گاهنامه انجمن علمی شبکه هوشمند انرژی ایران

شماره ۰۸- تیرماه ۱۴۰۲

آنچه در این شماره می خوانیم:

گاهنامه انجمن شبکه هوشمند انرژی ایران

انجمن علمی شبکه هوشمند انرژی ایران

شماره ۰۸-تیرماه ۱۴۰۲

صاحب امتیاز: انجمن شبکه هوشمند انرژی ایران

مدیر مسئول: دکتر مسعود رشیدی نژاد

تیم اجرایی نشریه: سیده سودابه زادسر

مفهوم امنیت سایبری در شبکه‌های هوشمند

شبکه‌های هوشمند برق، با بهره‌گیری از فناوری‌های نوین و دیجیتال، توانایی مدیریت هوشمند و کارآمدتر انرژی را دارند و در عین حال می‌توانند به توزیع انرژی پاک و پایدار کمک کنند. این شبکه‌ها از تجهیزات دیجیتال، ارتباطات پیشرفته، و دستگاه‌های اینترنت اشیا (IoT) برای بهینه‌سازی مصرف و توزیع انرژی بهره می‌برند. با این حال، این پیشرفت‌ها چالش‌های جدیدی نیز به همراه دارند، و امنیت سایبری یکی از بزرگ‌ترین نگرانی‌های این شبکه‌ها به شمار می‌رود. از آنجا که شبکه‌های هوشمند داده‌های حساس و ارتباطات حیاتی را مدیریت می‌کنند، حفظ امنیت سایبری آنها از اهمیت بالایی برخوردار است.

امنیت سایبری در شبکه‌های هوشمند، به مجموعه‌ای از تکنیک‌ها، پروتکل‌ها، و راهبردهایی اشاره دارد که هدف آن‌ها حفاظت از داده‌ها، تجهیزات، و ارتباطات در برابر نفوذ و حملات سایبری است. این امنیت در شبکه‌های هوشمند شامل سه عنصر اصلی است که هر یک به شکلی در محافظت از زیرساخت‌های حیاتی و حفظ پایداری سیستم نقش دارند. امنیت سایبری در شبکه‌های هوشمند شامل سه عنصر اصلی است:

۱) **محرمانگی (Confidentiality)**: حفظ محرمانگی داده‌ها به معنای جلوگیری از دسترسی‌های غیرمجاز به اطلاعات حساس است. در شبکه‌های هوشمند، داده‌ها شامل اطلاعات مصرف انرژی کاربران، وضعیت تجهیزات، و داده‌های کنترلی می‌شوند که دسترسی غیرمجاز به آن‌ها می‌تواند پیامدهای خطرناکی داشته باشد. برای مثال، اگر مهاجمان به اطلاعات مصرف خانگی یا صنعتی دست یابند، می‌توانند از این اطلاعات برای اهداف مخرب یا دسترسی به بخش‌های دیگر شبکه استفاده کنند. بنابراین، استفاده از رمزنگاری قوی و روش‌های مدیریت دسترسی، برای حفاظت از محرمانگی داده‌ها ضروری است.

۲) **یکپارچگی (Integrity)**: تضمین یکپارچگی داده‌ها به این معناست که داده‌ها و سیگنال‌ها در طول انتقال، دستکاری یا تغییر نمی‌کنند. در شبکه‌های هوشمند، تغییرات غیرمجاز در داده‌ها می‌تواند به اختلال در عملکرد سیستم و تصمیم‌گیری‌های اشتباه منجر شود. برای مثال، دستکاری داده‌های کنتورهای هوشمند یا تغییر داده‌های مربوط به بار شبکه می‌تواند به توزیع نادرست برق و حتی خرابی گسترده منجر شود. استفاده از پروتکل‌های یکپارچگی داده‌ها و امضای دیجیتال، راهکارهایی هستند که در حفظ یکپارچگی اطلاعات به کار می‌روند.

۳) **دسترس‌پذیری (Availability)**: دسترس‌پذیری به معنای حفظ عملکرد مداوم و پایدار شبکه برای ارائه خدمات به کاربران در هر زمان است. شبکه‌های هوشمند نیاز به پاسخگویی سریع و پایدار دارند و هر گونه اختلال یا حمله‌ای که دسترس‌پذیری سیستم را تهدید کند، می‌تواند منجر به وقفه در توزیع برق یا حتی خاموشی‌های گسترده شود. حملات محروم‌سازی از سرویس (DoS) و محروم‌سازی توزیع‌شده از سرویس (DDoS) از جمله تهدیداتی هستند که می‌توانند دسترس‌پذیری را مختل کنند. بنابراین، شبکه‌های هوشمند باید از سیستم‌های قوی نظارت و محافظت در برابر این نوع حملات برخوردار باشند.

تهدیدات اصلی امنیت سایبری در شبکه‌های هوشمند

شبکه‌های هوشمند با تهدیدات سایبری متنوعی مواجه هستند که می‌تواند عملکرد و پایداری این سیستم‌ها را به خطر بیندازد:

حملات بدافزار (Malware Attacks): بدافزارها از طریق نفوذ به سیستم‌های شبکه، دسترسی مهاجمان به اطلاعات حساس و کنترل تجهیزات را ممکن می‌سازند. این حملات می‌توانند منجر به خرابی تجهیزات، دستکاری داده‌ها، یا حتی از کار افتادن کل سیستم شوند.

حملات محروم‌سازی از سرویس (DoS/DDoS): حملات DoS و DDoS با ایجاد ترافیک کاذب و سنگین، منابع سیستم را مصرف کرده و باعث از کار افتادن سرویس‌های شبکه می‌شوند. در شبکه‌های هوشمند، چنین حملاتی می‌توانند به قطع خدمات و توقف توزیع برق در یک منطقه منجر شوند.

حملات فیشینگ و مهندسی اجتماعی: مهاجمان از روش‌های فریبکارانه‌ای مانند ایمیل‌های فیشینگ برای دسترسی به اطلاعات حساس استفاده می‌کنند. در شبکه‌های هوشمند، چنین حملاتی می‌تواند دسترسی مهاجمان به سامانه‌های مدیریتی یا تجهیزات حیاتی را فراهم کند.

حملات مرد میانی (MITM): حملات مرد میانی به مهاجمان اجازه می‌دهد که داده‌های در حال تبادل بین دستگاه‌ها را رهگیری یا تغییر دهند. این نوع حملات می‌تواند به دستکاری داده‌های مصرف و مختل کردن تصمیمات کنترلی منجر شود.

چالش‌های امنیتی شبکه‌های هوشمند

در شبکه‌های هوشمند، امنیت سایبری با چالش‌های متعددی مواجه است که برخی از آنها به دلیل ویژگی‌های زیرساختی و پیچیدگی‌های فنی به وجود آمده‌اند. بنابراین چهار چالش اصلی که شبکه‌های هوشمند را در برابر تهدیدات سایبری آسیب‌پذیرتر می‌کند، به صورت زیر بیان می شود:

زیرساخت‌های قدیمی: بسیاری از شبکه‌های برق، همچنان از زیرساخت‌های قدیمی و فناوری‌های سنتی استفاده می‌کنند که برای مقابله با تهدیدات سایبری پیشرفته طراحی نشده‌اند. این زیرساخت‌ها به دلیل عدم تطبیق با فناوری‌های جدیدتر، قادر به ارائه دفاع‌های قوی در برابر حملات پیچیده نیستند. به عنوان مثال، سیستم‌های کنترلی که سال‌ها پیش توسعه یافته‌اند، ممکن است فاقد ویژگی‌های رمزنگاری و احراز هویت باشند و این موضوع باعث می‌شود مهاجمان بتوانند به راحتی به آن‌ها نفوذ کنند یا از داده‌های آن‌ها سوءاستفاده کنند. بنابراین، نوسازی زیرساخت‌ها و همگام‌سازی آن‌ها با فناوری‌های مدرن یکی از چالش‌های اساسی است که باید برای ارتقاء امنیت سایبری شبکه‌های هوشمند به آن پرداخته شود.

ارتباطات پیچیده: شبکه‌های هوشمند از پروتکل‌ها و استانداردهای مختلفی برای ارتباطات بین دستگاه‌ها و سیستم‌های مختلف استفاده می‌کنند. این ارتباطات ممکن است شامل پروتکل‌های ارتباطی بی‌سیم، پروتکل‌های محلی و پروتکل‌های استاندارد صنعتی باشند. با این حال، هماهنگ‌سازی بین این پروتکل‌ها دشوار است و هر کدام ممکن است به نوعی دچار ضعف‌های امنیتی باشند. به عنوان مثال، پروتکل‌های قدیمی‌تر ممکن است از رمزنگاری قوی پشتیبانی نکنند و در مقابل تهدیدات جدید آسیب‌پذیر باشند. عدم هماهنگی میان این پروتکل‌ها و سازگاری نداشتن دستگاه‌ها با استانداردهای امنیتی واحد، موجب می‌شود که شبکه نقاط ضعفی برای نفوذ مهاجمان

ایجاد کند. ایجاد استانداردهای جامع و سازگاری پروتکل‌ها با یکدیگر یکی از نیازهای اساسی برای کاهش این نقاط ضعف امنیتی است.

گستردگی دستگاه‌های IoT : استفاده گسترده از دستگاه‌های اینترنت اشیا (IoT) در شبکه‌های هوشمند، باعث افزایش چشمگیر تعداد نقاط ورودی شبکه می‌شود. این دستگاه‌ها به دلیل اتصال دائمی به شبکه، به هدفی برای مهاجمان سایبری تبدیل شده‌اند. با افزایش دستگاه‌های IoT مانند کنتورهای هوشمند، حسگرها، و تجهیزات کنترلی، مدیریت امنیت همه دستگاه‌ها چالش‌برانگیزتر می‌شود. علاوه بر این، بسیاری از این دستگاه‌ها دارای پردازنده‌های کم‌مصرف و حافظه محدود هستند، که امکان پیاده‌سازی کامل پروتکل‌های امنیتی را کاهش می‌دهد. این محدودیت‌ها می‌تواند زمینه‌ساز حملات مختلفی مانند دستکاری داده‌ها، حملات منع سرویس و دسترسی غیرمجاز به شبکه شود. بنابراین، اطمینان از امنیت هر یک از دستگاه‌های IoTدر شبکه‌های هوشمند، نیازمند راهکارهای مدیریت متمرکز و نظارت دقیق است.

تاخیر در به‌روزرسانی‌ها: یکی از مسائل اساسی در امنیت شبکه‌های هوشمند، تاخیر در به‌روزرسانی‌ها و پچ‌های امنیتی است. با توجه به گستردگی زیرساخت‌ها و تعداد زیاد دستگاه‌ها و سیستم‌های متصل به شبکه، به‌روزرسانی به موقع و هماهنگ همه تجهیزات کار پیچیده‌ای است. این تاخیر می‌تواند به مهاجمان فرصت دهد تا از آسیب‌پذیری‌های شناخته‌شده سوءاستفاده کنند و به شبکه نفوذ کنند. علاوه بر این، برخی از دستگاه‌های قدیمی یا دستگاه‌هایی که به صورت پراکنده نصب شده‌اند، ممکن است حتی به‌روزرسانی‌های امنیتی را دریافت نکنند، و این موضوع می‌تواند امنیت کلی شبکه را به خطر بیندازد. به همین دلیل، ایجاد فرآیندهای سریع و کارآمد برای به‌روزرسانی و اطمینان از این که همه دستگاه‌ها از آخرین نسخه‌های نرم‌افزاری بهره‌مند هستند، از اهمیت زیادی برخوردار است.

روش‌های تشخیص تهدید در شبکه‌های هوشمند

برای مقابله با تهدیدات سایبری که شبکه‌های هوشمند را هدف قرار می‌دهند، استفاده از تکنیک‌های پیشرفته شناسایی و جلوگیری از حملات امری ضروری است. این تکنیک‌ها به شبکه‌های هوشمند اجازه می‌دهند که علاوه بر شناسایی تهدیدات، به سرعت و با دقت بیشتری به حملات پاسخ دهند. در ادامه به توضیح برخی از این روش‌های پیشرفته پرداخته می‌شود:

۱. سیستم‌های تشخیص نفوذ (Intrusion Detection Systems – IDS) : سیستم‌های تشخیص نفوذ یا IDS یکی از ابزارهای کلیدی برای شناسایی نفوذهای احتمالی در شبکه‌های هوشمند هستند. IDS با تجزیه و تحلیل داده‌های شبکه و بررسی الگوهای رفتاری، به شناسایی فعالیت‌های مشکوک و حملات احتمالی می‌پردازد. این سیستم‌ها می‌توانند به دو صورت کار کنند:

- **سیستم‌های تشخیص مبتنی بر امضاء (Signature-based IDS):** این سیستم‌ها الگوهای شناخته‌شده حملات (مانند بدافزارها و حملات DDoS) را شناسایی کرده و هرگونه فعالیت مشابه را به عنوان یک تهدید تشخیص می‌دهند. این نوع IDS برای مقابله با تهدیدات رایج و شناخته‌شده موثر است.
- **سیستم‌های تشخیص مبتنی بر رفتار (Anomaly-based IDS):** این سیستم‌ها بر اساس تحلیل رفتار عادی شبکه، به شناسایی الگوهای غیرمعمول و فعالیت‌های ناشناخته می‌پردازند. این نوع IDS برای شناسایی حملات جدید و ناشناخته که الگوهای

مشخصی ندارند، مفید است و به خصوص در شبکه‌های هوشمند با ویژگی‌های پویا کاربرد بالایی دارد.

۲. نظارت و پایش لحظه‌ای(Real-time Monitoring) :

نظارت و پایش لحظه‌ای شبکه‌های هوشمند از جمله ابزارهای پیشرفته‌ای است که به شناسایی رفتارهای غیرعادی و فعالیت‌های مشکوک کمک می‌کند. در این روش، داده‌های شبکه به صورت لحظه‌ای پایش و تحلیل می‌شوند و هرگونه تغییر در وضعیت شبکه بلافاصله گزارش می‌شود. از مزایای نظارت لحظه‌ای می‌توان به موارد زیر اشاره کرد:

واکنش سریع به تهدیدات: با شناسایی لحظه‌ای تهدیدات، تیم‌های امنیتی قادر خواهند بود در کوتاه‌ترین زمان ممکن به حملات پاسخ دهند و از گسترش آنها جلوگیری کنند.

تشخیص رفتارهای غیرعادی: نظارت لحظه‌ای با تحلیل رفتارهای طبیعی شبکه، می‌تواند هر گونه رفتار غیرعادی یا تغییر ناگهانی در الگوهای مصرف، ترافیک شبکه و عملکرد تجهیزات را شناسایی کند.

ایجاد گزارشات جامع: سیستم‌های پایش لحظه‌ای امکان تهیه گزارشات فوری و دقیق از وضعیت شبکه را فراهم می‌کنند که به تیم‌های امنیتی در تحلیل و بهبود تدابیر امنیتی کمک می‌کند.

۳. یادگیری ماشین و هوش مصنوعی (Machine Learning and Artificial Intelligence): تکنیک‌های یادگیری ماشین و هوش مصنوعی به شبکه‌های هوشمند این امکان را می‌دهند که با استفاده از داده‌های گذشته و تحلیل الگوهای رفتاری، تهدیدات ناشناخته و جدید را شناسایی کنند. این تکنیک‌ها می‌توانند به صورت خودکار شبکه را از رفتارهای مشکوک آگاه کنند و به پیشگیری از حملات کمک کنند.

برخی از روش‌های کاربردی هوش مصنوعی و یادگیری ماشین در امنیت سایبری شبکه‌های هوشمند عبارتند از:

الگوریتم‌های یادگیری نظارت‌شده و بدون نظارت: در یادگیری نظارت‌شده، الگوریتم‌ها بر اساس داده‌های برچسب‌دار آموزش می‌بینند و تهدیدات مشابه را شناسایی می‌کنند. در یادگیری بدون نظارت، الگوریتم‌ها بدون نیاز به برچسب‌گذاری قبلی، به شناسایی الگوهای ناهنجار و رفتارهای غیرمعمول می‌پردازند.

شبکه‌های عصبی و شبکه‌های عصبی عمیق (Deep Learning): شبکه‌های عصبی با ساختارهای پیچیده و چندلایه، توانایی شناسایی الگوهای پیچیده و غیرمعمول در ترافیک شبکه را دارند و به شناسایی حملات پیشرفته کمک می‌کنند.

تشخیص رفتارهای مشکوک با تحلیل سری‌های زمانی: تحلیل سری‌های زمانی به شبکه‌های هوشمند این امکان را می‌دهد که تغییرات ناگهانی در رفتارهای عادی سیستم را شناسایی کرده و در صورت نیاز، اقدامات پیشگیرانه اتخاذ کنند.

استفاده از مدل‌های پیش‌بینی‌کننده: مدل‌های پیش‌بینی بر اساس تحلیل داده‌های تاریخی می‌توانند رفتارهای آینده شبکه را پیش‌بینی کنند و در صورت تشخیص رفتارهای غیرعادی، به شبکه هشدار دهند. این ویژگی به شناسایی و جلوگیری از حملات قبل از وقوع کمک می‌کند.

۴. فایروال‌های پیشرفته و فایروال‌های مبتنی بر هوش مصنوعی (Next-generation Firewalls): فایروال‌های پیشرفته که با فناوری هوش مصنوعی تقویت شده‌اند، قابلیت شناسایی و مسدود کردن ترافیک مشکوک را دارند. این فایروال‌ها می‌توانند به صورت خودکار الگوهای ترافیکی شبکه را تحلیل کرده و از نفوذ حملات جلوگیری کنند. استفاده از این فایروال‌ها به خصوص در شبکه‌های هوشمند، که ترافیک زیادی بین تجهیزات مختلف برقرار است، بسیار موثر و کارآمد است.

۵. رمزنگاری داده‌ها و احراز هویت چند عاملی (Multi-factor Authentication): رمزنگاری داده‌ها و احراز هویت چند عاملی از دیگر روش‌های مهم در امنیت سایبری شبکه‌های هوشمند هستند. رمزنگاری داده‌ها تضمین می‌کند که اطلاعات حساس در طول انتقال محافظت شوند و از دسترسی غیرمجاز به آن‌ها جلوگیری شود. احراز هویت چند عاملی نیز سطح امنیت را با افزودن لایه‌های اضافی به فرآیند احراز هویت افزایش می‌دهد و از دسترسی‌های غیرمجاز جلوگیری می‌کند.

راهکارهای امنیتی در شبکه‌های هوشمند

برای مقابله با تهدیدات سایبری و ارتقاء امنیت شبکه‌های هوشمند، تکنیک‌ها و پروتکل‌های مختلفی به کار گرفته می‌شود:

رمزنگاری پیشرفته: استفاده از الگوریتم‌های رمزنگاری قوی برای حفاظت از داده‌های حساس و جلوگیری از دسترسی غیرمجاز. این روش به حفظ محرمانگی داده‌ها کمک کرده و امنیت اطلاعات را در طول انتقال تضمین می‌کند.

سیستم‌های تشخیص نفوذ (IDS) : این سیستم‌ها با تحلیل رفتارهای شبکه و شناسایی الگوهای مشکوک، به شناسایی و مقابله با حملات احتمالی کمک می‌کنند.

احراز هویت چندعاملی (MFA) : احراز هویت چندعاملی با افزایش سطح امنیت، از دسترسی‌های غیرمجاز جلوگیری می‌کند. این روش به خصوص در حفاظت از سامانه‌های مدیریتی شبکه‌های هوشمند بسیار مؤثر است.

بلاکچین: استفاده از بلاکچین به شبکه‌های هوشمند امکان می‌دهد تا داده‌ها و تراکنش‌ها را به صورت شفاف و غیرقابل تغییر ثبت و ذخیره کنند. بلاکچین به حفظ یکپارچگی داده‌ها کمک کرده و از دستکاری‌های احتمالی جلوگیری می‌کند.

تقسیم‌بندی شبکه (Network Segmentation) : با تقسیم‌بندی شبکه به بخش‌های کوچکتر، امکان محدود کردن تاثیر حملات و جلوگیری از گسترش تهدیدات در کل شبکه فراهم می‌شود.

آموزش و آگاهی‌بخشی به کاربران: کاربران و پرسنل شبکه‌های هوشمند باید با جدیدترین تهدیدات و روش‌های مقابله با آنها آشنا شوند. آموزش کاربران در شناسایی حملات مهندسی اجتماعی و فیشینگ و ارائه راهکارهای امن می‌تواند از وقوع بسیاری از حملات جلوگیری کند.

استانداردها و مقررات امنیت سایبری در شبکه‌های هوشمند

برای تضمین امنیت شبکه‌های هوشمند، استانداردهای مختلفی در سطح بین‌المللی تدوین شده‌اند. برخی از مهم‌ترین این استانداردها عبارتند از:

NIST(موسسه ملی استاندارد و فناوری آمریکا): مجموعه‌ای از راهنماها و چارچوب‌های امنیتی برای محافظت از شبکه‌های هوشمند.

ISO/IEC 27001: استاندارد بین‌المللی امنیت اطلاعات که راهنمایی برای ایجاد و مدیریت سیستم‌های امنیتی ارائه می‌دهد.

IEC 62351: استاندارد امنیتی مخصوص سیستم‌های برق که شامل پروتکل‌ها و روش‌های حفاظتی برای حفاظت از ارتباطات شبکه‌های هوشمند است.

روندهای آینده در ارتقاء امنیت سایبری شبکه‌های هوشمند

چندین روند نوظهور و آینده‌نگرانه در حوزه امنیت سایبری می‌تواند به ارتقاء امنیت شبکه‌های هوشمند کمک کرده و آن‌ها را در برابر تهدیدات پیچیده و پیشرفته مقاوم‌تر کند. در ادامه به توضیح جزئیات این روندها می‌پردازیم:

۱ . اتحاد امنیتی بین‌المللی

در جهانی که شبکه‌های هوشمند به عنوان زیرساخت‌های حیاتی برای تامین انرژی در مقیاس جهانی اهمیت دارند، کشورها و سازمان‌های بین‌المللی می‌توانند با ایجاد اتحادهای امنیتی به مقابله موثرتر با تهدیدات سایبری بپردازند. این همکاری‌ها می‌توانند شامل تبادل اطلاعات امنیتی، اشتراک‌گذاری بهترین روش‌ها و استانداردها، و هماهنگی در واکنش به تهدیدات سایبری جهانی باشند.

علاوه بر این، ایجاد اتحادیه‌های امنیتی و تدوین چارچوب‌های مشترک در مقابله با حملات سایبری می‌تواند شبکه‌های هوشمند را از نظر امنیتی تقویت کرده و به کاهش آسیب‌پذیری‌های مشترک کمک کند. این نوع همکاری‌ها به ویژه در شرایطی که حملات سایبری به صورت هماهنگ و بین‌المللی انجام می‌شوند، بسیار حیاتی هستند.

۲ . هوش مصنوعی و تحلیل داده‌های پیشرفته

هوش مصنوعی و یادگیری ماشین نقش برجسته‌ای در تحلیل داده‌ها و شناسایی تهدیدات سایبری ایفا می‌کنند. توسعه الگوریتم‌های هوشمند می‌تواند به شبکه‌های هوشمند این امکان را دهد که با تحلیل داده‌های گذشته و شناسایی الگوهای مشکوک، تهدیدات سایبری را در مراحل ابتدایی شناسایی و خنثی کنند. هوش مصنوعی می‌تواند به صورت خودکار رفتارهای غیرعادی را تشخیص داده و با تحلیل آنی داده‌ها به شناسایی حملات جدید کمک کند. علاوه بر این، استفاده از هوش مصنوعی به ویژه در ترکیب با یادگیری عمیق و الگوریتم‌های پیش‌بینی، امکان مدل‌سازی تهدیدات و شبیه‌سازی حملات را فراهم می‌کند. این تکنولوژی‌ها به شبکه‌های هوشمند کمک می‌کنند تا در برابر تهدیدات ناشناخته و پیچیده‌ای که به صورت روزافزون به وجود می‌آیند، آمادگی بیشتری داشته باشند.

۳ . شبکه‌های خودترمیم

یکی از قابلیت‌های پیشرفته‌ای که در آینده در شبکه‌های هوشمند به کار خواهد رفت، توانایی خودترمیمی یا Self-Healing است. شبکه‌های خودترمیم به سیستم‌ها این امکان را می‌دهند که در هنگام مواجهه با حملات یا نقص‌های فنی، به صورت خودکار و بدون نیاز به دخالت انسانی خود را بازیابی کنند. این شبکه‌ها با استفاده از فناوری‌هایی مانند هوش مصنوعی و یادگیری ماشین، می‌توانند نقاط آسیب‌دیده را شناسایی و تعمیر کنند یا از مسیرهای جایگزین برای انتقال داده‌ها استفاده نمایند. شبکه‌های خودترمیم نه تنها از زمان و هزینه‌های ناشی از خرابی‌های طولانی جلوگیری می‌کنند، بلکه می‌توانند به طور موثر در برابر حملات پیچیده‌ای مانند DDoS که به دنبال ایجاد اختلال در سرویس‌ها هستند، مقاومت کنند. با پیشرفت این قابلیت، شبکه‌های هوشمند قادر خواهند بود به پایداری بیشتری در شرایط بحرانی دست یابند.

۴ . استفاده گسترده از بلاکچین

بلاکچین با ایجاد یک سیستم توزیع‌شده و غیرقابل تغییر، می‌تواند نقش کلیدی در امنیت سایبری شبکه‌های هوشمند ایفا کند. بلاکچین به شبکه‌ها این امکان را می‌دهد که داده‌ها و تراکنش‌ها را به صورت شفاف و امن ذخیره کنند. از آنجا که بلاکچین قابلیت ثبت تراکنش‌ها به صورت دائمی و بدون تغییر را فراهم می‌کند، می‌توان از آن برای مدیریت دسترسی‌ها و جلوگیری از دستکاری داده‌ها استفاده کرد.

این فناوری همچنین می‌تواند برای احراز هویت دستگاه‌های متصل به شبکه‌های هوشمند، ایجاد سیستم‌های شفاف و قابل ردیابی، و جلوگیری از دسترسی‌های غیرمجاز به کار رود. در شبکه‌های هوشمند، بلاکچین می‌تواند به ایجاد اطمینان از یکپارچگی داده‌ها و جلوگیری از تقلب کمک کند و به عنوان یک لایه امنیتی قوی در برابر تهدیدات سایبری عمل کند.

۵ .سیستم‌های امنیتی مبتنی بر رفتار (Behavioral-based Security Systems)

سیستم‌های امنیتی مبتنی بر رفتار به شبکه‌های هوشمند این امکان را می‌دهند که الگوهای رفتاری معمول و ناهنجاری‌ها را تشخیص دهند. این سیستم‌ها بر اساس تحلیل الگوهای رفتاری کاربران و دستگاه‌ها، به سرعت متوجه رفتارهای غیرعادی می‌شوند و می‌توانند اقدامات پیشگیرانه‌ای اتخاذ کنند. این رویکرد به خصوص در مقابله با حملات مهندسی اجتماعی و فیشینگ، که از روش‌های رایج در حملات سایبری به شبکه‌های هوشمند هستند، بسیار کارآمد است. با توسعه این سیستم‌ها، شبکه‌های هوشمند می‌توانند رفتارهای مشکوک را به صورت خودکار شناسایی کرده و پیش از وقوع حمله، دسترسی مهاجمان را مسدود کنند.

۶ . رایانش مرزی(Edge Computing)

با افزایش دستگاه‌های اینترنت اشیا در شبکه‌های هوشمند، رایانش مرزی به عنوان راه‌حلی برای پردازش داده‌ها در نزدیکی منبع داده، اهمیت پیدا کرده است. این روش می‌تواند داده‌های حساس را به جای ارسال به سرورهای مرکزی، در دستگاه‌های مرزی (مانند کنتورهای هوشمند و حسگرها) پردازش کند. رایانش مرزی با کاهش حجم داده‌های منتقل‌شده و افزایش سرعت پاسخگویی، امنیت و کارایی شبکه‌های هوشمند را ارتقاء می‌دهد. در نتیجه، اگر حمله‌ای به یک دستگاه مرزی انجام شود، اثر آن محدود به همان دستگاه باقی مانده و از گسترش حمله به کل شبکه جلوگیری می‌شود.

۷ . استانداردسازی و به‌روزرسانی‌های منظم امنیتی

یکی از روندهای مهم در ارتقاء امنیت سایبری شبکه‌های هوشمند، استانداردسازی پروتکل‌ها و به‌روزرسانی‌های منظم است. با تدوین استانداردهای امنیتی جامع و اجرای به‌روزرسانی‌های منظم، می‌توان شبکه‌های هوشمند را در برابر تهدیدات جدید مقاوم‌تر کرد.

این امر نیازمند هماهنگی بین تولیدکنندگان تجهیزات، ارائه‌دهندگان خدمات شبکه، و نهادهای قانونی است تا با ایجاد استانداردهای واحد، نقاط ضعف امنیتی کاهش یابد. به‌روزرسانی‌های منظم نرم‌افزاری و سخت‌افزاری نیز می‌تواند به جلوگیری از نفوذ و سوءاستفاده از آسیب‌پذیری‌های شناخته‌شده کمک کند.

➢ تازه ترین اخبار حوزه شبکه های هوشمند

- اولین دوره مسابقه ملی شهر هوشمند ایران در تیرماه ۱۴۰۲ برگزار خواهد شد. لذا جهت شرکت در مسابقه، مستندات مربوطه را حداکثر تا ۴ تیرماه ۱۴۰۲ ارسال نمایید.
- انستیتو فناوری دانمارک(DTI) از سوی آژانس فضایی اروپا(ESA) انتخاب شده تا یک پوست هوشمند برای بازوهای رباتیک در فضا بسازد. در همین راستا محققان تصمیم دارند یک پوست هوشمند مخصوص برای ربات ها بسازند که از مواد نرم ساخته شده و می توان با کمک چاپ سه بعدی قطعات الکترونیکی را به طور مستقیم روی پارچه پرینت کرد. فرایند مهندسی پوست سبب می شود تا برای استفاده در فضا ایمن باشد و به ربات حامل آن کمک می کند فعالیت های مختلفی انجام دهد.

گاهنامه انجمن شبکه هوشمند انرژی ایران

انجمن علمی شبکه هوشمند انرژی ایران

شماره ۰۸-تیرماه ۱۴۰۲

گاهنامه انجمن علمی شبکه هوشمند انرژی ایران از تمامی دانشجویان، فارغ تحصیلان و صنعتگران مرتبط با حوزه شبکه های هوشمند دعوت به عمل می آورد تا با ارسال مقالات خود به این گاهنامه موجبات غنای علمی بیشتر این گاهنامه را فراهم آورند.