, X., Wang, Z., Hu, X. S., Kim, C. H., Yu, S., Pajic, M., Li, H. (2023). *Neuro-symbolic computing: Advancements and challenges in hardware-software co-design*. IEEE Transactions on Circuits and Systems II: Express Brie