تبیین قابلیت‌های هوش مصنوعی در مدیریت ریسک زنجیره‌ی تأمین منبع‌باز در چارچوب حکمرانی هوشمند

نوع مقاله:
پژوهشی اصیل

تاریخ ارسال: ۱٤۰٤/۰۹/۰۲
تاریخ بازنگری: ۱٤۰٤/۱۰/۱۷
تاریخ پذیرش: ۱٤۰٤/۱۲/۱۳
تاریخ چاپ: ۱٤۰۵/۰۳/۳۱

مشخصات نویسندگان:

۱. محمدحسن علیپور: گروه مدیریت، واحد سنندج، دانشگاه آزاد اسلامی، سنندج، ایران
۲. هیرش سلطان‌پناه*: گروه مدیریت، واحد سنندج، دانشگاه آزاد اسلامی، سنندج، ایران
۳. کامیار چالاکی: گروه مهندسی صنایع، واحد سنندج، دانشگاه آزاد اسلامی، سنندج، ایران
۴. سامان شیخ اسمعیلی: گروه مدیریت، واحد سنندج، دانشگاه آزاد اسلامی، سنندج، ایران

* پست الکترونیکی نویسنده مسئول: heirsh@iau.ac.ir

شیوه استناددهی: علیپور، محمدحسن.، سلطان‌پناه، هیرش.، چالاکی، کامیار.، و شیخ اسمعیلی، سامان. (۱۴۰۵). تبیین قابلیت‌های هوش مصنوعی در مدیریت ریسک زنجیره‌ی تأمین منبع‌باز در چارچوب حکمرانی هوشمند. *حکمرانی و شهر هوشمند*،۲(۱)، ۱۹-۱.

چکیده

پژوهش حاضر باهدف تبیین قابلیت‌های هوش مصنوعی در مدیریت ریسک زنجیرهی تأمین منبع‌باز در چارچوب حکمرانی هوشمند طراحی شد. این پژوهش از نوع پژوهش‌های کیفی است که به‌صورت میدانی و با استفاده از نظریه‌ی داده‌بنیاد اجرا شده است. مشارکت‌کنندگان در پژوهش شامل خبرگان آگاه به موضوع پژوهش بودند که از منظر علمی و عملی سوابق ارزشمندی در این خصوص داشتند. این افراد با استفاده از نمونه‌گیری هدفمند، با رویکرد نمونه‌گیری همگون و با رعایت حداکثر تنوع انتخاب شدند. نمونه‌گیری تا رسیدن به اشباع نظری پیش رفت. درنهایت تعداد ۱۳ مصاحبه در این خصوص انجام شد. ابزار گردآوری اطلاعات مصاحبه‌ی نیمه‌ساختاریافته بود. با توجه به نتایج نشان داد قابلیت‌های هوش مصنوعی در مدیریت ریسک زنجیرهی تأمین منبع‌باز در چارچوب حکمرانی هوشمند شامل پیش‌بینی و شناسایی پیش‌دستانهی ریسک‌ها؛ تحلیل هوشمند داده‌ها و ریسک‌های ساختاری؛ بهبود تصمیم‌گیری و مدیریت پاسخ به ریسک؛ نظارت، کنترل و پایش مستمر هوشمند؛ خودکارسازی و افزایش کارایی مدیریت ریسک است.

واژگان کلیدی: حکمرانی، شهر هوشمند، زنجیره‌ی تأمین، منبع‌باز.

Explaining the Capabilities of Artificial Intelligence in Open Source Supply Chain Risk Management within the Framework of Smart Governance

Article Type:
Original Research

Submit Date: 2025/11/23
Revise Date: 2026/01/07
Accept Date: 2026/03/04
Publish Date: 2026/06/21

Authors' Information:

1. Mohammadhassan Alipour: Department of management, Sa. C., Islamic Azad University, Sanandaj, Iran
2. Heirsh Sultanpanah*: Department of management, Sa. C., Islamic Azad University, Sanandaj, Iran
3. Kamyar Chalaki: Department of Industrial Engineering, Sa. C., Islamic Azad University, Sanandaj, Iran
4. Saman Sheikh Esmaeili: Department of management, Sa. C., Islamic Azad University, Sanandaj, Iran

* Corresponding author's email: heirsh@iau.ac.ir

How to cite this article: Alipour, M., Sultanpanah, H., Chalaki, K., & Sheikh Esmaeili, S. (2026). Explaining the Capabilities of Artificial Intelligence in Open Source Supply Chain Risk Management within the Framework of Smart Governance. Governance and Smart City, 2(1), 1-19.

Abstract

The present study was designed with the aim of explaining the capabilities of artificial intelligence in open source supply chain risk management within the framework of smart governance. The present study was a qualitative research that was implemented in the field. The qualitative method used in the present study was of the grounded theory type. The participants in the present study included experts aware of the research topic. The participants in this study were sampled using purposive sampling and with a homogeneous sampling approach while observing maximum diversity. This issue was shaped until theoretical saturation was reached. Finally, 13 interviews were conducted in this regard. These individuals included experts who were fully aware of the subject of the present study. In other words, they had valuable background in this regard from a scientific and practical perspective. The data collection tool in the present study was a semi-structured interview. According to the results of this study, it was determined that the capabilities of artificial intelligence in open source supply chain risk management within the framework of smart governance include proactive prediction and identification of risks, intelligent analysis of data and structural risks, improved decision-making and risk response management, intelligent continuous monitoring, control and surveillance, and automation and increased efficiency of risk management.

Keywords: *Governance, Smart City, Supply Chain, Open Source*

مقدمه

در سال‌های اخیر، توسعه‌ی فناوری‌های نوین اطلاعاتی و ارتباطی، به‌ویژه هوش مصنوعی، کلان‌داده و اینترنت اشیا، تحولات گسترده‌ای در شیوه‌های مدیریت، تصمیم‌گیری و حکمرانی ایجاد کرده است. این تحولات موجب شکل‌گیری مفهوم «حکمرانی هوشمند» شده است، که به‌مثابه‌ی یکی از ارکان اساسی شهرهای هوشمند، بر بهره‌گیری از فناوری‌های پیشرفته برای ارتقای کیفیت تصمیم‌گیری، افزایش شفافیت، بهبود پاسخ‌گویی و ارتقای کارایی فرایندهای مدیریتی تأکید دارد (Amft et al., 2024). حکمرانی هوشمند با ایجاد زیرساخت‌های فناورانه و اطلاعاتی، امکان جمع‌آوری، تحلیل و استفاده‌ی مؤثر از داده‌ها را فراهم کرده، به سازمان‌ها و نهادهای مدیریتی کمک می‌کند تا تصمیمات دقیق‌تر، سریع‌تر و مبتنی بر شواهد اتخاذ کنند (Han & Fang, 2024). در چارچوب حکمرانی هوشمند، استفاده از فناوری‌های هوشمند، به‌ویژه هوش مصنوعی، نقشی کلیدی در شناسایی، تحلیل و مدیریت ریسک‌ها ایفا می‌کند. هوش مصنوعی باقابلیت تحلیل حجم وسیعی از داده‌ها، شناسایی الگوها، پیش‌بینی رخدادهای آینده و پشتیبانی از تصمیم‌گیری یکی از ابزارهای مهم در بهبود فرایندهای حکمرانی شناخته می‌شود (Jackson et al., 2024). این قابلیت‌ها به سازمان‌ها کمک می‌کند تا ضمن افزایش شفافیت و هماهنگی، بتوانند ریسک‌های موجود در سیستم‌های پیچیده را به‌صورت مؤثرتر مدیریت کنند (Adenekan et al., 2024).

یکی از حوزه‌هایی که حکمرانی هوشمند و فناوری‌های هوشمند می‌توانند نقشی مهم در آن ایفا کنند، زنجیره‌ی تأمین منبع‌باز است. زنجیره‌ی تأمین منبع‌باز به‌دلیل ماهیت غیرمتمرکز، مشارکت ذی‌نفعان متعدد، وابستگی متقابل اجزا و پویایی زیاد با انواع مختلفی از ریسک‌ها مواجه است که می‌توانند عملکرد، امنیت و پایداری آن را تحت تأثیر قرار دهند (Younis et al., 2023). در چنین وضعیتی، استفاده از رویکردهای سنتی مدیریت ریسک به‌تنهایی پاسخ‌گوی پیچیدگی‌ها و عدم قطعیت‌های موجود نیست و نیاز به بهره‌گیری از رویکردهای هوشمند و مبتنی بر فناوری بیش از پیش احساس می‌شود. در این راستا، هوش مصنوعی، به‌عنوان یکی از مؤلفه‌های کلیدی حکمرانی هوشمند، می‌تواند با فراهم آوردن قابلیت‌هایی نظیر شناسایی هوشمند ریسک‌ها، تحلیل داده‌های پیچیده، پیش‌بینی تهدیدات بالقوه و پشتیبانی از تصمیم‌گیری نقش مؤثری در بهبود مدیریت ریسک در زنجیره‌ی تأمین منبع‌باز ایفا کند (Ayala et al., 2024). بهره‌گیری از این قابلیت‌ها می‌تواند منجر به افزایش شفافیت، کاهش عدم قطعیت، بهبود هماهنگی بین ذینفعان و ارتقای سطح تاب‌آوری زنجیره تأمین شود. بر این اساس، تبیین قابلیت‌های هوش مصنوعی در مدیریت ریسک زنجیره‌ی تأمین منبع‌باز در چارچوب حکمرانی هوشمند، می‌تواند گامی مهم در جهت بهبود فرایندهای مدیریتی و ارتقای کارایی سیستم‌های مبتنی بر منبع‌باز باشد (Zhu et al., 2021).

مدیریت ریسک در زنجیره‌ی تأمین به مجموعه‌ای از فعالیت‌ها و راهبردها اطلاق می‌شود که با هدف شناسایی، ارزیابی و کاهش تأثیرات احتمالی ریسک‌ها بر عملکرد زنجیره‌ی تأمین طراحی‌شده‌اند. با گسترش پیچیدگی‌ها و تغییرات محیطی در دهه‌های اخیر، مدل‌های متنوعی برای مدیریت ریسک در زنجیره‌ی تأمین معرفی شده‌اند که هر یک با رویکردی خاص به طبقه‌بندی و کنترل ریسک‌ها پرداخته‌اند (Younis et

al., 2023). این مدل‌ها در قالب دسته‌های مفهومی قابل‌تحلیل‌اند. مدل‌های سنتی واکنشی[1] بر پایه‌ی رویکردهای کلاسیک مدیریت بحران بناشده‌اند و عمدتاً بر واکنش به ریسک پس از وقوع آن تمرکز دارند. در این مدل‌ها، برنامه‌هایی برای بازیابی وضعیت و کاهش خسارات تدوین می‌شود، بااین‌حال کارایی آن‌ها در مواجهه با ریسک‌های نوظهور یا پیچیده محدود است (Tseng et al., 2022). در مقابل، مدل‌های پیش‌نگر[2] به شناسایی و پیش‌بینی ریسک‌ها پیش از وقوع آن‌ها می‌پردازند و بر اقدامات پیشگیرانه تأکید دارند. این مدل‌ها با بهره‌گیری از تحلیل سناریو، ارزیابی آسیب‌پذیری و طراحی زنجیره‌های تأمین منعطف، چرخه‌ای از شناسایی، ارزیابی، پاسخ و نظارت بر ریسک‌ها را شکل می‌دهند (Kalu et al., 2024).

از سوی دیگر، مدل‌های یکپارچه[3] مدیریت ریسک را در بستر کل سیستم زنجیره‌ی تأمین نهادینه می‌کنند. در این مدل‌ها، مدیریت ریسک جزئی از استراتژی کلان سازمان در نظر گرفته می‌شود و ریسک‌های داخلی و خارجی به‌صورت هم‌زمان ارزیابی می‌شوند (Zhu et al., 2021). با پیشرفت فناوری‌های اطلاعاتی، مدل‌های داده‌محور[4] نیز توسعه‌یافته‌اند که با تکیه بر کلان‌داده‌ها، الگوریتم‌های یادگیری ماشین و شبکه‌های عصبی، امکان پیش‌بینی دقیق ریسک‌های آتی را فراهم می‌کنند. این مدل‌ها به‌ویژه در ساختارهای منبع‌باز، که با تعاملات گسترده و غیرمتمرکز همراه‌اند، نقشی کلیدی ایفا می‌کنند (Younis et al., 2023). در محیط‌هایی با چندین ذی‌نفع فعال، مدل‌های مشارکتی[5] به‌عنوان راه‌حلی مؤثر برای مدیریت ریسک معرفی‌شده‌اند. این مدل‌ها با تأکید بر همکاری میان اجزای زنجیره‌ی تأمین، بسترهایی برای اشتراک‌گذاری اطلاعات، تدوین استانداردهای مشترک و تصمیم‌گیری جمعی فراهم می‌کنند. همچنین، مدل‌های مبتنی بر انعطاف‌پذیری[6] به‌جای کنترل مستقیم ریسک‌ها، به توسعه‌ی ظرفیت‌های سازمانی به‌منظور تاب‌آوری در برابر اختلالات می‌پردازند. تمرکز این مدل‌ها بر افزایش توان بازیابی سریع پس از بحران‌هاست (Zhu et al., 2021). درنهایت، مدل‌های مدیریت ریسک ویژه‌ی زنجیره‌های منبع‌باز[7] به‌گونه‌ای طراحی‌شده‌اند که پیچیدگی‌های محیط‌های غیرمتمرکز و داوطلب‌محور را لحاظ کنند. این مدل‌ها عمدتاً بر پایه‌ی مفاهیمی همچون شبکه‌های پیچیده، پویایی سیستم و مشارکت جوامع کاربرمحور توسعه‌یافته‌اند و رفتار غیرخطی و پیش‌بینی‌ناپذیر بازیگران را در نظر می‌گیرند (Younis et al., 2023).

زنجیره‌ی تأمین منبع‌باز به رویکردی نوین در تأمین کالاها و خدمات اشاره دارد که مبتنی بر همکاری و مشارکت بین سازمان‌ها و افراد است. در این نوع زنجیره‌ی تأمین، اطلاعات، منابع و فرایندها آزادانه در دسترس قرار می‌گیرند و همه‌ی ذی‌نفعان، از تأمین‌کنندگان و تولیدکنندگان تا مصرف‌کنندگان، می‌توانند در تولید و بهبود محصولات مشارکت کنند (Adenekan et al., 2024). یکی از ویژگی‌های کلیدی زنجیره‌ی تأمین منبع‌باز، تعدد تأمین‌کنندگان و مشارکت‌کنندگان است که موجب افزایش نوآوری و کاهش هزینه‌ها می‌شود. این رویکرد به سازمان‌ها امکان می‌دهد تا سریع‌تر به تغییرات بازار پاسخ دهند و از ایده‌ها و قابلیت‌های افراد و شرکت‌های مختلف بهره‌مند شوند (Han & Fang, 2024).

1 Reactive Models
2 Proactive Models
3 Integrated Models
4 Data-driven Models
5 Collaborative Models
6 Resilience Models
7 Open-source Risk Management Models

بااین‌حال، زنجیره‌ی تأمین منبع‌باز با چالش‌هایی نظیر عدم‌شفافیت، مشکلات مربوط به کنترل کیفیت و مسائل حقوقی مواجه است (Yang et al., 2024). ازجمله مزایای زنجیره‌ی تأمین منبع‌باز، افزایش سرعت در توسعه‌ی محصولات و خدمات، بهبود کیفیت و کاهش هزینه‌های تولید است. همچنین، این زنجیره‌ها قادرند با استفاده از ظرفیت‌های مشارکت‌کنندگان به‌راحتی نوآوری‌های جدیدی را معرفی کنند و به‌این‌ترتیب، رقابت‌پذیری بیش‌تری در بازارهای جهانی داشته باشند (Younis et al., 2023). علاوه بر این، زنجیره‌ی تأمین منبع‌باز به سازمان‌ها اجازه می‌دهد تا از خطرات حاصل از وابستگی به تأمین‌کنندگان واحد جلوگیری کنند و در عوض، به شبکه‌ای گسترده‌تر از منابع و تأمین‌کنندگان متکی باشند. این رویکرد، به‌ویژه در شرایط بحرانی یا تغییرات ناگهانی بازار، موجب افزایش انعطاف‌پذیری و پایداری زنجیره‌ی تأمین می‌شود. باوجوداین، برای بهره‌مندی حداکثری از زنجیره‌ی تأمین منبع‌باز، لازم است سازمان‌ها بینش واضحی از چالش‌ها و ریسک‌های مرتبط با آن داشته باشند. این شامل نیاز به استراتژی‌های مؤثر برای مدیریت ریسک‌های مختلف و همچنین استفاده از فناوری‌های مناسب برای تسهیل ارتباطات و همکاری‌ها در زنجیره‌ی تأمین است (Jackson et al., 2024).

زنجیره‌ی تأمین منبع‌باز مدلی نوین از زنجیره‌های تأمین است که بر مبنای اصول شفافیت، همکاری جمعی، اشتراک دانش و توسعه‌ی داوطلبانه شکل‌گرفته است. برخلاف زنجیره‌های تأمین سنتی که به‌صورت سلسله‌مراتبی و متمرکز اداره می‌شوند، زنجیره‌های منبع‌باز ماهیتی غیرمتمرکز، توزیع‌شده و مبتنی بر مشارکت داوطلبانه دارند (Adenekan et al., 2024). در این نوع زنجیره‌ها، بازیگران متعددی شامل توسعه‌دهندگان داوطلب، شرکت‌های تجاری، سازمان‌های دولتی، کاربران نهایی و نهادهای واسط حضور دارند که هر یک می‌توانند نقش‌های متفاوتی در طراحی، تولید، به‌روزرسانی، نگهداری و توزیع محصول ایفا کنند. ساختار این زنجیره‌ها پویا و غیرخطی است و به تعاملات آزاد میان مشارکت‌کنندگان وابسته است (Amft et al., 2024). یکی از ویژگی‌های کلیدی زنجیره‌ی تأمین منبع‌باز شفافیت اطلاعاتی است؛ بدین معنا که داده‌ها، کد منبع، فرایندها و نتایج به‌صورت عمومی در دسترس همه‌ی مشارکت‌کنندگان قرار دارند. این شفافیت موجب می‌شود فرایند تصمیم‌گیری، کنترل کیفیت و نوآوری به‌صورت جمعی انجام شود (Wermke et al., 2023). ویژگی مهم دیگر، مشارکت داوطلبانه و جامعه‌محور بودن است. در زنجیره‌های تأمین منبع‌باز، بسیاری از فرایندهای توسعه و نگهداری به‌وسیله‌ی گروه‌های داوطلب یا اجتماعات مختلف انجام می‌شود که انگیزه‌ی آن‌ها می‌تواند اقتصادی، فنی یا ایدئولوژیک باشد. از همین رو، زنجیره‌ی تأمین منبع‌باز مستعد ریسک‌هایی از جنس بی‌ثباتی منابع انسانی، ناپیوستگی مشارکت و پیش‌بینی‌ناپذیری زمان تحویل است (Adenekan et al., 2024). در این زنجیره‌ها همچنین مفهومی به نام زنجیره‌ی ارزش توزیع‌شده مطرح می‌شود که در آن خلق ارزش، نه در نهادی مشخص بلکه در تعامل مستمر بین نهادهای مختلف رخ می‌دهد. این ویژگی باعث شکل‌گیری ساختاری باز، تطبیق‌پذیر و مقیاس‌پذیر در برابر تغییرات محیطی می‌شود و مزیت رقابتی بزرگی ایجاد می‌کند، هرچند ریسک‌های سیستمی، امنیتی، اخلاقی و حقوقی خاص خود را نیز به همراه دارد. همچنین، زنجیره‌ی تأمین منبع‌باز به‌طور گسترده در حوزه‌هایی مانند نرم‌افزارهای آزاد و متن‌باز، پروژه‌های سخت‌افزاری متن‌باز و حتی در حوزه‌هایی نوظهور مانند داروسازی، کشاورزی و انرژی تجدیدپذیر استفاده شده است. بر این اساس، زنجیره‌ی تأمین منبع‌باز را می‌توان مدلی پویاتر، بازتر و مشارکتی‌تر از زنجیره‌های سنتی در نظر گرفت که ظرفیت زیادی برای نوآوری و چابکی دارد، اما به‌دلیل ساختار غیرمتمرکزش، نیازمند الگوهای خاصی

برای مدیریت ریسک، اطمینان از کیفیت و حفظ پایداری در عملکرد است (Amft et al., 2024).

زنجیره‌ی تأمین منبع‌باز نمایانگر تغییری در نحوه‌ی تعامل سازمان‌ها با یکدیگر و با بازار است که می‌تواند به بهبود کارایی و نوآوری در تمامی بخش‌ها منجر شود. این رویکرد به سازمان‌ها این فرصت را می‌دهد تا با استفاده‌ی بهینه از پتانسیل‌های موجود، به نتایج بهتری دست یابند و درعین‌حال، به نیازهای مشتریان و بازار پاسخ دهند (Adenekan et al., 2024). ازآنجاکه سازمان‌ها به‌طور فزاینده‌ای برای انعطاف‌پذیری و مقرون‌به‌صرفه بودن به زنجیره‌ی تأمین منبع‌باز اتکا دارند، با چالش‌های منحصربه‌فردی ازجمله آسیب‌پذیری‌های حاصل از کد تأییدنشده، وابستگی به مشارکت‌کنندگان خارجی و نقض‌های امنیتی احتمالی مواجه می‌شوند (Zhu et al., 2021). در این زمینه، حوادث پرمخاطب سبب شده‌اند بر اهمیت مدیریت ریسک مؤثر تأکید شود که درنتیجه، نیاز فوری به اقدامات امنیتی قوی در سراسر زنجیره‌ی تأمین منبع‌باز را برجسته می‌کند (Tseng et al., 2022). به‌طور کلی با گسترش روزافزون فناوری اطلاعات و ارتباطات، توجه صنایع مختلف به شکلی فزاینده به زنجیره‌ی تأمین منبع‌باز معطوف شده است. سیستم‌های منبع‌باز، به‌رغم مزایای قابل‌توجهی که دارند، ازجمله کاهش هزینه‌ها و افزایش انعطاف‌پذیری، با چالش‌های امنیتی متعددی نیز مواجه‌اند (Amft et al., 2024). تهدیدات سایبری، فقدان اعتماد به تأمین‌کنندگان و دشواری در حفظ اطلاعات حیاتی ازجمله‌ی این چالش‌ها به شمار می‌روند (Kalu et al., 2024). تحریم‌های بین‌المللی و شرایط اقتصادی خاص برخی کشورها این چالش‌ها را شدیدتر می‌کند، به‌گونه‌ای که می‌تواند به اختلال در زنجیره‌ی تأمین و کاهش کارایی منجر شود (حجازی فر و همکاران، ۱۴۰۳). به همین دلیل، شناسایی و تحلیل این مشکلات از اهمیت بسزایی برخوردار است. هوش مصنوعی می‌تواند ابزاری مؤثر در شناسایی و مدیریت تهدیدات امنیتی باشد. محققان نشان داده‌اند که استفاده از تکنیک‌های هوش مصنوعی مانند یادگیری ماشین، قادر است نقاط ضعف زنجیره‌ی تأمین را شناسایی و پیش‌بینی تهدیدات احتمالی را تسهیل کند (Sammak et al., 2023).

با گسترش روزافزون استفاده از سیستم‌ها و فناوری‌های مبتنی بر منبع‌باز در حوزه‌های مختلف، ازجمله زیرساخت‌های شهری، سامانه‌های اطلاعاتی و خدمات هوشمند، زنجیره‌ی تأمین منبع‌باز به یکی از اجزای کلیدی در توسعه و پایداری این سیستم‌ها تبدیل‌شده است. بااین‌حال، ماهیت غیرمتمرکز، وابستگی به مشارکت‌کنندگان متعدد، نبود ساختار کنترلی یکپارچه و پویایی زیاد این زنجیره‌ها آن‌ها را در معرض انواع مختلفی از ریسک‌ها، ازجمله ریسک‌های امنیتی، عملیاتی، کیفیتی و مدیریتی قرار داده است. این ریسک‌ها می‌توانند عملکرد سیستم‌های منبع‌باز را تحت تأثیر قرار دهند و پیامدهایی جدی برای سازمان‌ها، زیرساخت‌های هوشمند و فرایندهای حکمرانی داشته باشند. در چنین شرایطی، مدیریت مؤثر ریسک در زنجیره‌ی تأمین منبع‌باز به یکی از چالش‌های اساسی در حوزه‌ی حکمرانی هوشمند تبدیل‌شده است. از سوی دیگر، رویکردهای سنتی مدیریت ریسک به‌دلیل محدودیت در پردازش حجم زیاد داده‌ها، ناتوانی از تحلیل روابط پیچیده میان عوامل مختلف و ضعف در پیش‌بینی ریسک‌های نوظهور، توانایی پاسخ‌گویی کامل به پیچیدگی‌های زنجیره‌ی تأمین منبع‌باز را ندارند. در این راستا، هوش مصنوعی به‌عنوان یکی از فناوری‌های کلیدی در حکمرانی هوشمند، با قابلیت‌هایی نظیر تحلیل داده‌های گسترده، شناسایی الگوهای پنهان، پیش‌بینی رخدادهای احتمالی و پشتیبانی از تصمیم‌گیری، ظرفیت چشم‌گیری برای بهبود فرایند مدیریت ریسک دارد. بهره‌گیری از قابلیت‌های هوش مصنوعی می‌تواند به شناسایی دقیق‌تر ریسک‌ها، ارزیابی بهتر پیامدهای آن‌ها و ارائه‌ی راهکارهای مؤثر برای کاهش و کنترل

ریسک منجر شود. باوجود اهمیت روزافزون هوش مصنوعی در بهبود فرایندهای مدیریتی و نقش آن در تحقق حکمرانی هوشمند، بررسی‌های انجام‌شده نشان می‌دهند هنوز چارچوب مشخص و جامعی برای تبیین قابلیت‌های هوش مصنوعی در مدیریت ریسک زنجیره‌ی تأمین منبع‌باز ارائه نشده است و بسیاری از مطالعات موجود، به بررسی کلی کاربردهای هوش مصنوعی یا مدیریت ریسک پرداخته‌اند و کم‌تر به‌صورت یکپارچه به نقش قابلیت‌های هوش مصنوعی در مدیریت ریسک در این نوع خاص از زنجیره‌های تأمین توجه کرده‌اند. این خلأ پژوهشی، ضرورت انجام مطالعاتی را که بتوانند قابلیت‌های هوش مصنوعی را در زمینه‌ی مدیریت ریسک زنجیره‌ی تأمین منبع‌باز در چارچوب حکمرانی هوشمند تبیین کنند، بیش از پیش آشکار می‌کند. بر این اساس، پژوهش حاضر باهدف تبیین قابلیت‌های هوش مصنوعی در مدیریت ریسک زنجیره‌ی تأمین منبع‌باز در چارچوب حکمرانی هوشمند انجام‌شده است. نتایج این پژوهش می‌تواند ضمن کمک به درک بهتر نقش هوش مصنوعی در بهبود فرایندهای مدیریت ریسک، زمینه‌ی لازم برای توسعه‌ی رویکردهای هوشمند در مدیریت زنجیره‌ی تأمین منبع‌باز را فراهم آورد و به ارتقای کارایی، شفافیت و تاب‌آوری سیستم‌های مبتنی بر منبع باز در چارچوب حکمرانی هوشمند کمک کند. همچنین، یافته‌های این پژوهش می‌تواند در اتخاذ تصمیمات مؤثرتر و کاهش ریسک‌های مرتبط با زنجیره‌ی تأمین منبع‌باز برای مدیران، سیاست‌گذاران و ذی‌نفعان حوزه‌ی حکمرانی هوشمند مفید واقع شود.

روش‌شناسی

پژوهش حاضر از نوع پژوهش‌های کیفی بود که به‌صورت میدانی اجرایی شد. روش کیفی استفاده‌شده نظریه‌ی داده‌بنیاد[1] از نوع گلیزر[2] بود. جامعه‌ی آماری بخش کیفی پژوهش شامل نخبگان و خبرگان آگاه به حوزه‌ی زنجیره‌ی تأمین منبع‌باز در صنعت فناوری اطلاعات و نرم‌افزار بود. ماهیت چندبعدی و پیچیده‌ی موضوع پژوهش ــ به‌ویژه پیوند میان زنجیره‌ی تأمین منبع‌باز، مدیریت ریسک و کاربردهای هوش مصنوعی ــ ایجاب می‌کرد اطلاعات از افرادی گردآوری شود که دارای دانش تخصصی، تجربه‌ی عملی و شناخت عمیق از روندهای فناورانه و امنیتی در این حوزه باشند. بر همین اساس، جامعه‌ی آماری شامل متخصصانی بود که در یکی از حوزه‌های مدیریت زنجیره‌ی تأمین در صنایع دیجیتال، توسعه یا مدیریت پروژه‌های متن‌باز، امنیت زنجیره‌ی تأمین نرم‌افزار، مدیریت ریسک در سامانه‌های نرم‌افزاری، کاربرد هوش مصنوعی در تحلیل و پایش ریسک، و یا مدیریت عملیات فناوری اطلاعات (مانند DevOps، SRE، امنیت نرم‌افزار و غیره) تجربه و شناخت معتبری داشته باشند.

در این پژوهش، نمونه‌گیری در بخش کیفی به‌صورت هدفمند و با رویکرد قضاوتی-خبره‌محور انجام شد. با توجه به آن‌که هدف مرحله‌ی کیفی استخراج مفاهیم، شناخت الگوهای پدیده و تدوین مدل اولیه بود، استفاده از این روش امکان انتخاب افرادی را فراهم می‌کرد که بیش‌ترین آگاهی و تجربه را در حوزه‌ی پژوهش داشته باشند. به‌منظور غنی‌سازی داده‌ها، درصورت نیاز، از روش گلوله‌برفی نیز استفاده شد تا نظرات متخصصانی که به‌وسیله‌ی خبرگان اولیه معرفی می‌شوند نیز بررسی شود. حجم نمونه در پژوهش‌های کیفی به عدد ثابت وابسته نیست و بر اساس اصل اشباع نظری مشخص می‌شود. در این پژوهش مصاحبه‌ها تا جایی ادامه یافت که اطلاعات جدیدی حاصل نشود و دسته‌بندی‌های

[1] Grounded theory
2 Glaser

مفهومی ثبات پیدا کنند؛ به‌طوری‌که بر اساس تجربیات مطالعات مشابه، با مصاحبه با ۱۴ نفر اشباع نظری شکل گرفت. افراد انتخاب‌شده برای این‌که درک عمیقی از موضوع پژوهش داشته باشند، باید دست‌کم دارای شرایطی نظیر سابقه‌ی تحصیلی مرتبط شامل تحصیلات دانشگاهی در یکی از رشته‌های مدیریت زنجیره‌ی تأمین، مهندسی نرم‌افزار، فناوری اطلاعات، امنیت سایبری، مدیریت فناوری یا رشته‌های نزدیک می‌بودند. همچنین برخورداری از دست‌کم ۵ سال سابقه‌ی شغلی یا پژوهشی در زمینه‌هایی مانند مدیریت یا تحلیل زنجیره‌ی تأمین دیجیتال، توسعه یا نگهداری پروژه‌های متن‌باز، مدیریت امنیت نرم‌افزار و زنجیره‌ی تأمین، فعالیت در حوزه‌های توسعه و عملیات (DevOps)، مهندسی قابلیت اطمینان سایت (SRE) یا مدیریت سیستم‌های نرم‌افزاری و همچنین پژوهش یا مشاوره‌ی حرفه‌ای مرتبط با مدیریت ریسک در فناوری اطلاعات از دیگر معیارهای ورود بود. علاوه بر این موارد، داشتن دانش و آگاهی تخصصی شامل آشنایی عمیق با مفاهیم زنجیره‌ی تأمین منبع‌باز، آگاهی از چالش‌های امنیتی و ریسک‌های مرتبط و شناخت نقش هوش مصنوعی در تحلیل، پیش‌بینی یا مدیریت ریسک، در کنار توانایی مشارکت مؤثر، تمایل و امکان حضور در مصاحبه و توانایی بیان تجربه، تحلیل و توصیف فرایندها ضروری بود.

در مقابل، افرادی که فاقد دانش فنی یا عملیاتی لازم در خصوص زنجیره‌ی تأمین منبع‌باز در صنعت فناوری اطلاعات و نرم‌افزار بودند یا تجربه‌ی کاری معتبری در حوزه‌های مرتبط با زنجیره‌ی تأمین، امنیت نرم‌افزار یا مدیریت ریسک نداشتند، از نمونه‌ی کیفی کنار گذاشته شدند. افزون بر این، ناآشنایی با کاربردهای هوش مصنوعی در تحلیل یا مدیریت ریسک، عدم تمایل یا عدم امکان حضور در مصاحبه و همچنین عدم امکان ارائه‌ی اطلاعات معتبر به‌دلیل محدودیت‌های سازمانی یا شخصی، از دیگر معیارهای خروج از مطالعه به شمار می‌رفت.

به‌طور کلی در مرحله‌ی کیفی پژوهش، تمرکز بر انتخاب افرادی بود که بتوانند بیشترین داده‌های تخصصی و معتبر را در مورد ریسک‌های زنجیره‌ی تأمین منبع‌باز و نقش هوش مصنوعی ارائه کنند تا این بخش بتواند مبنای طراحی مدل اولیه و اساس مرحله‌ی کمّی پژوهش را تشکیل دهد.

ابزار گردآوری اطلاعات در پژوهش حاضر مصاحبه‌ی نیمه‌ساختاریافته بود. برای بررسی روایی از قابلیت باورپذیری (اعتبار)، انتقال‌پذیری و تأییدپذیری استفاده شد. برای بررسی قابلیت باورپذیری از تأیید فرایند پژوهش به‌وسیله‌ی هفت متخصص استفاده شد. همچنین دو کدگذار برای کدگذاری چند نمونه مصاحبه به کار گرفته شدند تا از یکسانی دیدگاه کدگذاران اطمینان حاصل شود. علاوه بر این، برای بررسی انتقال‌پذیری ازنظرات سه متخصص استفاده شد که در پژوهش مشارکت نداشتند، ولی در مورد یافته‌های پژوهش با آن‌ها مشورت شد. همچنین به‌منظور بررسی قابلیت تأییدپذیری، تمامی مصاحبه‌ها ثبت و ضبط و در زمان‌های موردنیاز برسی شدند. برای بررسی پایایی، از کمیته‌های تخصصی استفاده شد، بدین‌صورت که از اعضای این کمیته‌های تخصصی برای کدگذاری موازی برخی مصاحبه‌ها و همچنین ارزیابی و برنامه‌های مربوط به مصاحبه‌ها کمک گرفته شد. کدگذاری در این پژوهش به دو صورت شامل کدگذاری اولیه و کدگذاری ثانویه انجام شد. کدگذاری اولیه شامل خواندن خط‌به‌خط داده‌ها، استخراج مفاهیم و جملات اصلی، تشکیل مقولات و طبقات اولیه بود. کدگذاری ثانویه شامل طبقه‌بندی داده‌ها، مشخص کردن زیرطبقات و تشکیل طبقات نهایی بود. به‌منظور تجزیه‌وتحلیل داده‌های کیفی، از تحلیل موضوعی استفاده شد که از کارآمدترین روش‌های تحلیل داده‌های کیفی به‌ویژه در پژوهش‌های داده‌بنیاد است. طی انجام این تحلیل، مضمون‌های فرعی

و اصلی در خصوص اهداف پژوهش شناسایی شدند. همچنین به‌منظور بررسی یافته‌های جمعیت‌شناختی مربوط به مشارکت‌کنندگان از آمار توصیفی شامل فراوانی و درصد استفاده شد.

یافته‌ها

یافته‌های توصیفی مربوط به مشارکت‌کنندگان پژوهش حاضر در جدول ۱ به نمایش گذاشته شده است.

جدول ۱. ویژگی‌های مشارکت‌کنندگان

نمونه	جنسیت	تحصیلات
مصاحبه‌شونده‌ی ۱	زن	دکتری
مصاحبه‌شونده‌ی ۲	مرد	کارشناسی ارشد
مصاحبه‌شونده‌ی ۳	زن	کارشناسی
مصاحبه‌شونده‌ی ۴	مرد	کارشناسی
مصاحبه‌شونده‌ی ۵	زن	دکتری
مصاحبه‌شونده‌ی ۶	مرد	دکتری
مصاحبه‌شونده‌ی ۷	مرد	دکتری
مصاحبه‌شونده‌ی ۸	مرد	کارشناسی ارشد
مصاحبه‌شونده‌ی ۹	مرد	دکتری
مصاحبه‌شونده‌ی ۱۰	مرد	کارشناسی ارشد
مصاحبه‌شونده‌ی ۱۱	زن	کارشناسی ارشد
مصاحبه‌شونده‌ی ۱۲	زن	دکتری
مصاحبه‌شونده‌ی ۱۳	مرد	کارشناسی ارشد

جدول ۲ بخشی از مصاحبه‌های پژوهش را نشان می‌دهد.

جدول ۲. بخشی از مصاحبه‌های پژوهش

متن مصاحبه	کد استخراجی (کدباز)	شماره‌ی مصاحبه‌شونده
ساختار غیرمتمرکز جامعه‌های متن‌باز باعث می‌شود تصمیم‌گیری سریع در مواقع بحران دشوار باشد. برای اعمال تغییری اساسی باید نظر افراد مختلف جلب شود و این فرایند زمان‌بر است. در برخی موارد فرصت واکنش سریع از دست می‌رود.	کندی تصمیم‌گیری جمعی	مصاحبه‌ی ۴
تحریم‌ها و محدودیت‌های بین‌المللی باعث شده است برخی خدمات یا ابزارها برای ما در دسترس نباشند. حتی در مواردی دسترسی به مخازن اصلی قطع شده و مجبور به استفاده از مسیرهای جایگزین شده‌ایم. این موضوع سطح ریسک عملیاتی را افزایش داده است.	ریسک ژئوپلیتیکی	مصاحبه‌ی ۵
کیفیت خروجی در پروژه‌های منبع‌باز همیشه یکنواخت نیست. وقتی مشارکت فعال کاهش پیدا می‌کند، سرعت رفع باگ‌ها و به‌روزرسانی‌ها هم کم می‌شود. این موضوع بر اعتماد کاربران نهایی تأثیر می‌گذارد.	نوسان کیفیت درنتیجه‌ی مشارکت داوطلبانه	مصاحبه‌ی ۶
ما چارچوب مشخصی برای ارزیابی میزان ریسک هر ماژول متن‌باز نداریم. انتخاب ابزارها بیش‌تر مبتنی بر تجربه‌ی تیم فنی است تا تحلیلی ساختاریافته. این موضوع باعث فقدان انسجام در مدیریت ریسک می‌شود.	فقدان سیستم ارزیابی ریسک	مصاحبه‌ی ۸
شفافیت کامل کدها از یک جهت مزیت است، اما از جهت دیگر رقبا می‌توانند به‌سرعت از ایده‌ها استفاده کنند. برای شرکت‌هایی که مدل درآمدی دارند، این مسئله نوعی ریسک رقابتی ایجاد می‌کند.	ریسک افشای دانش رقابتی	مصاحبه‌ی ۱۳

متن مصاحبه	کد استخراجی (کدباز)	شماره‌ی مصاحبه‌شونده
در چند مورد مشاهده کردیم توسعه‌دهندگان کلیدی بدون اطلاع قبلی پروژه را ترک کردند. چون جایگزین آماده‌ای وجود نداشت، پیشرفت پروژه متوقف شد. این مسئله نشان‌دهنده‌ی ناپایداری منابع انسانی در این فضاست.	خروج ناگهانی مشارکت‌کنندگان	مصاحبه‌ی ۱۲
در پروژه‌های منبع‌باز که ما درگیر آن هستیم، معمولاً چند نفر نقش کلیدی دارند که عملاً دانش اصلی سیستم در اختیار آن‌هاست. اگر یکی از این افراد به هر دلیل کنار بکشد، تیم برای جایگزینی او با مشکل جدی مواجه می‌شود. این موضوع باعث شده همیشه نگران تداوم همکاری نیروهای کلیدی باشیم.	وابستگی به افراد کلیدی	مصاحبه‌ی ۱
ازنظر حقوقی، ما همیشه دغدغه‌ی تفسیر لایسنس‌های متن‌باز را داریم. بعضی لایسنس‌ها محدودیت‌هایی دارند که اگر دقیق رعایت نشود ممکن است در آینده برای شرکت تبعات قانونی ایجاد کند. این عدم‌قطعیت تصمیم‌گیری را سخت‌تر می‌کند.	ابهام در لایسنس و مالکیت معنوی	مصاحبه‌ی ۲
یک بار به‌دلیل وجود یک آسیب‌پذیری در یک کتابخانه‌ی متن‌باز، کل زیرساخت ما دچار اختلال شد. چون آن کتابخانه در چند بخش سیستم استفاده‌شده بود، اصلاح آن زمان‌بر و پرهزینه بود. این تجربه نشان داد ریسک امنیتی در این فضا به‌شدت سیستمی است.	سرایت‌پذیری ریسک امنیتی	مصاحبه‌ی ۳
در برخی پروژه‌ها تعارض بین اهداف تجاری شرکت و ارزش‌های جامعه‌ی متن‌باز ایجاد تنش می‌کند. جامعه به شفافیت و آزادی بیش‌تر تمایل دارد، اما شرکت دغدغه‌ی درآمد و کنترل دارد. این تعارض گاهی تصمیم‌گیری را پیچیده می‌کند.	تعارض منافع ذی‌نفعان	مصاحبه‌ی ۹
مستندسازی در بسیاری از پروژه‌های متن‌باز کامل نیست و این موضوع فرایند یادگیری تیم‌های جدید را دشوار می‌کند. برای درک ساختار سیستم باید زمان زیادی صرف بررسی کدها شود. این مسئله بهره‌وری را کاهش می‌دهد.	ضعف مستندسازی فنی	مصاحبه‌ی ۱۰
به نظر من اگر از ابزارهای هوش مصنوعی برای تحلیل الگوهای خطا و پیش‌بینی آسیب‌پذیری استفاده شود، می‌توانیم بخشی از ریسک‌ها را قبل از وقوع مدیریت کنیم. در حال حاضر این کار بیش‌تر واکنشی است تا پیش‌نگر.	ظرفیت پیش‌بینی با هوش مصنوعی	مصاحبه‌ی ۱۴
تغییرات ناگهانی در سیاست‌های یک پلتفرم میزبان باعث شد بخشی از زیرساخت ما نیاز به بازطراحی داشته باشد. این موضوع خارج از کنترل ما بود و هزینه‌ی اضافی ایجاد کرد. چنین وابستگی‌هایی ریسک سیستم را افزایش می‌دهند.	وابستگی به سیاست‌های پلتفرمی	مصاحبه‌ی ۱۱
یکی از مشکلات ما نبود یک سیستم یکپارچه برای پایش تغییرات است. تغییرات در مخازن مختلف ثبت می‌شوند، اما تصویر کلی از وضعیت ریسک وجود ندارد. معمولاً بعد از بروز مشکل متوجه آن می‌شویم.	ضعف پایش مستمر	مصاحبه‌ی ۷

جدول ۳، نتایج مربوط به کدهای استخراجی و فراوانی آن‌ها را نشان می‌دهد.

جدول ۳. نتایج کدگذاری باز

ردیف	کدهای استخراجی	فراوانی	مقدار آنتروپی	ضریب اهمیت
۱	پیش‌بینی آسیب‌پذیری‌های امنیتی در مخازن متن‌باز	۷	۰/۷۸۲۵۱۷	۰/۰۸۵۲۴۷۰
۲	تشخیص زودهنگام وابستگی‌های خطرناک در کد	۷	۰/۷۸۲۵۱۷	۰/۰۸۵۲۴۷۰
۳	شناسایی ماژول‌های دارای ریسک عملکردی بالا	۷	۰/۷۸۲۵۱۷	۰/۰۸۵۲۴۷۰
۴	پایش هوشمند رفتار مشارکت‌کنندگان و تشخیص نوسانات فعالیت	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۵	تشخیص الگوهای ناسازگاری در نسخه‌ها و پکیج‌ها	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۶	پیش‌بینی ترک مشارکت‌کنندگان کلیدی	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۷	ارزیابی احتمال شکست در یک کامیت	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۸	شناسایی مخازن آلوده یا مشکوک به بدافزار	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۹	پیش‌بینی خطاهای ناشی از کد غیرقابل‌اعتماد	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۱۰	شناسایی نقاط گلوگاهی در جریان توسعه و تحویل	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸

ردیف	کدهای استخراجی	فراوانی	مقدار آنتروپی	ضریب اهمیت
۱۱	تحلیل وابستگی‌های پیچیده‌ی نرم‌افزار با گراف‌های هوشمند	۱۱	۰/۷۹۴۴۱۹	۰/۰۹۴۵۹۶
۱۲	تحلیل ریسک‌های انتشار نسخه‌های جدید	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۱۳	تحلیل تناقضات میان پکیج‌ها و کتابخانه‌ها	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۱۴	تحلیل ریسک‌های زنجیره‌ی تأمین مبتنی بر داده‌های واقعی مصرف‌کنندگان	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۱۵	اولویت‌بندی خودکار ریسک‌های بحرانی	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۱۶	تحلیل پیامدهای تغییرات کد بر کل اکوسیستم	۱۰	۰/۶۹۵۸۱۴	۰/۰۸۱۴۷۹
۱۷	تحلیل رفتار عملکردی ماژول‌ها در محیط عملیاتی	۱۰	۰/۶۹۵۸۱۴	۰/۰۸۱۴۷۹
۱۸	تحلیل الگوهای امنیتی و انحرافات رفتاری در کد	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۱۹	یادگیری از تاریخچه‌ی خطاها برای پیش‌بینی ریسک‌های مشابه	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۲۰	تحلیل مقایسه‌ای پروژه‌های متن‌باز برای تشخیص منابع سالم‌تر	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۲۱	پیشنهاد راهکارهای اصلاحی خودکار برای ریسک‌های شناسایی‌شده	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۲۲	ارائه‌ی پیشنهادهای مبتنی بر تجربه‌ی پروژه‌های مشابه	۷	۰/۷۸۲۵۱۷	۰/۰۸۵۲۴۷۰
۲۳	بهینه‌سازی تخصیص منابع برای مدیریت ریسک	۷	۰/۷۸۲۵۱۷	۰/۰۸۵۲۴۷۰
۲۴	تصمیم‌گیری مبتنی بر داده برای انتخاب تأمین‌کننده‌ی متن‌باز مناسب	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۲۵	تولید هشدارهای اولویت‌بندی برای مدیران	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۲۶	مدیریت خودکار نسخه‌ها و به‌روزرسانی‌های امن	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۲۷	پیش‌بینی تأثیر تصمیمات توسعه بر کل اکوسیستم	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۲۸	پیشنهاد سیاست‌های امنیتی و محتوامحور	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۲۹	مدیریت هوشمند ریسک‌های حقوق مالکیت فکری	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۳۰	تصمیم‌گیری در انتخاب مسیر توسعه‌ی امن‌تر	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۳۱	پایش لحظه‌ای فعالیت در مخازن متن‌باز	۱۱	۰/۷۹۴۴۱۹	۰/۰۹۴۵۹۶
۳۲	رصد تغییرات مشکوک در ریپازیتوری‌ها	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۳۳	کشف خودکار آسیب‌پذیری‌های روز صفر	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۳۴	کنترل کیفیت خودکار کد	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۳۵	پایش رفتار کاربران و مشارکت‌کنندگان مشکوک	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۳۶	پایش امنیت شبکه‌ی زنجیره‌ی تأمین نرم‌افزار	۱۰	۰/۶۹۵۸۱۴	۰/۰۸۱۴۷۹
۳۷	مانیتورینگ مستمر ریسک‌های اجتماعی (کاهش مشارکت، تنش در جامعه و...)	۱۰	۰/۶۹۵۸۱۴	۰/۰۸۱۴۷۹
۳۸	کنترل سلامت کل اکوسیستم متن‌باز	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۳۹	پایش خطرات مرتبط با وابستگی‌های قدیمی یا رهاشده	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۴۰	خودکارسازی تحلیل کد برای کشف ریسک‌ها	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۴۱	خودکارسازی فرایند آزمون امنیت و عملکرد	۸	۰/۴۷۵۸۴۹	۰/۰۵۷۴۱۸
۴۲	خودکارسازی بررسی مجوزها و لایسنس‌های متن‌باز	۷	۰/۷۸۲۵۱۷	۰/۰۸۵۲۴۷۰
۴۳	خودکارسازی مدیریت وابستگی‌ها	۷	۰/۷۸۲۵۱۷	۰/۰۸۵۲۴۷۰
۴۴	مدیریت خودکار به‌روزرسانی‌ها و وصله‌های امنیتی	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۴۵	خودکارسازی نظارت بر مسیر تحویل نرم‌افزار	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۴۶	بهینه‌سازی فرایندهای انتشار نسخه‌ها	۷	۰/۷۸۲۵۱۷	۰/۰۸۵۲۴۷۰
۴۷	ایجاد جریان‌های هوشمند واکنش به حوادث	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸
۴۸	کاهش خطای انسانی در مدیریت ریسک	۹	۰/۵۲۴۷۱۴	۰/۰۶۲۱۴۸

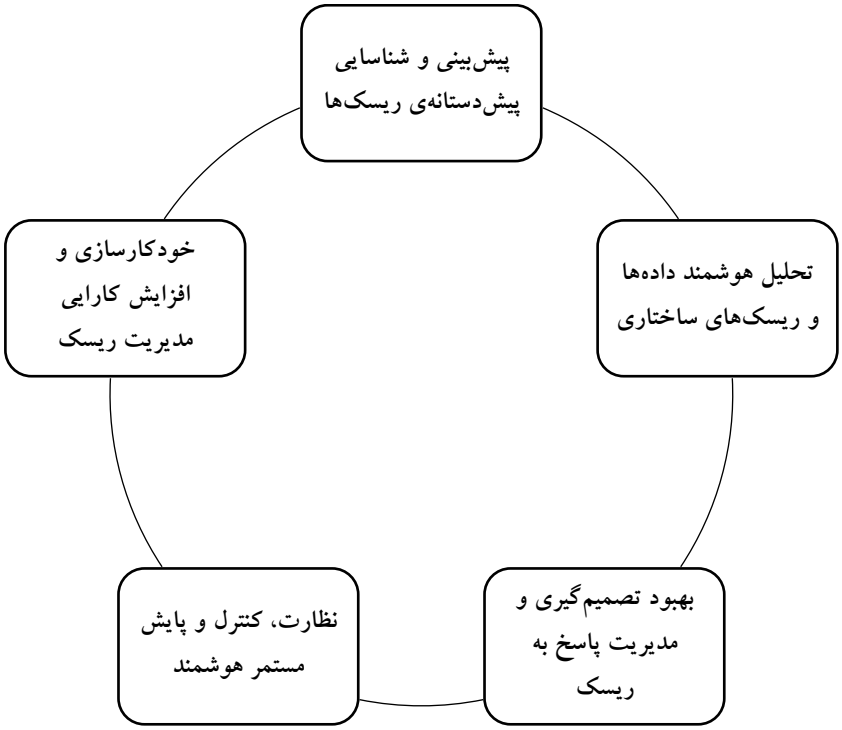
در ادامه‌ی بخش کیفی، ضمن دسته‌بندی کدهای استخراج‌شده، کدگذاری محوری نیز اجرا شد. جدول ۴ نتایج کدگذاری محوری مربوط به قابلیت‌های هوش مصنوعی در مدیریت ریسک زنجیره‌ی تأمین منبع‌باز در چارچوب حکمرانی هوشمند را نشان می‌دهد.

جدول ۴. نتایج کدگذاری محوری

کد مفهومی	کدهای استخراجی
پیش‌بینی و شناسایی پیش‌دستانه‌ی ریسک‌ها	پیش‌بینی آسیب‌پذیری‌های امنیتی در مخازن متن‌باز
	تشخیص زودهنگام وابستگی‌های خطرناک در کد
	شناسایی ماژول‌های دارای ریسک عملکردی بالا
	پایش هوشمند رفتار مشارکت‌کنندگان و تشخیص نوسانات فعالیت
	تشخیص الگوهای ناسازگاری در نسخه‌ها و پکیج‌ها
	پیش‌بینی ترک مشارکت‌کنندگان کلیدی
	ارزیابی احتمال شکست در یک کامیت
	شناسایی مخازن آلوده یا مشکوک به بدافزار
	پیش‌بینی خطاهای ناشی از کد غیرقابل‌اعتماد
	شناسایی نقاط گلوگاهی در جریان توسعه و تحویل
تحلیل هوشمند داده‌ها و ریسک‌های ساختاری	تحلیل وابستگی‌های پیچیده‌ی نرم‌افزار با گراف‌های هوشمند
	تحلیل ریسک‌های انتشار نسخه‌های جدید
	تحلیل تناقضات میان پکیج‌ها و کتابخانه‌ها
	تحلیل ریسک‌های زنجیره‌ی تأمین مبتنی بر داده‌های واقعی مصرف‌کنندگان
	اولویت‌بندی خودکار ریسک‌های بحرانی
	تحلیل پیامدهای تغییرات کد بر کل اکوسیستم
	تحلیل رفتار عملکردی ماژول‌ها در محیط عملیاتی
	تحلیل الگوهای امنیتی و انحرافات رفتاری در کد
	یادگیری از تاریخچه‌ی خطاها برای پیش‌بینی ریسک‌های مشابه
	تحلیل مقایسه‌ای پروژه‌های متن‌باز برای تشخیص منابع سالم‌تر
بهبود تصمیم‌گیری و مدیریت پاسخ به ریسک	پیشنهاد راهکارهای اصلاحی خودکار برای ریسک‌های شناسایی‌شده
	ارائه‌ی پیشنهادهای مبتنی بر تجربه‌ی پروژه‌های مشابه
	بهینه‌سازی تخصیص منابع برای مدیریت ریسک
	تصمیم‌گیری مبتنی بر داده برای انتخاب تأمین‌کننده‌ی متن‌باز مناسب
	تولید هشدارهای اولویت‌بندی‌شده برای مدیران
	مدیریت خودکار نسخه‌ها و به‌روزرسانی‌های امن
	پیش‌بینی تأثیر تصمیمات توسعه بر کل اکوسیستم
	پیشنهاد سیاست‌های امنیتی و محتوامحور
	مدیریت هوشمند ریسک‌های حقوق مالکیت فکری
	تصمیم‌گیری در انتخاب مسیر توسعه‌ی امن‌تر
نظارت، کنترل و پایش مستمر هوشمند	پایش لحظه‌ای فعالیت در مخازن متن‌باز
	رصد تغییرات مشکوک در ریپازیتوری‌ها
	کشف خودکار آسیب‌پذیری‌های روز صفر
	کنترل کیفیت خودکار کد
	پایش رفتار کاربران و مشارکت‌کنندگان مشکوک
	پایش امنیت شبکه‌ی زنجیره‌ی تأمین نرم‌افزار
	مانیتورینگ مستمر ریسک‌های اجتماعی (کاهش مشارکت، تنش در کامیونیتی و...)
	کنترل سلامت کل اکوسیستم متن‌باز
	پایش خطرات مرتبط با وابستگی‌های قدیمی یا رهاشده
خودکارسازی و افزایش کارایی مدیریت ریسک	خودکارسازی تحلیل کد برای کشف ریسک‌ها
	خودکارسازی فرایند آزمون امنیت و عملکرد

کد مفهومی	کدهای استخراجی
	خودکارسازی بررسی مجوزها و لایسنس‌های متن‌باز
	خودکارسازی مدیریت وابستگی‌ها
	مدیریت خودکار به‌روزرسانی‌ها و وصله‌های امنیتی
	خودکارسازی نظارت بر مسیر تحویل نرم‌افزار
	بهینه‌سازی فرایندهای انتشار نسخه‌ها
	ایجاد جریان‌های هوشمند واکنش به حوادث
	کاهش خطای انسانی در مدیریت ریسک

با توجه به نتایج پژوهش حاضر مشخص شد که قابلیت‌های هوش مصنوعی در مدیریت ریسک زنجیره‌ی تأمین منبع‌باز در چارچوب حکمرانی هوشمند شامل پیش‌بینی و شناسایی پیش‌دستانه‌ی ریسک‌ها، تحلیل هوشمند داده‌ها و ریسک‌های ساختاری، بهبود تصمیم‌گیری و مدیریت پاسخ به ریسک، نظارت، کنترل و پایش مستمر هوشمند و خودکارسازی و افزایش کارایی مدیریت ریسک است. شکل ۱ این جنبه‌ها را نشان می‌دهد.



شکل ۱. کدگذاری محوری قابلیت‌های هوش مصنوعی در مدیریت ریسک زنجیره‌ی تأمین منبع‌باز در چارچوب حکمرانی هوشمند

مدل ارائه‌شده نشان می‌دهد که هوش مصنوعی از طریق چهار دسته قابلیت اصلی نقشی تعیین‌کننده در شناسایی، تحلیل، کنترل و کاهش ریسک‌های موجود در زنجیره‌ی تأمین منبع‌باز ایفا می‌کند. این قابلیت‌ها پیوسته و مکمل یکدیگرند و به‌گونه‌ای عمل می‌کنند که از مرحله‌ی پیش‌بینی تا واکنش، کل چرخه‌ی مدیریت ریسک را پشتیبانی کنند.

این چهار دسته‌ی اصلی عبارت‌اند از:

۱. **پیش‌بینی و شناسایی پیش‌دستانه‌ی ریسک‌ها:** در این بخش، سیستم‌های هوشمند با استفاده از یادگیری ماشین، تحلیل روندها و الگوهای مشارکت‌کنندگان، تغییرات رفتار کاربران، وضعیت پویای مخازن منبع‌باز و داده‌های وابستگی نرم‌افزار، قادرند ریسک‌ها را پیش از وقوع شناسایی کنند. این امر موجب کاهش آسیب‌پذیری‌های ناشی از تهدیدات سایبری، اختلالات عملیاتی و ناپایداری مشارکت‌کنندگان می‌شود.

۲. **تحلیل هوشمند داده‌ها و ریسک‌های ساختاری:** هوش مصنوعی با پردازش کلان‌داده‌ها، تحلیل گراف وابستگی‌های نرم‌افزار، پایش فعالیت مخازن و شناسایی نقاط بحرانی، امکان تحلیل عمیق و ساختاری ریسک‌ها را فراهم می‌کند. این تحلیل‌ها شامل مواردی مانند کشف آسیب‌پذیری‌ها، ضعف کد، الگوهای معیوب انتشار نسخه‌ها و ارزیابی پایداری جامعه‌ی توسعه‌دهندگان است.

۳. **بهبود تصمیم‌گیری و مدیریت پاسخ به ریسک:** مدل‌های هوشمند با ایجاد سناریوهای مختلف، تحلیل پیامدها و ارائه‌ی راه‌حل‌های بهینه به مدیران کمک می‌کنند تا تصمیمات دقیق‌تر و سریع‌تری در مواجهه با ریسک بگیرند. همچنین سیستم‌های توصیه‌گر هوشمند می‌توانند راهبردهای مناسب کاهش ریسک را پیشنهاد دهند و از تصمیم‌گیری شهودی و غیرعلمی جلوگیری کنند.

۴. **نظارت، کنترل و پایش مستمر هوشمند:** هوش مصنوعی از طریق پایش لحظه‌ای تغییرات کد، فعالیت مشارکت‌کنندگان، وضعیت امنیت مخازن، عملکرد بسته‌های نرم‌افزاری و هشداردهی خودکار، امکان کنترل مستمر و واکنش سریع را فراهم می‌کند. این بخش موجب کاهش زمان شناسایی خطا، جلوگیری از گسترش تهدیدات و افزایش تاب‌آوری زنجیره‌ی تأمین می‌شود.

۵. **خودکارسازی و افزایش کارایی مدیریت ریسک:** با استفاده از الگوریتم‌های هوشمند، فرایندهایی مانند غربالگری کد، ارزیابی امنیت بسته‌ها، اولویت‌بندی تهدیدات و نظارت عملیاتی به‌صورت خودکار انجام می‌شوند. این امر موجب کاهش هزینه، افزایش سرعت واکنش و کاهش خطاهای انسانی می‌شود و ساختار مدیریت ریسک را به‌طور چشمگیری کارآمدتر می‌کند.

قابلیت‌های هوش مصنوعی در این مدل به‌صورت چرخه‌ای و پیوسته عمل می‌کنند و پوششی کامل از مراحل مدیریت ریسک ارائه می‌دهند؛ از پیش‌بینی و شناسایی ریسک‌ها تا تحلیل، تصمیم‌گیری، کنترل و خودکارسازی. این چارچوب، بستر مناسبی برای طراحی مدلی جامع برای مدیریت ریسک در زنجیره‌ی تأمین منبع‌باز فراهم می‌کند.

بحث و نتیجه‌گیری

مطابق با نتایج مشخص شد که قابلیت‌های هوش مصنوعی در مدیریت ریسک در زنجیره‌ی تأمین منبع‌باز شامل پیش‌بینی و شناسایی پیش‌دستانه‌ی ریسک‌ها، تحلیل هوشمند داده‌ها و ریسک‌های ساختاری، بهبود تصمیم‌گیری و مدیریت پاسخ به ریسک، نظارت، کنترل و پایش مستمر هوشمند و خودکارسازی و افزایش کارایی مدیریت ریسک است. نتایج تحلیل محتوای مصاحبه‌های انجام‌شده با خبرگان و متخصصان حوزه‌ی فناوری اطلاعات و مدیریت زنجیره‌ی تأمین، نشان داد قابلیت‌های هوش مصنوعی می‌تواند در پنج محور اصلی و کلیدی برای مدیریت ریسک در زنجیره‌ی تأمین منبع‌باز به کار گرفته شود: پیش‌بینی و شناسایی پیش‌دستانه‌ی ریسک‌ها، تحلیل هوشمند داده‌ها و ریسک‌های

ساختاری، بهبود تصمیم‌گیری و مدیریت پاسخ به ریسک، نظارت، کنترل و پایش مستمر هوشمند و خودکارسازی و افزایش کارایی مدیریت ریسک. این دسته‌بندی نشان می‌دهد که هوش مصنوعی نه ابزاری تک‌کارکردی، بلکه بستر توانمندساز جامعی است که می‌تواند چرخه‌ی کامل مدیریت ریسک ــ از شناسایی تا پاسخ و نظارت ــ را متحول کند. درواقع، این فناوری با افزودن لایه‌ای از هوشمندی، پیش‌بینی‌پذیری و سرعت به فرایندهای سنتی، پاسخی مناسب به ماهیت پویا، پیچیده و داده‌محور ریسک‌ها در محیط‌های منبع‌باز ارائه می‌دهد.

یافته‌های این بخش از پژوهش، ضمن تأیید روند کلی جهانی در به‌کارگیری هوش مصنوعی برای مدیریت ریسک، آن را در زمینه‌ی خاص و پرچالشِ زنجیره‌ی تأمین منبع‌باز بومی‌سازی و عملیاتی می‌کند. برای مثال، قابلیت پیش‌بینی و شناسایی پیش‌دستانه‌ی ریسک‌ها که در این پژوهش بر آن تأکید شده است، به‌طور مستقیم با یافته‌های پژوهش Ohm & Stuke (2023) هم‌خوانی دارد که در آن از الگوریتم‌های یادگیری ماشین برای کشف الگوهای پنهان و پیش‌بینی حملات سایبری در زنجیره‌ی نرم‌افزار استفاده‌شده بود. این هم‌پوشانی نشان می‌دهد قابلیت پیش‌بینی هوش مصنوعی نیازی جهانی و شناخته‌شده است. همچنین، محور تحلیل هوشمند داده‌ها و ریسک‌های ساختار یافته در این پژوهش، مؤید نتایج پژوهش حجازی‌فر و همکاران (۱۴۰۳) است که بر طراحی مدل‌های هوشمند برای تحلیل داده‌های حجیم زنجیره‌ی تأمین و شناسایی نقاط ضعف ساختاری تأکید داشتند. وجه تمایز و ارزش‌افزوده‌ی پژوهش حاضر در جامعیت نگاه آن است، به‌طوری‌که علاوه بر ابعاد تحلیلی و پیش‌بینی، بر نقش هوش مصنوعی در بهبود تصمیم‌گیری و مدیریت پاسخ نیز تمرکز کرده است. این بعد، حلقه‌ی گم‌شده‌ی بسیاری از راه‌حل‌های فنیِ صرف است و یافته‌های این پژوهش نشان می‌دهند سیستم‌های توصیه‌گر هوشمند می‌توانند با تحلیل سناریوهای مختلف، بهترین راهبرد کاهش یا انتقال ریسک را به مدیران پیشنهاد دهند. این یافته، مکملِ یافته‌های پژوهش‌هایی مانند Akinsola & Akinde (2024) است که بیش‌تر بر جنبه‌های امنیتی و نظارتی تمرکز داشتند.

علاوه بر این، تأکید این پژوهش بر خودکارسازی و افزایش کارایی، پاسخی مستقیم به یکی از چالش‌های اصلی زنجیره‌های منبع‌باز ــ یعنی محدودیت منابع انسانی تخصصی و مقیاس بسیار بزرگ تعاملات ــ است. این یافته با جهت‌گیری پژوهش‌هایی مانند Sun (2024)، که بر خودکارسازی فرایندهای آزمون و یکپارچه‌سازی در توسعه‌ی نرم‌افزار تأکید می‌کرد، هم‌سوست و آن را به حوزه‌ی مدیریت ریسک تعمیم می‌دهد. درنهایت، شناسایی قابلیت نظارت و پایش مستمر هوشمند به‌عنوان محوری کلیدی، بر ضرورت تحول از مدل‌های واکنشی به مدل‌های پیش‌فعال و انطباق‌پذیر در مدیریت ریسک تأکید دارد. این نتیجه با چارچوب نظری Younis et al. (2023)، که بر لزوم پویایی و انعطاف در مدیریت ریسک زنجیره‌های باز تأکید داشتند، کاملاً منطبق است.

در جمع‌بندی می‌توان گفت که یافته‌های این پژوهش در پاسخ سؤالات نشان می‌دهند هوش مصنوعی به‌مثابه‌ی «تسهیل‌گری هوشمند» می‌تواند بر سه شکاف اصلی در مدیریت ریسک زنجیره‌های منبع‌باز غلبه کند: شکاف سرعت (از طریق خودکارسازی و پایش بلادرنگ)، شکاف پیش‌بینی (از طریق تحلیل‌های پیشرفته) و شکاف تصمیم‌گیری (از طریق سیستم‌های پشتیبان هوشمند)؛ بنابراین، به‌کارگیری این قابلیت‌ها نه انتخابی لوکس، بلکه ضرورتی راهبردی برای تضمین تاب‌آوری و پایداری اکوسیستم‌های حیاتی مبتنی بر منبع باز است.

بنا بر نتایج، پیشنهاد می‌شود سازمان‌ها با طراحی و استقرار پلتفرم‌های رایگان و امن برای اشتراک‌گذاری شفاف اطلاعات ریسک (مانند گزارش

آسیب‌پذیری، تحلیل ریشه‌ای خرابی‌ها و رتبه‌بندی اعتبار تأمین‌کنندگان) بین تمامی ذی‌نفعان زنجیره زمینه‌ساز شکل‌گیری یک «حافظه‌ی جمعی سازمانی» شود و شرایطی را برای تشخیص سریع‌تر تهدیدات و هماهنگی در پاسخ‌گویی فراهم کنند. مطابق با نتایج، پیشنهاد می‌شود شرکت‌های پیش‌رو در زنجیره‌ی تأمین با سرمایه‌گذاری بر توسعه یا خرید سامانه‌های پیش‌بین هوشمند که با الگوریتم‌های یادگیری ماشین الگوهای ناهنجاری در کد، وابستگی‌ها و فعالیت شبکه را تحلیل می‌کنند، امکان شناسایی ریسک‌های امنیتی و عملیاتی را پیش از وقوع بحران فراهم کنند. همچنین، پیشنهاد می‌شود بنیادها و کنسرسیوم‌های حاکم بر پروژه‌های منبع‌باز با طراحی و اجرای سازوکارهای هوشمند انگیزشی همچون جوایز مالی برای گزارش آسیب‌پذیری، اعطای جایگاه‌های افتخاری بر مبنای مشارکت و حمایت از دوره‌های آموزشی تخصصی برای مشارکت‌کنندگان برتر، مشارکت فعال و پایدار جامعه‌ی توسعه‌دهندگان را در فرایند مدیریت ریسک تضمین کنند. بنا بر نتایج پژوهش، پیشنهاد می‌شود واحدهای حقوقی سازمان‌ها با تدوین و ابلاغ چارچوب استاندارد ملی برای مجوزهای نرم‌افزاری شامل ابزارهای خودکار بررسی انطباق و الگوهای قراردادی استاندارد برای همکاری با تأمین‌کنندگان منبع‌باز از وقوع دعاوی قضایی پرهزینه و آسیب به اعتبار برند جلوگیری کنند. همچنین، پیشنهاد می‌شود مدیران فنی با پیاده‌سازی راهبردهای عملیاتی-ارتباطی، مانند ایجاد نقشه‌ی وابستگی زنده برای پروژه‌های حیاتی و تعیین رسمی نگهبانان فنی برای هر ماژول کلیدی، شفافیت و مسئولیت‌پذیری را افزایش و اثر خروج ناگهانی اعضای کلیدی را کاهش دهند. بر اساس نتایج پژوهش، پیشنهاد می‌شود نهادهای آموزشی و پژوهشی با طراحی و ارائه‌ی دوره‌های آموزشی تخصصی مدیریت ریسک زنجیره‌ی تأمین منبع‌باز در قالب بوت‌کمپ‌ها و دوره‌های آنلاین رایگان به تربیت نیروی انسانی متبحر در این حوزه بپردازند و ضمن کاهش شکاف مهارتی، پایداری بلندمدت اکوسیستم را نیز تضمین کنند.

تعارض منافع

درانجام معالعه حاضر، هیچگونه تضاد منافعی وجود ندارد.

تشکر و قدردانی

نگارندگان بر خود واجب می‌دانند از تمامی افرادی که به تیم پژوهش کمک کردند و نظرات ارزشمندشان را در مورد متن مقاله‌ی حاضر ارائه دادند، سپاسگزاری کنند. این مقاله برگرفته از رساله دانشجویی مقطع دکتری می باشد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

موازین اخلاقی

این پژوهش با رعایت تمامی اصول اخلاق درپژوهش‌های انسانی انجام شده است.

شفافیت داده‌ها

داده‌ها و مآخذ پژوهش حاضر در صورت درخواست از نویسنده مسئول و ضمن رعایت اصول کپی رایت ارسال خواهد شد.

حامی مالی

این پژوهش حامی مالی نداشته است.

References

Adenekan, O. A., Ezeigweneme, C., & Chukwurah, E. G. (2024). Strategies for protecting IT supply chains against cybersecurity threats. *International Journal of Management & Entrepreneurship Research, 6*(5), 1598-1606. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=mLhyCV4AAAAJ&citation_for_view=mLhyCV4AAAAJ:LkGwnXOMwfcC

Akinsola, A., & Akinde, A. (2024). *Enhancing software supply chain resilience: Strategy for mitigating software supply chain security risks and ensuring security continuity in development lifecycle* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2407.13785

Amft, S., Höltervennhoff, S., Panskus, R., Marky, K., & Fahl, S. (2024, May). Everyone for themselves? A qualitative study about individual security setups of open source software contributors. In *2024 IEEE Symposium on Security and Privacy (SP)* (pp. 1065-1082). IEEE. https://saschafahl.de/static/paper/ossc2024.pdf

Ayala, J., Tung, Y. J., & Garcia, J. (2024). *A mixed-methods study of open-source software maintainers on vulnerability management and platform security features* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2409.07669

Han, Y., & Fang, X. (2024). Systematic review of adopting blockchain in supply chain management: Bibliometric analysis and theme discussion. *International Journal of Production Research, 62*(3), 991-1016. https://doi.org/10.1080/00207543.2023.2236241

Hejazifar, M., Ghaffari, A., & Soltani, M. (2024). Designing an intelligent model of risk management in the supply chain using machine learning techniques. *Intelligent Strategic Management, 3*(2), 57-72. https://www.sid.ir/paper/1500428/fa

Jackson, I., Ivanov, D., Dolgui, A., & Namdar, J. (2024). Generative artificial intelligence in supply chain and operations management: A capability-based framework for analysis and implementation. *International Journal of Production Research*, 1-26. https://doi.org/10.1080/00207543.2024.2309309

Kalu, K. G., Singla, T., Okafor, C., Torres-Arias, S., & Davis, J. C. (2024). *An industry interview study of software signing for supply chain security* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2406.08198

Ohm, M., & Stuke, C. (2023). SoK: Practical detection of software supply chain attacks. In *Proceedings of the 18th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3600160.3600162

Sammak, R., Rotthaler, A. L., Ramulu, H. S., Wermke, D., & Acar, Y. (2023, November). Developers' approaches to software supply chain security: An interview study. In *Proceedings of the 2024 Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses* (pp. 56-66). https://dwermke.com/pdf/conf-scored-sammak24.pdf

Sun, L. (2024). Securing supply chains in open source ecosystems: Methodologies for determining version numbers of components without package management files. *Journal of Computing and Electronic Information Management, 12*(1), 32-36. https://doi.org/10.54097/n8djwto1zb

Tseng, M. L., Bui, T. D., Lim, M. K., Fujii, M., & Mishra, U. (2022). Assessing data-driven sustainable supply chain management indicators for the textile industry under industrial disruption and ambidexterity. *International Journal of Production Economics, 245*, 108401. https://doi.org/10.1016/j.ijpe.2021.108401

Wermke, D., Klemmer, J. H., Wöhler, N., Schmüser, J., Ramulu, H. S., Acar, Y., & Fahl, S. (2023, May). "Always contribute back": A qualitative study on security challenges of the open source supply chain. In *2023 IEEE Symposium on Security and Privacy (SP)* (pp. 1545-1560). IEEE. https://doi.org/10.1109/SP46215.2023.10179378

Yang, H., Zhang, B., Wang, N., Guo, C., Zhang, X., Lin, L., & Wang, C. D. (2024). *FinRobot: An open-source AI agent platform for financial applications using large language models* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2405.14767

Younis, A. A., Hu, Y., & Abdunabi, R. (2023, August). Analyzing software supply chain security risks in industrial control system protocols: An OpenSSF scorecard approach. In *2023 10th International Conference on Dependable Systems and Their Applications (DSA)* (pp. 302-311). IEEE. https://doi.org/10.1109/DSA59317.2023.00044

Zhu, Z., Lan, K., Rao, Z., & Zhang, Y. (2021). Risk assessment method for IoT software supply chain vulnerabilities. In *Journal of Physics: Conference Series, 1732*(1), Article 012051. IOP Publishing. https://doi.org/10.1088/1742-6596/1732/1/012051

Explaining the Capabilities of Artificial Intelligence in Open Source Supply Chain Risk Management within the Framework of Smart Governance

Extended Abstract

Introduction

In recent years, the development of new information and communication technologies, especially artificial intelligence, big data, and the Internet of Things, has created extensive changes in management, decision-making, and governance practices. These developments have led to the formation of the concept of "smart governance," which, as one of the fundamental pillars of smart cities, emphasizes the use of advanced technologies to improve the quality of decision-making, increase transparency, improve accountability, and improve the efficiency of management processes. By providing technological and information infrastructure, smart governance enables the collection, analysis, and effective use of data and helps organizations and management institutions make more accurate, faster, and evidence-based decisions. Accordingly, the present study aims to explain the capabilities of artificial intelligence in open source supply chain risk management within the framework of smart governance. The results of this research can help to better understand the role of artificial intelligence in improving risk management processes, provide the necessary basis for the development of intelligent approaches in open source supply chain management, and help to improve the efficiency, transparency, and resilience of open source-based systems within the framework of smart governance. Also, the findings of this research can be useful for managers, policymakers, and stakeholders in the field of smart governance to make more effective decisions and reduce risks associated with open source supply chains.

Methodology

The present study was a qualitative research conducted in the field. The qualitative method used in the present study was Glaser's grounded theory. The statistical population of the qualitative part of this study includes elites and experts knowledgeable in the field of open source supply chain in the information technology and software industry. The multidimensional and complex nature of the research topic—especially the link between open source supply chain, risk management, and artificial intelligence applications—requires that information be collected from individuals who have specialized knowledge, practical experience, and deep understanding of technological and security trends in this field. Accordingly, at this stage of the study, the statistical population does not include the general public, but includes experts.

Findings

According to the results of this study, it was determined that the capabilities of artificial intelligence in open source supply chain risk management within the framework of smart governance include proactive prediction and identification of risks, intelligent analysis of data and structural risks, improved decision-making and risk response management, intelligent continuous monitoring, control, and automation, and increased efficiency of risk management.

Discussion and Conclusion

According to the results, it was determined that the capabilities of artificial intelligence in risk management in the open source supply chain include proactive risk prediction and identification, intelligent data analysis and structural risk, improved decision-making and risk response management, intelligent continuous monitoring, control and monitoring, and automation and increasing the efficiency of risk management. According to the results of the content analysis of interviews with experts and specialists in the field of information technology and supply chain management, it was determined that the capabilities of artificial intelligence can be used in five main and key areas for risk management in the open source supply chain: proactive risk prediction and identification, intelligent data analysis and structural risk, improved decision-making and risk response

management, intelligent continuous monitoring, control and monitoring, and automation and increasing the efficiency of risk management. This categorization shows that artificial intelligence is not a single-function tool, but a comprehensive enabling platform that can transform the entire risk management cycle—from identification to response and monitoring. In fact, this technology provides an appropriate response to the dynamic, complex, and data-driven nature of risks in open source environments by adding a layer of intelligence, predictability, and speed to traditional processes.

Keywords: Governance, Smart City, Supply Chain, Open Source

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this study.

Acknowledgment

The authors would like to express their sincere gratitude to all individuals who assisted the research team and provided valuable feedback on the manuscript of this article. This study is derived from a doctoral dissertation.

Author Contributions

All authors contributed equally to the preparation of this manuscript.

Ethical Considerations

This study was conducted in accordance with all ethical principles for human research.

Data Transparency

The data and references supporting the findings of this study are available from the corresponding author upon reasonable request, provided that copyright and privacy policies are respected.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.