راهبردهای مواجهه با فناوری‌های نوظهور از منظر امنیت سایبری

محمدحسن فرخی[۱]، خداداد هلیلی[۲]

[۱]دانشجوی دکتری امنیت سایبر، دانشگاه عالی دفاع ملی
mhf1364@gmail.com
[۲]استادیار، عضو هیات علمی دانشکده کامپیوتر، دانشگاه شهید ستاری، تهران
kh.halili@ssau.ac.ir

چکیده

همزمان با گسترش فضای سایبر و فناوری‌های مرتبط با آن، حملات و تهدیدات سایبری نیز مدام درحال‌توسعه هستند. در بسیاری از کشورها، امنیت سایبری به یکی از اولویت‌های اساسی در دستیابی به امنیت ملی تبدیل شده است. به‌منظور پیشگیری از آثار مخرب این حملات و جلوگیری از ایجاد خدشه در امنیت ملی، لازم است علاوه بر تمهیدات فنی، راهبردهای مناسبی در سطح ملی، تدوین و اجرا شود. هدف اصلی این مقاله بررسی راهکارهای مؤثر برای بهبود امنیت سایبری و ارائه راهبردهایی برای مواجهه هوشمند با فناوری‌های مورداستفاده در فضای سایبر، است. بدین منظور پس از بررسی فناوری‌های هوش مصنوعی، زنجیره‌بلوکی، اینترنت اشیا، رایانش ابری، بیومتریک و رباتیک و کاربردهای آن‌ها، راهبردهای پیشنهادی مطرح شده است. نتایج این تحقیق نشان می‌دهد توسعه فناوری‌های امنیتی، آموزش و افزایش آگاهی کاربران، توسعه قوانین و سیاست‌های امنیتی، همکاری بین کشورها، و توسعه فرهنگ امنیت سایبری موجب بهبود امنیت سایبری می‌شود بدین منظور راهبردهایی مانند توسعه فناوری‌های امنیتی، آموزش و افزایش آگاهی کاربران، توسعه قوانین و سیاست‌های امنیتی، همکاری بین کشورها، و توسعه فرهنگ امنیت سایبری در این مقاله موردتوجه و بررسی قرار گرفته است.

کلمات کلیدی: فضای سایبر، فناوری‌های نوظهور، امنیت سایبری، هوش مصنوعی.

۱ مقدمه

فناوری‌های نوظهور به سرعت درحال توسعه و استفاده در همه جای جهان هستند. با پیشرفت فناوری، فضای سایبر نیز به یکی از مهم‌ترین بخش‌های زندگی انسان تبدیل شده است. با افزایش استفاده از این فناوری‌ها، حملات سایبری نیز درحال گسترش بوده و برای مقابله با آنها، نیاز به راهبردهای مناسب و هوشمند داریم. حمله بدافزار استاکس‌نت – ساخت مشترک دولت متخاصم آمریکا و رژیم جعلی اسرائیل - که در سال ۱۳۸۹

تأسیسات هسته‌ای ایران از جمله نیروگاه بوشهر را هدف قرار داد، از جمله رخدادهای سایبری مورد توجه در سال‌های گذشته است که زیرساخت‌های حیاتی ملی کشور را مورد هدف قرار داده است.

امنیت سایبری به‌عنوان یکی از مهم‌ترین اولویت‌های امنیت ملی در جهان مطرح است و سرمایه‌گذاری وسیعی در این زمینه انجام شده است. برای درک اهمیت موضوع، در انگلیس در سال ۲۰۲۲، شرکت‌های کوچک ۱۸۷ میلیون پوند در بخش امنیت سایبری سرمایه‌گذاری کردند که درآمد تولید شده توسط این شرکت‌ها با ۱۴ درصد افزایش به ۱.۱۰ میلیارد پوند رسیده است[1]؛ بنابراین، برای جلوگیری از حملات سایبری و حفاظت از اطلاعات حساس و مهم کشور، لازم است تا راهبردهای مناسبی در این زمینه تدوین و اجرا شود. در این مقاله، ابزارها و راهکارهایی برای بهبود امنیت سایبری مورد توجه قرار گرفته است.

برای بهبود امنیت سایبری، مقوله‌هایی مانند توسعه فناوری‌های امنیتی، آموزش و افزایش آگاهی کاربران، توسعه قوانین و سیاست‌های امنیتی، همکاری بین کشورها و توسعه فرهنگ امنیت سایبری، حائز اهمیت است. در این تحقیق، ضمن معرفی برخی از فناوری‌های نوظهور در عرصه فضای سایبر، راهبردهایی به‌صورت تجویزی برای بهبود امنیت سایبری و مواجهه با این فناوری‌ها ارائه شده است.

۲ پیشینه تحقیق

در مقاله شکری و موسوی (۱۳۹۸) هوش مصنوعی به‌عنوان یکی از ابزارهای مفید برای تشخیص و پیشگیری از حملات سایبری مطرح شده است. در این مقاله به استفاده از الگوریتم‌های هوش مصنوعی و تحلیل داده‌های سایبری، برای شناسایی الگوهای غیرعادی در رفتار کاربران، دستگاه‌ها و شبکه‌ها پرداخته شده است. محمدی و همکاران (۱۳۹۹) نیز کاربردهای هوش مصنوعی را در امنیت سایبری بررسی کرده‌اند.

کراسبی و همکاران (۲۰۱۶) و ناریامن (۲۰۱۶) با بررسی کاربردهای بلاک‌چین، آنها را به‌عنوان یک راه‌حل امنیتی برای محافظت از داده‌های حساس و ارائه خدمات امن به کاربران در فضای سایبر، مورد بررسی قرار داده‌اند.

رومن و همکاران (۲۰۱۳)، در مقاله‌ای با عنوان قابلیت‌ها و چالش‌های امنیت و حریم خصوصی در اینترنت اشیا، راهکارهای امنیتی برای محافظت از اطلاعات و کاربران را ارائه داده‌اند. لی و همکاران (۲۰۱۸) نیز در مقاله‌ای با عنوان امنیت و حریم خصوصی در اینترنت اشیا به این مسئله پرداخته‌اند.

در مقاله خسروی و عرفانی (۲۰۲۱) با اشاره به تهدیدات امنیتی در فناوری رباتیک، مدیریت دسترسی به ربات‌ها و اطمینان از دسترسی افراد مجاز، به‌عنوان راه‌حل‌های امنیتی در این حوزه مطرح شده است.

۳ فناوری‌های نوظهور درفضای سایبر و چالش‌های امنیتی آنها

در این بخش به معرفی برخی از پرکاربردترین فناوری‌های مرتبط با فضای سایبر اعم از هوش مصنوعی و الگوریتم‌های آن، فناوری بلاک‌چین، اینترنت اشیا، رایانش ابری، فناوری رباتیک و کاربردهای آنها و برخی مکانیسم‌های امن‌سازی آنها پرداخته شده است.

[1] https://www.gov.uk

۱.۳ هوش مصنوعی

در حوزه امنیت سایبری، هوش مصنوعی می‌تواند به‌عنوان یکی از ابزارهای مفید برای تشخیص و پیشگیری از حملات سایبری استفاده شود. هوش مصنوعی می‌تواند در تشخیص و پیشگیری از تهدیداتی که از سمت افراد خطرناک، گروه‌های تروریستی و افرادی که با اهداف خلاف قانون شکل می‌گیرند، مفید باشد. با استفاده از الگوریتم‌های هوش مصنوعی و تحلیل داده‌های مختلف، می‌توان به شناسایی الگوهای غیرعادی در رفتار افراد و گروه‌های مشکوک، و همچنین پیش‌بینی عملیات تروریستی و خطرات مختلف پرداخت. باتوجه‌به پیشرفت‌های روزافزون در حوزه هوش مصنوعی، انتظار می‌رود که در آینده این فناوری به‌عنوان یکی از ابزارهای اصلی در حوزه امنیت سایبری مورد استفاده قرار گیرد [۱]. برای تشخیص حملات سایبری با استفاده از هوش مصنوعی، الگوریتم‌های مختلفی وجود دارند که هرکدام به‌صورت خاص برای تشخیص انواع مختلفی از حملات سایبری طراحی شده‌اند [۲]. در جدول ۱، برخی از کاربردهای الگوریتم‌های هوش مصنوعی در امنیت سایبری دسته‌بندی شده‌اند.

۲.۳ بلاک‌چین

بلاک‌چین به‌صورت یک زنجیره از بلوک‌ها که حاوی اطلاعات مختلفی ازجمله تراکنش‌ها و معاملات است، عمل می‌کند. هر بلوک، شامل یک هش[۲] از داده‌های قبلی، هش داده‌های جدید و یک مهر زمانی[۳] است که نشان‌دهنده زمان ایجاد بلوک می‌باشد. هش، یک مقدار رمزگذاری شده است که با استفاده از تابع هش، از داده‌های ورودی به‌عنوان ورودی تولید می‌شود. بلاک‌چین به‌عنوان یک فناوری متن‌باز، در ابتدا برای پشتیبانی از ارزهای دیجیتال مانند بیت‌کوین طراحی شده بود؛ اما امروزه، در صنایع متنوعی از جمله بانکداری، بیمه، صنایع غذایی، حوزه حمل‌ونقل و غیره به کار گرفته شده است [۳].

بلاک‌چین به‌عنوان یک سیستم توزیع‌شده، از مشکلات امنیتی و نقص‌های سامانه‌های مرکزی برخوردار نیست. بااین‌وجود، توسعه شبکه‌های خصوصی بلاک‌چین، به‌عنوان یک راه‌حل امنیتی و افزایش کارایی در فضای سایبری، مورد توجه قرار گرفته است و بسیاری از سازمان‌ها و شرکت‌ها از این روش برای محافظت از داده‌های حساس و ارائه خدمات امن به کاربران استفاده می‌کنند [۵] و [۸].

۳.۳ اینترنت اشیا

در اینترنت اشیا[۴]، داده‌های حساس جمع‌آوری و منتقل می‌شوند، امنیت اطلاعات از جمله چالش‌های اصلی در این فناوری به حساب می‌آید. برای حفاظت از اطلاعات حساس، از راهکارهایی همچون رمزنگاری، شناسایی و احراز هویت، مدیریت دسترسی و مانیتورینگ استفاده می‌شود [۹].

برای مقابله با چالش‌های امنیتی در حوزه اینترنت اشیا، لازم است که به توسعه نیروی انسانی متخصص در امنیت سایبری و آشنایی با فناوری‌های نوظهور توجه شود. توسعه قوانین و مقررات مناسب برای حفاظت

[2] Hash
[3] Timestamp
[4] IoT: Internet of Things

جدول ۱: الگوریتم‌های هوش مصنوعی در امنیت سایبر

عنوان	شرح الگوریتم
شبکه‌های عصبی مصنوعی	در این الگوریتم ابتدا داده‌های مربوط به حملات سایبری و داده‌های عادی جمع‌آوری می‌شود. سپس با انجام آموزش‌های لازم و یادگیری ماشینی، شبکه عصبی مصنوعی، داده‌های حاوی حملات سایبری را تشخیص داده و اقدامات مناسب برای مقابله با این حملات را نیز به‌صورت خودکار انجام می‌دهد.
درخت تصمیم Decision Trees	الگوریتم‌های درخت تصمیم یکی از پرکاربردترین الگوریتم‌های یادگیری ماشینی هستند و برای حل مسائل طبقه‌بندی و پیش‌بینی از آنها استفاده می‌شود. درخت تصمیم، ساختاری سلسله‌مراتبی دارد که در هر سطح آن، یک مجموعه از تصمیم‌ها برای تقسیم داده‌ها به دو گروه انجام می‌شود. هر برگ این درخت، به یک کلاس خاص یا یک مقدار پیش‌بینی برای داده‌های ورودی متصل می‌شود. درخت تصمیم با استفاده از الگوریتم‌هایی مانند ID3، C4.5 و CART ساخته می‌شود.
درون‌یابی	با استفاده از الگوریتم‌های درون‌یابی، می‌توان گروه‌هایی از داده‌های مشابه را شناسایی کرد و برای ارائه پیش‌بینی‌های دقیق‌تر، از آنها استفاده کرد. در الگوریتم‌های درون‌یابی، داده‌ها به دو صورت مختلف می‌توانند گروه‌بندی شوند: گروه‌بندی سلسله‌مراتبی (Hierarchical) و گروه‌بندی غیر سلسله‌مراتبی (Non-hierarchical). در این مدل، گروه‌ها به‌صورت سلسله‌مراتبی تشکیل می‌شوند و می‌توان به‌راحتی به سطح‌های مختلف درخت دسترسی داشت. در گروه‌بندی غیر سلسله‌مراتبی، داده‌ها به گروه‌های مشابه تقسیم می‌شوند، بدون توجه به سطح سلسله‌مراتبی. برخی از مهم‌ترین الگوریتم‌های درون‌یابی عبارت‌اند از: K-Means، DBSCAN، Gaussian Mixture Mod-els (GMM) و Hierarchical Clustering.
ماشین بردار پشتیبان Support Vector Machines	الگوریتم‌های ماشین بردار پشتیبان یا SVM، یکی از الگوریتم‌های پرکاربرد در یادگیری ماشین است که برای مسائل طبقه‌بندی و بازشناسی الگو استفاده می‌شود. این الگوریتم‌ها با استفاده از داده‌های برچسب‌گذاری شده، سعی می‌کنند بهینه‌سازی مدل خود را انجام دهند و سپس با استفاده از مدل به‌دست آمده، برچسب‌گذاری داده‌های بدون برچسب را انجام می‌دهند. یکی از الگوریتم‌های شبه نظارتی معروف، الگوریتم شبکه‌های مولد است که در آن با استفاده از داده‌های برچسب‌گذاری شده، یک مدل شبکه عصبی برای تولید داده‌های مصنوعی آموزش داده می‌شود.

از اطلاعات حساس در این حوزه و ارتقای امنیت شبکه‌های اینترنت اشیا باید به طور جدی مورد توجه قرار گیرد. برای این منظور، باید از روش‌های مانیتورینگ و شناسایی تهدیدات و فایروال و آنتی‌ویروس استفاده کرد. همچنین، باید از روش‌های دسترسی محدود به داده‌ها و شناسایی دومرحله‌ای استفاده کرد [۴].

باتوجه به اینکه اینترنت اشیا به‌عنوان یکی از فناوری‌های نوظهور و مهم در دنیای دیجیتال شناخته می‌شود، توجه به امنیت در این حوزه بسیار حائز اهمیت است. باتوجه به رشد روزافزون اینترنت اشیا و تعداد دستگاه‌های هوشمند، لازم است که راهکارهای امنیتی مناسب برای حفاظت از اطلاعات حساس در این حوزه توسعه داده شود تا بتوان از امنیت اطلاعات کاربران و جامعه محافظت کرد. در جدول ۲ برخی از چالش‌های امنیتی در حوزه اینترنت اشیا آمده است.

۴.۳ رایانش ابری

رایانش ابری به‌عنوان یکی از فناوری‌های نوظهور در فضای سایبر، شامل استفاده از سرورهای ابری برای ذخیره‌سازی و پردازش اطلاعات است. این فناوری باعث شده است که سازمان‌ها و شرکت‌ها بتوانند به راحتی از خدمات ذخیره‌سازی و پردازش ابری استفاده کنند و نیازی به سرورهای خود نداشته باشند. از دیگر مزایای استفاده از فناوری ابر می‌توان به دسترسی سریع و آسان به داده‌ها، افزایش قابلیت اطمینان و کارایی در پردازش داده‌ها، کاهش هزینه‌های سرورها و مراکز داده، افزایش قابلیت اطمینان و پایداری در ارائه خدمات اشاره کرد. این امر به‌عنوان یک راه‌حل اقتصادی و عملی برای ذخیره‌سازی داده‌ها و پردازش آنها در نظر گرفته می‌شود [۱۰].

باتوجه‌به اینکه این فناوری از طریق اینترنت وصل می‌شود، تهدیدات امنیتی متعددی نیز برای آن وجود دارد. برای مقابله با این تهدیدات، باید دقت ویژه در مدیریت داده‌ها و اطلاعات حساس و افزایش امنیت این سرورها و رمزگذاری اطلاعات بر روی آنها داشت. همچنین، باید از روش‌های امنیتی مانند دسترسی محدود به داده‌ها و شناسایی دومرحله‌ای استفاده کرد. روش‌های رمزگذاری نیز می‌توانند به‌عنوان یک راهکار مؤثر برای افزایش امنیت در فناوری ابر مورداستفاده قرار گیرند. همچنین برای افزایش امنیت در فضای ابری، باید از روش‌های پیشگیرانه و شناسایی تهدیدات استفاده کرد. به‌عنوان مثال: شناسایی و جلوگیری از حملات DDoS (حملات توزیع‌شده از سرویس)، هوشمندسازی فرایندهای مدیریت و افزایش سطح اطمینان از امنیت و محرمانگی داده‌ها می‌تواند مؤثر باشد.

۵.۳ فناوری بیومتریک

فناوری بیومتریک یکی از فناوری‌های مهم و پیشرفته در حوزه امنیتی است که برای شناسایی افراد بر اساس ویژگی‌های فیزیکی مانند اثر انگشت، چهره و قلب استفاده می‌شود. این فناوری برای بسیاری از کاربردهای امنیتی، از جمله ورود به سیستم‌های کامپیوتری، حضوروغیاب در محیط کار، ورود به ساختمان‌های خصوصی و عمومی و ... استفاده می‌شود. باتوجه‌به اینکه در فناوری بیومتریک، اطلاعات حساس و شخصی کاربران شامل ویژگی‌های فیزیکی آنها مانند اثر انگشت و چهره استفاده می‌شود، تهدیدات امنیتی متعددی نیز برای آن وجود دارد. برای مقابله با این تهدیدات، باید از روش‌های امنیتی مانند رمزنگاری داده‌ها و افزایش امنیت

جدول ۲: چالش‌های امنیتی در اینترنت اشیا

عنوان	چالش‌های امنیتی
ارتباطات امن	در حوزه اینترنت اشیا، ارتباطات امن به‌عنوان یکی از چالش‌های اصلی مطرح است. برای ایجاد ارتباط امن در اینترنت اشیا، از روش‌هایی مانند رمزنگاری، شناسایی و احراز هویت، مدیریت دسترسی و مانیتورینگ استفاده می‌شود. همچنین، محافظت از اطلاعات حساس در ارتباطات در اینترنت اشیا بسیار حائز اهمیت است. برای محافظت از اطلاعات حساس کاربران، از روش‌هایی مانند رمزنگاری، توکن‌سازی و احراز هویت استفاده می‌شود. به‌عنوان‌مثال، از پروتکل امنیتی OAuth برای احراز هویت و توکن‌سازی استفاده می‌شود.
تهدیدات امنیتی	در حوزه اینترنت اشیا، تهدیدات امنیتی به‌عنوان یکی از چالش‌های اصلی مطرح است. یکی از نقاط ضعف موجود در اینترنت اشیا، نبود استانداردهای امنیتی مناسب است. باتوجه به اینکه بسیاری از دستگاه‌های اینترنت اشیا از پورت‌های باز و ناامن برای ارتباط با اینترنت استفاده می‌کنند، دسترسی به دستگاه‌ها توسط هکرها ممکن است بسیار ساده باشد. همچنین، حملات سایبری مانند حملات DDoS و malware نیز می‌توانند برای دستگاه‌های اینترنت اشیا خطرناک باشند.
رویکردهای امنیتی	فناوری رمزنگاری یکی از رویکردهای امنیتی اساسی در اینترنت اشیا است. با استفاده از رمزنگاری، اطلاعات جمع‌آوری‌شده در دستگاه‌های اینترنت اشیا رمزگذاری شده و به‌صورت ایمنی به سرورهای مرکزی ارسال می‌شوند. مدیریت دسترسی به دستگاه‌های اینترنت اشیا نیز یکی از رویکردهای مهم در حوزه امنیت است. با استفاده از این رویکرد، دسترسی به دستگاه‌ها و داده‌های حساس، تنها برای کاربران مجاز در دسترس خواهد بود و افراد نامتعهد نخواهند توانست به آنها دسترسی پیدا کنند. این رویکرد با استفاده از فناوری‌هایی مانند الگوریتم‌های تشخیص تهدیدات و تشخیص شبکه‌های نفوذی انجام می‌شود.
نیروی انسانی	متخصص در حوزه اینترنت اشیا، دسترسی غیرمجاز به داده‌های حساس، تهدیدات سایبری جدی برای امنیت گسترش این حوزه در آینده نزدیک محسوب می‌شوند. یکی از نیازهای اساسی در حوزه امنیت اینترنت اشیا، توسعه دانش و مهارت‌های متخصصان در حوزه امنیت سایبری است. متخصصانی که به این حوزه مسلط هستند، می‌توانند تهدیدات سایبری را تشخیص داده و در برابر آنها مقابله کنند. برای این منظور، توسعه دوره‌های آموزشی و مدارک مرتبط با امنیت سایبری می‌تواند به افزایش دانش و مهارت‌های متخصصان در این حوزه کمک کند.

اطلاعات حساس استفاده کرد تا داده‌های حساس موجود در این فناوری محافظت شوند.

یکی از تهدیدات امنیتی در فضای فناوری بیومتریک، حملات سایبری است که می‌تواند باعث دسترسی غیرمجاز به داده‌های حساس و اطلاعات شخصی کاربران شود. برای محافظت از داده‌های حساس و اطلاعات شخصی کاربران در فضای فناوری بیومتریک، باید از روش‌های رمزنگاری داده‌ها استفاده کرد تا داده‌های موجود در سامانه‌های بیومتریکی در هنگام انتقال و ذخیره‌سازی محافظت شوند. همچنین، برای افزایش امنیت در فضای فناوری بیومتریک، باید از روش‌های شناسایی تهدیدات و جلوگیری از وقوع حملات استفاده کرد [۷].

۶.۳ فناوری رباتیک

یکی از تهدیدات امنیتی در فضای رباتیک، دسترسی غیرمجاز به ربات‌ها است. برای مقابله با این تهدید، باید از روش‌های مدیریت دسترسی به ربات‌ها استفاده کرد تا دسترسی به ربات‌های حساس فقط برای افراد مجاز امکان‌پذیر باشد. همچنین، برای افزایش امنیت در فضای رباتیک، باید از روش‌های شناسایی تهدیدات و جلوگیری از وقوع حملات استفاده کرد. یکی دیگر از تهدیدات امنیتی در فضای رباتیک، سرقت اطلاعات حساس و داده‌های مربوط به فعالیت‌های رباتیک است. برای مقابله با این تهدید، باید از روش‌های امنیتی مانند رمزنگاری داده‌ها استفاده کرد تا از دسترسی غیرمجاز به داده‌های حساس در ربات‌ها جلوگیری شود [۶].

۴ راهبردهای مواجهه با فناوری‌های نوظهور در فضای سایبر

برای مواجهه هوشمند با فناوری‌های نوظهور در فضای سایبر و بهبود امنیت ملی سایبری جمهوری اسلامی ایران، در این مقاله، راهبردهای زیر بر اساس مطالعه مبانی نظری و به‌صورت تجویزی به شرح زیر احصاء شده است:

۱. **تقویت همکاری و تعامل با سازمان‌ها و نهادهای امنیت سایبری جهانی:** با توسعه روابط بین‌المللی، می‌توان به شناسایی و تبدیل تهدیدات سایبری به فرصت‌های اقتصادی و تجاری کمک کرد. در سطح بین‌الملل، سازمان‌هایی مانند اتحادیه اروپا، سازمان همکاری اقتصادی و توسعه و سازمان همکاری شانگهای و... در حوزه امنیت سایبری فعالیت می‌کنند. ایجاد شبکه‌های همکاری بین سازمان‌ها و تشکیل گروه‌های کاری مشترک در حوزه امنیت سایبری، می‌تواند به افزایش همکاری‌های بین‌المللی و تبادل تجربیات و دانش کمک کند.

۲. **به‌کارگیری فناوری هوش مصنوعی در تحلیل داده‌های سایبری:** به‌وسیله هوش مصنوعی، می‌توان الگوها و رفتارهای غیرعادی را در داده‌های سایبری شناسایی کرده و به رصد و پیشگیری از حملات سایبری کمک کرد. یکی از روش‌های استفاده از هوش مصنوعی در تحلیل داده‌های سایبری، استفاده از شبکه‌های عصبی پیچشی است. با استفاده از این روش، می‌توان به شناسایی الگوهای غیرعادی در داده‌های

سایبری پرداخت. همچنین، استفاده از الگوریتم‌های یادگیری ماشین مانند شبکه‌های عصبی بازگشتی[5]، می‌تواند به شناسایی الگوهای پیچیده‌تر در داده‌های سایبری کمک کند.

۳. استفاده از بلاک‌چین برای جلوگیری از حملات سایبری: بلاک‌چین به‌عنوان یک فناوری نوین، به جلوگیری از حملات سایبری مورد توجه قرار گرفته است. بلاک‌چین به‌عنوان یک فناوری توزیع‌شده، این امکان را فراهم می‌کند تا اطلاعاتی که در آن ذخیره می‌شوند، بدون وساطت ثبت و بازیابی شوند. این به این معنی است که هیچ‌کس نمی‌تواند به‌راحتی اطلاعات را تغییر دهد یا حذف کند. این امکان از بلاک‌چین، به جلوگیری از حملات سایبری و تغییر داده‌های مربوط به آنها کمک می‌کند.

۴. توسعه سیاست‌های امنیتی مبتنی بر ریسک: در این رویکرد، به‌جای تمرکز بر روی حملات و تهدیدات خاص، به تشخیص خطرات و ریسک‌های موجود در سازمان‌ها و اطلاعات مرتبط با آنها پرداخته می‌شود تا بتوان بهبود امنیت ملی را تسهیل کرد.

۵. ارتقای آموزش کاربران در زمینه امنیت سایبری: یکی از مزایای آموزش کاربران در مورد امنیت سایبری، کاهش خطرات سایبری است. با آموزش کاربران در مورد رفتارهای امنیتی، می‌توان خطرات سایبری را کاهش داد و از حملات سایبری جلوگیری کرد. همچنین، با آموزش کاربران در مورد محافظت از داده‌های مرتبط با امنیت ملی، می‌توان از دسترسی غیرمجاز به اطلاعات حساس و سوءاستفاده از آنها جلوگیری کرد.

۶. توسعه فرهنگ امنیت سایبری: برای توسعه فرهنگ امنیت سایبری، راهکارهای زیر پیشنهاد می‌شود: ۱. آموزش و آگاهی‌بخشی، ۲. ترویج مسئولیت‌پذیری ۳. ترویج امنیت در سازمان‌ها، ۴. ترویج امنیت در محصولات و خدمات، ۵. ترویج همکاری و هماهنگی، ۶. ترویج ارزش‌های امنیتی، و ۷. ترویج تحقیق و توسعه.

۵ نتیجه‌گیری

فناوری‌های نوینی که در فضای سایبر به کار می‌روند، می‌توانند برای توسعه و پیشرفت جوامع و کشورها بسیار مفید باشند. بااین‌حال، برای استفاده مؤثر و امن از این فناوری‌ها، نیاز به برخورداری از راهبردهای مناسب در فضای سایبر و امنیت ملی جمهوری اسلامی ایران است.

یکی از راهبردهای مهم در این زمینه، آموزش و آگاهی‌بخشی افراد و کاربران این فناوری‌ها است. باید به آنها آموزش داد که چگونه از این فناوری‌ها به نحو مؤثر و امن استفاده کنند و به اطلاعات شخصی و امنیت خود دقت کنند. همچنین، باید از طریق توسعه و ارتقای فناوری‌های امنیتی مانند رمزنگاری، تشخیص نفوذ، و مانیتورینگ، در فضای سایبر امنیت را تضمین کرد. علاوه بر این، باید مقررات و قوانین مناسبی برای استفاده

[5] Recurrent Neural Networks

از این فناوری‌ها در فضای سایبر و امنیت ملی جمهوری اسلامی ایران، تنظیم و اجرا کرد. این قوانین باید در جهت حفاظت از امنیت و حریم خصوصی کاربران و جامعه به کار گرفته شوند.

در نهایت، باید همکاری میان دولت، خصوصی‌سازی، و دانشگاه‌ها به‌منظور توسعه فناوری‌های امنیتی در فضای سایبر و امنیت ملی جمهوری اسلامی ایران، تقویت شود. این همکاری‌ها می‌توانند به افزایش امنیت و توسعه پایدار در فضای سایبر کمک کنند و تأثیر مثبتی بر رشد و پیشرفت جامعه و کشور داشته باشند. برخی از پیشنهادهای اجرایی برای این موضوع عبارت‌اند از:

- تشکیل واحد ملی اقدام‌کننده در خصوص فناوری‌های نوظهور سایبری ذیل مرکز ملی فضای مجازی
- توسعه و تدوین سند ملی راهبردی مواجهه با فناوری‌های نوظهور سایبر کشور
- تدوین سند ملی هوش مصنوعی و اخلاق به‌کارگیری آن

مراجع

[۱] محمدی، محمدجواد و علیجانی، بهاره (۱۳۹۸). هوش مصنوعی و نقش آن در امنیت سایبری، صص ۶۲-۷۷.

[۲] شکری، علی و موسوی، سید مجید (۱۳۹۸). کاربردهای هوش مصنوعی در امنیت سایبری. هشتمین کنفرانس ملی فناوری اطلاعات و ارتباطات، تهران، ایران

[۳] محمدی، علی؛ آقایی، علیرضا و رحمانی، مهدی (۱۳۹۹). هوش مصنوعی و کاربردهای آن در امنیت سایبری. مجله فناوری اطلاعات و ارتباطات در علوم تربیتی، صص ۶۹-۸۲.

[4] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys , Tutorials 247-276.

[5] Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. Applied Innovation, 71-81.

[6] Khosravi, H., Erfani, S. M. (2021). Security Threats and Solutions in Robotics Technology. Journal of Information Security and Cybercrimes 1-7.

[7] Li, S., Xu, L. D., Zhao, S. (2018). Security and privacy in the internet of things: Current status and future directions. Future Generation Computer Systems, 339-346.

[8] Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

[9] Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

[10] Tapscott, D., Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.