به نام خدا

کاربرد هوش مصنوعی در امنیت سایبری

مرضیه علیدادی ۸۱۰۱۰۱۲۳۶

تعریف مسئله

امروزه کاربرد هوش مصنوعی در حوزه‌ی امنیت سایبری برای افزایش حفاظت از اطلاعات حساس و سیستم‌های حیاتی در حوزه‌ی مدیریت فناوری اطلاعات بسیار مورد توجه قرار گرفته‌است. راه‌حل‌های مبتنی بر هوش مصنوعی، طیف گسترده‌ای از مزایای بالقوه‌ای، از جمله تشخیص پیشرفته‌ی تهدید، واکنش سریع به حادثه، و مدیریت فعال ریسک ارائه می‌کند. با این حال، با توجه به این که سازمان‌ها به پذیرش هوش مصنوعی در امنیت سایبری فکر می‌کنند، با چالش مدیریت مؤثر ریسک‌های مرتبط و پیمایش در چشم‌انداز پیچیده‌ی پیامدهای مدیریتی و تجاری مواجه می‌شوند.

این پروژه‌ی تحقیقاتی به دنبال بررسی مفاهیم چندوجهی استفاده از هوش مصنوعی در امنیت سایبری در زمینه‌ی مدیریت فناوری اطلاعات است. به طور خاص، هدف این مطالعه روشن کردن مزایای بالقوه‌ی استفاده از هوش مصنوعی، مانند بهبود دقت تشخیص تهدید، کاهش زمان پاسخ به حوادث امنیتی، و افزایش سازگاری با تهدیدات سایبری است. علاوه بر این، پیچیدگی‌های مدیریت ریسک در استقرار راه‌حل‌های امنیت سایبری مبتنی بر هوش مصنوعی، شامل ملاحظات مربوط به حریم خصوصی داده‌ها، سوگیری‌های الگوریتمی و آسیب‌پذیری‌های بالقوه‌ی ناشی از اتکا به هوش مصنوعی بررسی خواهد شد.

در این مطالعه علاوه بر مزایا و مدیریت ریسک، به چالش‌های مدیریتی و تجاری مربوط به استفاده از هوش مصنوعی در امنیت سایبری نیز پرداخته خواهد شد. این چالش‌ها شامل ارزیابی مقیاس‌پذیری راه‌حل‌های هوش مصنوعی، آمادگی سازمانی برای پذیرش آن، همسویی مهارت‌های نیروی کار و تأثیر گسترده‌تر بر عملیات تجاری و تصمیم‌گیری استراتژیک است. با روشن کردن این جنبه‌های چندوجهی، تلاش خواهد شد تا کسب‌وکارها و متخصصان مدیریت فناوری اطلاعات به بینش‌های آگاهانه‌ای مجهز شوند که آن‌ها را در تصمیم‌گیری در رابطه با استفاده از هوش مصنوعی در امنیت سایبری هدایت کند.

در اصل، هدف این پروژه‌ی تحقیقاتی پر کردن شکاف بین وعده‌های هوش مصنوعی در امنیت سایبری و ملاحظات عملی کسب‌وکارها و سازمان‌ها، در راستای حرکت در چشم‌انداز تهدید سایبری است. با ارائه‌ی درک جامعی از مزایا، مدیریت ریسک و چالش‌های مدیریتی،

در جهت دستیابی به هدف توانمندسازی ذی‌نفعان برای اتخاذ تصمیمات آگاهانه در مورد کاربرد هوش مصنوعی در امنیت سایبری در حوزه‌ی مدیریت فناوری اطلاعات تلاش خواهد شد.

در ادامه یک مطالعه‌ی موردی به عنوان نمونه‌ای از استفاده‌ی موفق از هوش مصنوعی در حوزه‌ی امنیت سایبری ارائه شده‌است.
مطالعه‌ی موردی "IBM Watson برای امنیت سایبری" [۱] [۲]:
قابلیت‌های IBM Watson، به عنوان یک بستر پیشرو هوش مصنوعی، آن را قادر می‌سازد تا حجم وسیعی از داده‌های امنیتی را تجزیه و تحلیل کرده، تهدیدهای بالقوه را شناسایی کرده و به سرعت پاسخ‌های آگاهانه را فرموله کند. IBM Watson با بهره‌گیری از تجزیه و تحلیل مبتنی بر هوش مصنوعی و زمینه‌سازی داده‌های امنیتی، شناسایی پیشگیرانه‌ی تهدید و پاسخ به حادثه را تسهیل می‌کند و در نهایت انعطاف‌پذیری سایبری کلی سازمان را تقویت می‌کند [۱] [۲].

مراجعی که در انتها معرفی شده‌اند، برای بررسی مسئله‌ی تعریف‌شده شناسایی شده‌اند.

مراجع

[۱] IBM Security. *"IBM Security: Cognitive Security with Watson."* [Online]. Available: https://www.ibm.com/security/cognitive. Accessed on: Sep. 2019.

[۲] A. Singh and S. Choudhary, *"Leveraging IBM Watson for Cyber Security: A Case Study in AI-Driven Threat Detection,"* Journal of Cybersecurity and Information Assurance, vol. 6, no. 2, pp. 112–125, 2020.

[۳] B. Alhayani, H. Jasim Mohammed, I. Zeghaiton Chaloob, and J. Saleh Ahmed, *"Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry,"* Materials Today: Proceedings, Mar. 2021, doi: https://doi.org/10.1016/j.matpr.2021.02.531.

[۴] N. Abbas, T. Ahmed, S. H. U. Shah, M. Omar, and H. W. Park, *"Investigating the applications of artificial intelligence in cyber security,"* Scientometrics, vol. 121, no. 2, pp. 1189–1211, Sep. 2019, doi: 10.1007/s11192-019-03222-9.

[۵] J. Li, *"Cyber security meets artificial intelligence: a survey,"* Frontiers of Information Technology & Electronic Engineering, vol. 19, no. 12, pp. 1462–1474, Dec. 2018, doi: https://doi.org/10.1631/fitee.1800573.

[۶] A. A. Mughal, *"Artificial Intelligence in Information Security: Exploring the Advantages, Challenges, and Future Directions"*, JAMM, vol. 2, no. 1, pp. 22–34, Jan. 2018.

[۷] I. H. Sarker, H. Furhad, and R. Nowrozy, *"AI-Driven Cybersecurity: An Overview, security intelligence modeling and research directions,"* SN Computer Science, vol. 2, no. 3, Mar. 2021, doi: 10.1007/s42979-021-00557-0.

[۸] R. Kaur, D. Gabrijelčič, and T. Klobučar, *"Artificial intelligence for cybersecurity: Literature review and future research directions,"* Information Fusion, vol. 97, p. 101804, Sep. 2023, doi: 10.1016/j.inffus.2023.101804.