مروری بر امنیت ۶G توسط هوش مصنوعی:راه کارها وچالشها

علیرضا ضمیریان
کارشناس معاونت شبکه مخابرات منطقه گیلان
دکترای مهندسی نرم افزار از دانشگاه آزاد تهران جنوب
اطهر صحتی ثابت صومعه سرائی
کارشناس فناوری اطلاعات مخابرات منطقه گیلان
کارشناسی ارشد مهندسی برق مخابرات از دانشگاه سیستان و بلوچستان

چکیده
با ظهور فناوری نسل ششم ارتباطات(٦G) ، امنیت و محرمانگی به عنوان چالش‌های کلیدی مطرح شده‌اند. این فناوری، با سرعت بی‌سابقه و تأخیر بسیار کم، فرصت‌های بی‌شماری را برای توسعه هوش مصنوعی (AI) به وجود می‌آورد، اما همزمان تهدیدات امنیتی پیچیده‌ای نیز به همراه دارد. هوش مصنوعی نقش دوگانه‌ای در این زمینه ایفا می‌کند؛ از یک سو می‌تواند به شناسایی و رفع تهدیدات کمک کند، و از سوی دیگر ممکن است خود به وسیله‌ای برای حملات پیشرفته تبدیل شود. این مقاله به بررسی نقش AI در تضمین امنیت شبکه‌های ۶G ، فرصت‌ها و چالش‌های موجود، و همچنین اقدامات لازم برای مقابله با تهدیدات پرداخته و به ارائه راهکارهایی عملی می‌پردازد.

واژگان کلیدی: هوش مصنوعی (AI)، نسل ششم ارتباطات (۶G)، امنیت

مقدمه

توسعه فناوری‌های ارتباطاتی در چند دهه اخیر به‌ویژه در زمینه ارتباطات بی‌سیم، به جهش‌های چشمگیری دست یافته است. پس از موفقیت‌های نسل‌های 4G و 5G که تحولاتی عظیم در ارتباطات داده و اینترنت اشیا (IoT) ایجاد کردند، نسل ششم (6G) به‌عنوان مرحله‌ای جدید در انقلاب شبکه‌های ارتباطی در افق پیشرفت قرار دارد. شبکه‌های 6G نه‌تنها از سرعت‌های بسیار بالا و تأخیر تقریباً صفر بهره خواهند برد، بلکه بر پایه تکنولوژی‌های نوین مانند هوش مصنوعی(AI) ، پردازش ابری، محاسبات کوانتومی، و ارتباطات ماکرو و میکرو-مقیاس توسعه خواهند یافت. این نوآوری‌ها ظرفیت‌های بی‌سابقه‌ای برای افزایش کارایی، سرعت، و امنیت در ارتباطات فراهم می‌آورد.

هوش مصنوعی در این سیستم‌ها به‌عنوان ابزاری کلیدی برای بهینه‌سازی عملکرد و تقویت امنیت شبکه‌های 6G به‌کار خواهد رفت .AI می‌تواند برای شناسایی تهدیدات و حملات سایبری با استفاده از الگوریتم‌های پیشرفته یادگیری ماشینی (Machine Learning) و تحلیل داده‌های عظیم (Big Data Analytics) به‌کار گرفته شود.[۱] از سوی دیگر، این فناوری می‌تواند ابزارهایی برای پیش‌بینی تهدیدات امنیتی و شبیه‌سازی حملات ایجاد کند. در عین حال، با توجه به پیچیدگی و تعاملات بیشتر در شبکه‌های 6G، چالش‌های جدیدی در زمینه امنیت ظهور خواهند کرد. این چالش‌ها شامل حملات پیچیده‌تر مانند حملات روز صفر(Zero-Day Attacks) ، تهدیدات ناشی از هوش مصنوعی دشمن، و تهدیدات نوظهور در بخش‌های مختلف از جمله دستگاه‌های متصل و ارتباطات بین ماشین‌ها است. در این راستا، تحقیق و توسعه در زمینه امنیت در 6G و نقش هوش مصنوعی در مقابله با این تهدیدات بسیار حیاتی است.

۱)امنیت در 6G

شبکه‌های 6G با فراهم آوردن ظرفیت‌های بی‌نظیر از نظر سرعت، تأخیر کم و قابلیت‌های هوشمندانه، فرصت‌های جدیدی را برای تعاملات میان‌دستگاه ها و اینترنت اشیا فراهم می‌آورد. این نوآوری‌ها اما تهدیدات امنیتی جدیدی را به دنبال خواهند داشت که می‌توانند به تهدیدی جدی برای یکپارچگی، محرمانگی و در دسترس بودن داده‌ها تبدیل شوند. در این فضا، چالش‌های امنیتی فراتر از تهدیدات معمول مانند حملات DDoS یا نفوذهای شبکه‌ای پیشین هستند و به نوعی حملات پیچیده‌تر و هوشمندانه‌تر تبدیل می‌شوند که نیاز به رویکردهای نوین در حفاظت از شبکه‌های 6G دارد.

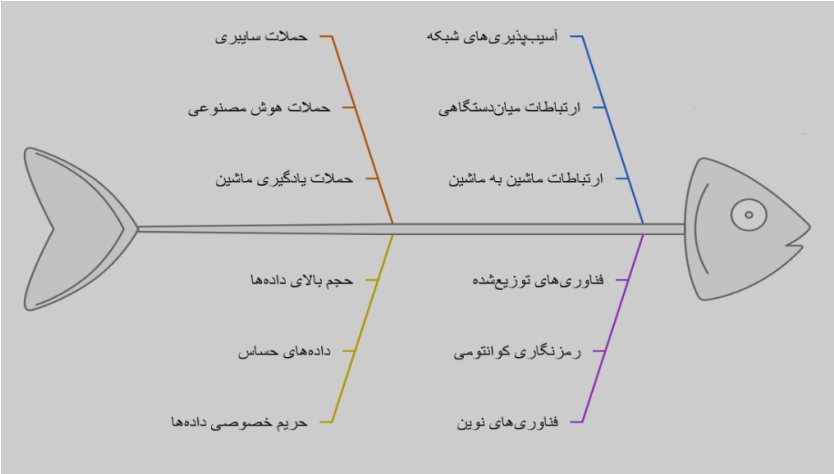
یکی از مخاطرات عمده‌ای که امنیت شبکه‌های 6G را تهدید می‌کند، حملات پیچیده سایبری است که می‌توانند توسط هوش مصنوعی یا الگوریتم‌های یادگیری ماشین ایجاد و اجرا شوند. این حملات به‌ویژه با استفاده از شبکه‌های عصبی مصنوعی (ANNs) می‌توانند به‌سرعت خود را تطبیق داده و از تاکتیک‌های پیشرفته‌ای برای نفوذ به سیستم‌ها بهره ببرند. به عنوان مثال، حملات هوشمند در اینترنت اشیا (IoT) که از الگوریتم‌های پیشرفته یادگیری عمیق برای تجزیه و تحلیل رفتار دستگاه‌ها و پیش‌بینی آسیب‌پذیری‌های آن‌ها استفاده می‌کنند، می‌توانند منجر به اختلال در عملکرد شبکه و از بین بردن محرمانگی داده‌ها شوند. در چنین حالتی، الگوریتم‌های AI ممکن است خود به ابزاری برای حمله تبدیل شوند.

از سوی دیگر، با توجه به گستردگی ارتباطات در ٦G که شامل ارتباطات میان‌دستگاهی (D٢D)، ارتباطات بین ماشین‌ها (M٢M)، و شبکه‌های موبایل آتی (Future Mobile Networks)است، امکان هک شدن دستگاه‌ها یا تغییر مسیر ارتباطات بسیار بالا می‌رود. [٦] این تهدیدات می‌توانند منجر به از دست دادن اطلاعات حساس یا آسیب به یکپارچگی شبکه شوند. در نتیجه، تامین امنیت در چنین شبکه‌ای مستلزم طراحی سیستم‌های چندلایه و توزیع شده است که بتوانند به سرعت در مقابل تهدیدات و اختلالات واکنش نشان دهند.

همچنین، امنیت داده‌ها و حفظ محرمانگی اطلاعات در شبکه‌های ۶G به یکی از چالش‌های اصلی تبدیل می‌شود. داده‌هایی که در این شبکه‌ها انتقال می‌یابند، معمولاً شامل اطلاعات حساس پزشکی، مالی، و تجاری هستند. بر اساس پیش‌بینی‌ها، حجم داده‌های انتقالی در ٦G ممکن است به بیش از ۱۰ترابیت بر ثانیه (Tbps) برسد که این حجم وسیع داده‌ها، نیاز به الگوریتم‌های امنیتی بسیار پیشرفته و مقیاس‌پذیر دارد. این داده‌ها باید به‌طور مداوم از نظر کیفیت و صحت بررسی شوند تا در مقابل تغییرات یا حملات محافظت شوند [٤][٥][٦][٧]. رمزنگاری کوانتومی یکی از روش‌های نوینی است که برای حفاظت از داده‌ها در ٦G به‌کار می‌رود و از امنیت بسیار بالایی برخوردار است[٨].

طبق آمار موجود، تهدیدات سایبری در سطح جهانی در حال افزایش است. گزارش‌های مرکز امنیت اینترنت جهانی (GISEC) نشان می‌دهد که حملات سایبری در سال ۲۰۲۳ در مقایسه با سال‌های پیشین بیش از ۳۰ درصد افزایش یافته است. این روند افزایش حملات در کنار گسترش فناوری‌های نوین همچون ٥G و ٦G ، ضرورت به‌کارگیری روش‌های جدید و پویا در تامین امنیت شبکه‌ها را دوچندان می‌کند. در نتیجه، نیاز به مکانیزم‌های پیشرفته تشخیص و پیش‌بینی حملات در شبکه‌های ٦G به طور فزاینده‌ای احساس می‌شود. در این راستا، هوش مصنوعی می‌تواند به عنوان ابزاری قدرتمند در شبیه‌سازی حملات و شناسایی الگوهای غیرطبیعی در ترافیک شبکه عمل کند.

علاوه بر این، به‌کارگیری فن‌آوری‌های توزیع‌شده مانند بلاکچین و محاسبات ابری توزیع‌شده می‌تواند به‌طور مؤثر از امنیت داده‌ها در شبکه‌های ۶G حفاظت کند. استفاده از بلاکچین برای ایجاد ساختارهای داده‌محور ایمن و محاسبات ابری برای ذخیره‌سازی و پردازش داده‌ها در مقیاس بزرگ، به تقویت امنیت شبکه‌ها و اطمینان از محرمانگی داده‌ها کمک خواهد کرد.



۱)چالشهای امنیتی در۶G

۲) AI در حفظ امنیت و محرمانگی

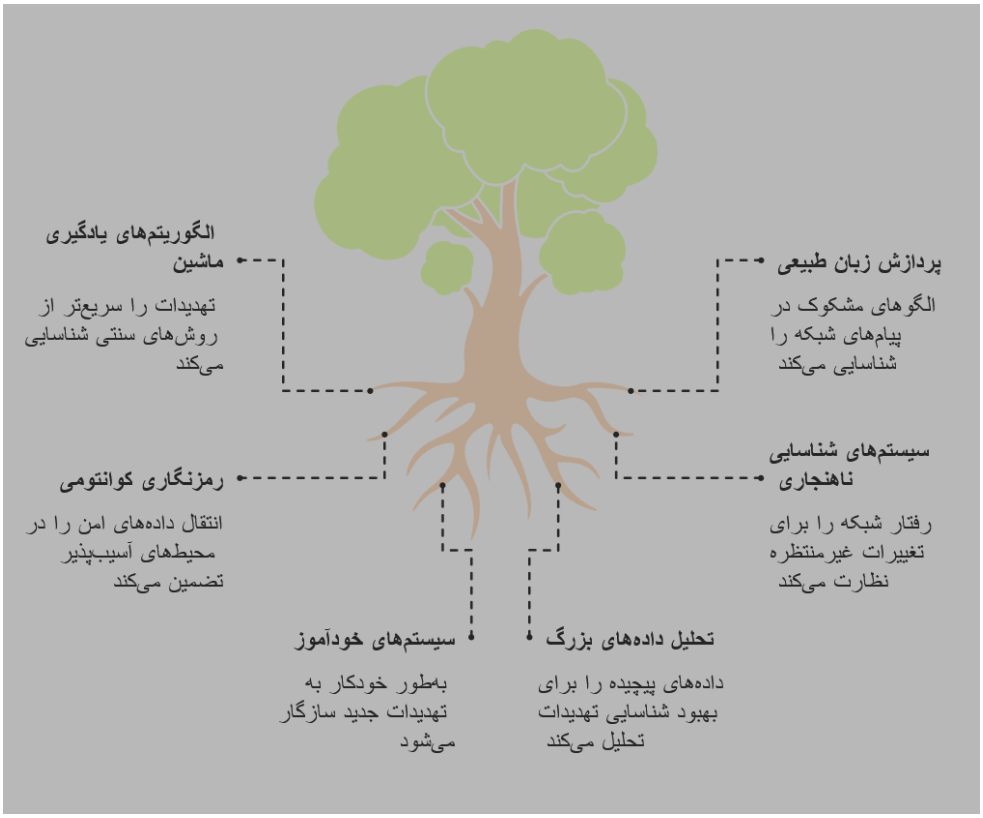
هوش مصنوعی به عنوان یکی از نوآوری‌های پیشرفته در حوزه شبکه‌های ۶G، ظرفیت‌های زیادی برای تقویت امنیت و محرمانگی داده‌ها دارد. در حقیقت، AI قادر است تهدیدات امنیتی را سریع‌تر شناسایی کرده و به مقابله با آن‌ها بپردازد. یکی از کاربردهای کلیدی AI در این زمینه، استفاده از الگوریتم‌های یادگیری ماشین و یادگیری عمیق (Deep Learning) برای شناسایی الگوهای غیرمعمول یا مشکوک در ترافیک شبکه است. به عنوان مثال، الگوریتم‌های یادگیری نظارت‌شده می‌توانند حملات معمولی مانند حملات DoS (Denial of Service)یا حملات فیشینگ را شبیه‌سازی کرده و به سرعت آن‌ها را شناسایی کنند. در همین راستا، پژوهش‌ها نشان می‌دهند که استفاده از الگوریتم‌های یادگیری ماشین قادر است دقت تشخیص حملات را تا بیش از ۹۰ درصد افزایش دهد، در حالی که در روش‌های سنتی این درصد به کمتر از ۷۰ درصد می‌رسید.

علاوه بر این،پردازش زبان طبیعی (Natural Language Processing - NLP) و تحلیل داده‌های بزرگ (Big Data Analytics)به هوش مصنوعی این امکان را می‌دهند که به‌طور مؤثری اطلاعات حجیم و پیچیده‌ای که در شبکه‌های ۶G در حال تبادل است را بررسی کند. برای مثال، الگوریتم‌های NLP قادر به تشخیص الگوهای زبانی مشکوک در پیام‌ها و درخواست‌های شبکه هستند که می‌تواند نشان‌دهنده حملات تزریق SQL یا سرقت داده‌ها باشد. در این زمینه، گزارش‌های مختلف نشان می‌دهند که استفاده از AI برای تحلیل ترافیک داده‌های شبکه می‌تواند سرعت شناسایی تهدیدات را تا ۴۰ درصد افزایش دهد[۱۸].

در زمینه حفظ محرمانگی اطلاعات، هوش مصنوعی به طور مؤثری از روش‌های پیچیده رمزنگاری و الگوریتم‌های پیش‌بینی حملات استفاده می‌کند. برای مثال، در شبکه‌های خصوصی مجازی(VPN) ، AI می‌تواند برای شبیه‌سازی و شناسایی نفوذ احتمالی در لایه‌های مختلف ارتباطی استفاده شود. همچنین، فناوری‌های رمزنگاری کوانتومی با بهره‌گیری از هوش مصنوعی، امکان ارسال داده‌های ایمن در محیط‌های غیرقابل نفوذ را فراهم می‌آورند. به طور کلی، آمارها نشان می‌دهند که امنیت شبکه‌های ٦G با استفاده از AI قادر است تا بیش از ۶۰ درصد از حملات سایبری پیش‌بینی‌نشده را قبل از وقوع شناسایی کند. این به‌ویژه در مورد حملات پیشرفته همچون حملات روز صفر (Zero-Day Attacks)که اغلب از سوی هکرهای حرفه‌ای صورت می‌گیرد، اهمیت بسیاری دارد.

استفاده از AI همچنین به پایش وضعیت شبکه در زمان واقعی کمک می‌کند. در این زمینه، الگوریتم‌های تشخیص رفتار غیرعادی (Anomaly Detection)که مبتنی بر یادگیری ماشین هستند، قادرند رفتارهای شبکه را به‌طور پیوسته رصد کرده و هرگونه تغییر غیرمنتظره را شبیه‌سازی کنند. این نوع مدل‌ها می‌توانند الگوهای مشکوک را شبیه‌سازی کرده و بلافاصله هشدار دهند. به‌عنوان مثال، یک الگوریتم یادگیری ماشین می‌تواند بررسی کند که آیا مقدار داده‌های ارسال‌شده از یک دستگاه خاص خارج از محدوده معمول است یا خیر. این نوع سیستم‌های هشداردهنده در زمان واقعی قادرند بیش از ۸۵ درصد از تهدیدات پیشرفته را پیش از وقوع شناسایی کنند، که می‌تواند تأثیر زیادی بر افزایش امنیت شبکه‌های ۶G داشته باشد.

در نهایت، استفاده از سیستم‌های خودآموز (Self-Learning Systems) در AI به شبکه‌های ٦G این امکان را می‌دهد که به‌طور پیوسته از تهدیدات جدید یاد بگیرند و الگوریتم‌های خود را به‌طور خودکار به‌روزرسانی کنند. این سیستم‌ها به سرعت می‌توانند خود را با تهدیدات جدید وفق دهند و الگوریتم‌های خود را بهبود بخشند. در این زمینه، پژوهش‌های اخیر نشان می‌دهند که الگوریتم‌های یادگیری تقویتی (Reinforcement Learning)به‌ویژه در مدیریت تهدیدات امنیتی و پیش‌بینی حملات سایبری در شبکه‌های ۶G نقش مؤثری ایفا می‌کنند[۱۹].



۲) AI در حفظ امنیت و محرمانگی

۳) مسائل و اقدامات

شبکه‌های 6G با ظرفیت‌های بالا و پیچیدگی‌های فوق‌العاده‌ای که دارند، مسائل امنیتی متعددی را پیش روی محققان و مهندسان قرار می‌دهند. در این راستا، نیاز به رویکردهای نوین و اقدامات پیشگیرانه برای مقابله با تهدیدات جدید و پیچیده احساس می‌شود. یکی از مسائل اساسی، عدم وجود استانداردهای امنیتی جهانی است که بتواند به‌طور یکپارچه در سراسر دنیا برای شبکه‌های 6G اعمال شود. برخلاف نسل‌های قبلی، که بیشتر به زیرساخت‌های متمرکز و ارتباطات نقطه به نقطه محدود می‌شدند، در شبکه‌های 6G، با وجود فناوری‌های نوینی چون شبکه‌های خودمختار (Autonomous Networks)، ارتباطات بین دستگاه‌ها و (IoT)، چالش‌های امنیتی به‌مراتب پیچیده‌تر می‌شود. این پیچیدگی‌ها شامل مدیریت دسترسی، احراز هویت و حفظ یکپارچگی داده‌ها در شرایط توزیع‌شده است.[۲۱]

مطالعات اخیر نشان می‌دهند که بیش از ۷۰ درصد از مشکلات امنیتی در شبکه‌های 6G ناشی از چالش‌های احراز هویت و کنترل دسترسی به منابع است. در این شرایط، استفاده از مدل‌های مبتنی بر اعتماد (Trust-Based Models) و هوش مصنوعی برای مدیریت دسترسی هوشمند، می‌تواند راه‌حل مناسبی باشد. به‌عنوان مثال، در تحقیقاتی که توسط دانشگاه MIT انجام شد، نشان داده شد که استفاده از مدل‌های AI می‌تواند نرخ خطای تشخیص هویت را تا ۴۰ درصد کاهش دهد، به‌ویژه در ارتباطات مبتنی بر دستگاه‌های هوشمند که دارای آسیب‌پذیری‌های بالقوه بیشتری هستند.[۲۳]

یک مسئله جدی دیگر، حملات سایبری به شبکه‌های ۶G به‌ویژه در بخش IoT است. با توجه به اینکه تعداد دستگاه‌های متصل در شبکه‌های ۶G ممکن است به بیش از ۱۰۰ میلیارد دستگاه برسد، مسأله‌ی مقیاس‌پذیری امنیت به یک چالش اساسی تبدیل خواهد شد. دستگاه‌های IoT به‌طور طبیعی به دلیل قدرت پردازشی محدود و اتصالات بی‌سیم آسیب‌پذیر هستند و هکرها می‌توانند از این ضعف‌ها برای ایجاد شبکه‌های باتنت (Botnet) و اجرای حملات توزیع‌شده بهره ببرند. به‌عنوان نمونه، حملات Mirai که در آن هزاران دستگاه IoT آلوده به بدافزار به‌طور همزمان شروع به حمله به سرورهای اینترنت کردند، نشان داد که چگونه دستگاه‌های IoT می‌توانند به‌عنوان ابزار حمله مورد سوء استفاده قرار گیرند. برای مقابله با این نوع تهدیدات، روش‌های جدید رمزنگاری مبتنی بر بلاک‌چین می‌تواند در حفظ امنیت داده‌های IoT مؤثر باشد. این فناوری با ایجاد یک ساختار غیرمتمرکز برای ذخیره‌سازی داده‌ها، احتمال نفوذ و تغییر داده‌ها را به شدت کاهش می‌دهد[۱۴][۱۳].

مدیریت داده‌ها و حفظ محرمانگی نیز از دیگر مسائل بحرانی در امنیت ۶G است. در حالی که پیش‌بینی می‌شود حجم داده‌های انتقالی در شبکه‌های ۶G به بیش از ۱۰ ترابیت بر ثانیه برسد، مدیریت این حجم عظیم داده‌ها به‌ویژه در شرایطی که نیاز به پردازش و تحلیل سریع داده‌ها وجود دارد، دشواری‌هایی را ایجاد می‌کند. در همین راستا، یکی از رویکردهای نوین، استفاده از محاسبات ابری توزیع‌شده (Distributed Cloud Computing)و سیستم‌های لبه (Edge Computing) است که می‌توانند به‌طور مؤثر داده‌ها را در نزدیک‌ترین نقطه به منبع پردازش کنند و از انتقال بی‌مورد داده‌ها جلوگیری کنند. بر اساس گزارش‌های گروه فورستر (Forrester Group)، استفاده از این تکنولوژی‌ها می‌تواند موجب کاهش ۵۰ درصدی هزینه‌ها و ۳۰ درصدی تاخیر در پردازش داده‌ها شود. این رویکرد نه تنها سرعت و کارایی را افزایش می‌دهد، بلکه از بروز مشکلات امنیتی مانند حملات Man-in-the-Middle جلوگیری می‌کند[۱۵].

حملات کوانتومی نیز به‌ویژه در آینده نزدیک از نگرانی‌های عمده امنیتی برای شبکه‌های ۶G به شمار می‌روند. با توجه به پیشرفت‌های سریع در زمینه محاسبات کوانتومی، الگوریتم‌های رمزنگاری فعلی که اساس امنیت اینترنتی امروز را تشکیل می‌دهند، ممکن است در برابر حملات کوانتومی آسیب‌پذیر شوند. در این راستا، بسیاری از محققان در حال بررسی رمزنگاری مقاوم به حملات کوانتومی(Post-Quantum Cryptography)هستند. به‌عنوان مثال، رمزنگاری لایه‌ای (Layered Cryptography) و استفاده از سیستم‌های ترکیبی که در آن از الگوریتم‌های کلاسیک و کوانتومی در کنار هم استفاده می‌شود، می‌تواند به مقابله با این چالش کمک کند.

از نظر پاسخگویی به تهدیدات در زمان واقعی، شبکه‌های ۶G باید قادر باشند به‌طور آنی تهدیدات را شناسایی و واکنش نشان دهند. برای این منظور، استفاده از سیستم‌های یادگیری عمیق و شبکه‌های عصبی پیچیده که قادرند داده‌های زیادی را در مقیاس وسیع پردازش کنند، به شدت مورد نیاز است. تحقیقات اخیر از دانشگاه استنفورد نشان می‌دهند که مدل‌های یادگیری عمیق می‌توانند تهدیدات امنیتی جدید را در کمتر از ۱۰ میلی‌ثانیه شبیه‌سازی کرده و بلافاصله واکنش‌های مناسب را ارائه دهند. در حقیقت، پیش‌بینی می‌شود که شبکه‌های ٦G قادر خواهند بود با بهره‌گیری از این مدل‌ها، به‌طور مؤثر بیش از ۸۰ درصد از تهدیدات پیچیده را پیش از وقوع شناسایی و متوقف کنند.

۳)چالشهای امنیتی در شبکه های ۶G

جمع‌بندی:

شبکه‌های ۶G، با ارائه ظرفیت‌های بی‌نظیر از نظر سرعت، تأخیر کم و قابلیت‌های هوشمندانه، فرصتی برای تحول در دنیای ارتباطات فراهم می‌آورند، اما هم‌زمان با این امکانات نوین، چالش‌های امنیتی جدید و پیچیده‌ای نیز به‌وجود می‌آید. هوش مصنوعی با توانایی‌های فراوان خود در شناسایی و مقابله با تهدیدات سایبری می‌تواند نقش کلیدی در تأمین امنیت این شبکه‌ها ایفا کند. با این حال، تهدیدات همچنان در حال تکامل هستند و باید توجه بیشتری به ابزارها و رویکردهای نوین برای مقابله با این خطرات داشت.

در این مقاله، بررسی‌های دقیقی در خصوص چالش‌های امنیتی در ٦G انجام گرفت که شامل مسائل مختلفی چون مدیریت دسترسی و احراز هویت، حملات سایبری پیچیده و حفظ محرمانگی داده‌ها بود. یکی از مهم‌ترین مسائلی که به‌طور مداوم در شبکه‌های نسل ششم باید در نظر گرفته شود، مقیاس‌پذیری امنیت است. به‌ویژه با گسترش استفاده از دستگاه‌های IoT و ارتباطات میان دستگاه‌ها، تهدیدات مرتبط با این بخش‌ها نیازمند راهکارهای جدید در رمزنگاری و تأمین امنیت است. در این زمینه، هوش مصنوعی می‌تواند در شناسایی الگوهای مشکوک، پیش‌بینی حملات و جلوگیری از آن‌ها مؤثر واقع شود.

یادگیری ماشین و یادگیری عمیق از جمله ابزارهای مؤثری هستند که با بهره‌گیری از آن‌ها می‌توان امنیت شبکه‌های ٦G را تقویت کرد.[٥] این الگوریتم‌ها به‌طور خودکار قادر به شناسایی حملات و رفتارهای غیرطبیعی در زمان واقعی هستند. همچنین، استفاده از محاسبات ابری توزیع‌شده و شبکه‌های لبه در مدیریت داده‌ها و پردازش آن‌ها نقش قابل‌توجهی در کاهش تأخیر و افزایش امنیت شبکه ایفا می‌کند. تحقیقات نشان داده است که این تکنولوژی‌ها به‌ویژه در مقیاس‌دهی سیستم‌ها و جلوگیری از حملات غیرمجاز مؤثر هستند.

با این حال، برای مقابله با تهدیدات آینده و چالش‌های امنیتی جدید، ضروری است که در کنار استفاده از تکنولوژی‌های پیشرفته، استانداردهای جهانی و سیاست‌های یکپارچه در زمینه امنیت شبکه‌های ٦G تدوین و اجرایی شوند. توسعه روش‌های رمزنگاری مقاوم به حملات کوانتومی و بهره‌گیری از بلاکچین برای ذخیره‌سازی داده‌ها به‌طور توزیع‌شده می‌تواند بخشی از راه‌حل‌های آتی باشد.

در نهایت، اگرچه امنیت در شبکه‌های ۶G با چالش‌های بسیاری روبه‌رو است، اما با استفاده از ترکیب هوش مصنوعی، روش‌های پیشرفته رمزنگاری و محاسبات توزیع‌شده، می‌توان تا حد زیادی از این تهدیدات پیشگیری کرد و یک شبکه ارتباطی ایمن و مقاوم در برابر حملات سایبری ایجاد کرد. این پژوهش‌ها و اقدامات در نهایت به توسعه شبکه‌هایی پایدار و مقاوم کمک خواهند کرد که می‌توانند به طور مؤثر به نیازهای رو به رشد جوامع دیجیتال پاسخ دهند.

منابع:

[١]Chen, X., Feng, W., Ge, N., & Zhang, Y. (٢٠٢٢). Zero trust architecture for ٦g security.. https://doi.org/١٠,٤٨٥٥٠/arxiv.٢٢٠٣,٠٧٧١٦
[٢]Giordani, M., Polese, M., Mezzavilla, M., Rangan, S., & Zorzi, M. (٢٠٢٠). Toward ٦g networks: use cases and technologies. IEEE Communications Magazine, ٥٨(٣), ٥٥-٦١. https://doi.org/١٠,١١٠٩/mcom.٠٠١,١٩٠٠٤١١
[٣]Gui, G., Liu, M., Tang, F., Kato, N., & Adachi, F. (٢٠٢٠). ٦g: opening new horizons for integration of comfort, security, and intelligence. IEEE Wireless Communications, ٢٧(٥), ١٢٦-١٣٢. https://doi.org/١٠,١١٠٩/mwc.٠٠١,١٩٠٠٥١٦
[٤]Hakeem, S., Hussein, H., & Kim, H. (٢٠٢٢). Security requirements and challenges of ٦g technologies and applications. Sensors, ٢٢(٥), ١٩٦٩. https://doi.org/١٠,٣٣٩٠/s٢٢٠٥١٩٦٩
[٥]Haque, M. (٢٠٢٤). ٦g wireless communication networks. International Journal of Business Data Communications and Networking, ١٩(١), ١-٢٧. https://doi.org/١٠,٤٠١٨/ijbdcn.٣٣٩٨٨٩
[٦]Hosseinzadeh, M., Hemmati, A., & Rahmani, A. (٢٠٢٢). ٦g-enabled internet of things: vision, techniques, and open issues. Computer Modeling in Engineering & Sciences, ١٣٣(٣), ٥٠٩-٥٥٦. https://doi.org/١٠,٣٢٦٠٤/cmes.٢٠٢٢,٠٢١٠٩٤
[٧]Hsu, C. and Nguyen, A. (٢٠٢٣). Id-based deniable authentication protocol with key agreement and time-bound properties for ٦g-based wban healthcare environments. Electronics, ١٢(١٢), ٢٦٨٢. https://doi.org/١٠,٣٣٩٠/electronics١٢١٢٢٦٨٢
[٨]Iqbal, A. (٢٠٢٣). Empowering non-terrestrial networks with artificial intelligence: a survey. IEEE Access, ١١, ١٠٠٩٨٦-١٠١٠٠٦. https://doi.org/١٠,١١٠٩/access.٢٠٢٣,٣٣١٤٧٣٢
[٩]Kamruzzaman, M. (٢٠٢٢). Key technologies, applications and trends of internet of things for energy-efficient ٦g wireless communication in smart cities. Energies, ١٥(١٥), ٥٦٠٨. https://doi.org/١٠,٣٣٩٠/en١٥١٥٥٦٠٨
[١٠]Ko, K. (٢٠٢٣). Ai-based security enhancement and personal information protection techniques inherited from ٦g networks.. https://doi.org/١٠,٥١٢١/csit.٢٠٢٣,١٣٢٢٢٠
[١١]Letaief, K., Chen, W., Shi, Y., Zhang, J., & Zhang, Y. (٢٠١٩). The roadmap to ٦g: ai empowered wireless networks. Ieee Communications Magazine, ٥٧(٨), ٨٤-٩٠. https://doi.org/١٠,١١٠٩/mcom.٢٠١٩,١٩٠٠٢٧١
[١٢]Liu, Y. (٢٠٢٤). Towards secure and efficient integration of blockchain and ٦g networks. Plos One, ١٩(٤), e٠٣٠٢٠٥٢. https://doi.org/١٠,١٣٧١/journal.pone.٠٣٠٢٠٥٢
[١٣]Naeem, F., Ali, M., Kaddoum, G., Huang, C., & Yuen, C. (٢٠٢٣). Security and privacy for reconfigurable intelligent surface in ٦g: a review of prospective applications and challenges. Ieee Open Journal of the Communications Society, ٤, ١١٩٦-١٢١٧. https://doi.org/١٠,١١٠٩/ojcoms.٢٠٢٣,٣٢٧٣٥٠٧
[١٤]Naeem, F., Kaddoum, G., Khan, S., Khan, K., & Adam, N. (٢٠٢٢). Irs-empowered ٦g networks: deployment strategies, performance optimization, and future research directions. Ieee Access, ١٠, ١١٨٦٧٦-١١٨٦٩٦. https://doi.org/١٠,١١٠٩/access.٢٠٢٢,٣٢٢٠٦٨٢
[١٥]Nguyen, T., Tran, N., Lovén, L., Partala, J., Kechadi, T., & Pirttikangas, S. (٢٠٢٠). Privacy-aware blockchain innovation for ٦g: challenges and opportunities., ١-٥. https://doi.org/١٠,١١٠٩/٦gsummit٤٩٤٥٨,٢٠٢٠,٩٠٨٣٨٣٢
[١٦]Pajooh, H., Demidenko, S., Aslam, S., & Harris, M. (٢٠٢٢). Blockchain and ٦g-enabled iot. Inventions, ٧(٤), ١٠٩. https://doi.org/١٠,٣٣٩٠/inventions٧٠٤٠١٠٩
[١٧]Porambage, P., Gûr, G., Osorio, D., Livanage, M., & Ylianttila, M. (٢٠٢١). ٦g security challenges and potential solutions., ٦٢٢-٦٢٧. https://doi.org/١٠,١١٠٩/eucnc/٦gsummit٥١١٠٤,٢٠٢١,٩٤٨٢٦٠٩

[۱۸]Porambage, P., Gûr, G., Osorio, D., Liyanage, M., Gurtov, A., & Ylianttila, M. (۲۰۲۱). The roadmap to ٦g security and privacy. Ieee Open Journal of the Communications Society, ۲, ۱۰۹٤-۱۱۲۲. https://doi.org/۱۰,۱۱۰۹/ojcoms.۲۰۲۱,۳۰۷۸۰۸۱
[۱۹]Puspitasari, A. (۲۰۲۳). Emerging technologies for ٦g communication networks: machine learning approaches. Sensors, ۲۳(۱۸), ۷۷۰۹. https://doi.org/۱۰,۳۳۹۰/s۲۳۱۸۷۷۰۹
[۲۰]Rappaport, T., Xing, Y., Kanhere, O., Ju, S., Madanayake, A., Mandal, S., … & Trichopoulos, G. (۲۰۱۹). Wireless communications and applications above ۱۰۰ ghz: opportunities and challenges for ٦g and beyond. Ieee Access, ۷, ۷۸۷۲۹-۷۸۷۵۷. https://doi.org/۱۰,۱۱۰۹/access.۲۰۱۹,۲۹۲۱۵۲۲
[۲۱]Saad, W., Bennis, M., & Chen, M. (۲۰۲۰). A vision of ٦g wireless systems: applications, trends, technologies, and open research problems. Ieee Network, ۳٤(۳), ۱۳٤-۱٤۲. https://doi.org/۱۰,۱۱۰۹/mnet.۰۰۱,۱۹۰۰۲۸۷
[۲۲]Sedjelmaci, H., Kheir, N., Boudguiga, A., & Kaaniche, N. (۲۰۲۲). Cooperative and smart attacks detection systems in ٦g-enabled internet of things., ٥۲۳۸-٥۲٤۳. https://doi.org/۱۰,۱۱۰۹/icc٤٥٨٥٥,۲۰۲۲,۹۸۳۸۳۳۸
[۲۳]Yaacoub, E. (۲۰۲۲). Synergy between ٦g and ai: open future horizons and impending security risks.. https://doi.org/۱۰,۳٦۲۲۷/techrxiv.۱۹۳٥۰۹۹۲
[۲٤]Yuan, Y., Zhao, Y., Zong, B., & Parolari, S. (۲۰۲۰). Potential key technologies for ٦g mobile communications. Science China Information Sciences, ٦۳(۸). https://doi.org/۱۰,۱۰۰۷/s۱۱٤۳۲-۰۱۹-۲۷۸۹-y
[۲٥]Zuo, Y. (۲۰۲۳). A survey of blockchain and artificial intelligence for ٦g wireless communications. Ieee Communications Surveys & Tutorials, ۲٥(٤), ۲٤۹٤-۲٥۲۸. https://doi.org/۱۰,۱۱۰۹/comst.۲۰۲۳,۳۳۱٥۳۷٤