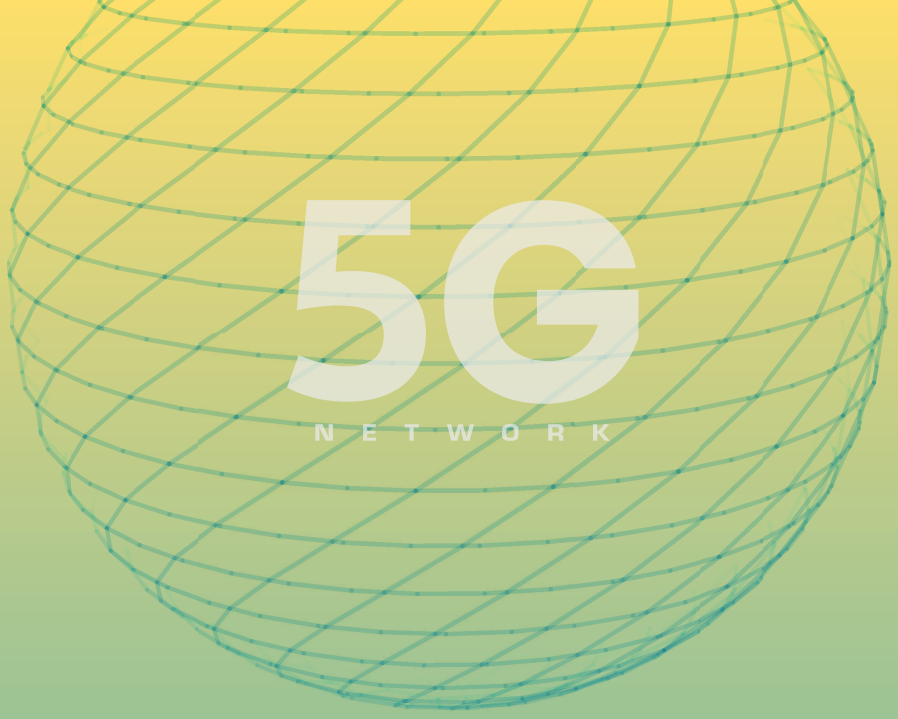


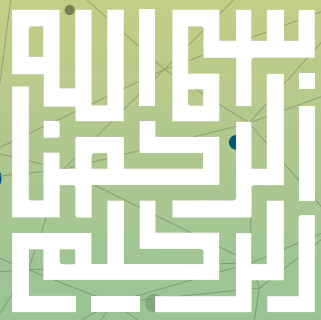
ITRC
پژوهشگاه ارتباطات
و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)

مجموعه حملات مبتنی بر هوش مصنوعی در شبکه‌های سیّار نسل پنجم

تاریخ انتشار: شهریور ۱۴۰۴

ITRC

پژوهشگاه ارتباطات
و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)



عنوان گزارش: مجموعه حملات مبتنی بر هوش مصنوعی در شبکه‌های سیّار نسل پنجم

کلمات کلیدی: هوش مصنوعی، شبکه‌های نسل پنجم و حملات سایبری

تهیه کنندگان: محمد جاویدنیا، محمدعلی سبقتی و علیرضا عنایتی

راهبر علمی (مجری پژوهش): امیرمنصور یادگاری

گروه پژوهشی: ارزیابی امنیت شبکه و سامانه‌ها (پروژه پژوهشی تدوین طرح مقابله با تهدیدات سایبری بهره‌مند از هوش مصنوعی)

تاریخ نشر: شهریور ۱۴۰۴

ITRC

پژوهشگاه ارتباطات
و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)

خلاصه مدیریتی

این گزارش تحلیلی جامع و عمیق از رابطه همزیستانه و در عین حال مخاطره‌آمیز بین هوش مصنوعی (AI)[1] و شبکه‌های سیار نسل پنجم (5G) ارائه می‌دهد. معماری نسل پنجم، با ماهیت نرم‌افزارمحور، مجزاسازی‌شده و توزیع‌شده خود، سطح حمله‌ای بی‌سابقه ایجاد می‌کند که ابزارهای تهاجمی مبتنی بر هوش مصنوعی قادرند با سرعت و مقیاس ماشین آن را مورد بهره‌برداری قرار دهند. این تحول، پارادایم‌های امنیتی سنتی را منسوخ کرده و چالش‌های جدیدی را پیش روی اپراتورها، شرکت‌ها و نهادهای امنیتی قرار می‌دهد. از یک سو، هوش مصنوعی به عنوان یک سلاح، توانایی مهاجمان را در تمامی مراحل چرخه حیات حمله—از شناسایی و تحلیل آسیب‌پذیری گرفته تا اجرای حملات پیچیده انکار سرویس (DDoS) و بدافزارهای خودآموز—به‌طور چشمگیری افزایش می‌دهد. این پدیده منجر به «دموکراتیزه شدن تهدیدات پایدار پیشرفته (APT)» شده است، جایی که تکنیک‌های پیشرفته‌ای که زمانی در انحصار بازیگران دولتی بود، اکنون در دسترس طیف وسیع‌تری از مهاجمان قرار گرفته است.

از سوی دیگر، این گزارش تهدید بازگشتی و حیاتی حمله به خود سیستم‌های هوش مصنوعی را که وظیفه مدیریت، بهینه‌سازی و حفاظت از شبکه‌های 5G را بر عهده دارند، مورد بررسی قرار می‌دهد. حملات تخاصمی، مانند مسموم‌سازی داده‌ها، نمونه‌های تخاصمی (گریز) و استخراج مدل، می‌توانند یکپارچگی و محرمانگی این سیستم‌های هوشمند را تضعیف کرده و زیرساخت‌های حیاتی 5G را از درون به خطر اندازند. این آسیب‌پذیری، هدف «اتوماسیون بدون دخالت انسان»[2] را در شبکه‌های 5G به شدت تهدید می‌کند، زیرا یک سیستم هوش مصنوعی به خطر افتاده می‌تواند تصمیمات فاجعه‌بار و خودکاری را اتخاذ نماید.

یافته‌های کلیدی این تحلیل نشان می‌دهد که دفاع مؤثر در برابر این تهدیدات دوگانه، نیازمند یک تغییر پارادایم از امنیت مبتنی بر محیط پیرامونی به یک معماری امنیتی «اعتماد صفر» (Zero Trust) است که به صورت ذاتی در تمام لایه‌های معماری 5G —از هسته مبتنی بر سرویس (SBA) و مجازی‌سازی توابع شبکه (NFV) گرفته تا برش شبکه، رایانش لبه و شبکه دسترسی رادیویی باز (O-RAN)—پیاده‌سازی شده باشد. علاوه بر این، مقابله با حملات هوشمند نیازمند دفاع هوشمند

1. Artificial intelligence (AI)
2. Zero-Touch Automation

است. این گزارش استدلال می‌کند که آینده امنیت 5G در یک مسابقه تسلیحاتی اجتناب‌ناپذیر بین هوش مصنوعی تهاجمی و هوش مصنوعی تدافعی نهفته است. بنابراین، توصیه‌های استراتژیک اصلی بر توسعه و استقرار سیستم‌های تشخیص و پاسخ خودکار مبتنی بر هوش مصنوعی، معماری‌های امنیتی انعطاف‌پذیر و پویا، و ایجاد چارچوب‌های قوی برای امنیت و استحکام خط لوله یادگیری ماشین (ML) متمرکز است.

فهرست مطالب

فهرست مطالب

۱ چشم‌انداز امنیتی: 5G معماری و آسیب‌پذیری‌های ذاتی

امنیت در شبکه‌های 5G یک تکامل تدریجی از شبکه‌های نسل چهارم (4G) نیست، بلکه یک تغییر پارادایم کامل و بنیادین است. معماری 4G، با ماهیت متمرکز و مبتنی بر سخت‌افزار، دارای مرزهای امنیتی نسبتاً مشخصی بود. در مقابل، ارکان معماری 5G -که بر اصول نرم‌افزارمحوری، مجازی‌سازی و توزیع‌شدگی استوار است- این محیط‌های پیرامونی سنتی را از بین برده و یک چشم‌انداز تهدید جدید و پویا ایجاد می‌کند که به طور منحصربه‌فردی برای بهره‌برداری توسط حملات مبتنی بر هوش مصنوعی مناسب است. این بخش به تشریح این موضوع می‌پردازد که چگونه ستون‌های اصلی معماری 5G، سطح حمله را به طور اساسی گسترش داده و زمینه را برای نسل جدیدی از تهدیدات سایبری هوشمند فراهم می‌کنند.

شبکه‌های 4G عمدتاً بر روی تجهیزات سخت‌افزاری اختصاصی و یکپارچه از یک فروشنده خاص اجرا می‌شدند. ترافیک از مسیرهای مشخصی عبور می‌کرد و توابع شبکه در یک سیستم ثابت و کنترل‌شده عمل می‌کردند. این ساختار، اعمال سیاست‌های امنیتی یکنواخت و جداسازی ریسک‌ها را ساده‌تر می‌ساخت. در مقابل، 5G با تجزیه هسته شبکه و اجرای توابع به عنوان ماشین‌های مجازی (VMs) یا کانتینرها بر روی زیرساخت‌های مشترک، این مدل را کاملاً دگرگون کرده است. این تغییر، ضمن افزایش انعطاف‌پذیری و کاهش هزینه‌ها، سطح حمله را به طور قابل توجهی گسترش می‌دهد، زیرا آسیب‌پذیری‌های جدیدی در هر لایه—از هایپروایزر و کانتینر گرفته تا APIهای باز و استقرارهای چندابری—ظهور می‌کنند.

سطح حمله گسترده 5G بر پنج ستون معماری اصلی استوار است که هر یک به تنهایی و در تعامل با یکدیگر، فرصت‌های جدیدی برای مهاجمان مبتنی بر هوش مصنوعی ایجاد می‌کنند که در ادامه معرفی می‌شوند.

۱-۱ معماری مبتنی بر سرویس (SBA) و هسته API-محور

قلب هسته 5G (5GC)، معماری مبتنی بر سرویس (SBA)[1] است. در این مدل، توابع شبکه (NFs) به صورت واحدهای نرم‌افزاری ماژولار (میکروسرویس) طراحی شده‌اند که قابلیت‌های خود را از طریق

1. Service Based Architecture (SBA)

APIهای RESTful مبتنی بر پروتکل HTTP/2 به عنوان سرویس ارائه می‌دهند. این رویکرد، شبکه را در معرض دسته‌ای از حملات که پیش از این در دنیای وب رایج بودند، قرار می‌دهد.

- **آسیب‌پذیری‌های API:** وابستگی SBA به فناوری‌های وب، آن را مستقیماً در برابر تهدیدات رایج API مانند موارد ذکر شده در سند امنیتی API مربوط به OWASP[1] آسیب‌پذیر می‌سازد. این موارد شامل کنترل دسترسی شکسته در سطح اشیاء (که به مهاجم اجازه می‌دهد داده‌های کاربر دیگری را دستکاری کند)، احراز هویت شکسته (که امکان جعل هویت یک تابع شبکه دیگر را فراهم می‌کند) و مصرف بی‌رویه منابع (که منجر به حملات DoS از طریق سیل درخواست‌های API می‌شود) است.

- **نقاط حیاتی در SBA:**

- **تابع مخزن شبکه (NRF)[2]:** به عنوان مرکز کشف سرویس، NRF یک هدف اصلی است. به خطر افتادن آن می‌تواند به نقشه‌برداری کامل شبکه یا منحرف کردن ترافیک به سمت یک تابع شبکه مخرب منجر شود.
- **پراکسی ارتباطات سرویس (SCP)[3]:** به عنوان یک نقطه متمرکز برای مسیریابی و بازرسی ترافیک، در صورت به خطر افتادن می‌تواند به یک نقطه شکست واحد تبدیل شود و امکان شنود یا دستکاری گسترده را فراهم کند.
- **پراکسی حفاظت لبه امنیتی (SEPP)[4]:** SEPP که دروازه‌بان ترافیک رومینگ است، جایگزین پروتکل ناامن Diameter در 4G شده است. با این حال، به دلیل قرار گرفتن در لبه شبکه، یک هدف باارزش است و به خطر افتادن آن می‌تواند کل سیگنالینگ رومینگ را افشا کند.

۱-۲ مجازی‌سازی توابع شبکه (NFV) و کانتینرسازی

تحول از توابع شبکه مجازی مبتنی بر ماشین مجازی (VNFs) به توابع شبکه بومی ابر (CNFs)[5] که در کانتینرهای سبک و چابک (مانند Docker) اجرا شده و توسط پلتفرم‌هایی مانند Kubernetes مدیریت می‌شوند، یکی دیگر از ارکان 5G است. این رویکرد، ریسک‌های ناشی از زیرساخت‌های اشتراکی را به هسته شبکه مخابراتی وارد می‌کند.

1. OWASP API Security Top 10
2. Network Repository Function
3. Secure copy protocol (SCP)
4. Substantially equal periodic payments (SEPP)
5. Cloud-Native Network Functions (CNF)

- **ریسک‌های زیرساخت اشتراکی:**

- **گریز از هایپروایزر/کانتینر[1]:** یک آسیب‌پذیری در هایپروایزر یا زمان اجرای کانتینر می‌تواند به یک تابع شبکه به خطر افتاده اجازه دهد تا از محیط ایزوله خود «فرار» کرده و به سیستم‌عامل میزبان یا سایر توابع شبکه روی همان میزبان حمله کند. این یک آسیب‌پذیری کلاسیک در محیط‌های ابری است که اکنون مستقیماً در هسته 5G نیز کاربرد دارد.
- **حملات کانال جانبی:** مهاجمان می‌توانند با مشاهده اثرات غیرمستقیم مانند مصرف برق، الگوهای دسترسی به حافظه یا زمان‌بندی حافظه نهان CPU در سخت‌افزارهای اشتراکی، اطلاعات حساس (مانند کلیدهای رمزنگاری) را استنتاج کنند.
- **امنیت لایه ارکستراسیون (Kubernetes):** امنیت هسته 5G اکنون به طور ذاتی با امنیت پلتفرم ارکستراسیون آن گره خورده است. آسیب‌پذیری‌های خاص Kubernetes عبارتند از:
  - پیکربندی نادرست RBAC[2]: کنترل دسترسی مبتنی بر نقش (RBAC) با مجوزهای بیش از حد، می‌توانند در صورت به خطر افتادن یک حساب کاربری یا سرویس، به مهاجم دسترسی گسترده‌ای بدهند.
  - ایمیج‌های کانتینر به خطر افتاده: استفاده از ایمیج‌های کانتینر از مخازن نامعتبر یا ایمیج‌هایی با آسیب‌پذیری‌های شناخته‌شده، می‌تواند بدافزار را مستقیماً به هسته شبکه تزریق کند.
  - افشای etcd: دسترسی غیرمجاز به پایگاه داده etcd، که مخزن مرکزی وضعیت Kubernetes است، به مهاجم اجازه می‌دهد تمام اطلاعات محرمانه را سرقت کرده و کنترل کامل کلاستر را به دست گیرد.

۳-۱ برش شبکه[3]

برش شبکه امکان ایجاد چندین شبکه مجازی سرتاسری بر روی یک زیرساخت فیزیکی مشترک را فراهم می‌کند که هر کدام برای یک مورد استفاده خاص (مانند پهنای باند موبایل پیشرفته (eMBB)، ارتباطات بسیار قابل اعتماد با تأخیر کم (URLLC) یا ارتباطات ماشینی انبوه (mMTC)) بهینه‌سازی شده‌اند. تهدید اصلی در اینجا، شکست در دستیابی به ایزولاسیون کامل است.

- **حملات بین برشی[4]:** یک آسیب‌پذیری در یک مؤلفه مشترک (مانند AMF، یک سرور فیزیکی یا هایپروایزر) می‌تواند به مهاجمی که یک برش با امنیت پایین (مانند برش Wi-Fi مهمان) را

1. Container Breakout
2. Role-Based Access Control
3. Network Slicing
4. Cross-Slice Attacks

به خطر انداخته است، اجازه دهد تا به صورت جانبی حرکت کرده و به یک برش با امنیت بالا (مانند برش زیرساخت‌های حیاتی) حمله کند.

- **اتمام منابع[1]:** یک مهاجم در یک برش می‌تواند با اجرای یک حمله مصرف منابع، منابع اشتراکی (CPU، حافظه، پهنای باند) را به اتمام رسانده و منجر به یک حمله منع سرویس شود که بر عملکرد و در دسترس بودن سایر برش‌ها تأثیر می‌گذارد.
- **نشت داده و ربودن برش:** آسیب‌پذیری افشا شده توسط GSMA با کد 0047-CVD-2021، که عدم وجود نگاشت بین هویت‌های لایه انتقال و لایه کاربرد را نشان می‌دهد، یک نمونه بارز است. این نقص می‌تواند به مهاجم اجازه دهد به داده‌ها دسترسی پیدا کرده یا جلسات متعلق به برش‌های دیگر را برباید.
- **پیچیدگی پیکربندی:** پیچیدگی محض پیکربندی و مدیریت سیاست‌ها برای تعداد زیادی برش، احتمال خطای انسانی را افزایش می‌دهد و منجر به پیکربندی‌های نادرست امنیتی می‌شود که مهاجم می‌تواند از آنها بهره‌برداری کند.

۱-۴ رایانش لبه چند دسترسی[2]

رایانش لبه چند دسترسی (MEC) محاسبات و ذخیره‌سازی را از ابر متمرکز به لبه شبکه، نزدیک‌تر به کاربر، منتقل می‌کند تا برنامه‌های کاربردی با تأخیر کم را فعال سازد. این امر هزاران نقطه حضور فیزیکی توزیع‌شده جدید ایجاد می‌کند که باید ایمن شوند.

- **امنیت فیزیکی:** برخلاف یک مرکز داده متمرکز و امن، گره‌های MEC ممکن است در مکان‌های با امنیت کمتر (مانند روی تیرهای برق یا در زیرزمین‌ها) مستقر شوند که آنها را در برابر دستکاری فیزیکی آسیب‌پذیر می‌کند.
- **ریسک برنامه‌های کاربردی شخص ثالث:** MEC به عنوان یک محیط باز برای توسعه‌دهندگان شخص ثالث طراحی شده است تا برنامه‌های خود را مستقر کنند. این امر یک ریسک زنجیره تأمین قابل توجه ایجاد می‌کند. یک برنامه شخص ثالث مخرب یا با کدنویسی ضعیف می‌تواند حاوی آسیب‌پذیری باشد، به عنوان یک ناقل برای بدافزار عمل کند یا از دسترسی خود به اطلاعات شبکه و داده‌های کاربر سوءاستفاده کند.
- **حریم خصوصی و محرمانگی داده‌ها:** برنامه‌های MEC اغلب داده‌های بسیار حساس و شخصی مانند موقعیت مکانی، فیدهای ویدیویی و داده‌های حسگر IoT را مستقیماً در لبه پردازش می‌کنند. ماهیت توزیع‌شده و چندمستأجری MEC، حفاظت از این داده‌ها در برابر

1. Resource Exhaustion
2. Multi-access Edge Computing (MEC)

دسترسی غیرمجاز یا نشت را به یک چالش حیاتی تبدیل می‌کند.

۱-۵ شبکه دسترسی رادیویی باز (O-RAN)

معماری O-RAN[1] ایستگاه پایه سنتی را به مؤلفه‌های قابل تعامل از فروشندگان مختلف (RU, DU, CU) تجزیه می‌کند و کنترل‌کننده هوشمند رادیویی (RIC) را برای کنترل و بهینه‌سازی مبتنی بر هوش مصنوعی معرفی می‌کند. RIC به عنوان مغز RAN، به یک هدف اصلی برای حملات تبدیل می‌شود.

- **آسیب‌پذیری‌های رابط:** تحقیقات آسیب‌پذیری‌های حیاتی را در رابط‌های کلیدی RIC آشکار کرده‌اند. مشخص شده است که رابط A1 (بین Non-RT RIC و Near-RT RIC) و رابط E2 (بین Near-RT RIC و CU/DU) در برخی پیاده‌سازی‌ها فاقد TLS اجباری و مکانیزم‌های مجوزدهی مناسب هستند.
- **پیامدهای بهره‌برداری از رابط:** بهره‌برداری از این آسیب‌پذیری‌ها می‌تواند به مهاجم اجازه دهد تا سیاست‌های مخرب تزریق کند، منطق بهینه‌سازی RAN را دستکاری کند، RIC را انگشت‌نگاری کند، کانال‌های مخفی ایجاد کند یا حملات منع سرویس را علیه خود RIC اجرا کند.
- **حمله زنجیره تأمین xApp/rApp:** مشابه MEC، اکوسیستم RIC به برنامه‌های شخص ثالث (xApps/rApps) اجازه استقرار می‌دهد. یک xApp مخرب می‌تواند برای دستکاری رفتار RAN، شنود داده‌های کنترلی یا حمله به سایر عناصر شبکه استفاده شود، که این امر اعتبارسنجی امنیتی این برنامه‌ها را بسیار مهم می‌سازد.

استفاده از فناوری‌های رایج IT و ابر در معماری 5G، در حالی که نوآوری را تسریع می‌کند، به طور همزمان موانع ورود برای مهاجمان پیشرفته را کاهش می‌دهد. حملات 4G اغلب به دانش تخصصی مخابرات و تجهیزات خاص (مثلاً برای سیگنالینگ Diameter) نیاز داشتند. اکنون، مهاجمان می‌توانند از ابزارها و تکنیک‌های شناخته‌شده در حوزه‌های امنیت وب و ابر-مانند ابزارهای بهره‌برداری از Ku-bernetes، چارچوب‌های استاندارد حمله به API و نرم‌افزارهای منبع باز -برای هدف قرار دادن هسته 5G استفاده کنند. این امر منجر به یک «همگرایی مهارت‌ها» برای تیم‌های امنیتی مخابراتی می‌شود که اکنون علاوه بر پروتکل‌های سنتی، به تخصص عمیق در امنیت بومی ابر، امنیت کانتینر و امنیت API نیز نیاز دارند.

علاوه بر این، حرکت به سمت مدل‌های تجزیه‌شده و چندفروشندگی در O-RAN و برنامه‌های شخص ثالث در MEC یک «پارادوکس اعتماد» ایجاد می‌کند. در RAN یکپارچه 4G، اعتماد به طور ضمنی به یک فروشنده واحد واگذار می‌شد. در 5G، اعتماد باید به طور صریح در هر رابط و برای

1. Open Radio Access Network (O-RAN)

هر مؤلفه و برنامه مدیریت شود. امنیت شبکه به یک مسئله "ضعیف‌ترین حلقه" تبدیل می‌شود که به امنیت ناامن‌ترین xApp یا برنامه MEC بستگی دارد. این امر طرح‌های تضمین امنیت (مانند 3GPP SCAS و GSMA NESAS) و یک معماری مبتنی بر اعتماد صفر را به الزاماتی بنیادین و غیرقابل چشم‌پوشی تبدیل می‌کند.

این پنج ستون معماری به صورت مجزا عمل نمی‌کنند؛ آسیب‌پذیری‌های آن‌ها به هم مرتبط بوده و یکدیگر را تشدید می‌کنند. به عنوان مثال، یک پیکربندی نادرست در زیرساخت ابری (یک تهدید NFV) می‌تواند یک API در SBA را در معرض خطر قرار دهد. این API به خطر افتاده ممکن است برای نفوذ به سیستم ارکستراسیون که برش‌های شبکه را مدیریت می‌کند، استفاده شود و در نهایت منجر به یک حمله بین-برشی و نقض داده‌ها شود. ابزارهای حمله مبتنی بر هوش مصنوعی به طور منحصربه‌فردی قادر به کشف و بهره‌برداری از این مسیرهای حمله پیچیده و چندمرحله‌ای در میان حوزه‌های مختلف معماری هستند. این توانایی، تمایز کلیدی بین تهدیدات سنتی و تهدیدات هوشمند در اکوسیستم 5G است.

جدول ۱: ستون‌های معماری ۵G و بردارهای تهدید مبتنی بر هوش مصنوعی

ستون معماری ۵G	شرح	بردارهای تهدید اصلی مبتنی بر هوش مصنوعی
هسته مبتنی بر سرویس API / (SBA)	هسته کنترل مبتنی بر میکروسرویس که از طریق APIهای RESTful ارتباط برقرار می‌کند.	بهره‌برداری هوشمند از API، جعل هویت توابع شبکه، حملات تزریق پیشرفته، حملات مرد میانی (Man-in-the-Middle)
مجازی‌سازی توابع شبکه (NFV) / کانتینرها	اجرای توابع شبکه به عنوان نرم‌افزار (VNF/CNF) بر روی زیرساخت ابری مشترک.	بدافزارهای خودآموز و چندریختی، حملات کانال جانبی، فرار از کانتینر، حرکت جانبی هوشمند در ترافیک شرق به غرب.
برش شبکه (Network Slicing)	ایجاد شبکه‌های مجازی منطقاً ایزوله بر روی زیرساخت فیزیکی مشترک.	حملات انکار سرویس هدفمند بر روی برش، بهره‌برداری از منابع مشترک برای حملات بین-برشی، حملات به ارکستراتور.
رایانش لبه چند دسترسی (MEC)	توزیع قابلیت‌های پردازشی و ذخیره‌سازی به لبه شبکه برای کاهش تأخیر.	حملات فیزیکی هوشمند، جعل بیومتریک برای برنامه‌های کاربردی لبه، مسموم‌سازی کش، حملات به زنجیره تأمین نرم‌افزار.
شبکه دسترسی رادیویی باز (O-RAN)	تجزیه RAN با رابط‌های باز و کنترل هوشمند از طریق RIC و xApps/ rApps.	حملات تخاصمی به مدل‌های هوش مصنوعی RIC، جمینگ هوشمند، تزریق xAppهای مخرب، حملات به رابط‌های باز.

۲ کمپین‌های تهاجمی مبتنی بر هوش مصنوعی: از شناسایی تا بهره‌برداری

چرخه حیات یک حمله سایبری با مرحله شناسایی[1] آغاز می‌شود. در این مرحله، مهاجم اطلاعاتی در مورد هدف جمع‌آوری کرده، پروفایل آن را تهیه می‌کند و آسیب‌پذیری‌های بالقوه را شناسایی می‌نماید. هوش مصنوعی این مرحله را به طور کامل متحول کرده و به مهاجمان اجازه می‌دهد تا با سرعت، دقت و پنهان‌کاری بی‌سابقه‌ای، سطح حمله گسترده و پیچیده 5G را تحلیل کنند.

۲-۱ شناسایی و پروفایل‌سازی هدف با هوش مصنوعی

اسکن سنتی آسیب‌پذیری، مانند اسکن پورت‌ها، پر سر و صدا بوده و به راحتی توسط سیستم‌های تشخیص نفوذ شناسایی می‌شود. شناسایی مبتنی بر هوش مصنوعی یک پارادایم کاملاً متفاوت است؛ این رویکرد می‌تواند رفتار و زمینه را تحلیل کرده و به صورت هوشمندانه و غیرفعال، اطلاعات جمع‌آوری کند. به جای ارسال بسته‌های تهاجمی، یک عامل هوش مصنوعی می‌تواند الگوهای ترافیک API در SBA را تحلیل کند تا وابستگی‌های بین توابع شبکه (NFs) را استنتاج نماید، یا مخازن کد عمومی برای xAppهای O-RAN را بررسی کند تا نقص‌های منطقی را بیابد. این امر شناسایی متخاصم را بسیار پنهان‌کارتر و مؤثرتر می‌سازد.

- **تحلیل ترافیک شبکه مبتنی بر هوش مصنوعی:** مهاجمان می‌توانند از مدل‌های یادگیری ماشین برای تحلیل الگوهای ترافیک رمزگذاری‌شده 5G (فراداده‌ها) استفاده کنند. حتی بدون رمزگشایی محتوای بسته‌ها، تحلیل فراداده‌هایی مانند حجم، زمان‌بندی و مبدأ/مقصد ترافیک بین NFs در SBA، می‌تواند به استنتاج توپولوژی شبکه، شناسایی دارایی‌های با ارزش (مانند «تابع مدیریت دسترسی و پویایی» (AMF) یا «مدیریت داده یکپارچه» (UDM)) و ترسیم جریان‌های ارتباطی کمک کند.
- **پروفایل‌سازی هوشمند هدف‌محور:** هوش مصنوعی قادر است فرآیند جمع‌آوری و مرتبط‌سازی داده‌ها از منابع عمومی (مانند آگهی‌های شغلی برای مهندسان شبکه 5G، مستندات فروشندگان) و انجمن‌های وب تاریک را خودکار کند تا پروفایل‌های دقیقی از شبکه‌های هدف، پرسنل و فناوری‌های مستقرشده بسازد. این اطلاعات برای طراحی حملات

1. Reconnaissance

مهندسی اجتماعی و فیشینگ هدفمند بسیار حیاتی است.

- **یافتن مسیر و شناسایی مبتنی بر هوش مصنوعی:** ابزارهای مبتنی بر هوش مصنوعی، به‌ویژه چارچوب‌های عامل هوشمند[1]، می‌توانند به صورت مداوم و خودکار سطح حمله وسیع 5G را اسکن کنند. این عوامل می‌توانند APIهای در معرض خطر در SBA، پیکربندی‌های نادرست محیط‌های ابری میزبان VNFs، و رابط‌های باز در O-RAN را شناسایی کرده تا شبکه را نقشه‌برداری و نقاط ورود بالقوه را مشخص نمایند.

۲-۲ کشف و تحلیل خودکار آسیب‌پذیری

پس از شناسایی اولیه، مرحله بعدی یافتن آسیب‌پذیری‌های قابل بهره‌برداری است. هوش مصنوعی در این زمینه نیز قابلیت‌های مهاجمان را به شدت افزایش می‌دهد.

- **تشخیص آسیب‌پذیری مبتنی بر هوش مصنوعی:** هوش مصنوعی، تحلیل استاتیک و دینامیک کد منبع (SAST/DAST) سنتی را با درک زمینه و منطق کد تقویت می‌کند. این قابلیت امکان کشف آسیب‌پذیری‌های روز-صفر (Zero-Day) را در نرم‌افزار NFs، برنامه‌های کاربردی MEC و xAppهای O-RAN فراهم می‌آورد. در اکوسیستم نرم‌افزارمحور و چندفروشندگی 5G، این تهدید بسیار جدی است.
- **تحلیل رفتاری برای یافتن راه‌های جدید سوءاستفاده:** یادگیری تقویتی[2] می‌تواند در ابزارهای پیشرفته فازینگ (Fuzzing) به کار گرفته شود. این تکنیک، تولید ورودی‌ها را به سمت مسیرهای کدی که احتمالاً حاوی باگ هستند هدایت می‌کند و به طور مؤثری راه‌های جدیدی برای بهره‌برداری از نقص‌های نرم‌افزاری در مؤلفه‌های 5G کشف می‌نماید.
- **مهندسی معکوس مبتنی بر هوش مصنوعی:** هوش مصنوعی می‌تواند به فرآیند مهندسی معکوس باینری‌های VNF/CNF یا پروتکل‌های API اختصاصی کمک کرده و کشف نقاط ضعف قابل بهره‌برداری را تسریع بخشد.

۲-۳ برنامه‌ریزی و شبیه‌سازی حمله با هوش مصنوعی

هوش مصنوعی نه تنها به مهاجمان در یافتن آسیب‌پذیری‌ها کمک می‌کند، بلکه به آن‌ها اجازه می‌دهد تا حملات خود را با دقت بیشتری برنامه‌ریزی و هماهنگ کنند.

- **پیش‌بینی نتایج حملات:** مهاجمان می‌توانند از هوش مصنوعی برای مدل‌سازی محیط شبکه 5G و شبیه‌سازی بردارهای حمله مختلف استفاده کنند تا احتمال موفقیت و تأثیر بالقوه آن‌ها را قبل از اجرا پیش‌بینی نمایند. این قابلیت، بهینه‌سازی حملات پیچیده و

1. Agentic AI
2. Reinforcement Learning

چندمرحله‌ای، مانند حرکت جانبی بین برش‌های شبکه را ممکن می‌سازد.

- **هماهنگی حملات:** چارچوب‌های عامل هوشمند می‌توانند چندین عامل هوش مصنوعی تخصصی را برای اجرای مراحل مختلف یک حمله به صورت خودکار هماهنگ کنند. این عوامل می‌توانند از شناسایی تا استخراج داده‌ها، تاکتیک‌های خود را به صورت آنی و بر اساس پاسخ‌های دفاعی شبکه، تطبیق دهند.

۳ حملات مبتنی بر هوش مصنوعی به هویت، دسترسی و اعتماد

مکانیسم‌های هویت، دسترسی و اعتماد، سنگ بنای امنیت هر شبکه‌ای هستند. در معماری توزیع‌شده و نرم‌افزارمحور 5G، این مکانیسم‌ها پیچیده‌تر و در عین حال حیاتی‌تر می‌شوند. هوش مصنوعی به مهاجمان ابزارهای قدرتمندی برای به چالش کشیدن و دور زدن این کنترل‌های امنیتی بنیادین ارائه می‌دهد.

۳-۱ به خطر انداختن اعتبارنامه‌ها و احراز هویت

- **حدس، سرقت و بروت فورس رمز عبور و سرقت اعتبارنامه مبتنی بر هوش مصنوعی:** مدل‌های هوش مصنوعی می‌توانند با یادگیری الگوهای رمز عبور از مجموعه داده‌های نقض‌شده، حملات حدس رمز عبور را به طور قابل توجهی بهبود بخشند و فراتر از حملات مبتنی بر دیکشنری ساده عمل کنند. این حملات، رابط‌های مدیریتی برای NFV، کنسول‌های ابری و پورتال‌های ورود به برنامه‌های کاربردی MEC را هدف قرار می‌دهند. هوش مصنوعی همچنین می‌تواند فرآیند «پرکردن اعتبارنامه»[1] را خودکار کند، جایی که اعتبارنامه‌های سرقت‌شده به صورت انبوه در برابر APIهای متعدد خدمات 5G (مانند NEF) آزمایش می‌شوند، در حالی که با چرخاندن آدرس‌های IP و تقلید رفتار انسان، از شناسایی فرار می‌کنند.
- **فیشینگ هدفمند:** هوش مصنوعی مولد[2] قادر است ایمیل‌های فیشینگ بسیار شخصی‌سازی‌شده و متقاعدکننده را در مقیاس بزرگ تولید کند. این ایمیل‌ها می‌توانند مدیران شبکه 5G یا مستأجران سازمانی برش‌های شبکه را هدف قرار دهند. نرخ موفقیت بالای فیشینگ تولیدشده توسط هوش مصنوعی این روش را به یک تهدید حیاتی تبدیل کرده است.

۳-۲ جعل و سرقت هویت

- **جعل مبتنی بر هوش مصنوعی:** یک مهاجم می‌تواند از هوش مصنوعی برای یادگیری الگوهای سیگنالینگ توابع شبکه (NFs) قانونی در SBA استفاده کرده و سپس آن‌ها را جعل کند. این

1. Credential Stuffing
2. Generative AI

کار می‌تواند سایر NFs را فریب دهد تا اطلاعات حساس را فاش کنند یا دستورات مخرب را بپذیرند. این حمله به ویژه در محیط‌هایی که احراز هویت متقابل TLS (mTLS) به درستی پیکربندی نشده باشد، خطرناک است.

- **جعل بیومتریک:** دیپ‌فیک (Deepfake) می‌تواند برای دور زدن سیستم‌های احراز هویت بیومتریک استفاده شود. این سیستم‌ها ممکن است برای دسترسی فیزیکی به مراکز داده MEC یا برای احراز هویت در سرویس‌های سازمانی که بر روی یک برش 5G اجرا می‌شوند، به کار روند.
- **سرقت هویت:** هوش مصنوعی با مرتبط‌سازی داده‌ها از منابع متعدد، به مهاجمان کمک می‌کند تا پروفایل‌های کاملی برای سرقت هویت بسازند. این هویت‌های جعلی می‌توانند برای دریافت خدمات به صورت متقلبانه یا دسترسی به داده‌های حساس در اکوسیستم 5G استفاده شوند.
- **دیپ‌فیک برای مهندسی اجتماعی:** مهاجمان می‌توانند از صدا یا ویدیوی دیپ‌فیک برای فریب مدیران اجرایی یا پرسنل مورد اعتماد استفاده کنند تا تراکنش‌های مالی متقلبانه را تأیید کنند یا کارمندان را برای ارائه دسترسی به سیستم‌های امن فریب دهند. تأثیر دیپ‌فیک‌ها فراتر از مهندسی اجتماعی ساده است و به یک تهدید در لایه سرویس تبدیل می‌شود. به عنوان مثال، یک دیپ‌فیک می‌تواند برای دور زدن تشخیص زنده بودن[1] در یک برنامه خدمات مالی که بر روی یک برش امن MEC اجرا می‌شود، استفاده شود. این امر تهدید را از سطح شبکه به سطح برنامه و سرویس ارتقا می‌دهد و شرکت‌هایی را که از شبکه 5G استفاده می‌کنند، تحت تأثیر قرار می‌دهد.

۳-۳ تضعیف رمزنگاری و اعتماد

- **رمزشکنی:** اگرچه هنوز برای الگوریتم‌های مدرن بیشتر جنبه نظری دارد، اما تکنیک‌های یادگیری ماشین می‌توانند برای تحلیل نشت اطلاعات از کانال‌های جانبی (مانند مصرف برق یا زمان‌بندی) از سخت‌افزارهای رمزنگاری یا توابع رمزنگاری مجازی‌شده، به کار گرفته شوند و به طور بالقوه کلیدهای رمز را استخراج کنند.
- **کانال جانبی:** در محیط‌های مشترک NFV/Cloud، یک VNF متعلق به مهاجم می‌تواند از هوش مصنوعی برای نظارت بر تغییرات نامحسوس در حافظه پنهان (Cache) پردازنده یا الگوهای دسترسی به حافظه استفاده کند تا داده‌های در حال پردازش توسط یک VNF قربانی بر روی همان میزبان فیزیکی را استنتاج نماید. این حمله، ایزوله‌سازی منطقی را دور می‌زند و یک تهدید جدی در محیط‌های چندمستأجری 5G محسوب می‌شود.

1. Liveness Detection

- **ثبت کلید ضمنی:** مدل‌های پیشرفته هوش مصنوعی می‌توانند با تحلیل سیگنال‌های غیرمستقیم مانند صدای تایپ کردن یا لرزش‌های میز، کلیدهای فشرده‌شده را با دقت بالایی بازسازی کنند. این تکنیک می‌تواند برای سرقت اعتبارنامه‌ها در مراکز عملیات شبکه (NOC) یا از مدیران سیستم به کار رود.

۴ حملات دستکاری کد و داده مبتنی بر هوش مصنوعی

ماهیت نرم‌افزارمحور 5G به این معناست که یکپارچگی کد و داده‌ها برای عملکرد امن شبکه ضروری است. هوش مصنوعی توانایی مهاجمان را برای تزریق کد مخرب، دستکاری داده‌ها و توزیع بدافزار در سراسر پشته نرم‌افزاری 5G، از APIهای مواجه با وب تا توابع اصلی شبکه، به طور چشمگیری افزایش می‌دهد.

۴-۱ تزریق هوشمند کد و حملات وب

- **تزریق اسکریپت‌های بین سایتی (XSS) و تزریق SQL:** هوش مصنوعی می‌تواند برای ساخت محموله‌های (Payloads) تزریق پیچیده و مبهم‌سازی‌شده استفاده شود که برای دور زدن «دیواره‌های آتش برنامه کاربردی وب» (WAFs) طراحی شده‌اند. این WAFها از APIهای در معرض خطر مانند NEF یا پورتال‌های مدیریتی MEC محافظت می‌کنند. یک مدل هوش مصنوعی می‌تواند با کاوش یک WAF، مجموعه قوانین آن را یاد بگیرد و سپس محموله‌هایی تولید کند که از شناسایی فرار می‌کنند.
- **مبهم‌سازی بدافزار:** هوش مصنوعی، به ویژه «شبکه‌های مولد تخاصمی» (GANs)، می‌تواند برای ایجاد بدافزارهای چندریختی (Polymorphic) و دگردیسی (Metamorphic) استفاده شود. این نوع بدافزارها به طور مداوم کد خود را بازنویسی می‌کنند و امضاهای منحصربه‌فرد بی‌پایانی ایجاد می‌نمایند که شناسایی آن‌ها را برای موتورهای آنتی‌ویروس مبتنی بر امضا در داخل VNFs یا بر روی میزبان‌های MEC بسیار دشوار می‌سازد.

۴-۲ تزریق هوشمند کد و حملات وب

- **تولید داده‌های مصنوعی:** مهاجمان می‌توانند مقادیر عظیمی از داده‌های واقع‌گرایانه اما مخرب تولید کنند تا مجموعه داده‌های آموزشی مدل‌های هوش مصنوعی مورد استفاده در شبکه 5G (مثلاً برای تحلیل شبکه یا امنیت) را مسموم سازند. این موضوع در بخش ۶ به تفصیل بررسی خواهد شد.
- **تولید نظرات جعلی و اطلاعات نادرست:** اگرچه این‌ها حملات مستقیم به شبکه نیستند، اما می‌توانند از طریق زیرساخت 5G برای دستکاری افکار عمومی یا اختلال در سرویس‌هایی که به فیدهای داده عمومی متکی هستند، مستقر شوند. پهنای باند بالا و تأخیر کم 5G،

انتشار سریع اطلاعات نادرست تولیدشده توسط هوش مصنوعی، از جمله دیپ‌فیک‌ها را تسهیل می‌کند.

- **دستکاری رکوردها:** در یک وضعیت به خطر افتاده، یک ابزار مبتنی بر هوش مصنوعی می‌تواند به طور هوشمندانه لاگ‌ها (مانند سوابق صورت‌حساب، لاگ‌های امنیتی) را برای پنهان کردن ردپای حمله یا ارتکاب کلاهبرداری تغییر دهد. این ابزار با یادگیری فرمت عادی لاگ‌ها، دستکاری‌ها را به گونه‌ای انجام می‌دهد که شناسایی آن‌ها دشوار باشد.
- حمله به CAPTCHA: مدل‌های پیشرفته بینایی کامپیوتر می‌توانند بسیاری از سیستم‌های CAPTCHA را که برای جلوگیری از دسترسی ربات‌ها به سرویس‌ها طراحی شده‌اند، شکست دهند. این امر به مهاجمان اجازه می‌دهد تا حملات خودکار را در مقیاس بزرگ علیه سرویس‌های مبتنی بر 5G اجرا کنند.

۴-۳ بدافزارهای پیشرفته و توزیع آن‌ها

- **توزیع بدافزار:** هوش مصنوعی می‌تواند توزیع بدافزار را با شناسایی آسیب‌پذیرترین اهداف یا مؤثرترین مسیرهای انتشار در شبکه 5G بهینه کند، مانند حرکت از یک برش سازمانی با امنیت کمتر به یک برش حیاتی‌تر.
- **بدافزارهای خودآموز:** بدافزارها می‌توانند یادگیری تقویتی را در خود جای دهند تا رفتار خود را به صورت آنی و بر اساس محیطی که در آن قرار دارند، تطبیق دهند. به عنوان مثال، یک بدافزار می‌تواند یاد بگیرد که در صورت شناسایی ابزارهای نظارتی، فعالیت خود را کاهش دهد یا در صورت مسدود شدن یک کانال، روش استخراج داده خود را تغییر دهد.
- **بدافزارهای مبتنی بر هوش مصنوعی برای فرار از تشخیص:** این یک دسته گسترده‌تر است که تکنیک‌های فوق را در بر می‌گیرد، جایی که هدف اصلی هوش مصنوعی اطمینان از عدم شناسایی بدافزار از طریق تقلید ترافیک قانونی و تغییر پویای ویژگی‌های آن است. این مفهوم به پارادایم «زندگی با ابزارهای موجود ۲.۰»[1] منجر می‌شود. حملات سنتی «زندگی با ابزارهای موجود» از ابزارهای قانونی سیستم برای جلوگیری از شناسایی استفاده می‌کنند. بدافزارهای مبتنی بر هوش مصنوعی این مفهوم را یک قدم فراتر می‌برند. یک VNF مخرب مبتنی بر هوش مصنوعی می‌تواند الگوهای ارتباطی عادی API در SBA را یاد بگیرد و سپس از همان APIهای قانونی برای فرمان و کنترل (C2) و استخراج داده‌ها استفاده کند، و کاملاً با ترافیک عادی سرویس به سرویس ترکیب شود. این امر شناسایی مبتنی بر تحلیل ترافیک را فوق‌العاده دشوار می‌سازد، زیرا شکل ارتباط عادی است، حتی اگر قصد آن مخرب باشد.

1. Living Off the Land 2.0

۵ حملات مبتنی بر هوش مصنوعی به دسترس‌پذیری و یکپارچگی شبکه

دسترس‌پذیری[1] و یکپارچگی[2] از ارکان اصلی هر سرویس مخابراتی هستند. معماری ۵G، با وابستگی به مجازی‌سازی، برش‌بندی و رابط‌های باز، بردارهای حمله جدیدی را برای مختل کردن خدمات ایجاد می‌کند. هوش مصنوعی به مهاجمان این امکان را می‌دهد که حملات پیچیده‌ای را برای از کار انداختن، تضعیف یا غیرفعال کردن سرویس‌های شبکه ۵G با کارایی و پنهان‌کاری بیشتری اجرا کنند.

۵-۱ بدافزارهای پیشرفته و توزیع آن‌ها

- **حملات DDoS مبتنی بر هوش مصنوعی:** هوش مصنوعی می‌تواند برای سازماندهی حملات انکار سرویس توزیع‌شده (DDoS) عظیم و بسیار تطبیق‌پذیر استفاده شود. بات‌نت‌های کنترل‌شده توسط هوش مصنوعی می‌توانند بردارهای حمله خود را به صورت آنی تغییر دهند (مثلاً از یک حمله حجمی به یک حمله لایه کاربرد) تا اقدامات کاهشی را دور بزنند. این حملات می‌توانند توابع شبکه حیاتی، برش‌های شبکه یا برنامه‌های کاربردی MEC را هدف قرار دهند.
- **طوفان سیگنالینگ مبتنی بر هوش مصنوعی:** این یک نوع خاص از DDoS است که در آن هوش مصنوعی برای تولید سیلی از پیام‌های سیگنالینگ با ظاهر قانونی (مانند درخواست‌های اتصال) استفاده می‌شود تا توابع صفحه کنترل مانند AMF را تحت فشار قرار دهد. این یک آسیب‌پذیری شناخته‌شده است که از LTE به ارث رسیده و با قابلیت‌های هوش مصنوعی تشدید می‌شود.

۵-۲ حملات به شبکه دسترسی رادیویی (RAN)

- **جمینگ:** جمینگ‌های هوشمند می‌توانند از هوش مصنوعی برای تحلیل محیط رادیویی و تغییر پویای فرکانس و شکل موج جمینگ خود استفاده کنند تا مؤثرتر و شناسایی آن‌ها دشوارتر باشد. این یک تهدید قابل توجه در O-RAN است، جایی که حلقه‌های کنترل بازتر هستند و یک مهاجم می‌تواند با تحلیل پاسخ‌های RIC، استراتژی جمینگ خود را بهینه کند.

1. Availability
2. Integrity

- **سیاه چاله:** در یک حمله سیاه‌چاله، یک گره مخرب خود را به عنوان بهترین مسیر به یک مقصد معرفی می‌کند، ترافیک را به سمت خود جذب کرده و سپس آن را حذف می‌کند. هوش مصنوعی می‌تواند این حمله را پویاتر و هدفمندتر کند. به عنوان مثال، یک gNB یا O-RAN DU سرکش می‌تواند به صورت انتخابی ترافیک مربوط به یک برش شبکه خاص یا یک نوع کاربر خاص را حذف کند، در حالی که ترافیک دیگر را به طور عادی عبور می‌دهد تا از شناسایی جلوگیری کند.

۵-۳ بهره‌برداری از مجازی‌سازی و برش‌بندی برای اختلال

- **تخلیه منابع برش‌ها با هوش مصنوعی:** مهاجمان می‌توانند از هوش مصنوعی برای تولید ترافیکی استفاده کنند که به طور خاص برای تخلیه منابع مشترک (مانند CPU، حافظه در NFVI) اختصاص‌یافته به یک برش خاص طراحی شده است. این امر می‌تواند باعث تضعیف عملکرد برای سایر برش‌هایی شود که از همان زیرساخت مشترک استفاده می‌کنند. این نوع حمله، که می‌توان آن را «حمله آگاه از کیفیت سرویس (QoS-aware)» نامید، یکی از پیچیده‌ترین تهدیدات برای 5G است. یک مهاجم هوشمند نیازی به راه‌اندازی یک DDoS حجمی و پر سر و صدا ندارد. در عوض، می‌تواند از هوش مصنوعی برای تولید حجم کمی از ترافیک بسیار پیچیده استفاده کند که به طور خاص منبع محدود یک برش با ارزش (مثلاً ظرفیت پردازش برای یک برش URLLC) را هدف قرار داده و تخلیه کند. این حمله بسیار پنهان‌کارتر و کارآمدتر است و ویژگی‌های بهینه‌سازی خود شبکه را علیه آن به کار می‌گیرد.
- **کش‌کاوی:** در محیط‌های MEC که برای تأخیر کم به شدت به کشینگ متکی هستند، هوش مصنوعی می‌تواند برای یافتن راه‌های نامحسوس برای مسموم کردن کش محتوا یا DNS استفاده شود. این امر می‌تواند کاربران یک برنامه MEC را به سایت‌های مخرب هدایت کند یا باعث از کار افتادن سرویس شود.
- **باج‌افزارهای مبتنی بر هوش مصنوعی:** باج‌افزارهای مدرن، مانند Scattered Spider، از مهندسی اجتماعی پیشرفته برای نفوذ به زیرساخت‌های حیاتی، از جمله محیط‌های مجازی‌سازی‌شده VMware که در 5G NFV استفاده می‌شوند، بهره می‌برند. هوش مصنوعی می‌تواند این فرآیند را با خودکارسازی شناسایی اهداف با ارزش (مانند مدیران vSphere) و حرکت جانبی سریع در شبکه، تسریع بخشد. یک باج‌افزار مبتنی بر هوش مصنوعی می‌تواند به طور خودکار دارایی‌های حیاتی در یک شبکه 5G (مانند توابع اصلی یا ارکستراتور برش) را شناسایی کرده، آن‌ها را رمزگذاری کند و سپس به صورت هوشمندانه در شبکه منتشر شود.

۶ تهدید درونی: حملات تخاصمی به سیستم‌های هوش مصنوعی/یادگیری ماشین 5G

تا اینجای گزارش، هوش مصنوعی به عنوان سلاحی در دست مهاجمان بررسی شد. اما در این بخش، تمرکز از هوش مصنوعی به عنوان سلاح به هوش مصنوعی به عنوان هدف تغییر می‌کند. شبکه‌های 5G به طور فزاینده‌ای برای مدیریت، بهینه‌سازی و امنیت خود به مدل‌های هوش مصنوعی و یادگیری ماشین (AI/ML) متکی هستند. این مدل‌ها، از الگوریتم‌های بهینه‌سازی منابع در RIC O-RAN گرفته تا سیستم‌های تشخیص نفوذ در هسته شبکه، خود به یک سطح حمله جدید و حیاتی تبدیل شده‌اند. حملات تخاصمی[1] به طور خاص برای فریب دادن، خرابکاری یا سرقت این مدل‌های هوش مصنوعی طراحی شده‌اند.

موفقیت این حملات، چشم‌انداز «اتوماسیون بدون دخالت انسان» را که هدف نهایی 5G است، به طور مستقیم تهدید می‌کند. یک سیستم خودکار که بر پایه یک مدل هوش مصنوعی به خطر افتاده عمل می‌کند، می‌تواند تصمیمات فاجعه‌باری اتخاذ کند -مانند مسیریابی نادرست ترافیک، خاموش کردن یک برش شبکه حیاتی، یا نادیده گرفتن یک رخنه امنیتی بزرگ -بدون هیچ‌گونه نظارت انسانی. بنابراین، درک این تهدیدات برای دستیابی به اتوماسیون امن و قابل اعتماد ضروری است.

۶-۱ خرابکاری در فرآیند یادگیری: حملات مسموم‌سازی و در پشتی

این حملات در مرحله آموزش مدل رخ می‌دهند و هدف آن‌ها خرابکاری در پایه و اساس دانش مدل است.

- **مسمومیت مدل هوش مصنوعی:** مهاجمان داده‌های مخرب را به مجموعه داده‌های آموزشی یک مدل هوش مصنوعی 5G تزریق می‌کنند. به عنوان مثال، مسموم کردن داده‌های ترافیکی که برای آموزش «تابع تحلیل داده شبکه» (NWDAF) استفاده می‌شود، می‌تواند باعث شود که این تابع شرایط شبکه را به اشتباه تفسیر کند و منجر به تخصیص ناکارآمد منابع یا عدم شناسایی یک حمله واقعی شود.
- **مسمومیت با برچسب تمیز:** این یک حمله بسیار موذیانه است که در آن داده‌های تزریق‌شده به طور نامحسوسی دستکاری می‌شوند اما همچنان برچسب صحیح خود را

1. Adversarial Attacks

حفظ می‌کنند. این امر باعث می‌شود داده‌های مسموم برای بازرسان انسانی بی‌خطر به نظر برسند، اما همچنان در خرابکاری مرز تصمیم‌گیری مدل برای یک هدف خاص مؤثر هستند.

- **مسمومیت هدفمند:** مسموم‌سازی به گونه‌ای طراحی شده است که باعث یک رفتار نادرست خاص و هدفمند شود. به عنوان مثال، وادار کردن هوش مصنوعی زمان‌بند RAN به اینکه همیشه اولویت یک کاربر یا برنامه خاص را کاهش دهد.
- **مسمومیت درب پشتی:** مهاجم مجموعه داده‌های آموزشی را مسموم می‌کند تا یک «ماشه» (Trigger) مخفی را در مدل جاسازی کند. مدل بر روی داده‌های عادی به درستی عمل می‌کند، اما در صورت وجود ماشه در ورودی، رفتار مخربی از خود نشان می‌دهد. به عنوان مثال، یک سیستم تشخیص نفوذ مبتنی بر هوش مصنوعی می‌تواند به گونه‌ای دارای در پشتی شود که تمام ترافیک حمله از یک آدرس IP خاص (ماشه) را نادیده بگیرد.
- **مسمومیت در دسترس‌پذیری:** این نوع مسموم‌سازی به گونه‌ای طراحی شده است که عملکرد کلی مدل را تضعیف کرده و باعث افزایش نرخ خطا یا مصرف بیش از حد منابع شود و در نهایت منجر به انکار سرویس گردد.

۶-۲ فریب مدل در زمان استنتاج: حملات گریز

این حملات در زمان استفاده از مدل (استنتاج) رخ می‌دهند و هدف آن‌ها فریب دادن مدل با ورودی‌های دستکاری‌شده است.

- **گریز یا نمونه‌های تخاصمی:** مهاجمان تغییرات کوچک و اغلب نامحسوسی را در داده‌های ورودی در زمان استنتاج ایجاد می‌کنند تا باعث شوند مدل آن را به اشتباه طبقه‌بندی کند. به عنوان مثال، با تغییر جزئی داده‌های بسته شبکه، یک سیستم تشخیص نفوذ مبتنی بر هوش مصنوعی فریب می‌خورد و آن را به عنوان ترافیک خوش‌خیم طبقه‌بندی می‌کند و در نتیجه یک نفوذ شناسایی نمی‌شود. این یک تهدید بزرگ برای هر سیستم امنیتی مبتنی بر هوش مصنوعی در 5G است.

۶-۳ سرقت مالکیت معنوی و داده‌ها: حملات استنتاج و استخراج

این حملات محرمانگی مدل و داده‌های آموزشی آن را هدف قرار می‌دهند.

- **استخراج مدل:** یک مهاجم با دسترسی به پرس‌وجو از یک مدل هوش مصنوعی اختصاصی 5G (مثلاً یک مدل بهینه‌سازی شبکه که از طریق API در دسترس است) می‌تواند از این پرس‌وجوها برای آموزش یک کپی محلی از مدل استفاده کرده و به طور مؤثری مدل را سرقت کند.

- **بازسازی داده:** در برخی موارد، یک مهاجم می‌تواند با پرس‌وجو از یک مدل، اطلاعات حساس از داده‌های آموزشی اصلی آن را بازسازی کند. این امر در صورتی که مدل بر روی داده‌های کاربران آموزش دیده باشد، یک خطر حریم خصوصی جدی محسوب می‌شود.
- **استنتاج عضویت:** مهاجم تعیین می‌کند که آیا یک رکورد داده خاص بخشی از مجموعه داده‌های آموزشی مدل بوده است یا خیر. این یک نقض حریم خصوصی است که می‌تواند فاش کند، به عنوان مثال، آیا داده‌های یک فرد خاص برای آموزش یک مدل پیش‌بینی تحرک استفاده شده است.
- **استنتاج ویژگی:** مهاجم ویژگی‌های حساس یک رکورد داده را از پیش‌بینی مدل استنتاج می‌کند، حتی بدون بازسازی کامل رکورد.

۶-۴ حملات به مدل‌های زبانی بزرگ (LLMs)

با افزایش استفاده از LLMها در مدیریت شبکه، بردارهای حمله جدیدی ظهور کرده‌اند.

- **حمله مبتنی بر RAG:** اگر یک سیستم مدیریت 5G از یک مدل «تولید مبتنی بر بازیابی» (RAG) استفاده کند، مهاجم می‌تواند پایگاه دانشی را که مدل از آن بازیابی می‌کند، مسموم سازد. این کار باعث می‌شود مدل اطلاعات نادرست یا مخربی را به اپراتورهای شبکه ارائه دهد.
- **تزریق مستقیم و غیرمستقیم درخواست:** مهاجم می‌تواند درخواست‌هایی[1] را طراحی کند تا یک دستیار شبکه مبتنی بر LLM دستورالعمل‌های ایمنی خود را نادیده گرفته و دستورات غیرمجاز را اجرا کند (تزریق مستقیم). یا می‌تواند یک درخواست مخرب را در داده‌هایی که LLM بعداً پردازش خواهد کرد، مانند یک فایل لاگ شبکه، پنهان کند (تزریق غیرمستقیم).

1.Prompts

جدول۲: حملات به سامانه‌های هوش مصنوعی در شبکه‌های 5G

دسته‌بندی حمله	حمله خاص	هدف مهاجم	دانش مورد نیاز	برنامه کاربردی آسیب‌پذیر هوش مصنوعی در 5G
حملات یکپارچگی	مسمومیت مدل، مسمومیت با برچسب تمیز، مسمومیت در پشتی	خرابکاری در رفتار مدل برای اهداف خاص	دسترسی به داده‌های آموزشی	تحلیلگر داده شبکه (NW-DAF)، زمان‌بند هوشمند RAN، سیستم‌های مدیریت ترافیک
حملات دسترس‌پذیری	مسمومیت دسترس‌پذیری	کاهش عملکرد کلی مدل یا ایجاد انکار سرویس	دسترسی به داده‌های آموزشی	هر مدل هوش مصنوعی حیاتی برای عملیات شبکه (مانند بهینه‌سازی منابع)
حملات محرمانگی	استخراج مدل، بازسازی داده، استنتاج عضویت/ویژگی	سرقت مدل یا افشای داده‌های حساس آموزشی	دسترسی به پرس‌وجو از مدل (API)	مدل‌های اختصاصی بهینه‌سازی شبکه، مدل‌های پیش‌بینی رفتار کاربر
حملات گریز	نمونه‌های تخاصمی	دور زدن تشخیص در زمان استنتاج	دسترسی به پرس‌وجو (جعبه سیاه) یا مدل (جعبه سفید)	سیستم‌های تشخیص نفوذ (IDS/IPS)، فیلترهای بدافزار، سیستم‌های تشخیص جمینگ
حملات LLM	تزریق درخواست، حمله مبتنی بر RAG	کنترل خروجی LLM یا اجرای دستورات غیرمجاز	توانایی ارسال ورودی (درخواست)	دستیارهای عملیات شبکه، ابزارهای تحلیل لاگ مبتنی بر LLM

۷ دفاع سایبری در عصر هوش مصنوعی و شبکه‌های 5G

تحلیل‌های ارائه‌شده در بخش‌های قبل نشان می‌دهد که چشم‌انداز تهدیدات در شبکه‌های 5G به طور بنیادین تغییر کرده است. دفاع در برابر حملات هوشمند، سریع و تطبیق‌پذیر مبتنی بر هوش مصنوعی، نیازمند یک استراتژی دفاعی به همان اندازه هوشمند، پویا و چندلایه است. تکیه بر تحلیلگران انسانی و دفاع ایستا، در برابر تهدیداتی که با سرعت ماشین عمل می‌کنند، محکوم به شکست است. این بخش یک چارچوب دفاعی راهبردی و آینده‌نگر را ارائه می‌دهد که برای ایجاد یک معماری امنیتی انعطاف‌پذیر و مقاوم در برابر تهدیدات دوگانه هوش مصنوعی تهاجمی و تخاصمی طراحی شده است.

۷-۱ بهره‌گیری از هوش مصنوعی تدافعی

مقابله با هوش مصنوعی تهاجمی، نیازمند هوش مصنوعی تدافعی است. این یک مسابقه تسلیحاتی اجتناب‌ناپذیر است که در آن، سیستم‌های دفاعی باید بتوانند با سرعت و پیچیدگی مهاجمان رقابت کنند.

- **شکار و تشخیص تهدید مبتنی بر هوش مصنوعی:** استفاده از مدل‌های یادگیری ماشین برای تحلیل آنی جریان‌های عظیم داده در شبکه 5G، برای شناسایی ناهنجاری‌ها و الگوهایی که نشان‌دهنده حملات پیچیده هستند، ضروری است. سیستم‌های مبتنی بر قوانین، قادر به شناسایی بدافزارهای چندریختی یا حملات «زندگی با ابزارهای موجود ۲.۰» نیستند. سیستم‌های تشخیص نفوذ مبتنی بر هوش مصنوعی (AI-IDS/IPS) و پلتفرم‌های تشخیص و پاسخ گسترده (XDR) که از هوش مصنوعی بهره می‌برند، می‌توانند این تهدیدات را شناسایی کنند.
- **پاسخ و ارکستراسیون خودکار مبتنی بر هوش مصنوعی:** پس از تشخیص، پاسخ باید با سرعت ماشین انجام شود. پیاده‌سازی «ارکستراسیون امنیتی» (SCO) مبتنی بر هوش مصنوعی، به شبکه اجازه می‌دهد تا به صورت پویا مؤلفه‌های به خطر افتاده را ایزوله کند، ترافیک را مسیریابی مجدد نماید یا سیاست‌های امنیتی جدید را در چند میلی‌ثانیه اعمال کند. این امر زمان اقامت مهاجم در شبکه را به حداقل می‌رساند.

- **سیاست‌های امنیتی تطبیقی مبتنی بر هوش مصنوعی:** به جای استفاده از قوانین ایستا در فایروال‌ها، می‌توان از یادگیری تقویتی برای ایجاد سیاست‌های امنیتی تطبیقی استفاده کرد. این سیاست‌ها به صورت پویا و بر اساس چشم‌انداز تهدیدات آنی، خود را تنظیم می‌کنند و یک دفاع فعال و پیشگیرانه را ممکن می‌سازند.

۷-۲ معماری برای انعطاف‌پذیری: مدل اعتماد صفر

مدل امنیتی سنتی مبتنی بر محیط پیرامونی در 5G منسوخ شده است. یک «معماری اعتماد صفر» (ZTA) که بر سه اصل استوار است - هرگز اعتماد نکن، همیشه اثبات کن؛ اعمال دسترسی با حداقل امتیاز؛ و فرض رخنه امنیتی- برای امنیت 5G ضروری است.

- **اعتماد صفر در SBA:** این اصل به معنای پیاده‌سازی مدیریت هویت و دسترسی (IAM) قوی برای هر تابع شبکه است. تمام ارتباطات سرویس-به-سرویس باید از طریق احراز هویت متقابل TLS (mTLS) امن شوند و مجوزدهی API باید به صورت دانه‌ای و با استفاده از پروتکل‌هایی مانند OAuth 2.0 انجام شود.
- **اعتماد صفر در محیط‌های مجازی‌شده:** استفاده از «میکرو-بخش‌بندی»[1] برای ایجاد محیط‌های پیرامونی امنیتی دانه‌ای در اطراف هر VNF/CNF، از حرکت جانبی مهاجم جلوگیری می‌کند، حتی اگر یک مؤلفه به خطر بیفتد. این امر «شعاع انفجار»[2] یک حمله را به شدت محدود می‌کند.

۷-۳ ایمن‌سازی خط لوله هوش مصنوعی/یادگیری ماشین

از آنجایی که خود هوش مصنوعی یک هدف است، ایمن‌سازی چرخه حیات توسعه و استقرار آن حیاتی است.

- **منشأ و یکپارچگی داده‌ها:** باید کنترل‌های دقیقی بر روی داده‌های مورد استفاده برای آموزش مدل‌های هوش مصنوعی 5G اعمال شود. استفاده از تکنیک‌های پاک‌سازی داده‌ها، تشخیص داده‌های پرت و ردیابی منشأ داده‌ها برای دفاع در برابر حملات مسموم‌سازی ضروری است.
- **استحکام مدل و آموزش تخاصمی:** آموزش مدل‌های هوش مصنوعی با استفاده از نمونه‌های تخاصمی، آن‌ها را در برابر حملات گریز مقاوم‌تر می‌کند. تکنیک‌هایی مانند تقطیر دفاعی[3] و ماسک‌گذاری گرادیان نیز می‌توانند به کار گرفته شوند.
- **استقرار امن مدل:** باید از شیوه‌های امن زنجیره تأمین برای مدل‌های هوش مصنوعی استفاده

1. Micro-segmentation
2. Blast Radius
3. Defensive Distillation

کرد، از جمله امضای رمزنگاری‌شده و تأیید هش، تا از دستکاری و تزریق در پشتی جلوگیری شود.

۷-۴ دفاع پیشگیرانه و مشارکتی

تیم قرمز مبتنی بر هوش مصنوعی: به جای تست‌های نفوذ دوره‌ای و دستی، می‌توان از هوش مصنوعی برای آزمایش مداوم و خودکار دفاعیات شبکه استفاده کرد. این سیستم‌ها می‌توانند همان تکنیک‌های پیشرفته‌ای را که مهاجمان به کار می‌برند، شبیه‌سازی کرده و نقاط ضعف را قبل از بهره‌برداری شناسایی کنند.

- **به اشتراک‌گذاری هوش تهدید:** ایجاد چارچوب‌هایی برای به اشتراک‌گذاری هوش تهدید مخصوص حملات مبتنی بر هوش مصنوعی و آسیب‌پذیری‌های 5G بین اپراتورها، فروشندگان و نهادهای دولتی، برای ایجاد یک دفاع جمعی و هماهنگ ضروری است.

در نهایت، آینده امنیت 5G در یک مسابقه تسلیحاتی بین هوش مصنوعی تهاجمی و تدافعی تعریف می‌شود. یک استراتژی امنیتی که صرفاً به تحلیلگران انسانی و دفاع ایستا متکی باشد، به ناچار شکست خواهد خورد. هدف استراتژیک کلیدی برای یک اپراتور 5G نباید تنها خرید محصولات امنیتی مبتنی بر هوش مصنوعی باشد، بلکه باید توسعه یک قابلیت امنیتی هوش مصنوعی باشد که بتواند به همان سرعتی که تهدیدات تکامل می‌یابند، خود را تطبیق داده و یاد بگیرد. این امر تمرکز را از کسب ابزارهای ایستا به ساختن یک اکوسیستم دفاعی پویا و یادگیرنده منتقل می‌کند—یک شبکه خود-دفاعی که در آن عوامل هوش مصنوعی تدافعی به طور مداوم عوامل هوش مصنوعی تهاجمی را شکار، شناسایی و خنثی می‌کنند.

منابع

1. What Is 5G Security? A Primer on 5G Network Security - Palo Alto ..., accessed July 29, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-5g-security
2. What is 5G Security? | Future & Benefits - Zscaler, accessed July 29, 2025, https://www.zscaler.com/zpedia/what-is-5g-security
3. What Is 5G Security? A Primer on 5G Network Security - Palo Alto ..., accessed July 29, 2025, https://www.paloaltonetworks.com.au/cyberpedia/what-is-5g-security
4. 5G Standalone Security - 2024 update - new attack ... - SecurityGen, accessed July 29, 2025, https://security-gen.com/5G-Standalone-Security-2024-Update-New-Attack-Techniques.pdf
5. Security for 5G Service-Based Architecture: What you need to know - Ericsson, accessed July 29, 2025, https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture
6. 5G SECURITY ISSUES - GSMA, accessed July 29, 2025, https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2019/11/5G-Research_A4.pdf
7. 5G Security - F5 Networks, accessed July 29, 2025, https://www.f5.com/pdf/solution-guides/establishing-5g-security.pdf
8. 5G Security – Use Cases and Best Practices Webinar - November 2021 Q&A with Jyrki Penttinen, Senior Technology Manager, No - GSMA, accessed July 29, 2025, https://www.gsma.com/security/wp-content/uploads/2021/12/5G-Security-Use-Cases-QA.pdf
9. NFV Security in 5G - Challenges and Best Practices | ENISA, accessed July 29, 2025, https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices
10. Network Functions Virtualization (NFV) explained - Ericsson, accessed July 29, 2025, https://www.ericsson.com/en/nfv
11. Kubernetes and Network Virtualization in 4G/5G Telecom Infrastructure - P1 Security, accessed July 29, 2025, https://www.p1sec.com/blog/network-virtualization-and-automation-kubernetes-in-mobile-networks
12. 5G Network Slicing: Security Challenges, Attack Vectors, and Mitigation Approaches - PMC, accessed July 29, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC12251764/
13. How Network Slicing Impacts Security in 5G - Patsnap Eureka, accessed July 29, 2025, https://eureka.patsnap.com/article/how-network-slicing-impacts-security-in-5g
14. 5G MEC Security: How Secure is 5G Mobile Edge Computing? - Verizon, accessed July 29, 2025, https://www.verizon.com/business/resources/articles/s/how-secure-is-5g-mobile-edge-computing/
15. The Fundamentals of Ensuring 5G MEC Security, accessed July 29, 2025, https://assets.ctfassets.net/wcxs9ap8i19s/KyA8cYxJkvjHd212mJwrH/5eb3b2b84d1b0e2a0ff8b32012fcad11/WP_Fundamentals_5G_MEC_Security_RevB.pdf
16. Evolving Open RAN security - Ericsson, accessed July 29, 2025, https://www.ericsson.com/en/reports-and-papers/further-insights/evolving-open-ran-security

17. Open RAN: Deep Security Analysis, Benefits & Essential Best Practices, accessed July 29, 2025, https://www.p1sec.com/blog/comprehensive-guide-to-open-ran-understanding-benefits-deep-security-analysis-and-essential-best-practices

18. An Open-RAN Testbed for Detecting and Mitigating Radio ... - arXiv, accessed July 29, 2025, https://www.arxiv.org/pdf/2503.10255

19. AI Empowers Novices to Launch Cyberattacks – Communications of ..., accessed July 29, 2025, https://cacm.acm.org/news/ai-empowers-novices-to-launch-cyberattacks/

20. AI-Powered & Automated Vulnerability Discovery: The Future of Pentesting Has Arrived | by Ekene Joseph | Jul, 2025 | Medium, accessed July 29, 2025, https://medium.com/@Ekene-joseph/ai-powered-automated-vulnerability-discovery-the-future-of-pentesting-has-arrived-48b636c2dbc8

21. AI-Based Malicious Encrypted Traffic Detection in 5G Data Collection and Secure Sharing, accessed July 29, 2025, https://www.researchgate.net/publication/387444309_AI-Based_Malicious_Encrypted_Traffic_Detection_in_5G_Data_Collection_and_Secure_Sharing

22. AI-Powered Social Engineering Attacks | CrowdStrike, accessed July 29, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/ai-social-engineering/

23. ISR - Sky-Drones Technologies Ltd, accessed July 29, 2025, https://sky-drones.com/isr

24. (PDF) An AI-powered Network Threat Detection System, accessed July 29, 2025, https://www.researchgate.net/publication/360665337_An_AI-powered_Network_Threat_Detection_System

25. Unit 42 Develops Agentic AI Attack Framework - Palo Alto Networks, accessed July 29, 2025, https://www.paloaltonetworks.com/blog/2025/05/unit-42-develops-agentic-ai-attack-framework/

26. Automated Vulnerability Discovery and Exploitation in the Internet of ..., accessed July 29, 2025, https://www.mdpi.com/1424-8220/19/15/3362

27. The Potential of Generative AI Security Enhancements and Predictive Maintenance in 5G Networks, accessed July 29, 2025, https://www.5gamericas.org/the-potential-of-generative-ai-security-enhancements-and-predictive-maintenance-in-5g-networks/

28. What Is Credential Stuffing? - Palo Alto Networks, accessed July 29, 2025, https://www.paloaltonetworks.com/cyberpedia/credential-stuffing

29. AI-Enhanced Attacks Require Increased Vigilance From Federal ..., accessed July 29, 2025, https://fedtechmagazine.com/article/2025/07/ai-enhanced-attacks-require-increased-vigilance-federal-security-officers

30. What is Spear Phishing? - Trend Micro, accessed July 29, 2025, https://www.trendmicro.com/en_gb/what-is/phishing/types-of-phishing/spear-phishing.html

31. Configure 5G Multi-access Edge Computing Security - Palo Alto Networks, accessed July 29, 2025, https://docs.paloaltonetworks.com/service-providers/10-2/mobile-network-infrastructure-getting-started/5g-security/5g-multi-edge-security/configure-5g-multi-edge-security

32. Verizon collaborates with NVIDIA to power AI workloads on 5G private networks with Mobile Edge Compute | News Release, accessed July 29, 2025, https://www.verizon.com/about/news/verizon-nvidia-power-ai-workloads-5g-private-networks-mec

33. (PDF) Deepfakes in Social Engineering: New Frontiers for Cybercrime, accessed July 29, 2025, https://www.researchgate.net/publication/393631503_Deepfakes_in_Social_Engineering_New_Frontiers_for_Cybercrime

34. Deepfake It 'til You Make It: A Comprehensive View of the New AI ..., accessed July 29, 2025, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/deepfake-it-til-you-make-it-a-comprehensive-view-of-the-new-ai-criminal-toolset

35. The growing threat of AI-driven fraud and deepfakes, accessed July 29, 2025, https://member.texasbankers.com/Magazine/Magazine/ComplianceHotline/25-07-The-growing-threat-of-AI-driven-fraud-and-deepfakes.aspx

36. Why a Classic MCP Server Vulnerability Can Undermine Your Entire ..., accessed July 29, 2025, https://www.trendmicro.com/en_us/research/25/f/why-a-classic-mcp-server-vulnerability-can-undermine-your-entire-ai-agent.html

37. Effective AI Powered Malware Detection: Protecting Your Digital ..., accessed July 29, 2025, https://fidelissecurity.com/cybersecurity-101/cyberattacks/ai-powered-malware-detection/

38. AI/ML Security Attacks and Mitigation Strategies on 5G Network, accessed July 29, 2025, https://www.tcs.com/insights/blogs/ai-security-attacks-mitigation-strategies

39. The rise of generative artificial intelligence and the threat of fake news and disinformation online: Perspectives from sexual medicine, accessed July 29, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11076802/

40. The origin of public concerns over AI supercharging misinformation ..., accessed July 29, 2025, https://misinforeview.hks.harvard.edu/article/the-origin-of-public-concerns-over-ai-supercharging-misinformation-in-the-2024-u-s-presidential-election/

41. AI and the spread of fake news sites: Experts explain how to ..., accessed July 29, 2025, https://news.vt.edu/articles/2024/02/AI-generated-fake-news-experts.html

42. Cybersecurity in 5G Networks: AI-Based Solutions for Securing Next-Gen Connectivity, accessed July 29, 2025, https://www.researchgate.net/publication/388525617_Cybersecurity_in_5G_Networks_AI-Based_Solutions_for_Securing_Next-Gen_Connectivity

43. What Is an AI Worm? - Palo Alto Networks, accessed July 29, 2025, https://www.paloaltonetworks.com/cyberpedia/ai-worm

44. Botnets, scrapers and AI attacks: Why web security must evolve ..., accessed July 29, 2025, https://www.brightspot.com/cms-resources/technology-insights/web-security-and-the-new-threat-landscape

45. Battling AI-powered botnets: evolving challenges in mitigating non ..., accessed July 29, 2025, https://www.iotinsider.com/iot-insights/battling-ai-powered-botnets-evolving-challenges-in-mitigating-non-human-threats/

46. 5G Security Threats: Understanding the Risks in the Next-Gen Network Era | by Ekene Joseph | Jun, 2025 | Medium, accessed July 29, 2025, https://medium.com/@Ekenejoseph/5g-security-threats-understanding-the-risks-in-the-next-gen-network-era-e6001baa0274

47. Demo: Secure Edge Server for Network Slicing and Resource Allocation in Open RAN, accessed July 29, 2025, https://arxiv.org/html/2507.11499v1

48. 5G Network Slicing: Security Challenges, Attack Vectors, and Mitigation Approaches, accessed July 29, 2025, https://www.researchgate.net/publication/392972494_5G_Network_Slicing_Security_Challenges_Attack_Vectors_and_Mitigation_Approaches

49. AI-Driven Network Slicing in 5G and Beyond: Unlocking Intelligent Connectivity - Byanat, accessed July 29, 2025, https://www.byanat.ai/blog/ai-driven-network-slicing-in-5g-and-beyond-unlocking-intelligent-connectivity

50. AI-Based Malicious Encrypted Traffic Detection in 5G Data Collection and Secure Sharing, accessed July 29, 2025, https://www.mdpi.com/2079-9292/14/1/51

51. Improved Security Solutions for DDoS Mitigation in 5G Multi-access Edge Computing, accessed July 29, 2025, https://www.researchgate.net/publication/364522311_Improved_Security_Solutions_for_DDoS_Mitigation_in_5G_Multi-access_Edge_Computing

52. Online data poisoning attack against edge AI paradigm for IoT-enabled smart city - PubMed, accessed July 29, 2025, https://pubmed.ncbi.nlm.nih.gov/38052534/

53. What Is DNS Cache Poisoning or Spoofing? - Akamai, accessed July 29, 2025, https://www.akamai.com/glossary/what-is-dns-cache-poisoning

54. What is Cache Poisoning | DNS and Web Cache Attacks - Imperva, accessed July 29, 2025, https://www.imperva.com/learn/application-security/cache-poisoning/

55. Scattered Spider hackers are targeting US critical infrastructure via ..., accessed July 29, 2025, https://www.techradar.com/pro/security/scattered-spider-hackers-are-targeting-us-critical-infrastructure-via-vmware-attacks

56. Agentic AI: Pathway to autonomous network level 5 - Ericsson, accessed July 29, 2025, https://www.ericsson.com/en/blog/2025/7/agentic-ai-pathway-to-autonomous-network-level-5

57. (PDF) Security Orchestration in 5G and Beyond Smart Network ..., accessed July 29, 2025, https://www.researchgate.net/publication/390983334_Security_Orchestration_in_5G_and_Beyond_Smart_Network_Technologies

58. Towards Clean-Label Backdoor Attacks in the Physical World - arXiv, accessed July 29, 2025, https://arxiv.org/html/2407.19203v3

59. Exploiting Trust in Open-Source AI: The Hidden Supply Chain Risk ..., accessed July 29, 2025, https://www.trendmicro.com/vinfo/se/security/news/cybercrime-and-digital-threats/exploiting-trust-in-open-source-ai-the-hidden-supply-chain-risk-no-one-is-watching

60. Transferable Clean-Label Poisoning Attacks on Deep Neural Nets - Proceedings of Machine Learning Research, accessed July 29, 2025, http://proceedings.mlr.press/v97/zhu19a/zhu19a.pdf

61. Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks - AMiner, accessed July 29, 2025, https://static.aminer.cn/misc/pdf/NIPS/2018/5aed14d117c44a44381589d6.pdf

62. (PDF) Survey on Backdoor Attacks on Deep Learning: Current Trends, Categorization, Applications, Research Challenges, and Future Prospects - ResearchGate, accessed July 29, 2025, https://www.researchgate.net/publication/391923375_Survey_on_Backdoor_Attacks_on_Deep_Learning_Current_Trends_Categorization_Applications_Research_Challenges_and_Future_Prospects

63. Backdoor Learning: A Survey - PubMed, accessed July 29, 2025, https://pubmed.ncbi.nlm.nih.gov/35731760/

64. What Is Adversarial AI in Machine Learning? - Palo Alto Networks, accessed July 29, 2025, https://www.paloaltonetworks.com/cyberpedia/what-are-adversarial-attacks-on-AI-Machine-Learning

65. Adversarial Attacks: The Hidden Risk in AI Security - Securing.AI, accessed July 29, 2025, https://securing.ai/ai-security/adversarial-attacks-ai/

66. Adversarial Machine Learning for 5G Communications Security | Request PDF, accessed July 29, 2025, https://www.researchgate.net/publication/354540692_Adversarial_Machine_Learning_for_5G_Communications_Security

67. Examining Machine Learning for 5G and Beyond through an Adversarial Lens - Edinburgh Research Explorer, accessed July 29, 2025, https://www.research.ed.ac.uk/files/188895491/Examining_Machine_Learning_USAMA_DOA29122020_AFV.pdf

68. GenDRA: Generative Data Reconstruction Attacks on Federated ..., accessed July 29, 2025, https://www.mdpi.com/2079-9292/14/11/2263

69. Model Inversion: The Essential Guide | Nightfall AI Security 101, accessed July 29, 2025, https://www.nightfall.ai/ai-security-101/model-inversion

70. Akamai Firewall for AI: Get Powerful Protection for New LLM App ..., accessed July 29, 2025, https://www.akamai.com/blog/security/protect-against-llm-attacks-with-akamai-firewall-for-ai

71. Peer Review & Conference Management System - IEEE-CSR, accessed July 29, 2025, https://www.ieee-csr.org/registration/modules/request.php?module=program&action=summary.php&id=512777154

72. polvalls9/Transfer-Learning-Based-Intrusion-Detection-in ... - GitHub, accessed July 29, 2025, https://github.com/polvalls9/Transfer-Learning-Based-Intrusion-Detection-in-5G-and-IoT-Networks

73. AI-Powered Threat Hunting | How Artificial Intelligence Detects and ..., accessed July 29, 2025, https://www.webasha.com/blog/ai-powered-threat-hunting-how-artificial-intelligence-detects-and-prevents-cyber-threats

74. Automated Threat Hunting | AI Powered Cybersecurity - Seceon Inc, accessed July 29, 2025, https://seceon.com/automated-threat-hunting/

75. As hackers evolve, so does our defense: Securing 5G with AI - Nokia, accessed July 29, 2025, https://www.nokia.com/blog/as-hackers-evolve-so-does-our-defense-securing-5g-with-ai/

76. www.nokia.com, accessed July 29, 2025, https://www.nokia.com/blog/as-hackers-evolve-so-does-our-defense-securing-5g-with-ai/#:~:text=AI%20tools%20like%20the%20Hunt,use%20cases%20for%20human%20review.

77. AI-Driven Anomaly Detection for Securing IoT Devices in 5G-Enabled Smart Cities - MDPI, accessed July 29, 2025, https://www.mdpi.com/2079-9292/14/12/2492

78. AI Driven Anomaly Detection in Network Traffic Using Hybrid CNN-GAN - JAIT, accessed July 29, 2025, https://www.jait.us/articles/2024/JAIT-V15N7-886.pdf

79. Cortex XDR for Network Traffic Analysis - Palo Alto Networks, accessed July 29, 2025, https://

www.paloaltonetworks.com/resources/datasheets/cortex-xdr-for-network-traffic-analysis

80. 5G Security - Palo Alto Networks, accessed July 29, 2025, https://www.paloaltonetworks.com/network-security/5g-security

81. Information Security Policy Enforcement AI Agents - Akira AI, accessed July 29, 2025, https://www.akira.ai/ai-agents/policy-enforcement-agent

82. Enhancing Security in 5G and Future 6G Networks: Machine Learning Approaches for Adaptive Intrusion Detection and Prevention - MDPI, accessed July 29, 2025, https://www.mdpi.com/1999-5903/17/7/312

83. Adaptive Security Policy Management in Cloud Environments ... - arXiv, accessed July 29, 2025, https://arxiv.org/abs/2505.08837

84. Zero Trust Architecture enabled by 3GPP security - Ericsson, accessed July 29, 2025, https://www.ericsson.com/en/blog/2025/2/zero-trust-architecture-enabled-by-3gpp-security

85. What is Zero Trust Architecture? - Palo Alto Networks, accessed July 29, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

86. 5G Security - NCTI, accessed July 29, 2025, https://ncti.com/5g-security/

87. Carnegie Mellon Researchers Show How AI Can Autonomously Hack Enterprise Networks, accessed July 2

88. 9, 2025, https://www.hstoday.us/subject-matter-areas/cybersecurity/carnegie-mellon-researchers-show-how-ai-can-autonomously-hack-enterprise-networks/

89. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence - Biden White House Archives, accessed July 29, 2025, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

90. 5G network AI models: Threats and Mitigations - Check Point Blog, accessed July 29, 2025, https://blog.checkpoint.com/artificial-intelligence/5g-network-ai-models-threats-and-mitigations/

91. Securing 5G Private Networks: The Opportunities and Risks of AI - CTOne, accessed July 29, 2025, https://ctone.com/2025/05/securing-5g-private-networks-the-opportunities-and-risks-of-ai/