Information Technology Innovations and Applied Communication
Vol. 4, No. 1, Spring, 2026, Serial No. 9,pp.49-62

Security threats and opportunities of generative artificial intelligence in the Internet of Things

Mohammad Beheshti-Atashgah[1*], Mahdi Zareian Jahromi[2]

Researcher, Sharif Technology Complex; Sharif University, Tehran, Iran

(**Received:** 01 April 2026, **Revised:** 04 May 2026, **Accepted:** 12 May 2026, **Published:** 28 May 2026)

ABSTRACT

The Internet of Things (IoT) concept relies on various technologies to fulfill its primary objective of connecting numerous objects through a comprehensive network based on Internet Protocol, with generative artificial intelligence (AI) being one of those technologies. Each technology inherently offers unique opportunities and applications, but it also carries security and privacy risks. In this article, we will first explore how generative AI is fostering innovation within the IoT, followed by an investigation into the security and privacy risks associated with this technology, specifically when generative AI is utilized and how it can be misused within IoT ecosystems. These risks not only endanger the security, privacy, and effectiveness of IoT systems, but also have wider consequences for trust and security in AI-driven environments. The following explores the benefits and anticipated results of a thorough examination of the security risks and advantages posed by generative AI within the Internet of Things, along with strategic methods to address these risks using various approaches. This article aims to offer an equitable and thorough examination of the possible benefits and dangers associated with this technology, while highlighting its practical uses in enhancing the security and privacy of the Internet of Things, and also emphasizes the necessity of acknowledging its drawbacks and challenges.

Keywords Artificial intelligence, Internet of Things, security, privacy.

* Corresponding Author E-mail: mohammad.beheshti@researcher.sharif.edu

«نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی»
سال چهارم، شماره ۱، فصل بهار ۱۴۰۵؛ ص ۶۲-۴۹.

تهدیدها و فرصت‌های امنیتی هوش مصنوعی مولد در اینترنت اشیا

محمد بهشتی آتشگاه*[۱]، مهدی زارعیان جهرمی[۲]

۱- دکتری رشته مهندسی کامپیوتر گرایش امنیت اطلاعات؛ دفتر طراحی، تحلیل و پیاده‌سازی رمزنگاری و دستگاه‌های امنیت اطلاعات و ارتباطات شریف
۲- کارشناسی‌ارشد، مهندسی کامپیوتر گرایش هوش مصنوعی، دانشگاه صنعتی مالک‌اشتر، تهران، ایران

(**دریافت:** ۱۲ فروردین ۱۴۰۵ **بازنگری:** ۱۴ اردیبهشت ۱۴۰۵ **پذیرش:** ۲۲ اردیبهشت ۱۴۰۵ انتشار: ۰۷ خرداد ۱۴۰۵)

چکیده

مفهوم اینترنت اشیا برای رسیدن به هدف نهایی خود یعنی اتصال تمامی اشیا از طریق یک شبکه سرتاسری مبتنی بر پروتکل اینترنت از فناوری‌های مختلف بهره می‌برد که یکی از این فناوری‌های حیاتی، هوش مصنوعی مولد است. طبیعی است که هر فناوری فرصت‌ها و کاربردهای خاصی را با خود به ارمغان می‌آورد و هم‌زمان نیز، تهدیدات امنیتی و حریم خصوصی از خود به ارث می‌گذارد. در این مقاله، ابتدا بررسی می‌کنیم که چگونه هوش مصنوعی مولد باعث نوآوری در اینترنت اشیا می‌شود و پس از آن، تهدیدات امنیتی و حریم خصوصی ذاتی این فناوری را در هنگام بهره‌گیری از هوش مصنوعی مولد و استفاده نادرست از فناوری‌های هوش مصنوعی مولد در زیست‌بوم‌های اینترنت اشیا موردمطالعه قرار می‌دهیم. این تهدیدات نه‌تنها امنیت، حریم خصوصی و کارایی دستگاه‌های اینترنت اشیا را تهدید می‌کند، بلکه پیامدهای گسترده‌تری برای اعتماد و امنیت آن در محیط‌های مبتنی بر هوش مصنوعی ایجاد می‌کند. در ادامه، به مزیت‌ها و نتیجه مطلوب نگاه جامع به تهدیدها و فرصت‌های امنیتی هوش مصنوعی مولد در اینترنت اشیا پرداخته و همچنین رویکردهای راهبردی برای کاهش این تهدیدات با روش‌های مختلف بررسی می‌شود. این مقاله به دنبال ارائه یک نگاه متوازن و جامع از نقاط فرصت و تهدید بالقوه این فناوری است، به‌گونه‌ای که نه‌تنها به کاربردهای کاربردی آن در حوزه امنیت و حریم خصوصی اینترنت اشیا اشاره دارد، بلکه اهمیت توجه به جوانب منفی و چالش‌های آن را نیز یادآوری می‌کند.

کلیدواژه‌ها: هوش مصنوعی، اینترنت اشیا، امنیت، حریم خصوصی.

* رایانامه نویسنده مسئول: E-mail: mohammad.beheshti@researcher.sharif.edu

۱. مقدمه

ظهور و ورود فناوری هوش مصنوعی مولد[1] (AI) در مفهوم اینترنت اشیا[2] (IoT)، عصری دگرگون‌کننده در مفاهیم ارتباطی و فناوری تصویر می‌کند که می‌تواند مرزهای نوآوری و کاربرد را دوباره تعریف کند. هوش مصنوعی مولد، زیرمجموعه‌ای از هوش مصنوعی است که بر ایجاد نمونه‌های مصنوعی از داده‌ها برای تقلید از الگوهای دنیای واقعی متمرکزشده است، این قابلیت رادار است که بتواند روش عملیاتی در دستگاه‌های اینترنت اشیا را متحول کند. قابلیت‌های هوش مصنوعی مولد در اینترنت اشیا از افزایش تجربیات کاربر در خانه‌های هوشمند [۱]، [۲] گرفته تا تعمیر و نگهداری پیش‌بینی‌شده در تنظیمات صنعتی [۳]، گسترده و عمیقاً تأثیرگذار هستند. بااین‌حال، ادغام این فناوری پیشرفته در IoT، نگرانی‌های امنیتی و حریم خصوصی قابل‌توجهی را ایجاد می‌کند که نمی‌توان آن‌ها را نادیده گرفت [۴]، [۵]، [۶]. مرجع [۷] به بررسی کاربردهای هوش مصنوعی تولیدی در زمینه محاسبات اینترنت اشیا می‌پردازد. نویسندگان مقاله به طور سامان‌مند چالش‌ها و فرصت‌های ترکیب این دو حوزه را تحلیل کرده و نشان می‌دهند که چگونه هوش مصنوعی مولد می‌تواند در بهینه‌سازی پردازش داده‌های حجیم، تولید داده‌های جدید، پیش‌بینی‌های دقیق‌تر و کاهش مصرف منابع در دستگاه‌های IoT نقش داشته باشد. این مقاله همچنین به‌مرور تحقیقات پیشین در این زمینه پرداخته و مزایای بالقوه استفاده از این فنّاوری برای توسعه دستگاه‌های هوشمندتر و مقیاس‌پذیر در محیط‌های IoT را مورد بررسی قرار می‌دهد.

همچنین، مقاله [۸] به تحلیل چالش‌ها و فرصت‌هایی که استفاده از هوش مصنوعی تولیدی در حوزه امنیت IoT ایجاد می‌کند، می‌پردازد و بر اهمیت استفاده از این فنّاوری برای مقابله با تهدیدات و آسیب‌پذیری‌های امنیتی در دستگاه‌های IoT تأکید دارد. نویسندگان به بررسی نحوه استفاده از هوش مصنوعی مولد برای شبیه‌سازی حملات، بهبود فرایندهای تشخیص تهدیدات و ایجاد مدل‌های پیشرفته برای جلوگیری از نفوذ در این دستگاه‌ها می‌پردازند. در سیر تحقیقاتی چند سال اخیر، جنبه امنیتی و حریم خصوصی استفاده از فناوری هوش مصنوعی در اینترنت اشیا به طور ویژه موردتوجه قرار گرفته است. برای نمونه، مرجع [۹] به شناسایی تهدیدات و ریسک‌های امنیتی مرتبط با پیاده‌سازی این فنّاوری در محیط‌های IoT، مانند خطرات حملات سایبری، دست‌کاری داده‌ها و سوءاستفاده از الگوریتم‌های تولیدی برای نفوذ به شبکه‌های IoT، می‌پردازند. همچنین، مقاله به بررسی چالش‌ها و نگرانی‌هایی که در زمینه مدیریت و حفاظت از اطلاعات در برابر سوءاستفاده از AI تولیدی در دستگاه‌های IoT وجود دارد، می‌پردازد و راهکارهایی برای کاهش این ریسک‌ها و تقویت امنیت دستگاه‌های IoT پیشنهاد می‌کند. به‌عنوان نمونه دیگر، مرجع [۱۰] بر روی تحلیل چالش‌ها، تهدیدات و راهکارهای امنیتی برای محافظت از دستگاه‌های IoT در برابر حملات و آسیب‌پذیری‌ها در دنیای AI تمرکز می‌نماید. این مقاله نه‌تنها به بررسی تأثیرات مثبت و منفی هوش مصنوعی در ارتقای امنیت IoT می‌پردازد، بلکه به تحلیل فناوری‌های نوین، مانند الگوریتم‌های یادگیری ماشین و هوش مصنوعی تولیدی، و نحوه استفاده از آن‌ها برای بهبود امنیت دستگاه‌های IoT می‌پردازد. همچنین، نویسندگان به شناسایی روندها و رویکردهای آینده در این زمینه، چالش‌های امنیتی جدید ناشی از پیشرفت‌های هوش مصنوعی و روش‌های مقابله با آن‌ها در دنیای اینترنت اشیا می‌پردازند.

دستگاه‌های اینترنت اشیا در زمینه‌های مختلف زندگی روزمره بشر، ازجمله موارد حیاتی مانند مراقبت‌های بهداشتی، مالی و حمل‌ونقل حضور دارند. ازآنجایی‌که دستگاه‌های IoT اغلب در حاشیه اقدامات امنیتی سنتی عمل می‌کنند و مقادیر زیادی داده تولید می‌کنند، این دستگاه‌ها به‌راحتی توسط مجرمان سایبری مورد حمله و سوءاستفاده قرار می‌گیرند. به‌عنوان‌مثال، حمله بات‌نت[3] (همانند حمله مشهور Mirai [۱۱]) تعداد زیادی از دستگاه‌های متصل به اینترنت را به یک بات‌نت تبدیل کرد و بسیاری از حوادث پرمخاطب دیگر نیز بر آسیب‌پذیری زیست‌بوم‌های IoT در برابر نقض‌های امنیتی تأکید می‌کنند که نه‌تنها خدمات را مختل می‌کند، بلکه حریم خصوصی، امنیت و ایمنی افراد و سازمان‌ها را نیز به خطر می‌اندازد [۱۲]، [۱۳]. ازاین‌رو، بررسی این خطرات امنیتی ناشی از هوش مصنوعی مولد در اینترنت اشیا در افزایش پیچیدگی و شیوع تهدیدات سایبری در دنیایی که همیشه متصل‌تر می‌شود، ضروری و حیاتی است.

در این مقاله، هدف اصلی ارائه یک تحلیل عمیق از خطرات امنیتی و حریم خصوصی مرتبط با استفاده از هوش مصنوعی مولد در اینترنت اشیا است. اگرچه هوش مصنوعی مولد مزایای فراوانی را در افزایش عملکرد و کارایی دستگاه‌های IoT به ارمغان می‌آورد، اما نیاز مبرمی به درک و رسیدگی به مشکلات و تهدیدات امنیتی بالقوه وجود دارد که این هم‌افزایی فناوری بین هوش مصنوعی و مفهوم اینترنت اشیا را همراهی می‌کند. این مقاله تلاش می‌کند تا دیدگاهی جامع ارائه دهد که نه‌تنها چالش‌ها را ترسیم می‌کند، بلکه به راهبُردهای بالقوه برای کاهش این تهدیدات نیز می‌پردازد. این تجزیه‌وتحلیل برای ذی‌نفعان در زیست‌بوم اینترنت اشیا، ازجمله توسعه‌دهندگان فناوری، سیاست‌گذاران و کاربران نهایی، ضروری است تا اطمینان حاصل

[1] Generative Artificial Intelligence
[2] Internet of Things
[3] Botnet

شود که استقرار و بهره‌مندی از هوش مصنوعی مولد در اینترنت اشیا، امن و قابل‌اعتماد است.

ادامه این مقاله به این شرح است: در بخش دوم، مروری بر هوش مصنوعی مولد در اینترنت اشیا ارائه می‌گردد. پس از تفصیل تجزیه‌وتحلیل ریسک‌های امنیتی در بخش سوم، در مورد راهبُردهای کاهش تهدیدات در بخش چهارم بحث می‌شود. در بخش پنجم، بینشی در مورد جهت آینده هوش مصنوعی مولد در اینترنت اشیا ارائه می‌گردد. درنهایت، در بخش ششم با جمع‌بندی و نتیجه‌گیری به این مقاله پایان داده می‌شود.

۲. مروری بر هوش مصنوعی مولد در IoT

هوش مصنوعی مولد شامل الگوریتم‌های پیچیده‌ای است که برای تولید داده‌های مصنوعی طراحی‌شده‌اند که بسیار شبیه الگوهای دنیای واقعی هستند. در قلمرو دستگاه‌های اینترنت اشیا، شبکه‌ای از دستگاه‌های متصل‌به‌هم قابلیت ارتباط و پردازش داده‌ها را به‌صورت مستقل دارند. در چشم‌انداز فناوری امروزی، هوش مصنوعی مولد، اینترنت اشیا را به سمت سطوح بی‌سابقه‌ای از نوآوری و کارایی سوق می‌دهد و فرصت‌های جدیدی را برای راه‌حل‌های هوشمند و خودکار باز می‌کند. در ادامه، مروری جامع بر هوش مصنوعی مولد در چارچوب اینترنت اشیا با تمرکز بر چهار جنبه ازجمله کاربردها، مزایا، ضعف‌ها و نگرانی‌های امنیتی و حریم خصوصی ارائه خواهیم داد.

۲-۱. برنامه‌های کاربردی

کاربردهای مختلف هوش مصنوعی مولد در اینترنت اشیا وجود دارد. برای مثال، در شهرهای هوشمند، هوش مصنوعی مولد شبیه‌سازی محیط‌های پیچیده شهری را برای بهینه‌سازی ترافیک و مصرف انرژی کم ممکن می‌سازد [۱]، [۲]. در مراقبت‌های بهداشتی، هوش مصنوعی مولد به تولید داده‌های مصنوعی بیمار برای تحقیق و درعین‌حال حفظ حریم خصوصی کمک می‌کند [۱۴]، [۱۵] و در اینترنت اشیا صنعتی، تعمیر و نگهداری پیش‌بینی‌کننده مبتنی بر هوش مصنوعی به طور مؤثری با پیش‌بینی و شناسایی نقص‌های تجهیزات قبل از وقوع، زمان خرابی را کاهش می‌دهد [۳]. این برنامه‌ها بر پتانسیل هوش مصنوعی مولد برای افزایش کارایی، دقت و نوآوری در بخش‌های مختلف تأکید می‌کنند.

۲-۲. مزیت‌ها

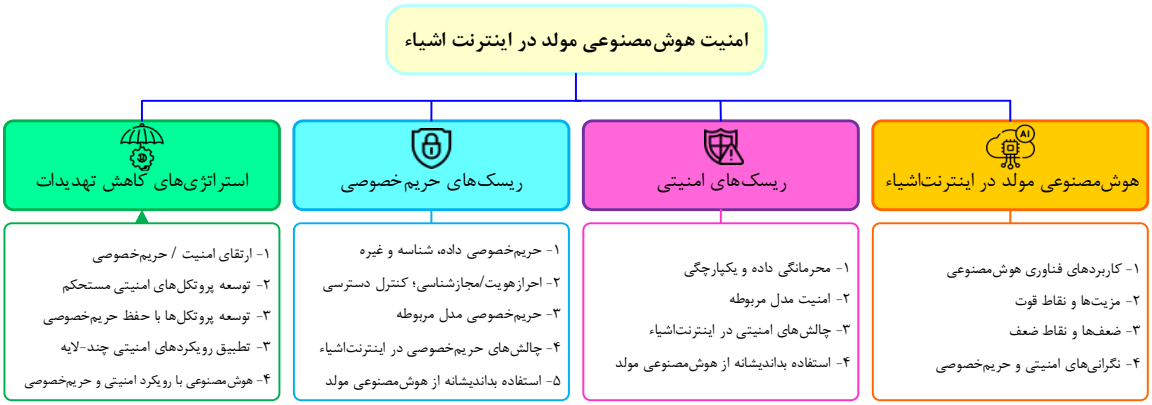
مزایای استفاده از هوش مصنوعی مولد در دستگاه‌های اینترنت اشیا بسیار زیاد و جالب‌توجه است. اولاً، فناوری هوش مصنوعی اجازه می‌دهد تا مجموعه‌داده‌های گسترده و متنوعی را برای آموزش مدل‌های یادگیری ماشینی که در آن داده‌های دنیای واقعی به‌احتمال زیاد کمیاب یا حساس باشند، تولید کند. این تولید داده مصنوعی در زمینه‌هایی که حفظ حریم خصوصی داده‌ها در اولویت است، بسیار مهم است. ثانیاً، هوش مصنوعی مولد تصمیم‌گیری و پیش‌بینی بهتر را امکان‌پذیر می‌کند. با شبیه‌سازی سناریوهای مختلف با استفاده از هوش مصنوعی مولد، دستگاه‌های IoT می‌توانند نتایج را پیش‌بینی کرده و فرایندها را بهینه کنند و متعاقباً منجر به افزایش کارایی عملیاتی شوند. درنهایت، هوش مصنوعی مولد با استفاده از طرح قابلیت‌ها و امکانات جدید در دستگاه‌های اینترنت اشیا می‌تواند نوآوری را هدایت کرده و راه را برای ایجاد محصولات و خدمات جدید هموار کند.

۲-۳. نقاط ضعف

ادغام هوش مصنوعی مولد در اینترنت اشیا دارای نقاط ضعفی نیز هست. پیچیدگی مدل‌های هوش مصنوعی مولد به این معنی است که آن‌ها به منابع محاسباتی قابل‌توجهی نیاز دارند که به‌ویژه در محیط‌های IoT که در آن دستگاه‌ها ممکن است قابلیت‌های پردازش محدودی داشته باشند، یک چالش خواهد بود. علاوه بر این، دقت داده‌های تولیدشده توسط این مدل‌های هوش مصنوعی بسیار مهم است؛ زیرا عدم دقت می‌تواند منجر به تصمیم‌گیری ناقص، به‌ویژه در برنامه‌های کاربردی حیاتی مانند مراقبت‌های بهداشتی شود. علاوه بر این، ادغام هوش مصنوعی مولد در زیست‌بوم‌های اینترنت اشیا موجود ممکن است چالش‌های ناهمگونی داده‌ها را ایجاد کند. به طور خاص، هنگام برخورد با دستگاه‌ها و فرمت‌های داده ناهمگن، اطمینان از یکپارچگی و سازگاری یکپارچه در بین اجزای مختلف اینترنت اشیا می‌تواند پیچیده باشد و ممکن است به منابع و تخصص بیشتری نیاز داشته باشد.

۲-۴. نگرانی‌های امنیتی و حریم خصوصی

بااین‌حال، مهم‌ترین نگرانی در حوزه امنیت و حریم خصوصی نهفته است. الگوریتم‌های مولد هوش مصنوعی قادر به تولید داده‌های بسیار واقعی هستند که می‌تواند یک شمشیر دو لبه باشد. از یک‌سو، این قابلیت برای ایجاد مجموعه‌داده‌های متنوع برای آموزش و شبیه‌سازی بسیار ارزشمند است. ازسوی‌دیگر، می‌توان از آن برای ایجاد حملات سایبری پیچیده، مانند دیپ‌فیک یا محتوای واقعی فیشینگ که محرمانگی، یکپارچگی و متعاقباً امنیت دستگاه‌های اینترنت اشیا را تهدید می‌کند، بهره‌برداری کرد. علاوه بر این، خود مدل‌های هوش مصنوعی می‌توانند به اهدافی برای حملات سایبری تبدیل شوند. به‌عنوان‌مثال، حملات بداندیشانِ می‌تواند منجر به خروجی‌های اشتباه از مدل‌های هوش مصنوعی شده و باعث شکست سامان‌مند در عملکرد اینترنت اشیا شود.



شکل ۱. نگرانی‌های تهدیدات امنیتی هوش مصنوعی مولد در اینترنت اشیا.

علاوه بر این، ماهیت به‌هم‌پیوسته دستگاه‌های اینترنت اشیا این مخاطرات را تشدید می‌کند، به این معنی که یک نقض امنیتی در یک دستگاه می‌تواند به طور بالقوه کل شبکه را به خطر بیندازد. به‌عبارت‌دیگر، با افزایش روزافزون تعداد دستگاه‌ها در دستگاه‌های اینترنت اشیا، ایجاد پروتکل‌های امنیتی قوی که می‌توانند همگام با تهدیدات سایبری در حال ظهور باشند، چالش‌برانگیزتر خواهد بود. شکل ۱ شماتیکی از نگرانی‌های مربوط به تهدیدات امنیتی هوش مصنوعی مولد در حوزه اینترنت اشیا را نشان می‌دهد.

۳. تحلیل ریسک‌های امنیتی و حریم خصوصی

ظهور هوش مصنوعی مولد در حوزه IoT نشان‌دهنده ادغام پیشگامانه دو فناوری و مفهوم پیشرفته است. بااین‌حال، در زیر سطح این پیشرفت‌های فنّاورانه شبکه پیچیده‌ای از خطرات امنیتی و حریم خصوصی نهفته است. این تهدیدات نه‌تنها چندوجهی هستند، بلکه با ویژگی‌های ذاتی هوش مصنوعی و ماهیت گسترده و به‌هم‌پیوسته شبکه‌های اینترنت اشیا نیز برجسته‌تر می‌شوند. در ادامه، ما یک تجزیه‌وتحلیل دقیق از این تهدیدات امنیتی و حریم خصوصی را توضیح خواهیم داد، بسیار مهم است که بدانیم پیامدها فراتر از چالش‌های فنی صرف هستند. هدف این تجزیه‌وتحلیل کشف این خطرات، ارائه بینشی در مورد ماهیت، تأثیر بالقوه، و فوریت‌هایی است که باید به آن‌ها پرداخته شود.

۳-۱. مقایسه ویژگی‌های حملات مبتنی بر AI با حملات مرسوم

در چشم‌انداز نوین تهدیدات سایبری، تفاوت‌های بنیادینی میان حملات سنتی و حملات نوین مبتنی بر هوش مصنوعی قابل‌مشاهده است. حملات سنتی عمدتاً بر پایه آسیب‌پذیری‌های شناخته‌شده، الگوهای ثابت و ابزارهای از پیش تعریف‌شده‌ای مانند بدافزار، فیشینگ، تزریق SQL و حملات انکار سرویس توزیع‌شده[1] (DDoS) طراحی می‌شوند. در مقابل، حملات مبتنی بر هوش مصنوعی از قابلیت‌های یادگیری، تطبیق‌پذیری و تصمیم‌گیری خودکار بهره می‌برند تا با تجزیه‌وتحلیل داده‌های رفتاری و محیطی، به شناسایی نقاط ضعف در سامانه‌های امنیتی پرداخته و از آن‌ها بهره‌برداری کنند. این دسته از تهدیدات با استفاده از فن‌هایی نظیر یادگیری ماشین، یادگیری عمیق، تولید محتوای جعلی (مانند دیپ‌فیک)، و مهندسی اجتماعی خودکار، توانایی فریب سامانه‌ها و کاربران را بادقت و مقیاس بالا فراهم می‌کنند. درنتیجه، حملات هوشمند به دلیل ماهیت پویا و غیرقابل‌پیش‌بینی خود، چالشی جدی‌تر و پیچیده‌تر برای سامانه‌های امنیتی مدرن محسوب می‌شوند.

از منظر محققان حوزه امنیت سایبری – هوش مصنوعی، تأثیر هوش مصنوعی بر امنیت سایبری شامل موارد زیر خواهد بود:

- گسترش تهدیدات موجود
- معرفی تهدیدهای جدید
- تغییر ویژگی‌های معمول تهدیدات جاری

گسترش تهدیدات موجود: فراگیری و دردسترس‌بودن دستگاه‌های متنوع هوش مصنوعی، باعث گسترش طیف گسترده بازیگرانی شده است که قادر به انجام حملات بالقوه قابل‌توجهی هستند. این حملات می‌تواند حملات علیه زیرساخت‌های حیاتی، استفاده مخرب از برنامه‌های کاربردی هوش مصنوعی و غیره باشند. همچنین مهاجمین با استفاده از فناوری هوش مصنوعی قادر به بهبود قابل‌توجه ابزارهای موجود مانند ابزارهای کشف آسیب‌پذیری هستند.

معرفی تهدیدهای جدید: علاوه بر گسترش تهدیدات موجود در مقیاس و دامنه، پیشرفت در هوش مصنوعی تهدیدهای کاملاً جدیدی را به فضای سایبری معرفی کرده است. ویژگی‌های هوش مصنوعی که محدود به توانایی‌های انسانی است، می‌تواند به مهاجمان اجازه دهد حملاتی را اجرا کنند که پیش‌تر امکان‌پذیر نبوده است.

[1] Distributrd Denial of Service

جدول ۱. مقایسه حملات امنیتی سایبری قبل و بعد از ظهور فناوری AI

ویژگی	حملات مبتنی بر هوش مصنوعی	حملات سایبری سنتی
ماهیت حمله	هوشمند، تطبیق‌پذیر، و گاهی خودکار	مبتنی بر قوانین، اغلب ایستا و به‌صورت دستی طراحی‌شده
برد حمله	مثال‌های خصمانه، آلوده‌سازی داده‌ها، سرقت مدل، دیپ‌فیک، فیشینگ هوشمند	بدافزار، فیشینگ، حملات منع سرویس‌دهی توزیع‌شده، حمله جستجوی فراگیر، تزریق SQL
اهداف حمله	مدل‌های یادگیری ماشین، زنجیره‌های پردازش هوش مصنوعی، مجموعه‌داده‌ها	سرورها، پایگاه‌های داده، شبکه‌ها، ایستگاه‌های کاری کاربران
استفاده از یادگیری	از یادگیری ماشین برای بهبود و تقویت حمله استفاده می‌شود	معمولاً بدون یادگیری، مبتنی بر آسیب‌پذیری‌های شناخته‌شده
سفارشی‌سازی	بسیار خاص و تطبیق‌پذیر - می‌تواند رفتار کاربر را تقلید کند	اغلب عمومی و قابل‌استفاده مجدد در اهداف مختلف
روش‌های گریز از شناسایی	پویا و تطبیق‌پذیر - تغییر رفتار برای عبور از دستگاه‌های امنیتی	روش‌های ایستا مانند کدگذاری یا مخفی‌سازی
قابلیت مقیاس‌پذیری	بسیار مقیاس‌پذیر با استفاده از خودکارسازی و مدل‌های قابل باز استفاده	گسترش سخت‌تر به دلیل نیاز به منابع انسانی بیشتر
سختی در شناسایی	دشوارتر - شبیه به داده یا رفتار واقعی کاربران عمل می‌کند	آسان‌تر - با ابزارهای شناسایی مبتنی بر امضا قابل‌شناسایی است
نمونه‌ها	دیپ‌فیک مدیرعامل، حملات خصمانه، بدافزار هوشمند، فیشینگ صوتی باهوش مصنوعی	باج‌افزار، تروجان، اسکریپت‌نویسی بین سایتی، جعل ایمیل
سازوکارهای دفاعی	ت	فایروال، آنتی‌ویروس، دستگاه‌های تشخیص نفوذ، به‌روزرسانی امنیتی

حملات متنوع مبتنی بر Deepfake مثالی از تهدیدهای جدید است.

تغییر ویژگی‌های معمول تهدیدات جاری: مهاجمین با استفاده از فناوری هوش مصنوعی قادر به گسترش تهدیدهای سنتی هستند. به‌عنوان‌مثال با استفاده از هوش مصنوعی می‌توان ویژگی‌های بدافزارها را به‌گونه‌ای تغییر داد که شناسایی آنان بسیار دشوار و گاهی غیرممکن شود. Deeplock نمونه‌ای از بدافزارهای فراری مبتنی بر هوش مصنوعی است.

در ادامه قصد داریم تا مقایسه‌ای از ویژگی‌های مربوط به حملات پیش از ظهور فناوری هوش مصنوعی و پس از گسترش این فناوری ارائه نماییم [۱۶-۲۱]. جدول ۱ این مقایسه را نشان می‌دهد.

۳-۲. محرمانگی و یکپارچگی داده‌ها و حریم خصوصی شناسه

حفظ محرمانگی و یکپارچگی داده‌ها به‌عنوان نگرانی‌های اساسی در تقاطع پویای فناوری هوش مصنوعی و مفهوم اینترنت اشیا ایجاد می‌شود. منظور از تقاطع پویای بین هوش مصنوعی و اینترنت اشیا هم‌زمانی و تعامل میان این فناوری و مفهوم در دنیای مدرن است که موجب ایجاد تحولی در نحوه عملکرد و بهره‌برداری از سامانه‌ها و شبکه‌های متصل‌به‌هم می‌شود. در این تقاطع، هوش مصنوعی به‌عنوان یک عامل فعال و هوشمند، داده‌های تولیدی توسط دستگاه‌های اینترنت اشیا را پردازش، تحلیل و بهینه‌سازی می‌کند. این تعامل پویا باعث می‌شود که IoT تنها یک شبکه از دستگاه‌های متصل نباشد، بلکه به یک سامانه هوشمند تبدیل شود که قادر است به طور خودکار تصمیم‌گیری کند، پیش‌بینی‌های دقیقی انجام دهد و رفتارهای خود را بر اساس داده‌های دریافت شده و تحلیل‌های AI تنظیم کند. اصل مسئله در توانایی هوش مصنوعی مولد برای ایجاد و دست‌کاری حجم وسیعی از داده‌ها نهفته است. بااین‌حال، اگر به‌درستی محافظت نشود، این فناوری می‌تواند منجر به نقض قابل‌توجهی در حریم خصوصی داده (محرمانگی) و به‌خطرافتادن یکپارچگی داده‌ها شود [۲۲]، [۲۳]. به‌خصوص، در محیط‌های IoT که در آن دستگاه‌ها به طور مداوم داده‌ها را جمع‌آوری و انتقال می‌دهند، پتانسیل نشت چنین داده‌ای به طور تصاعدی بزرگ می‌شود. علاوه بر این، ماهیت به‌هم‌پیوسته دستگاه‌های اینترنت اشیا نشان می‌دهد که یک نقطه آسیب‌پذیری می‌تواند اثرات آبشاری داشته باشد و داده‌های در معرض خطر را در سراسر شبکه پخش کند. این امر نه‌تنها حریم خصوصی کاربران را به خطر می‌اندازد، بلکه اعتماد کل دستگاه‌های اینترنت اشیا را نیز تضعیف می‌کند. به‌عنوان‌مثال، نقض یک دستگاه خانه هوشمند به طور بالقوه می‌تواند اطلاعات شخصی زیادی از کارهای روزمره گرفته تا اطلاعات شخصی حساس را در معرض دید و افشای قرار دهد. با پیشرفت روزافزون این سامانه‌ها، فن‌های مورداستفاده برای بهره‌برداری از آسیب‌پذیری‌های آن‌ها نیز قدرتمندتر می‌شوند؛ بنابراین، به یک رویکرد فعال و دائماً در حال تکامل برای امن‌سازی داده‌ها نیاز است که هم از محرمانگی و هم یکپارچگی آن اطمینان حاصل گردد و هم از حفظ ابعاد مختلف حریم خصوصی مطمئن شد.

۳-۳. امنیت و حریم خصوصی مدل‌های AI

امنیت و حریم خصوصی مدل‌های هوش مصنوعی مولد نیز یک نگرانی حیاتی در زیست‌بوم‌های اینترنت اشیا محسوب می‌شود. این مدل‌ها، هسته دستگاه‌های مبتنی بر هوش مصنوعی، مستعد اشکال مختلف مصالحه هستند که می‌تواند به‌شدت عملکرد و امنیت/حریم خصوصی کاربردهای IoT را تضعیف کند [۲۴]. یکی از شکل‌های رایج حمله، سرقت مدل‌های هوش مصنوعی است. مجرمان سایبری ممکن است این مدل‌ها را بدزدند تا ساختار و عملکرد آن‌ها را درک کنند و به آن‌ها امکان حملات مؤثرتر یا توسعه اقدامات متقابل علیه دستگاه‌های امنیتی مبتنی بر هوش مصنوعی را بدهند. تهدید مهم دیگر مسموم‌شدن مدل‌های هوش مصنوعی در مرحله آموزش و یا سوءاستفاده از اطلاعات شخصی کاربر موردنظر است. در این سناریو، مهاجمان داده‌های مخرب را به مجموعه آموزشی تزریق می‌کنند و باعث می‌شوند مدل الگوهای نادرست یا سوگیری‌های غلط را بیاموزد. هنگامی‌که این مدل در کاربردهای اینترنت اشیا در دنیای واقعی پیاده‌سازی می‌شود، می‌تواند منجر به اختلال در تصمیم‌گیری شود. به‌عنوان‌مثال، یک مدل هوش مصنوعی به خطر افتاده در یک سامانه امنیتی هوشمند ممکن است تهدیدات امنیتی واقعی را تشخیص ندهد و سامانه را آسیب‌پذیر کند. این خطرات بر اهمیت امن‌سازی مدل‌های هوش مصنوعی در برابر دسترسی و دست‌کاری غیرمجاز تأکید می‌کند.

۳-۴. چالش‌های امنیتی/حریم خصوصی در شبکه‌های اینترنت اشیا

پیچیدگی و تنوع ذاتی شبکه‌های اینترنت اشیا چالش‌های امنیتی ناشی از ادغام هوش مصنوعی مولد را تقویت می‌کند. هر دستگاه در زیست‌بوم اینترنت اشیا، از حسگرهای ساده گرفته تا پردازنده‌های پیچیده، نشان‌دهنده یک نقطه آسیب‌پذیری بالقوه است. یک رخنه در یک دستگاه می‌تواند یک اثر دومینو داشته باشد و به طور بالقوه کل شبکه را در معرض خطر قرار دهد. علاوه بر این، ناهمگونی دستگاه‌های اینترنت اشیا که هر یک از قابلیت‌ها و پروتکل‌های امنیتی متفاوت هستند، چالشی منحصربه‌فرد را ایجاد می‌کند. استانداردسازی اقدامات امنیتی در چنین طیف متنوعی از دستگاه‌ها دشوار است و اغلب منجر به ناهماهنگی در پیاده‌سازی‌های امنیتی می‌شود. این ناهماهنگی‌ها می‌تواند شکاف‌های امنیتی ایجاد کند و شبکه را در برابر حملات آسیب‌پذیر کند. در یک‌کلام، چالش کلیدی در امن‌سازی شبکه‌های IoT در ماهیت گسترده و به‌هم‌پیوسته آن‌ها نهفته است. این پیوستگی مستلزم یک راهبُرد امنیتی قوی و جامع است که فراتر از دستگاه‌های جداگانه گسترش می‌یابد و کل شبکه را در برمی‌گیرد.

۳-۵. استفاده مخرب از هوش مصنوعی مولد

هنگامی‌که این توانایی‌ها برای اهداف مخرب در زیست‌بوم اینترنت اشیا استفاده می‌شوند، قابلیت‌های پیشرفته هوش مصنوعی مولد در ایجاد داده‌های بسیار واقعی و متقاعدکننده، نگرانی‌های امنیتی قابل‌توجهی را نیز ایجاد می‌کند [۲۵]. ایجاد دیپ‌فیک‌های پیچیده یا ساخت داده‌های گمراه‌کننده با استفاده از فناوری‌های هوش مصنوعی مولد تهدیدی جدی برای یکپارچگی و قابلیت اطمینان دستگاه‌های اینترنت اشیا است. این جعلیات تولیدشده توسط هوش مصنوعی که می‌توانند صوتی، تصویری یا انواع داده‌های دیگر باشند، به طور فزاینده‌ای از محتوای معتبر قابل‌تشخیص نیستند. در زمینه اینترنت اشیا، جایی که دستگاه‌ها اغلب به ورودی داده‌ها برای تصمیم‌گیری خودکار متکی هستند، می‌توان از دیپ‌فیک برای گمراه‌کردن سامانه‌ها استفاده کرد. برای مثال، دیپ‌فیک‌های صوتی را می‌توان برای جعل هویت فرمان‌های صوتی به دستگاه‌های خانه هوشمند مورداستفاده قرارداد که منجر به دسترسی غیرمجاز یا انجام اقداماتی می‌شود که امنیت و حریم خصوصی کاربر را به خطر می‌اندازد. علاوه بر این، هوش مصنوعی مولد می‌تواند برای ساخت جریان‌های داده یا خروجی‌های حسگر در محیط‌های IoT مورد سوءاستفاده قرار گیرد که منجر به رفتارهای دست‌کاری‌شده در دستگاه‌های متصل می‌شود. این می‌تواند عواقب گسترده‌ای داشته باشد، به‌ویژه در کاربردهای حیاتی مانند دستگاه‌های نظارت بر مراقبت‌های بهداشتی یا خودکارسازی صنعتی که در آن تصمیم‌گیری به‌شدت به‌دقت و صحت داده‌ها متکی است. به‌این‌ترتیب، پتانسیل سوءاستفاده از هوش مصنوعی مولد در اینترنت اشیا نیازمند اقدامات متقابل قوی، ازجمله فن‌های تشخیص پیشرفته و پروتکل‌های امنیتی سخت‌گیرانه، برای محافظت در برابر این تهدیدات در حال تکامل و پیچیده است.

به طور خلاصه، درحالی‌که هوش مصنوعی مولد پتانسیل فوق‌العاده‌ای را در افزایش کاربردهای اینترنت اشیا ارائه می‌دهد، اذعان به خطرات امنیتی مرتبط نیز ضروری است. این خطرات، از نگرانی‌های مربوط به حریم خصوصی داده‌ها تا آسیب‌پذیری‌ها در الگوریتم‌های هوش مصنوعی، چالش‌های مهمی را برای استقرار امن و مؤثر این فناوری‌ها ایجاد می‌کند. همان‌طور که اینترنت اشیا به تکامل خود ادامه می‌دهد، یک رویکرد فعال و جامع به امنیت برای اطمینان از قابل‌اعتماد بودن و قابلیت اطمینان این دستگاه‌های به‌هم‌پیوسته ضروری است. توسعه آینده هوش مصنوعی و اینترنت اشیا مولد باید امنیت و حریم خصوصی را در اولویت قرار دهد تا به طور کامل پتانسیل آن‌ها را تحقق بخشد.

۴. راهبُرد برای کاهش تهدیدات

همان‌طور که در بالا ذکر شد، اگرچه هوش مصنوعی مولد اینترنت اشیا را به سمت ارتفاعات جدیدی از نوآوری و کارایی سوق می‌دهد، اما مجموعه‌ای از چالش‌ها را نیز به‌خصوص ازنظر امنیت به همراه دارد. پرداختن به این چالش‌ها برای استفاده از پتانسیل کامل هوش مصنوعی مولد در اینترنت اشیا و اطمینان از عملکرد ایمن و قابل‌اعتماد این دستگاه‌های به‌هم‌پیوسته بسیار مهم است؛ بنابراین، تمرکز پژوهش باید بر توسعه راهبُردهایی باشد که نه‌تنها از قابلیت‌های هوش مصنوعی مولد استفاده کند، بلکه از آسیب‌پذیری‌های بالقوه آن نیز محافظت کند. در ادامه، راهبُردهای مختلفی را برای کاهش خطرات امنیتی و حریم خصوصی ذاتی در ادغام هوش مصنوعی مولد در زیست‌بوم‌های اینترنت اشیا بررسی می‌کنیم.

۴-۱. ارتقای سطح امنیت و حریم خصوصی

در چشم‌انداز به‌سرعت در حال تحول هوش مصنوعی مولد در IoT، حفاظت از داده‌های حیاتی بسیار مهم است. چراکه داده‌ها سنگ بنای عملکرد هوش مصنوعی هستند و فرایندهای یادگیری و توانایی‌های تصمیم‌گیری این دستگاه‌های پیشرفته را هدایت می‌کنند. در حقیقت، داده‌ها در هوش مصنوعی به‌عنوان اساس و مبنای اصلی عمل می‌کنند. این سامانه‌ها برای یادگیری و تصمیم‌گیری از داده‌ها استفاده می‌کنند. به طور خاص، هوش مصنوعی با استفاده از داده‌ها آموزش می‌بینند و از آن‌ها برای شبیه‌سازی فرایندهای انسانی مانند تشخیص الگوها، پیش‌بینی‌ها و تصمیم‌گیری‌های خود استفاده می‌کند.

درواقع، عملکرد هوش مصنوعی بستگی به این دارد که داده‌های ورودی چقدر دقیق، غنی و متنوع باشند. هرچه داده‌ها بیشتر و باکیفیت‌تر باشند، مدل‌های هوش مصنوعی می‌توانند نتایج بهتری ارائه دهند. به همین دلیل، فرایند یادگیری ماشین درواقع به‌وسیله داده‌ها هدایت می‌شود؛ یعنی این داده‌ها به مدل کمک می‌کنند تا از آن‌ها ”بیاموزد“ و تصمیمات بهتری بگیرد. به عبارت ساده‌تر، داده‌ها مواد اولیه‌ای هستند که هوش مصنوعی با استفاده از آن‌ها ”آموخته“ و عملکرد خود را بهبود می‌بخشد. این باعث می‌شود که مدل‌ها در تصمیم‌گیری‌های پیچیده‌تر و دقیق‌تر موفق‌تر باشند.

برای افزایش محرمانگی، یکپارچگی داده‌ها و حریم خصوصی، وجود یک رویکرد چندوجهی ضروری است که شامل فن‌هایی مانند رمزگذاری، ناشناس‌سازی یا احراز اصالت گمنام/شبه‌گمنام، مجازشناسی و کنترل دسترسی دقیق و نظارت مستمر است. (۱) رمزگذاری به‌عنوان اولین خط دفاع عمل می‌کند که می‌تواند داده‌ها را به‌گونه‌ای رمزگذاری کند که فقط توسط نهادهای مجاز قابل‌دسترسی و تفسیر باشد. روش‌های رمزگذاری پیشرفته به‌ویژه در محیط‌های IoT که در آن داده‌ها اغلب در شبکه‌ها و دستگاه‌ها منتقل می‌شوند، حیاتی هستند. با اطمینان از این‌که داده‌ها در حین انتقال رمزگذاری شده باقی می‌مانند، می‌توان خطر دسترسی یا ره‌گیری غیرمجاز را به میزان قابل‌توجهی کاهش داد. (۲) ناشناس‌سازی یا گمنام‌سازی همچنین نقش مهمی در حفاظت از حریم خصوصی شناسه یا هویت کاربر دارد. فن‌هایی مانند حریم خصوصی متفاوت، استخراج اطلاعات مفید از مجموعه‌داده‌ها را درحالی‌که شناسه/هویت افراد را پنهان می‌کند، امکان‌پذیر می‌کند. این فن‌ها در حفظ تعادل ظریف بین ابزار داده و حریم خصوصی شخصی بسیار مهم هستند. (۳) مجازشناسی و کنترل دسترسی دقیق یکی دیگر از اجزای حیاتی راهبُرد حفاظت از داده‌های قوی است. این تعیین سطح دسترسی تضمین می‌کنند که فقط کارکنان یا کاربران مجاز به داده‌های حساس دسترسی دارند، بنابراین خطر نقض تصادفی یا مخرب داده‌ها به حداقل می‌رسد. این می‌تواند شامل احراز اصالت/هویت چندعاملی، کنترل‌های دسترسی مبتنی بر نقش، و ممیزی منظم گزارش‌های دسترسی برای شناسایی هرگونه فعالیت غیرمجاز یا مشکوک باشد. (۴) نظارت و به‌روزرسانی مستمر این اقدامات امنیتی برای انطباق با تهدیدات و آسیب‌پذیری‌های جدید در چشم‌انداز دیجیتال در حال تحول حیاتی است. با تقویت حس‌آگاهی امنیتی، سازمان‌ها می‌توانند دفاع خود را در برابر تهدیدات احتمالی دستگاه‌های IoT مبتنی بر AI-Driven خود تقویت کنند.

۴-۲. توسعه پروتکل‌های امنیتی/حریم خصوصی قوی

ماهیت در حال تحول تهدیدات سایبری، به‌روزرسانی‌ها و وصله‌های منظم را به‌عنوان یک جنبه اساسی برای امنیت دستگاه‌های IoT و مدل‌های هوش مصنوعی ضروری می‌کند، به این معنی که امنیت سایبری دیگر ثابت نیست، بنابراین به اقدامات پویا و فعال نیاز دارد. سازوکارهای به‌روزرسانی خودکار نقش مهمی در این فرایند ایفا می‌کنند و به طور مداوم تضمین می‌کنند که دستگاه‌ها و سامانه‌ها بر روی جدیدترین نسخه‌های نرم‌افزاری کار می‌کنند که شامل آخرین پیشرفت‌های امنیتی برای محافظت در برابر آسیب‌پذیری‌های نوظهور است. علاوه بر این، پروتکل‌های امنیتی قوی که می‌توانند کل چرخه عمر دستگاه‌های IoT و مدل‌های هوش مصنوعی مولد را در بربگیرند، می‌توانند خطر مؤثر را کاهش دهند. این پروتکل‌ها جزءلاینفک فرایند توسعه هستند، ازجمله شیوه‌های رمزنگاشتی امن و ممیزی‌های امنیتی منظم، می‌تواند تضمین کند که ملاحظات امنیتی از همان ابتدا تعبیه‌شده‌اند و درنتیجه دستگاه‌ها و سامانه‌ها را در برابر تهدیدات بالقوه تقویت می‌کنند. به طور

خلاصه، این پروتکل‌های امنیتی جامع برای حفظ یکپارچگی و قابلیت اطمینان IoT و فناوری‌های مولد هوش مصنوعی در مواجهه با تهدیدات سایبری دائماً در حال تغییر بسیار مهم هستند.

۴-۳. اتخاذ رویکردهای امنیتی چندلایه

رویکرد چندلایه یا دفاعی عمیق به امنیت در حوزه زیست‌بوم‌های اینترنت اشیا مفید و ضروری است [۲۶]. این سامانه امنیتی چندلایه به‌گونه‌ای طراحی‌شده است که اگر یکی از لایه‌ها از کار بیفتد یا در معرض خطر قرار گیرد، لایه‌های بعدی همچنان محافظت می‌کنند. این راهبُرد شامل اجرای چندین لایه دفاعی، ایجاد یک سامانه امنیتی است که بسیار انعطاف‌پذیرتر از هر رویکرد تک لایه‌ای است. در ابتدایی‌ترین سطح، این می‌تواند شامل استقرار دیوارهای آتش[1] باشد که به‌عنوان اولین خط دفاع در برابر حملات خارجی عمل می‌کنند و ترافیک شبکه ورودی و خروجی را بر اساس قوانین امنیتی ازپیش‌تعیین‌شده کنترل می‌کنند. علاوه بر فایروال‌ها، دستگاه‌های تشخیص نفوذ[2] (IDS) می‌توانند برای نظارت بر ترافیک شبکه برای فعالیت‌های مشکوک و تهدیدات بالقوه مورداستفاده قرار گیرند و مدیران شبکه را از هرگونه ناهنجاری آگاه کنند. علاوه بر این، ارزیابی‌های منظم آسیب‌پذیری نیز یکی دیگر از مؤلفه‌های کلیدی رویکرد امنیتی چندلایه است که در شناسایی و رسیدگی به شکاف‌های امنیتی احتمالی در سامانه، قبل از این‌که توسط مهاجمان مورد سوءاستفاده قرار گیرند، مفید است. علاوه بر این، رویکرد امنیتی چندلایه فراتر از اقدامات فنی است که می‌تواند شامل کنترل‌های اداری مانند سیاست‌های امنیتی، آموزش کاربر و طرح‌های واکنش به حادثه باشد. علاوه بر این، اقدامات امنیتی فیزیکی، مانند دسترسی ایمن به سخت‌افزار، نیز بخشی جدایی‌ناپذیر از یک رویکرد چندلایه است. در یک‌کلام، رویکرد چندلایه شامل ترکیبی جامع و راهبردی از اقدامات امنیتی فنی، اداری و فیزیکی است که همگی برای محافظت از اجزای وسیع و متنوع چشم‌انداز اینترنت اشیا در برابر تهدیدات سایبری در حال تحول تلاش می‌کنند.

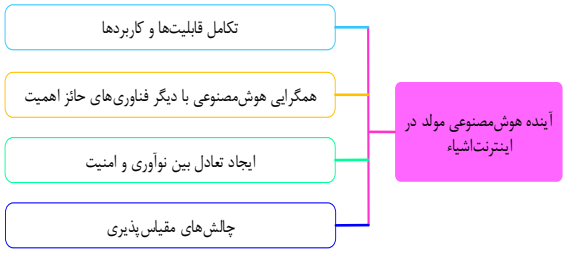
۵. استفاده از هوش مصنوعی برای امنیت و حریم خصوصی

اگرچه ظهور هوش مصنوعی پیچیدگی‌های جدیدی را به چشم‌انداز اینترنت اشیا وارد می‌کند، خود هوش مصنوعی می‌تواند به‌عنوان یک ابزار قدرتمند در نبرد با خطرات امنیتی مورداستفاده قرار داده شود. الگوریتم‌های یادگیری ماشین، به‌عنوان سنگ بنای هوش مصنوعی، می‌توانند مجموعه‌داده‌های گسترده را بسیار کارآمدتر از روش‌های سنتی تجزیه‌وتحلیل کنند. (۱) این الگوریتم‌ها در تشخیص الگوها یا ناهنجاری‌های غیرعادی در ترافیک شبکه که اغلب شاخص‌های تهدیدات امنیتی هستند، خوب هستند. این سامانه‌ها با یادگیری مداوم از داده‌هایی که پردازش می‌کنند، به طور فزاینده‌ای در شناسایی ریسک‌های بالقوه، حتی در صورت ظهور، مهارت پیدا می‌کنند. این تشخیص بلادرنگ برای شبکه‌های مدرن بسیار مهم است، جایی که تهدیدها می‌توانند به‌سرعت تکامل یابند و اقدامات امنیتی سنتی ممکن است عقب بمانند. (۲) فراتر از تشخیص، هوش مصنوعی می‌تواند فعالانه در کاهش تهدید شرکت کند. به‌عنوان‌مثال، پس از شناسایی یک نقض امنیتی احتمالی، دستگاه‌های هوش مصنوعی می‌توانند پروتکل‌هایی را برای جداسازی بخش شبکه آسیب‌دیده آغاز کنند و درنتیجه گسترش حمله را محدود کنند. این واکنش فوری می‌تواند در به‌حداقل‌رساندن آسیب درحالی‌که کارشناسان انسانی وضعیت را ارزیابی و رسیدگی می‌کنند بسیار ارزشمند باشد. (۳) قابلیت‌های پیش‌بینی هوش مصنوعی همچنین می‌تواند سناریوهای مختلف حمله سایبری را شبیه‌سازی کند تا به سازمان‌ها کمک کند تا دفاع خود را به‌دقت آزمایش کنند. این شبیه‌سازی‌ها می‌توانند آسیب‌پذیری‌هایی را نشان دهند که ممکن است در طول ممیزی‌های امنیتی استاندارد آشکار نباشند، و امکان تقویت پیشگیرانه دفاعی را فراهم می‌کنند، به‌ویژه در دوره‌ای که تهدیدات سایبری نه‌تنها مکرر هستند، بلکه به طور فزاینده‌ای پیچیده‌تر می‌شوند. (۴) نقش هوش مصنوعی در امنیت سایبری می‌تواند به تقویت سایر اقدامات امنیتی نیز گسترش یابد. به‌عنوان‌مثال، در حوزه تأیید هویت، هوش مصنوعی می‌تواند الگوهای رفتاری را برای تشخیص ناهنجاری‌ها تجزیه‌وتحلیل کند و یک‌لایه اضافی از احراز هویت اضافه کند. در رمزگذاری، هوش مصنوعی می‌تواند کلیدهای رمزگذاری پیچیده را به طور مؤثرتر مدیریت کند و اطمینان حاصل کند که داده‌ها امن و درعین‌حال برای کاربران مجاز قابل‌دسترسی هستند. در اصل، با استفاده از توانایی هوش مصنوعی برای پردازش و تجزیه‌وتحلیل داده‌ها در مقیاس‌های بی‌سابقه، می‌توانیم ماهیت واکنشی امنیت سنتی را به یک سامانه دفاعی پویا و سازگار از طریق ادغام هوش مصنوعی در راهبُردهای امنیت سایبری سنتی تبدیل کنیم.

به طور خلاصه، کاهش خطرات امنیتی مرتبط با استفاده از هوش مصنوعی مولد در اینترنت اشیا نیازمند یک رویکرد جامع است. ما می‌توانیم با افزایش حریم خصوصی و یکپارچگی داده‌ها، توسعه پروتکل‌های امنیتی قوی، اتخاذ رویکردهای امنیتی چندلایه و استفاده از خود هوش مصنوعی برای امنیت، به سازمان‌ها کمک کنیم تا وضعیت امنیتی زیست‌بوم‌های اینترنت

[1] Firewall
[2] Intrusion Detection System

اشیا خود را بهبود بخشند. بااین‌حال، محدودیت‌های راهبُردهای پیشنهادی برای کاهش خطرات در ادغام هوش مصنوعی و اینترنت اشیا مولد هنوز چالش‌های قابل‌توجهی را ایجاد می‌کند. (۱) افزایش حریم خصوصی و یکپارچگی داده‌ها، هزینه‌های سنگینی را برای سازمان‌های کوچک‌تر ایجاد می‌کند. به‌ویژه، ناشناس‌سازی و رمزگذاری خطا نیست، و حفظ حریم خصوصی در محیط‌های داده پویا یک مبارزه مداوم است. (۲) مدیریت پروتکل‌های امنیتی قوی همچنان می‌تواند سامانه‌ها را در مواجهه با تکامل سریع تهدیدها و پیچیدگی‌های ذاتی آسیب‌پذیر کند و خطای انسانی نیز نقطه‌ضعف قابل‌توجهی در اجرای پروتکل‌های امنیتی است. (۳) اتخاذ رویکردهای امنیتی چندلایه مجموعه‌ای از عوارض خود را به همراه دارد. به طور خاص، مدیریت این لایه‌ها می‌تواند پیچیده و نیازمند منابع باشد، و می‌تواند منجر به تضاد یا کار اضافی شود که به طور بالقوه احساس امنیت کاذبی را ارائه می‌دهد. (۴) استفاده از هوش مصنوعی برای امنیت به‌شدت به کیفیت داده‌ها بستگی دارد و به تخصص و منابع قابل‌توجهی نیاز دارد. این محدودیت‌ها بر نیاز به رویکردی پویا و تطبیقی برای امنیت تأکید می‌کند. سرمایه‌گذاری مداوم در امنیت برای حفاظت از پتانسیل ادغام‌های هوش مصنوعی و اینترنت اشیا ضروری است.



شکل ۲. آینده هوش مصنوعی مولد در اینترنت اشیا.

۵-۱. امن‌سازی مدل‌های هوش مصنوعی

تهدیدات سایبری برای هوش مصنوعی (AI) می‌تواند شامل طیف وسیعی از مسائل باشد که می‌توان آن‌ها را به چند دسته اصلی تقسیم کرد. در زیر به برخی از این تهدیدات و چالش‌ها اشاره می‌نماییم:

*** حملات داده‌ای**

- داده‌های آلوده: اگر داده‌هایی که برای آموزش مدل‌های هوش مصنوعی استفاده می‌شوند، شامل اطلاعات نادرست یا مخرب باشند، می‌توانند منجر به عملکرد نادرست مدل شوند.
- حملات تزریقی: در این نوع حمله، مهاجم داده‌های خاصی را به سامانه تزریق می‌کند تا مدل را فریب دهد و خروجی‌های نادرست تولید کند.

*** حملات مدل**

- سرقت مدل: مهاجمان می‌توانند سعی کنند مدل‌های هوش مصنوعی را به سرقت ببرند تا از آن‌ها برای اهداف خود استفاده کنند.
- تغییر مدل: با دست‌کاری عامل‌های مدل، مهاجمان می‌توانند عملکرد آن را تغییر دهند و از آن به نفع خود بهره‌برداری کنند.

*** حملات به دستگاه‌های هوش مصنوعی**

- حملات بر مبنای تخاصم (adversarial): این نوع حملات به‌گونه‌ای طراحی‌شده‌اند که ورودی‌های خاصی به سامانه داده شود تا باعث اشتباه در پیش‌بینی‌ها و تصمیم‌گیری‌های هوش مصنوعی شوند.
- حملات زمان واقعی: در سامانه‌هایی که به‌صورت زنده و آنی تصمیم‌گیری می‌کنند، مهاجم می‌تواند با ایجاد اختلال در داده‌های ورودی، سامانه را مختل کند.

۵-۲. مسائل حریم خصوصی و امنیت داده

- نشت اطلاعات: استفاده از داده‌های حساس برای آموزش مدل‌های هوش مصنوعی می‌تواند منجر به نشت اطلاعات شخصی شود.
- تحلیل‌های ناخواسته: مدل‌های هوش مصنوعی می‌توانند به طور غیرمستقیم اطلاعات حساس را از داده‌های عمومی استخراج کنند.

*** پیامدهای اخلاقی و اجتماعی**

- سوگیری: مدل‌های هوش مصنوعی ممکن است تحت‌تأثیر داده‌های نادرست یا ناقص قرار گیرند و تصمیمات سوگیری را اتخاذ کنند که می‌تواند تبعات اجتماعی داشته باشد.
- استفاده‌های مخرب: هوش مصنوعی می‌تواند در دست مهاجمان برای ایجاد حملات سایبری پیچیده‌تر و کارآمدتر استفاده شود.

برای مقابله با این تهدیدات، سازمان‌ها باید بر روی امنیت داده‌ها، آموزش مدل‌ها و پیاده‌سازی پروتکل‌های امنیتی مناسب تمرکز کنند. همچنین، نظارت مستمر بر عملکرد مدل‌ها و به‌روزرسانی آن‌ها در برابر تهدیدات جدید ضروری است.

۵. هوش مصنوعی آینده در IoT

همان‌طور که به آینده می‌نگریم، ادغام هوش مصنوعی مولد با اینترنت اشیا همچنان منظره‌ای پر از پتانسیل و چالش را ارائه می‌دهد. این بحث عمیقاً پیشرفت‌های پیش‌بینی‌شده آینده هوش مصنوعی مولد در اینترنت اشیا را بررسی می‌کند.

۵-۱. قابلیت‌ها و برنامه‌های در حال تکامل

پیشرفت مداوم در الگوریتم‌های هوش مصنوعی مولد نوید گسترش قابلیت‌ها و برنامه‌های کاربردی در اینترنت اشیا را می‌دهد. می‌توان تولید داده‌های پیچیده‌تر، تجزیه‌وتحلیل پیش‌بینی بهبودیافته و خودکارسازی پیشرفته در بخش‌های مختلف را پیش‌بینی نمود. به‌عنوان‌مثال، در شهرهای هوشمند، هوش مصنوعی مولد می‌تواند به دستگاه‌های برنامه‌ریزی و مدیریت شهری کارآمدتر منجر شود. در مراقبت‌های بهداشتی، مراقبت شخصی از بیمار از طریق برنامه‌های تشخیصی و درمانی مبتنی بر هوش مصنوعی می‌تواند به یک هنجار تبدیل شود. در صنعت، هوش مصنوعی مولد می‌تواند به بهبود خودکارسازی، نگهداری پیش‌بینی‌کننده و بهینه‌سازی فرایندهای تولید کمک کند تا بازدهی بهتر و کاهش زمان ازکارافتادگی را محقق کند. بااین‌حال، این پیشرفت‌ها همواره پیچیدگی‌ها و چالش‌های جدیدی را به‌ویژه ازنظر ملاحظات امنیتی و حریم خصوصی ایجاد خواهند کرد.

۵-۲. همگرایی هوش مصنوعی با سایر فناوری‌های نوظهور

در آینده احتمالاً هوش مصنوعی مولد نه‌تنها به‌صورت مجزا، بلکه در همگرایی با سایر فناوری‌های نوظهور مانند محاسبات کوانتومی، 5G، محاسبات لبه و یادگیری تقویتی خواهد بود. این همگرایی پتانسیل افزایش تصاعدی قابلیت‌های دستگاه‌های IoT را دارد، اما چشم‌انداز امنیتی را نیز پیچیده می‌کند. هوش مصنوعی مولد نقش مهمی در انقلاب صنعتی بعدی که اغلب صنعت ۴.۰ نامیده می‌شود، ایفا خواهد کرد. ادغام صنعت ۴.۰ با IoT در تنظیمات صنعتی منجر به فرایندهای تولید هوشمندتر و کارآمدتر می‌شود. این ادغام همچنین به این معنی است که خطرات نقض امنیتی بیشتر خواهد بود و به طور بالقوه بر زیرساخت‌ها و اقتصادهای حیاتی تأثیر می‌گذارد. علاوه بر این، ماهیت تطبیقی الگوریتم‌های یادگیری تقویتی مورداستفاده در هوش مصنوعی مولد ممکن است منجر به آسیب‌پذیری‌های پیش‌بینی‌نشده و حملات خصمانه شود. به هر صورت و با صرف‌نظر از تهدیدات و مخاطرات امنیتی، این همگرایی باعث ایجاد دستگاه‌های هوشمندتر و پیشرفته‌تری می‌شود که قادر به حل مسائل پیچیده‌تر و ارائه راه‌حل‌های نوآورانه‌تر هستند. برای درک این فرایند و اهمیت آن، به بررسی برخی از این همگرایی‌ها می‌پردازیم:

- **هوش مصنوعی و اینترنت اشیا:** هوش مصنوعی و IoT به طور فزاینده‌ای با یکدیگر ترکیب می‌شوند تا دستگاه‌های هوشمند و متصل ایجاد کنند. در این همگرایی، دستگاه‌های متصل به اینترنت داده‌هایی را جمع‌آوری کرده و هوش مصنوعی از این داده‌ها برای تجزیه‌وتحلیل، پیش‌بینی و بهینه‌سازی عملکرد دستگاه‌ها استفاده می‌کند. برای مثال، در یک‌خانه هوشمند، دستگاه‌های IoT مانند ترموستات‌ها، لامپ‌ها و دوربین‌های امنیتی می‌توانند داده‌ها را جمع‌آوری کرده و الگوریتم‌های هوش مصنوعی به کار گرفته شوند تا بر اساس رفتار کاربران، تنظیمات بهینه‌تری پیشنهاد دهند.
- **هوش مصنوعی و زنجیره قالبی:** در همگرایی هوش مصنوعی و زنجیره قالبی، می‌توان از زنجیره قالبی برای افزایش امنیت و شفافیت داده‌های مورداستفاده در دستگاه‌های هوش مصنوعی استفاده کرد. علاوه بر این، هوش مصنوعی می‌تواند به تحلیل و مدیریت داده‌های زنجیره قالبی کمک کند و روندهای پیچیده در زنجیره قالبی را شبیه‌سازی و پیش‌بینی کند. برای نمونه، در دستگاه‌های مالی و معاملات دیجیتال، زنجیره قالبی به‌عنوان بستر امن و غیرمتمرکز برای ذخیره داده‌ها عمل می‌کند، درحالی‌که هوش مصنوعی به شناسایی تقلب و پیش‌بینی نوسانات بازار کمک می‌کند.
- **هوش مصنوعی و واقعیت افزوده/مجازی (AR/VR):** ترکیب هوش مصنوعی با AR و VR به ایجاد تجربیات غنی‌تر و هوشمندتر در دنیای مجازی کمک می‌کند. هوش مصنوعی می‌تواند الگوهای حرکتی کاربران را تحلیل کرده و به آن‌ها تعاملات واقع‌گرایانه‌تری ارائه دهد. برای مثال، در آموزش پزشکی، واقعیت افزوده می‌تواند تصاویر سه‌بعدی از اندام‌های بدن انسان را نمایش دهد و هوش مصنوعی می‌تواند تحلیل‌های پزشکی پیشرفته را ارائه دهد تا پزشکان به طور مؤثرتری عمل کنند.
- **هوش مصنوعی و فناوری 5G:** فناوری 5G با فراهم‌کردن سرعت بالای انتقال داده و تأخیر کم، به هوش مصنوعی کمک می‌کند تا سریع‌تر و به‌صورت مقیاس‌پذیرتر به تحلیل داده‌ها بپردازد. این امر به‌ویژه در محیط‌های حساس به زمان، مانند خودروهای خودران، حیاتی است .برای نمونه، در خودروهای خودران، ارتباطات لحظه‌ای بین خودروها و زیرساخت‌ها با استفاده از 5G به هوش مصنوعی این امکان را می‌دهد که در زمان واقعی تصمیمات حیاتی را اتخاذ کند.
- **هوش مصنوعی و رایانش ابری:** رایانش ابری بستری مناسب برای ذخیره‌سازی و پردازش داده‌های عظیم موردنیاز برای آموزش و بهبود مدل‌های هوش مصنوعی فراهم می‌کند. این ترکیب به سازمان‌ها اجازه می‌دهد تا بدون نیاز به زیرساخت‌های سخت‌افزاری گران‌قیمت، از قدرت پردازش AI بهره‌برداری کنند. شرکت‌های بزرگی

مانند گوگل و آمازون از رایانش ابری برای ارائه سرویس‌های هوش مصنوعی خود استفاده می‌کنند که این امر به کاربران امکان می‌دهد تا به مدل‌های پیشرفته‌ای مانند یادگیری ماشین و پردازش زبان طبیعی دسترسی داشته باشند.

- **هوش مصنوعی و فناوری‌های زیستی:** ترکیب هوش مصنوعی با فناوری‌های زیستی می‌تواند پیشرفت‌های چشمگیری در درمان‌های پزشکی، کشف دارو و حتی ژنتیک ایجاد کند. هوش مصنوعی به‌ویژه در تحلیل داده‌های زیستی و کشف الگوهای پیچیده مفید است. در تشخیص بیماری‌ها، مدل‌های هوش مصنوعی می‌توانند تصاویر پزشکی را تحلیل کنند و به پزشکان در تشخیص زودهنگام بیماری‌ها مانند سرطان کمک کنند.

۵-۳. ایجاد تعادل بین نوآوری و امنیت

با قوی‌تر شدن هوش مصنوعی مولد، خطرات امنیتی که ایجاد می‌کند احتمالاً تکامل‌یافته و پیچیده‌تر می‌شوند. آینده نیازمند تعادل ظریفی بین پذیرش قابلیت‌های نوآورانه هوش مصنوعی مولد و اطمینان از برقراری تدابیر امنیتی قوی است. این تعادل مستلزم تحقیق‌وتوسعه مداوم در فناوری‌های امنیتی و همچنین چارچوب‌های نظارتی پویا است که می‌توانند با تکامل این فناوری‌های مولد هوش مصنوعی و اینترنت اشیا سازگار شوند. آینده به راهبُردهای پیشگیرانه برای حل انواع جدید حملات سایبری و آسیب‌پذیری نیاز دارد.

۵-۴. خطر امنیتی هوش مصنوعی مولد چندعاملی در اینترنت اشیا

تکثیر هوش مصنوعی مولد چندعاملی در اینترنت اشیا نگرانی‌های امنیتی را ایجاد می‌کند، زیرا ساختار غیرمتمرکز دستگاه‌های چندعاملی می‌تواند باعث آسیب‌پذیری در ارتباطات و هماهنگی عامل شود. این آسیب‌پذیری‌ها فرصت‌هایی را برای مهاجمان مخرب ایجاد می‌کند تا از آن‌ها سوءاستفاده کنند که به طور بالقوه منجر به دسترسی غیرمجاز، دست‌کاری داده‌ها یا اختلال در سامانه می‌شود. علاوه بر این، ویژگی‌های پویا و تطبیقی ذاتی در دستگاه‌های چندعاملی چالش شناسایی و رسیدگی سریع به تهدیدات امنیتی را تشدید می‌کند و خطرات قابل‌توجهی را برای یکپارچگی، محرمانه بودن و دردسترس‌بودن داده‌ها و خدمات اینترنت اشیا ایجاد می‌کند.

۵-۵. چالش‌های مقیاس‌پذیری

با ادامه گسترش شبکه‌های اینترنت اشیا، مدیریت و ایمن‌سازی این شبکه‌های وسیع به طور فزاینده‌ای چالش‌برانگیز خواهد شد. ازنظر کاربرد هوش مصنوعی مولد در اینترنت اشیا، چالش‌های مقیاس‌پذیری ناشی از افزایش حجم و پیچیدگی داده‌های تولیدشده توسط دستگاه‌های اینترنت اشیا است. در همین حال، برای پیشرفت‌های آینده، باید روی راه‌حل‌های امنیتی مقیاس‌پذیری نیز تمرکز کنیم که می‌توانند با اندازه و پیچیدگی روبه‌رشد شبکه‌های اینترنت اشیا سازگار شوند.

به طور خلاصه، آینده هوش مصنوعی مولد در IoT نوآوری و تکامل مستمر را تجربه خواهد کرد. به طور خاص، با اتخاذ رویکردی فعال و مشارکتی، می‌توان از پتانسیل کامل هوش مصنوعی مولد در اینترنت اشیا استفاده نمود و آینده‌ای را ایجاد کرد که ازنظر فناوری پیشرفته باشد. بااین‌وجود، هنگام آماده‌سازی برای ادغام این فناوری‌ها در بسیاری از برنامه‌های کاربردی واقعی، ما همچنین به تلاش برای رسیدگی به چالش‌های امنیتی در حال ظهور نیاز خواهد بود.

۶. نتیجه‌گیری

همان‌طور که در این مقاله بررسی شد، ترکیب هوش مصنوعی (AI) مولد با اینترنت اشیا (IoT) تأثیرات عمیق و گسترده‌ای در آینده فناوری و جامعه خواهد داشت. این همگرایی، با ایجاد امکان خودکارسازی بیشتر، بهره‌وری بالا و تحلیل‌های دقیق‌تری از داده‌ها، فرصت‌های بی‌نظیری برای صنایع مختلف فراهم می‌کند. به‌ویژه در بخش‌های مثل بهداشت، حمل‌ونقل و خانه‌های هوشمند، این ترکیب توانایی دارد که کاربردهای اینترنت اشیا را به سطحی نوین برساند، جایی که تصمیم‌گیری‌های هوشمند و پیش‌بینی‌های دقیق به‌صورت خودکار و در زمان واقعی صورت می‌گیرد.

بااین‌حال، همان‌طور که این فناوری‌ها فرصت‌های زیادی به دست می‌دهند، برخی چالش‌ها و تهدیدات نیز وجود دارند. یکی از نگرانی‌های اصلی، مسائل امنیتی است. تهدیدهایی مانند نقض حریم خصوصی داده‌ها، سوءاستفاده از فناوری‌های هوش مصنوعی و حملات سایبری می‌توانند نه‌تنها اعتماد کاربران را از بین ببرند، بلکه بر عملکرد سامانه‌ها و کارایی آن‌ها تأثیر منفی بگذارند؛ بنابراین، باید این تهدیدات به‌طورجدی موردتوجه قرار گیرد تا از بروز آسیب‌های احتمالی جلوگیری شود.

برای استفاده بهینه از این همگرایی و تبدیل تهدیدها به فرصت، ضروری است که ابتدا یک نگاه جامع به‌تمامی ابعاد این ترکیب داشته باشیم. در یک طرف، باید فرصت‌های عظیمی را که هوش مصنوعی مولد و اینترنت اشیا به‌دقت می‌دهند، شناسایی کرده و از آن‌ها برای بهبود عملکرد و بهره‌وری استفاده کنیم. در طرف دیگر، باید با استفاده از راهکارهای امنیتی پیشرفته و استفاده بهینه از داده‌ها، تهدیدات احتمالی را کاهش داده و

امنیت این سامانه‌ها را در اولویت قرار دهیم. به طور خاص، می‌توانیم از هوش مصنوعی برای پیش‌بینی حملات سایبری و شناسایی الگوهای خطرناک در داده‌ها استفاده کنیم. علاوه بر این، استفاده از فناوری‌های رمزنگاری پیشرفته و کنترل دسترسی‌های هوشمند در ترکیب با اینترنت اشیا، می‌تواند اطمینان حاصل کند که اطلاعات حساس به طور ایمن منتقل و ذخیره شوند. در همین راستا، همکاری با گروه‌های امنیتی و متخصصین برای طراحی زیرساخت‌های مقاوم در برابر تهدیدات، از اهمیت ویژه‌ای برخوردار است.

درنهایت، در نگاهی خوش‌بینانه اما واقع‌بینانه به آینده هوش مصنوعی مولد در اینترنت اشیا، باید با رویکردی متعادل حرکت نمود. این رویکرد باید شامل شوروشوق نوآوری‌های فناورانه همراه با ملاحظات دقیق امنیتی باشد تا هم بتوان از پیشرفت‌های فناورانه بهره‌برداری کرد و هم از آسیب‌های احتمالی جلوگیری نمود. با این رویکرد، می‌توانیم با ترکیب این دو فناوری، به فصل جدیدی از پیشرفت و تحول وارد شویم، جایی که نه‌تنها بهره‌وری و کارایی ارتقا می‌یابد، بلکه امنیت و اعتماد کاربران نیز در بالاترین سطح خود قرار خواهد گرفت. ترکیب هوش مصنوعی مولد و اینترنت اشیا قادر است انقلاب بزرگی در فناوری‌های نوین ایجاد کند، اما این تحول باید با مدیریت دقیق تهدیدات امنیتی همراه باشد. استفاده بهینه از این فرصت‌ها و تهدیدها، درنهایت به تحقق آینده‌ای پایدار و امن برای فناوری‌ها کمک خواهد کرد، جایی که امنیت، اعتماد و نوآوری در کنار هم قرار خواهند گرفت و پیشرفت‌های جامعه بشری را تسریع خواهند کرد.

۷. مراجع

[1] M. E. E. Alahi, A. Sukkuea, F. W. Tina, A. Nag, W. Kurdthongmee, K. Suwannarat, and S. C. Mukhopadhyay, “Integration of iot-enabled technologies and artificial intelligence (ai) for smart city scenario: Recent advancements and future trends,” Sensors, vol. 23, no. 11, p. 5206, 2023.

[2] B. Yamini, M. Jayaprakash, S. Logesswari, V. Ulagamuthalvi, R. Porselvi, and G. Uthayakumar, “Enhanced expectation-maximization algorithm for smart traffic iot systems using deep generative adversarial networks to reduce waiting time,” in 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE, 2023, pp. 380–385.

[3] X. Liang, Z. Liu, H. Chang, and L. Zhang, “Wireless channel data augmentation for artificial intelligence of things in industrial environment using generative adversarial networks,” in 2020 IEEE 18th International Conference on Industrial Informatics (INDIN), vol. 1. IEEE, pp. 502–507, 2020.

[4] Z. Xiong, W. Li, and Z. Cai, “Federated generative model on multisource heterogeneous data in iot,” in Proceedings of the AAAI Conference on Artificial Intelligence, vol. 37, no. 9. AAAI, pp. 10537–10545, 2023.

[5] S. De, M. Bermudez-Edo, H. Xu, and Z. Cai, “Deep generative models in the industrial internet of things: a survey,” IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 5728–5737, 2022.

[6] S. Malik, A. K. Tyagi, and S. Mahajan, “Architecture, generative model, and deep reinforcement learning for iot applications: Deep learning perspective,” Artificial Intelligence-based Internet of Things Systems, pp. 243–265, 2022.

[7]. F. Mangione, C. Savaglio, G. Fortino. “Generative Artificial Intelligence for Internet of Things Computing: A Systematic Survey. ” arXiv preprint arXiv:2504.07635, 2025.

[8]. YL Aung, I Christian, Y Dong, X Ye, S Chattopadhyay, J Zhou. “Generative ai for internet of things security: Challenges and opportunities.” arXiv preprint arXiv:2502.08886, 2025.

[9]. H Xu, Y Li, O Balogun, S Wu, Y Wang, Z Cai. “Security risks concerns of generative AI in the IoT.” IEEE Internet of Things Magazine 7, no. 3, pp: 62-67, 2024.

[10]. H. Mamoona, N. Tariq, M. Alfayad, M. Zakwan, Gh. Alwakid, and M. Assiri. “Securing the Internet of Things in artificial intelligence era: A comprehensive survey. ” IEEE access 12, pp: 25469-25490, 2024.

[11] A. Affinito, S. Zinno, G. Stanco, A. Botta and G. Ventre, “The evolution of Mirai botnet scans over a six-year period”. Journal of Information Security and Applications, 79, p.103629, 2023.

[12] N. Abdalgawad, A. Sajun, Y. Kaddoura, I. A. Zualkernan, and F. Aloul, “Generative deep learning to detect cyberattacks for the iot-23 dataset,” IEEE Access, vol. 10, pp. 6430–6441, 2021.

[13] M. A. Ferrag, M. Debbah, and M. Al-Hawawreh, “Generative ai for cyber threat-hunting in 6g-enabled iot networks,” arXiv preprint arXiv:2303.11751, 2023.

[14] K. Nova, “Generative ai in healthcare: advancements in electronic health records, facilitating medical languages, and personalized patient care,” Journal of Advanced Analytics in Healthcare Management, vol. 7, no. 1, pp. 115–131, 2023.

[15] R. E. Crossler, F. B´elanger, and D. Ormond, “The quest for complete security: An empirical analysis of users’ multi-layered protection from security threats,” Information Systems Frontiers, vol. 21, pp. 343–357, 2019.

[16]. MIT Technology Review (2023), How ChatGPT and AI Tools are Used in Phishing Campaigns, News article on NLP abuse in social engineering. https://www.technologyreview.com/

[17]. Symantec (2020), I See You: The Rise of AI-Powered Malware, Threat intelligence report.

[18]. Europol (2022), Facing Reality? Law Enforcement and the Challenge of Deepfakes, Europol Innovation Lab Report.

[19]. Y. Zhou, J. Xu & J. Liu, (2022). AI-powered cyber threats: Emerging risks and defenses. IEEE Transactions on Dependable and Secure Computing.

[20]. Andress, J. (2021), The Basics of Information Security (4th ed.) , Syngress / Elsevier.

[21]. OWASP Foundation, Top 10 Web Application Security Risks, OWASP.

[22] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, “From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy,” IEEE Access, 2023.

[23] T. Wang, Y. Zhang, S. Qi, R. Zhao, Z. Xia, and J. Weng, “Security and privacy on generative data in aigc: A survey,” arXiv preprint arXiv:2309.09435, 2023.

[24] S. A. Khowaja, K. Dev, N. M. F. Qureshi, P. Khuwaja, and L. Foschini, “Toward industrial private ai: A two-tier framework for data and model security,” IEEE Wireless Communications, vol. 29, no. 2, pp. 76–83, 2022.

[25] Z. Xiong, H. Xu, W. Li, and Z. Cai, “Multi-source adversarial sample attack on autonomous vehicles,” IEEE Transactions on Vehicular Technology, vol. 70, no. 3, pp. 2822–2835, 2021.

[26] C. Dilibal, B. L. Davis, and C. Chakraborty, “Generative design methodology for internet of medical things (iomt)-based wearable biomedical devices,” in 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2021, pp. 1–4.