Artificial Intelligence in the Security of Autonomous Systems

هوش مصنوعی در امنیت سیستم های خودمختار

فرزانه الشریف[۱]،شهرام محمدی[۲]،مرضیه ملک زاده[۳]

[۱]دانشکده مهندسی کامپیوتر،واحد اصفهان،دانشگاه ملی مهارت دختران،اصفهان،ایران

[۲]دانشکده مهندسی کامپیوتر،واحد اصفهان،دانشگاه ملی مهارت دختران،اصفهان،ایران

[۳]دانشکده مهندسی کامپیوتر،واحد اصفهان،دانشگاه ملی مهارت دختران،اصفهان،ایران

چکیده

با گسترش روزافزون سیستم‌های خودمختار در حوزه‌های مختلفی مانند خودروهای خودران، پهپادها و ربات‌های صنعتی، امنیت سایبری این سیستم‌ها اهمیت بی‌سابقه‌ای یافته است. با این حال، تعاملات پیچیده و ارتباطات شبکه‌ای این سیستم‌ها آن‌ها را در معرض تهدیدات سایبری فزاینده‌ای قرار داده است.

هوش مصنوعی، به ویژه هوش مصنوعی مولد (GenAI)[۱]،با توانایی تولید داده‌های مصنوعی، شناسایی تهدیدات، و مدیریت تطبیقی، ابزار قدرتمندی برای مقابله با این چالش‌ها ارائه می‌دهد از سوی دیگر، فناوری بلاکچین به دلیل ساختار غیرمتمرکز و تغییرناپذیر خود، مکملی ایده‌آل برای تأمین امنیت داده‌ها و ارتباطات در سیستم‌های خودمختار است. این مقاله با بررسی نقش دو فناوری نوظهور، یعنی هوش مصنوعی [۲] (AI)و بلاکچین، به دنبال ارائه راه حل‌های امنیتی برای مقابله با چالش‌های پیچیده موجود است.

کلمات کلیدی:امنیت،هوش مصنوعی،سیستم های خودمختار

[۱] Generative AI (GenAI)
[۲] Artificial intelligence (AI)

.مقدمه

سیستم‌های خودمختار امروزه در بسیاری از زمینه‌ها از جمله حمل‌ونقل، نظارت، تولید و خدمات عمومی کاربردهای گسترده‌ای پیدا کرده‌اند. این سیستم‌ها با استفاده از ترکیب پیچیده‌ای از سنسورها، الگوریتم‌های پیشرفته، یادگیری ماشین و ارتباطات شبکه‌ای، قادر به انجام وظایف به‌طور خودکار و بدون نیاز به دخالت انسانی هستند. به عنوان مثال، خودروهای خودران، ربات‌های جراحی، و سیستم‌های هوشمند نظارتی، از جمله کاربردهای رایج سیستم‌های خودمختار در دنیای مدرن هستند. این پیشرفت‌های تکنولوژیکی به‌طور قابل توجهی بهره‌وری، ایمنی و کیفیت زندگی انسان‌ها را ارتقا داده‌اند.

با این حال، یکی از چالش‌های اصلی که سیستم‌های خودمختار با آن روبه‌رو هستند، امنیت سایبری این سیستم‌ها است. سیستم‌های خودمختار، به دلیل تعامل گسترده با محیط‌های پیچیده و متغیر، به شدت در معرض تهدیدات سایبری قرار دارند. این تهدیدات می‌توانند از حملات ساده مانند تزریق داده‌های جعلی و حملات انکار سرویس [1] (DoS)تا حملات پیچیده‌تر مبتنی بر هوش مصنوعی خصمانه متغیر باشند. به عنوان مثال، حملات تزریق داده‌های جعلی می‌توانند باعث اختلال در تصمیم‌گیری‌های این سیستم‌ها شده و عملکرد آنها را به خطر بیندازند. از سوی دیگر، حملات DoS ممکن است موجب اختلال در شبکه‌های ارتباطی شده و کارایی سیستم‌های خودمختار را کاهش دهند. علاوه بر این، استفاده از هوش مصنوعی در برخی حملات می‌تواند سیستم‌های خودمختار را فریب داده و به آنها آسیب وارد کند.

امنیت این سیستم‌ها به‌ویژه از آن جهت اهمیت پیدا می‌کند که آن‌ها به داده‌های دقیق و به‌روزی نیاز دارند تا بتوانند تصمیمات صحیحی اتخاذ کنند. الگوریتم‌های پیچیده یادگیری ماشین که در قلب این سیستم‌ها قرار دارند، باید بتوانند بدون هیچ گونه خطا یا نقصی عمل کنند. به همین دلیل، هر گونه نقص یا آسیب در هر یک از اجزای این سیستم‌ها می‌تواند منجر به پیامدهای جبران‌ناپذیری از جمله خسارات مالی و جانی شود.

در این راستا، فناوری‌های نوینی نظیر هوش مصنوعی مولد و بلاکچین می‌توانند به‌طور چشمگیری به بهبود امنیت سیستم‌های خودمختار کمک کنند. هوش مصنوعی مولد به دلیل توانایی خود در تولید داده‌های مصنوعی و شبیه‌سازی سناریوهای مختلف، می‌تواند برای شناسایی تهدیدات و حملات سایبری به‌کار گرفته شود. این توانایی به سیستم‌های خودمختار این امکان را می‌دهد که با شبیه‌سازی حملات مختلف، نقاط ضعف خود را شناسایی کرده و آن‌ها را بهبود دهند. علاوه بر این، بلاکچین به عنوان یک فناوری برای تأمین امنیت و شفافیت داده‌ها، می‌تواند در زمینه حفاظت از داده‌های مورد استفاده در این سیستم‌ها و نیز اعتبارسنجی تراکنش‌ها و تصمیمات کمک کند. استفاده از بلاکچین در سیستم‌های خودمختار موجب ایجاد یک شبکه امن، مقاوم در برابر تغییرات غیرمجاز و قابل اعتماد خواهد شد.

با توجه به این چالش‌ها و فرصت‌ها، این مقاله به بررسی روش‌های مختلف مقابله با تهدیدات سایبری در سیستم‌های خودمختار پرداخته و تلاش دارد تا راهبردهای نوآورانه‌ای را برای بهبود امنیت این سیستم‌ها ارائه دهد. در این مسیر، به تحلیل نقش فناوری‌های نوین، نظیر هوش مصنوعی مولد و بلاکچین، و همچنین بررسی چالش‌ها و محدودیت‌های موجود در پیاده‌سازی این راهکارها خواهیم پرداخت. هدف نهایی مقاله، شناسایی راه‌حل‌های عملی و مؤثر برای مقابله با تهدیدات سایبری و افزایش قابلیت اطمینان و امنیت در سیستم‌های خودمختار است.

[1] Disk Operating System (DOS)

۲.سیستم‌های خودمختار و اهمیت امنیت آن‌ها

۲-۱. ویژگی‌ها و عملکرد سیستم‌های خودمختار[۱]

سیستم‌های خودمختار شامل ترکیبی از سنسورها، واحدهای پردازش داده و ماژول‌های تصمیم‌گیری مستقل هستند. این سیستم‌ها در حوزه‌های مختلفی مانند خودروهای خودران، پهپادهای نظارتی، ربات‌های صنعتی و سیستم‌های بهداشتی کاربرد دارند.

ویژگی‌های کلیدی:

- **جمع‌آوری داده‌ها :**استفاده از سنسورهای پیشرفته مانند LIDAR[۲] ، دوربین‌ها و حسگرهای حرارتی برای درک محیط.
- **پردازش اطلاعات :**تحلیل داده‌ها با استفاده از الگوریتم‌های هوش مصنوعی و یادگیری ماشین.
- **تصمیم‌گیری مستقل :**اقدام بر اساس تحلیل‌های انجام‌شده بدون نیاز به دخالت انسانی.

مثال‌ها:

- **خودروهای خودران** :مدیریت ترافیک و تصمیم‌گیری در لحظه.
- **پهپادهای نظامی** :انجام مأموریت‌های پیچیده در مناطق خطرناک.
- **ربات‌های صنعتی :**خودکارسازی فرآیندهای تولید با دقت بالا.

۲-۲. تهدیدات امنیتی سیستم‌های خودمختار

سیستم‌های خودمختار به دلیل وابستگی شدید به داده‌ها و الگوریتم‌ها، در معرض تهدیدات زیر قرار دارند:

الف. حملات سایبری

- **تزریق داده‌های جعلی** :مهاجمان با دستکاری داده‌های حسگرها می‌توانند عملکرد سیستم را مختل کنند مثل GPS.
- **حملات انکار سرویس** :(DoS) ارسال حجم زیادی از داده به سیستم برای متوقف کردن عملکرد آن.
- **حملات MIMT**[۳]:اطلاعات در حین انتقال ربوده شده و تغییر می‌یابند.
- **حملات خصمانه به الگوریتم‌ها** :تغییر ورودی‌ها برای ایجاد خطا در تصمیم‌گیری سیستم.

ب. مشکلات ایمنی و حریم خصوصی

- افشای داده‌های حساس کاربران.
- عدم اطمینان از صحت تصمیمات گرفته‌شده توسط سیستم.

[1] Autonomous systems
[2] Light detection and ranging lidar(LIDAR)
[3] Man-in-the-Middle (MIMT)

ج. ضعف در(ROS) [1]

- **رمزنگاری‌نشدن ترافیک شبکه :**مهاجمان می‌توانند داده‌های انتقالی را مشاهده و سرقت کنند.
- **مشکل در تأیید اعتبار داده‌ها :**بررسی نکردن یکپارچگی برای شناسایی فعالیت‌های مخرب.
- **آسیب‌پذیری در ساختار گراف** :ناشناس‌بودن گره‌های ارتباطی به مهاجمان امکان تزریق داده‌های مخرب می‌دهد.

۲-۳. هوش مصنوعی(AI)

هوش مصنوعی شاخه‌ای از علوم کامپیوتر است که به توسعه سیستم‌هایی می‌پردازد که می‌توانند رفتارهای هوشمندانه‌ای مانند یادگیری، استدلال و تصمیم‌گیری را شبیه‌سازی کنند.

۲-۴. هوش مصنوعی مولد

هوش مصنوعی مولد یکی از زیرشاخه های هوش مصنوعی است وبه عنوان ستاره‌ای نوظهور در آسمان فناوری، با توانایی‌های شگفت‌انگیز خود، امیدهای تازه‌ای برای مقابله با این تهدیدات به ارمغان آورده است. این فناوری، با خلق داده‌های مصنوعی و شبیه‌سازی سناریوهای پیچیده، افق‌های جدیدی برای تقویت امنیت سیستم‌های خودمختار گشوده است.

- **تولید داده‌های مصنوعی :**تصور کنید که بتوانیم پیش از وقوع حملات سایبری واقعی، آن‌ها را در دنیایی شبیه‌سازی‌شده تجربه و تحلیل کنیم. هوش مصنوعی مولد چنین امکانی را فراهم می‌کند و با شبیه‌سازی حملات، به شناسایی نقاط ضعف سیستم کمک می‌کند.
- **تقویت الگوریتم‌های دفاعی** :این فناوری می‌تواند با ایجاد داده‌های متنوع، مدل‌های یادگیری ماشین را توانمندتر کرده و قدرت آن‌ها را در شناسایی تهدیدات پنهان افزایش دهد.
- **شناسایی الگوهای پنهان :**هوش مصنوعی مولد مانند یک کارآگاه دیجیتال، به دقت داده‌ها و رفتارهای سیستم‌های خودمختار را تحلیل می‌کند تا ناهنجاری‌ها را پیش از آنکه به فاجعه تبدیل شوند، کشف کند.

۲-۵. نقش فناوری‌های پیشرفته مانند هوش مصنوعی مولد در امنیت سیستم‌های خودمختار

۱. **شبیه‌سازی حملات سایبری:**

فناوری‌هایی مشابه با هوش مصنوعی مولد می‌توانند سناریوهای حمله را شبیه‌سازی کنند، از جمله حملات تزریق داده، انکار سرویس(DoS) ، یا دستکاری فرمان‌های کنترلی. این شبیه‌سازی‌ها به توسعه روش‌های مقاوم‌سازی سیستم‌های خودمختار کمک می‌کنند.

۲. **شخیص و پیشگیری از تهدیدات:**

سیستم‌های مبتنی بر هوش مصنوعی مولد با تحلیل داده‌های جمع‌آوری‌شده توسط سنسورها، می‌توانند الگوهای غیرعادی را شناسایی کنند. این قابلیت باعث می‌شود که قبل از وقوع یک حمله سایبری یا اختلال، هشدارهای لازم صادر شود.

---

[1]Robot Operating System(ROS)

۳. **افزایش استحکام مدل‌های یادگیری ماشین:**

یکی از چالش‌های اصلی در امنیت سیستم‌های خودمختار، کمبود داده‌های واقعی برای آموزش مدل‌های یادگیری ماشین است. هوش مصنوعی مولد می‌تواند داده‌های مصنوعی با کیفیت بالا تولید کند که به بهبود دقت مدل‌های تشخیص تهدید کمک می‌کند.

٤. **بازسازی و تقویت پس از حمله:**

در صورت وقوع حمله یا اختلال، فناوری‌هایی مشابه با هوش مصنوعی مولد می‌توانند برای بازسازی داده‌ها و بازیابی سیستم‌ها استفاده شوند. این قابلیت به ویژه در مواقعی که سیستم‌های خودمختار دچار خرابی بحرانی شده‌اند، بسیار مفید است.

٥. **ترکیب با فناوری‌های مکمل مانند بلاکچین:**

بلاکچین با ایجاد زنجیره‌ای شفاف و غیرقابل تغییر برای ذخیره داده‌ها و ثبت رویدادها، امنیت سیستم‌های خودمختار را بهبود می‌بخشد. هوش مصنوعی مولد می‌تواند به تحلیل تهدیدهای مرتبط با این شبکه‌ها و تقویت امنیت آن‌ها کمک کند.

۲-۶. دلایل مهم بودن این فناوری ها برای سیستم های خودمختار

- **تعامل دائمی با محیط پویا** :سیستم‌های خودمختار مانند خودروهای هوشمند و پهپادها دائماً با محیط در ارتباط هستند و این تعامل باعث می‌شود در برابر حملات سایبری آسیب‌پذیر باشند. فناوری‌های پیشرفته مانند هوش مصنوعی مولد، با ارائه ابزارهای تحلیل و پیش‌بینی، این نقاط ضعف را کاهش می‌دهند.
- **تصمیم‌گیری بلادرنگReal-Time** : سیستم‌های خودمختار برای عملکرد صحیح نیاز به تصمیم‌گیری در زمان واقعی دارند. استفاده از مدل‌های تولیدکننده هوشمند، می‌تواند به شناسایی تهدیدات در لحظه و ارائه راه‌حل‌های سریع کمک کند.
- **انعطاف‌پذیری بالا در مقابله با حملات ناشناخته** :یکی از ویژگی‌های جذاب هوش مصنوعی مولد، توانایی تولید داده‌ها و سناریوهایی است که حتی فراتر از حملات شناخته‌شده عمل می‌کنند. این موضوع به پیش‌بینی تهدیدات آینده و آمادگی در برابر آن‌ها کمک می‌کند.

۲-۷. کاربردهای هوش مصنوعی مولد در امنیت سایبری

۱. **تولید داده‌های مصنوعی برای آموزش سیستم‌ها**

- هوش مصنوعی مولد قادر است داده‌های مصنوعی با ویژگی‌های مشابه داده‌های واقعی تولید کند که برای آموزش مدل‌های یادگیری ماشین بسیار حیاتی هستند. این داده‌ها می‌توانند شامل سناریوهای پیچیده‌ای باشند که در داده‌های واقعی کمتر مشاهده می‌شوند.

- *مثال کاربردی* :شبیه‌سازی شرایط نامطلوب ترافیکی برای خودروهای خودران.

۲. شبیه‌سازی تهدیدات سایبری

- شبکه‌های مولد تخاصمی(GANs) [۱] می‌توانند حملات سایبری مانند حملات انکار سرویس یا تزریق داده‌های جعلی را شبیه‌سازی کرده و به سیستم‌ها کمک کنند تا در برابر این تهدیدات آمادگی بیشتری داشته باشند.
- *مثال کاربردی* :تولید داده‌های جعلی برای آزمودن مقاومت سیستم‌های بانکی در برابر حملات فیشینگ.

۳. تشخیص و پیش‌بینی تهدیدات

- GenAIبا تحلیل بلادرنگ داده‌های شبکه، می‌تواند رفتارهای غیرعادی و حملات سایبری را شناسایی و پیش‌بینی کند.

الگوریتم‌های یادگیری عمیق (Deep Learning) :تشخیص الگوهای رفتاری غیرعادی در سیستم‌های خودمختار.

شبکه‌های عصبی (Neural Networks) :پیش‌بینی حملات سایبری از طریق تحلیل داده‌های ورودی سیستم.

- *مثال کاربردی* :شناسایی ایمیل‌های فیشینگ با استفاده از مدل‌های زبانی بزرگ.(LLMs)

٤. بهبود بازیابی پس از حمله

- GenAIمی‌تواند داده‌های ازدست‌رفته را بازسازی کرده و سیستم‌ها را به‌سرعت به حالت عادی بازگرداند.
- *مثال کاربردی* :بازیابی اطلاعات در صورت وقوع حملات باج‌افزاری.

۵. تحلیل رفتارهای غیرعادی در شبکه

- GenAIبا شناسایی الگوهای غیرمعمول در ترافیک شبکه، می‌تواند تهدیدات ناشناخته را کشف کند.

هوش مصنوعی می‌تواند رفتار سیستم‌های خودمختار را در زمان واقعی (Real-time) بررسی کند.

مثال کاربردی :پیشگیری از حملات DDoS با تحلیل رفتار کاربران در زمان واقعی، شناسایی ناهنجاری‌های سنسورها در خودروهای خودران برای جلوگیری از خطای عملکرد.

۳. تشخیص ناهنجاری در پهپادها و سیستم‌های رباتیک

بهبود تحلیل داده‌های سنسور پهپاد برای شناسایی شرایط غیرعادی، جهت افزایش قابلیت اطمینان و نگهداری پیش‌بینی‌کننده ضروری است . شبکه‌هایVAE [۲] در تشخیص و جداسازی خطاها مؤثر هستند و نشانگرهای اولیه مشکلات را شناسایی می‌کنند. با توجه به کمبود داده‌های

مربوط به شرایط نادر (مانند خطاها)، شبکه‌های مولد متخاصم (GAN) در تولید داده‌های مصنوعی برای آموزش مدل‌های یادگیری ماشین نقش کلیدی دارند.

[1] Generative Adversarial Networks(GANs)
[2] Variational Autoencoder(VAE)

- **روش‌های ترکیبی :**استفاده از مدل‌های GAN بهبودیافته مانند MSGAN وRoBiGAN ، داده‌های مصنوعی با کیفیت بالا تولید کرده و تشخیص ناهنجاری‌ها را در داده‌های سنسوری بهبود می‌دهند.
- **تحلیل پیشرفته :**ترکیب VAE با یادگیری ماشین سنتی برای شناسایی الگوهای غیرمعمول و سازگاری با تغییرات پویا، از جمله تکنیک‌هایی مانندGenDeX ، باعث افزایش دقت و استحکام سیستم‌های نظارتی شده است.
- **دسته‌بندی ناهنجاری‌ها :**پژوهش‌ها طبقه‌بندی جدیدی از ناهنجاری‌ها بر اساس ویژگی‌های فضایی-زمانی ارائه داده‌اند که برای بهبود شناسایی در مأموریت‌های رباتیک خودمختار اهمیت دارد.

همچنین، ترکیب هوش مصنوعی و هوش مصنوعی مولد با فناوری بلاکچین، ترکیبی قدرتمند و انقلابی به شمار می‌رود. بلاکچین با ارائه زیرساختی شفاف و تغییرناپذیر برای ذخیره و تبادل داده‌ها، امنیت را به سطحی فراتر ارتقا می‌دهد. در کنار آن، هوش مصنوعی مولد می‌تواند به شبیه‌سازی حملات و تقویت سازوکارهای امنیتی بلاکچین بپردازد و لایه‌های جدیدی از اطمینان را به سیستم‌های خودمختار بیفزاید.

۴. بلاکچین

بلاکچین یک دفتر کل توزیع‌شده و تغییرناپذیر است که تراکنش‌ها را به‌صورت امن و شفاف ثبت می‌کند.

کاربردها در امنیت سایبری

- ذخیره‌سازی امن داده‌ها :جلوگیری از تغییر داده‌ها.
- مدیریت هویت :احراز هویت کاربران به‌صورت غیرمتمرکز.
- شفافیت تراکنش‌ها :ردیابی تمامی تغییرات در سیستم.

۴-۱. نقش بلاکچین در امنیت سیستم‌های خودمختار

۱. ذخیره‌سازی امن و تغییرناپذیر داده‌ها

- تغییرناپذیری داده‌ها :بلاکچین با ذخیره داده‌ها در بلوک‌های رمزنگاری‌شده، از تغییر و حذف غیرمجاز اطلاعات جلوگیری می‌کند.
- ردیابی و شفافیت :هر تراکنش در بلاکچین ثبت و قابل ردیابی است؛ بنابراین، می‌توان تغییرات مشکوک را به‌راحتی شناسایی کرد.
- مثال کاربردی :در خودروهای خودران، اطلاعات حسگرها و مسیرها در بلاکچین ذخیره می‌شود و از دستکاری آن توسط مهاجمان جلوگیری می‌شود.

۲. امنیت ارتباطات و داده‌های انتقالی

- رمزنگاری پیشرفته :داده‌های انتقالی در سیستم‌های خودمختار (مانند خودروها و پهپادها) با استفاده از رمزنگاری بلاکچین محافظت می‌شوند.
- مقاومت در برابر حملات سایبری :بلاکچین به جلوگیری از حملات مردمیانی (MIMT)و تزریق داده‌های جعلی کمک می‌کند.
- مثال :در سیستم‌های کنترل ترافیک پهپادها، بلاکچین از ارسال داده‌های جعلی جلوگیری کرده و هماهنگی بین پهپادها را ایمن می‌کند.

۳. احراز هویت و کنترل دسترسی غیرمتمرکز

- مدیریت هویت دیجیتال :بلاکچین با استفاده از کلیدهای رمزنگاری‌شده، هویت کاربران و دستگاه‌های متصل به سیستم را احراز می‌کند.
- کنترل دسترسی ایمن :تنها افراد یا دستگاه‌های مجاز می‌توانند به سیستم‌ها دسترسی داشته باشند.
- مثال :در ربات‌های صنعتی، دسترسی به شبکه‌های کنترلی تنها برای کاربران مجاز از طریق بلاکچین امکان‌پذیر است.

٤. بهبود یکپارچگی و اعتماد در سیستم‌های چندعاملی

- توزیع غیرمتمرکز داده‌ها :در سیستم‌های خودمختار مانند خودروهای متصل(Connected Vehicles) ، داده‌ها به‌طور غیرمتمرکز بین چندین گره توزیع می‌شوند.
- کاهش خطای انسانی و حذف واسطه‌ها :عدم وابستگی به یک سرور مرکزی، خطر حملات به نقاط واحد (Single Point of Failure)را کاهش می‌دهد.
- مثال :در زنجیره تأمین هوشمند با استفاده از ربات‌های خودمختار، داده‌های مربوط به حمل‌ونقل و تحویل کالاها به‌شکل امن در بلاکچین ثبت می‌شوند.

۵. **مدیریت قراردادهای هوشمند**

- قراردادهای هوشمند :بلاکچین از قراردادهای هوشمند برای اجرای خودکار فرآیندها بدون نیاز به دخالت انسانی استفاده می‌کند.
- پیشگیری از تقلب :این قراردادها قابل‌بررسی و تغییرناپذیر هستند و احتمال تقلب را کاهش می‌دهند.
- مثال :در پهپادهای خودمختار، قراردادهای هوشمند وظایف پروازی را به‌شکل خودکار و ایمن تخصیص می‌دهند.

۴-۲. ادغام بلاک‌چین و هوش مصنوعی در امنیت سیستم‌های خودمختار

ادغام فناوری بلاک‌چین با هوش مصنوعی(AI) ، به‌ویژه در امنیت سیستم‌های خودمختار، رویکردی نوآورانه برای ایجاد زیرساخت‌هایی ایمن، شفاف و کارآمد ارائه می‌دهد. سیستم‌های خودمختار مانند پهپادها، خودروهای بدون سرنشین و ربات‌های صنعتی، به دلیل وابستگی شدید به داده‌ها و تصمیم‌گیری خودکار، در برابر تهدیدات امنیتی آسیب‌پذیرند. ترکیب این دو فناوری می‌تواند نه‌تنها از این سیستم‌ها در برابر حملات محافظت کند، بلکه قابلیت پیش‌بینی و مدیریت بحران را نیز بهبود بخشد.

۱ .امنیت سیستم‌های خودمختار با ادغام کلی هوش مصنوعی و بلاک‌چین

این ادغام، قابلیت‌های بلاک‌چین را با شاخه‌های مختلف هوش مصنوعی ترکیب می‌کند تا امنیت داده‌ها و فرآیندها در سیستم‌های خودمختار تضمین شود .کاربردهای کلیدی عبارتند از:

- **ثبت غیرقابل تغییر داده‌های حسگرها:**

  بلاک‌چین داده‌های حسگرهای سیستم‌های خودمختار را به‌صورت توزیع‌شده ذخیره می‌کند. این ویژگی از دستکاری داده‌ها جلوگیری کرده و شفافیت در تصمیم‌گیری را تضمین می‌کند.

- **تشخیص و پاسخ به تهدیدات سایبری:**

  هوش مصنوعی می‌تواند الگوهای مشکوک را در داده‌های ثبت‌شده شناسایی کند و بلاک‌چین به مستندسازی تغییرات مشکوک در سیستم کمک می‌کند. این دو فناوری با همکاری، سرعت و دقت در مقابله با تهدیدات را افزایش می‌دهند.

- **اشتراک‌گذاری ایمن داده‌ها بین سیستم‌های خودمختار:**

  در عملیات‌های چندعاملی (مانند دسته پهپادها)، بلاک‌چین بستری امن برای اشتراک‌گذاری داده‌ها فراهم می‌کند. این قابلیت همکاری بدون به خطر افتادن امنیت سیستم‌ها را ممکن می‌سازد.

- **ردیابی رفتار و تصمیم‌گیری سیستم‌های خودمختار:**

بلاک‌چین تمامی فرآیندهای تصمیم‌گیری سیستم را ثبت می‌کند و امکان بررسی و بازبینی دقیق را در صورت بروز خطا فراهم می‌سازد.

نمونه‌های کاربردی:

- **پهپادهای نظامی** :ردیابی و ثبت مأموریت‌ها و داده‌های محیطی برای اطمینان از دقت و امنیت عملیات.
- **خودروهای خودران** :محافظت از داده‌های حسگرهای LIDAR و GPS در برابر حملات سایبری و اطمینان از تصمیم‌گیری‌های ایمن.
- **ربات‌های صنعتی** :پیشگیری از دستکاری نرم‌افزاری که می‌تواند منجر به رفتار خطرناک در محیط‌های حساس شود.

۲ .امنیت سیستم‌های خودمختار با ادغام هوش مصنوعی مولد و بلاک‌چین

هوش مصنوعی مولد (Generative AI) به‌دلیل توانایی در تولید محتوای مصنوعی، می‌تواند در شبیه‌سازی، بازسازی داده‌ها، و حتی کشف تهدیدات جدید به کار رود. ادغام آن با بلاک‌چین در امنیت سیستم‌های خودمختار کاربردهای متمایزی دارد:

- تولید داده‌های شبیه‌سازی‌شده برای پیش‌بینی تهدیدات:

هوش مصنوعی مولد می‌تواند سناریوهای حمله احتمالی را شبیه‌سازی کند و بلاک‌چین این سناریوها و پاسخ‌های آن‌ها را برای ارزیابی و بهبود امنیت سیستم ذخیره کند.

- تضمین اصالت مدل‌های هوش مصنوعی:

مدل‌های هوش مصنوعی مورداستفاده در سیستم‌های خودمختار می‌توانند توسط بلاک‌چین ثبت شوند، به‌طوری‌که تغییرات یا جایگزینی آن‌ها توسط عوامل مخرب قابل شناسایی باشد.

- محافظت از محتواهای تولیدی:

در سیستم‌های خودمختار با قابلیت تولید محتوا (مانند گزارش‌های عملیات یا تصاویر حسگرها)، بلاک‌چین اصالت و تمامیت داده‌های تولیدشده را تضمین می‌کند و از انتشار اطلاعات جعلی جلوگیری می‌نماید.

- مدیریت چرخه عمر سیستم‌های خودمختار:

داده‌های مولد توسط هوش مصنوعی می‌توانند شامل اطلاعات عملکردی باشند که به‌طور مستقیم در بلاک‌چین ثبت می‌شوند. این قابلیت ردیابی مداوم سیستم و مدیریت هوشمند نگهداری را تسهیل می‌کند.

نمونه‌های کاربردی:

- پهپادهای نظارتی :تولید داده‌های جعلی برای فریب مهاجمان و جلوگیری از شناسایی مسیر واقعی.
- شبیه‌سازی سناریوهای بحرانی :کمک به سیستم‌های خودمختار برای آموزش بهتر در مواجهه با تهدیدات نادر.
- مدیریت محتواهای گزارش‌شده :تضمین صحت گزارش‌های عملیات حساس.

۳ .تفاوت‌های کلیدی در امنیت سیستم‌های خودمختار

ادغام بلاک‌چین و هوش مصنوعی، به‌ویژه در حوزه سیستم‌های خودمختار، ابزاری قدرتمند برای مقابله با تهدیدات امنیتی ارائه می‌دهد. در حالی که ادغام کلی هوش مصنوعی و بلاک‌چین بر امنیت داده‌ها و تصمیم‌گیری‌ها تمرکز دارد، ادغام هوش مصنوعی مولد با بلاک‌چین به شبیه‌سازی، پیش‌بینی و مدیریت محتواهای تولیدی می‌پردازد. این دو رویکرد در کنار یکدیگر، لایه‌های چندگانه‌ای از امنیت و قابلیت اطمینان را برای سیستم‌های خودمختار فراهم می‌کنند و نقشی حیاتی در ایجاد اعتماد و کارایی در محیط‌های پیچیده و پویا ایفا می‌نمایند.

۵.آتنا(Athena)

ویژگی	ادغام بلاک‌چین با هوش مصنوعی مولد	ادغام کلی هوش مصنوعی و بلاک‌چین
تمرکز اصلی	مدیریت و محافظت از داده‌های تولیدشده و شبیه‌سازی‌های امنیتی	شفافیت، ایمنی داده‌ها و تصمیم‌گیری‌های سیستم
کاربرد در امنیت	جلوگیری از دستکاری داده‌های حسگرها، ثبت رفتار سیستم	پیش‌بینی حملات، شبیه‌سازی تهدیدات و تضمین اصالت مدل‌ها
مزایا	بهبود قابلیت ردیابی و شفافیت سیستم‌های خودمختار	ارائه سناریوهای امنیتی جدید و مدیریت بهتر محتوای تولیدشده
چالش‌ها	هزینه‌های بالا و محدودیت مقیاس‌پذیری	مقابله با جعل داده‌های تولیدی و مدیریت پیچیدگی مدل‌ها

یک مفهوم در حوزه امنیت سایبری خودمختار است که برای مدیریت و مقابله با تهدیدات سایبری پیچیده و سریع طراحی شده است. آتنا به‌عنوان یک چارچوب امنیتی جامع، از تکنیک‌های هوش مصنوعی و یادگیری ماشین برای شناسایی، پاسخ‌دهی، و بازیابی سریع از حملات سایبری استفاده می‌کند. این سیستم تلاش می‌کند با کاهش نیاز به دخالت انسانی، امنیت را به صورت بلادرنگ تضمین کند.

۵-۱. ویژگی‌های کلیدی آتنا:

۱. **عملکردهای امنیتی یکپارچه :**آتنا از چارچوب امنیت سایبری NIST پیروی می‌کند که شامل پنج مرحله است:

- **شناسایی (Identify):** شناسایی نقاط ضعف و تهدیدات بالقوه.
- **محافظت (Protect) :**اجرای اقدامات پیشگیرانه برای کاهش ریسک‌ها.
- **تشخیص(Detect):** شناسایی حملات و ناهنجاری‌های سایبری به صورت بلادرنگ.
- **پاسخ (Respond):** اجرای اقدامات فوری برای کاهش اثرات حملات.
- **بازیابی (Recover):** بازگرداندن سیستم به حالت عادی با حداقل اختلال.

۲. **جهت‌گیری و یادگیری مداوم:**

آتنا محیط IT موردنظر را بررسی کرده و دانش لازم برای شناسایی و مقابله با تهدیدات را جمع‌آوری می‌کند. این یادگیری مداوم شامل شناسایی الگوهای تهدید جدید و به‌روزرسانی پایگاه دانش سیستم است.

۳. **کنترل خودمختار با تعامل انسانی:**

در حالی که آتنا به‌طور خودکار عملیات امنیتی را انجام می‌دهد، همچنان امکان کنترل انسانی معنادار وجود دارد تا از تصمیم‌گیری‌های نادرست جلوگیری شود.

٤. **استفاده از الگوریتم‌های پیشرفته:**

- **الگوریتم‌های تشخیص ناهنجاری :**برای شناسایی رفتارهای غیرمعمول در شبکه‌ها.
- **مدل‌های پیش‌بینی :**برای پیش‌بینی تهدیدات و نقص‌های سیستمی.
- **قراردادهای هوشمند مبتنی بر بلاکچین :**برای مدیریت امنیت و اجرای اقدامات بلادرنگ.

۵-۲. نمونه‌کاربرد آتنا:

فرض کنید سازمانی با یک حمله باج‌افزاری مواجه شود:

۱. آتنا به‌سرعت تهدید را شناسایی می‌کند و داده‌های چندمنبعی را تحلیل می‌کند.

۲. بهترین اقدام پاسخ را از میان گزینه‌های موجود انتخاب و اجرا می‌کند (مانند مسدود کردن دسترسی مهاجم).

۳. سیستم‌ها را به وضعیت عادی بازمی‌گرداند و امنیت را بازسازی می‌کند، بدون اینکه کاربران نهایی متوجه شوند.

مزایای آتنا:

- **سرعت بالا در شناسایی و پاسخ به تهدیدات.**
- **کاهش وابستگی به دخالت انسانی.**
- **افزایش تاب‌آوری سایبری سیستم‌ها.**
- **بهبود مدیریت منابع امنیتی.**

آتنا یک نمونه پیشرفته از سیستم‌های امنیت سایبری خودمختار است که نشان می‌دهد چگونه هوش مصنوعی و فناوری‌های نوین می‌توانند امنیت دیجیتال را متحول کنند

6.چالش‌ها

با وجود پیشرفت‌های سریع درGenAI ، ادغام این فناوری‌ها در سیستم‌های امنیت سایبری برای افزایش امنیت، ایمنی و انعطاف‌پذیری چالش‌های قابل توجهی را به همراه دارد. استقرارهای اولیه احتمالاً بر روی وظایف کم‌خطر و بهینه‌سازی توسعه الگوریتم‌هایML [۱] متمرکز خواهند شد و ممکن است منجر به راه‌حل‌های کارآمدتر و مؤثرتر شود.

هزینه و محاسبات :مشاهدات در صنعت نشان می‌دهد که با وجود سرمایه‌گذاری‌های قابل توجهی که از ۱۰۰ میلیارد دلار در خودروهای خودمختار فراتر می‌رود، این سیستم‌ها همچنان با موارد حاشیه‌ای دست و پنجه نرم می‌کنند و اغلب نیاز به مداخله انسانی دارند. پیشنهاد می‌شود کهLLM [۲]ها و سایر فناوری‌های GenAI ممکن است با موارد حاشیه‌ای چالش‌های مشابهی داشته باشند و قابلیت استفاده آن‌ها را برای کاربردهای حیاتی محدود کنند. علاوه بر این، هزینه‌های عملیاتی قابل توجه است؛ به عنوان مثال، استفاده ازGPT-4 [۳] حدود ۰.۰۰۶ دلار در هر ۷۵۰ کلمه هزینه دارد و تولید یک تصویر با تقریباً ۰.۱۸ دلار در هر تصویر است.LLMهای مبتنی بر ترانسفورمر، اجزای اساسی GenAI، به منابع محاسباتی قابل توجهی نیاز دارند که استقرار آن‌ها را به سرورهای سطح بالا محدود می‌کند که قادر به ادغام بلادرنگ با سیستم‌های خودمختار هستند. با این حال، پیشرفت‌های سخت‌افزاری به تدریج امکان اجرای این مدل‌های قدرتمند را مستقیماً روی سیستم‌های خودمختار فراهم می‌کند، وFPGA [۴]ها پتانسیل اجرای مدل‌های GenAI را کارآمدتر ازGPU [۵]ها یاCPU [۶]های سنتی نشان می‌دهند.

[۱] Machine Learning(ML)
[۲] Large Language Model(LLM)
[۳] Generative Pre-trained Transformer (GPT)
[4] Field-Programmable Gate Array(FPGA)
[5] Graphics Processing Unit(GPU)
[6] Central Processing Unit(CPU)

تطبیق و دقت :مدل‌های هوش مصنوعی معمولاً برای حفظ دقت با داده‌های تاریخی نیاز به تنظیم دقیق دارند و عملکرد آن‌ها ممکن است در شرایط محیطی یا عملیاتی متغیر کاهش یابد. همچنین ممکن است مهاجمان استراتژی‌های خود را برای دور زدن اقدامات امنیتی تطبیق

دهند. به‌روزرسانی‌های مداوم مدل و رویکردهای نوآورانه مانند یادگیری آنلاین، که ممکن است از GAN[1]ها استفاده کنند، برای حفظ دقت مدل‌ها در طول زمان امیدوارکننده هستند. تمایل مدل‌های GenAI به تولید توهمات نیاز به اقدامات اضافی در کاربردهای حیاتی برای اطمینان از قابلیت اطمینان و ایمنی دارد.

مسائل حریم خصوصی و امنیت :با جمع‌آوری داده‌های بیشتر توسط پهپادها و سایر سیستم‌های خودمختار در مورد افراد و املاک خصوصی، نگرانی‌های مربوط به حریم خصوصی افزایش می‌یابد. انکلاوهای امنیتی، یادگیری فدرال و رمزنگاری هومومورفیک می‌توانند حریم خصوصی را تقویت کرده و در عین حال عملکرد سیستم را حفظ کنند. پیشرفت‌های اخیر در GenAI منجر به روش‌هایی شده است که به طور خودکار داده‌های حساس را ماسک می‌کنند، مانند(ADGAN) [2]، که بر داده‌های ترافیکی مرتبط تمرکز می‌کند در حالی که پس‌زمینه‌ها را پنهان می‌کند، و TrajGAN [3]ها که مجموعه داده‌های مصنوعی را شبیه‌سازی حرکات انسانی بدون به خطر انداختن حریم خصوصی افراد ایجاد می‌کنند .با این حال، خطر افشای اطلاعات شخصی همچنان وجود دارد، به ویژه زمانی که مدل‌ها بر روی داده‌های بالقوه قابل شناسایی آموزش داده می‌شوند.

LLMها از طریق حملات استخراج داده خطرات حریم خصوصی قابل توجهی را ایجاد می‌کنند؛ هنگامی که این مدل‌ها بر روی داده‌های حساس یا محرمانه آموزش داده می‌شوند، ممکن است به طور ناخواسته چنین اطلاعاتی را فاش کنند و در نتیجه یکپارچگی زمینه داده‌ها را به خطر بیندازند

۷. راه‌حل‌ها و اقدامات احتمالی AI برای بهبود امنیت سیستم‌های خودمختار

۱. شناسایی و پاسخ به تهدیدات امنیتی در زمان واقعی

۲ .امنیت سایبری مبتنی برAI

۳ .بهبود قابلیت‌های تصمیم‌گیری در شرایط بحرانی

۴ .حفاظت از داده‌های حساس و جلوگیری از دست‌کاری

۵ .یادگیری مداوم و به‌روزرسانی امنیت

۶ .شبیه‌سازی و پیش‌آزمایش امنیتی

۷ .ایجاد اعتماد از طریق شفافیت و توضیح‌پذیری(Explainability)

۸ .استفاده از فناوری‌های هیبریدی.

[1] Generative Adversarial Network(GAN)
[2] Auto-Driving GAN (ADGAN)
[3] Trajectory Generative Adversarial Network(TrajGAN)

هوش مصنوعی نقش کلیدی در تضمین امنیت سیستم‌های خودمختار ایفا می‌کند. با توسعه مدل‌های پیشرفته‌تر، این سیستم‌ها قادر خواهند بود:

۱. تهدیدات را پیش‌بینی کنند.

۲. به تهدیدات به صورت پویا پاسخ دهند.

۳. از داده‌ها و ساختارهای داخلی خود حفاظت کنند.

8. نتیجه گیری:

تضمین امنیت نیازمند همکاری بین‌المللی، استانداردسازی، و ترکیب تکنیک‌های پیشرفته مانندAI ، بلاک‌چین و رمزنگاری است.درواقعه امنیت یک چیز کاملا نسبی است و نمیشود صد درصد آن را تضمین کرد.همیشه یک راه نفوذ برای رخنه کردن به سیستم ها وجود دارد،آینده گان باید بکوشند با بکار بردن رمزنگاری ها و الگوریتم های گوناگون و جدید و همچنین با بکاربردن هوش مصنوعی در کارها سطح امنیت را بالاتر ببرند و سطح دسترسی را سخت تر کنند.اگر میخواهیم هوش مصنوعی را در کارها دخالت دهیم بهتر است به آن ها اجازه دهیم بیشتر و دقیق تر یادبگیرند و همچنین سیستم امنیتی آن ها را هم بالا ببریم تا شخص یا اشخاصی نتوانند به آن ها نفوذ کنند.هرچیزی در این دنیا دارای ویژگی های خوب و بد است شاید نتوانیم کاملا به Aiاطمینان کنیم اما در آخر هوش مصنوعی ساخته دست بشر است و به هرنوعی میتواند آن را کنترل کند،خیلی مواقعه انسان قادر به انجام کارها نیست و بهتر است کار را به هوش مصنوعی بسپاریم.حتی در موضوع امنیت اگر ما به خوبی به هوش مصنوعی داده های کافی و درستی داده باشیم میتواند از داده ها و شبکه های ما مراقبت کند و روز به روز قوی تر شود.ترکیب هوش مصنوعی با فناوری های جدید میتواند دنیای بهتری به ارمغان بیاورد.سیستم های خودمختار به کمک هوش مصنوعی میتوانند روز به روز بیشتر یادبگیرند و تقویت شوند و امنیتشان با کمک هوش مصنوعی بالا تر رود.

الگوریتم‌های پیشرفته هوش مصنوعی، به‌ویژهGAN ها، VAEها، LLMها، و یادگیری تقویتی، ابزارهای حیاتی برای مقابله با تهدیدات سایبری در سیستم‌های خودمختار هستند. هوش مصنوعی مولد نقش اساسی در بهبود امنیت و پایداری سیستم‌های خودمختار ایفا می‌کند. از تولید داده‌های مصنوعی برای آموزش و بهبود مدل‌های امنیتی گرفته تا شبیه‌سازی حملات سایبری و بازسازی داده‌ها، GenAIمی‌تواند به افزایش تاب‌آوری و امنیت سایبری این سیستم‌ها کمک کند. با استفاده از این فناوری، سیستم‌های خودمختار می‌توانند به‌طور مؤثرتری از تهدیدات موجود محافظت شوند و در برابر حملات و اختلالات مقاوم‌تر شوند.

[1]F. Santoso and A. Finn, "An In-Depth Examination of Artificial Intelligence-Enhanced Cybersecurity in Robotics, Autonomous Systems, and Critical Infrastructures," in IEEE Transactions on Services .Computing, vol. 17, no. 3, pp. 1293-1310, May-June 2024, doi: 10.1109/TSC.2023.3331083 keywords: {Robots;Computer security;Robot sensing systems;Security;Autonomous systems;Operating systems;Middleware;Cybersecurity;artificial intelligence;machine learning;robotics;autonomous ,systems;and critical infrastructures}

[2]M. Andreoni, W. T. Lunardi, G. Lawton and S. Thakkar, "Enhancing Autonomous System Security and , ۱۰۹۴۹۳-۱۰۹۴۷۰, pp. ۱۲Resilience With Generative AI: A Comprehensive Survey," in IEEE Access, vol. .۲۰۲٤,۳٤۳۹۳٦۳/ACCESS.۱۰,۱۱۰۹, doi: ۲۰۲٤
keywords: {Security;Robots;Computer security;Surveys;Artificial intelligence;Safety;Task ,analysis;GenerativeAI;artificial intelligence;autonomous systems;security;UxV}

[3] O. Kuznetsov, P. Sernani, L. Romeo, E. Frontoni and A. Mancini, "On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security," in *IEEE Access*, vol. 12, pp. 3881-3897, 2024, doi: 10.1109/ACCESS.2023.3349019. keywords: {Blockchains;Artificial intelligence;Security;Task analysis;Deep learning;Decision making;Data models;Distributed ledger;AI;artificial intelligence;blockchain;distributed ledger technology;security}

[4]Autonomous Cyber Security 2023 october,Karin Bosch, Frank Fransen, Patrick de Graaf, Dimitri Hehanussa, Rick van der Kleij, Bert Jan te Paske, Berry Vetjens and Reinder Wolthuis

[5]Deema Almaskati, Sharareh Kermanshachi, Apurva Pamidimukkula ۷۳,۲۰۲۳Autonomous vehicles and traffic accidents,Transportation Research Procedia,Volume ۱٤٦٥-۲۳٥۲,ISSN ۳۲۸-۳۲۱,Pages

[6]Weng, Y., & Wu, J. (2024). Leveraging Artificial Intelligence to Enhance Data Security and Combat Cyber Attacks. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *5*(1), 392–399. https://doi.org/10.60087/jaigs.v5i1.211