امنیت الکترونیک

فصل‌نامهٔ اختصاصی صنعت تجهیزات ایمنی و حفاظت

سال هفتم | شماره ششم | بهار ۱۴۰۴ | ۲۵۰هزار تومان

در این شماره می‌خوانیم:

ماهواره‌های جاسوسی، چشمان الکترومغناطیسی در آسمان، مروری بر امنیت در اینترنت اشیا

تحلیل پیش‌بینانه با استفاده از تصاویر نظارتی، هاردنینگ امنیتی سیستم‌های نظارت تصویری

تاکیدرئیس پلیس فراجا بر الـزام نصب دوربین‌های مداربسته در تمامی واحدهای صنفی کشور

نشست با جناب آقای روح الامین دادگر: مدیرعامل شرکت سامان پایش تصویر امن (سپتام)


هزاربین
آتن
آزمایشگاه تجهیزات نظارت تصویری
سیمنا
سامانه یکپارچه مدیریت و نظارت ایکس-ری
Automation
IP
سامانه
میهن
سامانه مدیریت یکپارچه هشدار نفوذ
رخ پایش
نگهبان هوشمند
امن پایش
AmnPaayesh
هوبان
سامانه‌ی
اتوماسیون
پارکینگ
فرجا

بسم الله الرحمن الرحیم

امنیت الکترونیک

صاحب امتیاز و مدیرمسئول: محمد قلم‌چی
سردبیر: سارا قلم‌چی

هیئت تحریریه (به‌ترتیب حروف الفبا): مهسا بیگ رضایی
رسمیه پروانه
سید علی صموتی
محمد قلم‌چی

ویراستار: معصومه عباسیان
محمود سعیدی
صفحه‌آرایی و طراحی: سارا قلم‌چی

مشخصات نشر: تهران، مجتمع چاپ ایران‌کهن

نشانی دبیرخانه: تهران- اقدسیه- بلوار ارتش- اراج- شانزده‌متری ولیعصر- نبش خیابان پروین- پلاک ۲- واحد ۴
تلفن: ۲۲۹۶۷۷۶۳-۰۲۱
نمابر: ۲۲۹۶۷۷۶۹-۰۲۱
نشانی اینترنتی: www.electronicsecurity.ir
پست الکترونیک: info@electronicsecurity.ir

فهرست

سرمقاله

نویسنده:
محمد قلم‌چی

جنگ برای هیچ انسانی خوشایند نیست و جنگ‌افروزان بویی از انسانیت نبرده‌اند. نشریه تخصصی امنیت الکترونیک، ضمن محکومیت تجاوز رژیم صهیونیستی به میهن اسلامی‌مان، شهادت فرماندهان نظامی و دانشمندان کشور را به این شهدا تبریک و به آحاد مردم شریف ایران تسلیت عرض می‌نماید. دفاع ستودنی غیور مردان این سرزمین با تجهیزات بومی موجب مباهات است. این فصل‌نامهٔ تخصصی نیز بیش از پیش تلاش می‌نماید که سهم خود را ادا نموده و همانگونه که قبلاً با توسعه دانش و تخصص در این حوزه عملاً تعهد خود به ارتقای امنیت الکترونیک کشور را اثبات نموده، در این برهه حساس بیش از پیش در توسعه دانش و فنآوری بومی امنیت الکترونیک برای ایران عزیزمان خواهد کوشید. هیات تحریریه این نشریه، حتی در اولین روزهای این تجاوز نیز از انجام رسالت خود غافل نبود.

جنگ در جهان جدید، تغییراتی شگرفی داشته است. دانش الکترونیک و زیرمجموعهٔ فناوری اطلاعات و ارتباطات آن، موجب افزایش قابل توجه کارآمدی تجهیزات نظامی شده‌اند و همین دانش حفره‌های زیادی نیز در آن‌ها ایجاد نموده است، همچون چاقویی دولبه. تکنولوژی‌های جدید و نفوذ به آن‌ها را شاید بتوان کلید موفقیت در جنگ نامید. امنیت الکترونیک و زیرشاخهٔ امنیت سایبری آن نه‌تنها ابزار تامین امنیت اقتصادی و اجتماعی است، بلکه شرط موفقیت در جنگ نیز به‌شمار می‌رود.

تجهیزات امنیت الکترونیک، موثرترین ابزار شناسایی اقدامات مشکوک تروریستی در جهان به شمار می‌روند.

ترور دانشمند هسته‌ای ایران، محسن فخری‌زاده در نزدیکی پایتخت، نگرانی حضور تروریست‌ها و جاسوسان مزدور در کشور را افزایش داد. تجاوز اخیر رژیم صهیونیستی به ایران، دامنهٔ صدمات تروریسم صهیونی و لزوم افزایش سطح عملیاتی و کاربردی امنیت الکترونیک کشور را بیش از پیش نمایان ساخت. این جاسوسان و تروریست‌های مزدور و خود فروخته پا را از ارایه اطلاعات موقعیت مقامات ارشد نظامی و دانشمندان هسته ایران فراتر گذاشته و حتی نسبت به مونتاژ پهپاد در کشور اقدام نمودند. در سال‌های گذشته اقدامات ارزشمندی برای افزایش سطح امنیت الکترونیک کشور صورت گرفته است، لکن اگر برخی کارشکنی‌ها نبود، این اقدامات می‌توانستند بسیار موثرتر باشند و در شرایط حساس همچون امروز، از نفوذ جاسوسان و انجام اقدامات تروریستی در کشور بهتر پیشگیری نمایند.

یکی از کاربردی‌ترین زیرمجموعه‌های امنیت الکترونیک، سامانه‌های نظارت تصویری هستند. تالیف «الزامات پدافند غیرعامل سامانه‌های نظارت تصویری برای اماکن مهم، حیاتی و حساس» توسط سازمان پدافند غیرعامل کشور، ابلاغ سند «الزامات پایش تصویری اماکن عمومی و صنوف» توسط پلیس نظارت بر اماکن عمومی فراجا و اجرای طرح ملی سپتام (سامانه پایش تصویری امامن) با هدف استانداردسازی سامانههای نظارت تصویری در اصناف و اماکن عمومی به همراه ارتقای سطح امنیت سایبری این سامانه‌ها و همچنین تالیف «استاندارد ملی امنیت الکترونیک سامانه نظارت تصویری» توسط سازمان فناوری اطلاعات ایران با همکاری سازمان ملی استاندارد ایران، اقدامات ارزشمندی بودند که در راستای ارتقای سطح امنیت الکترونیک کشور انجام شده است.

همچنین ارایه سرویس کامل نظارت تصویری به عنوان خدمت (VSaaS) توسط شرکت مخابرات ایران با نام‌تجاری «هوبان» و همچنین خدمت جامع همراه نظارت تصویری (mVSaaS) توسط شرکت جیرینگ با نام تجاری «شاهین» که تمامی فناوری هر دوی این اپراتورهای تصویری، بومی است، برخی از اقدامات ارزشمندی است که اکثر آن‌ها با برخی کارشکنی‌ها مواجه شده‌اند. در سال‌های گذشته، نرم‌افزارهای ضبط، مدیریت و آنالیز تصاویر با تکنولوژی هوش مصنوعی تصویری متعددی در کشور تولید شده است که برخی همچون «هزاربین» حتی از رقبای خارجی خود کارآمدتر هستند.

دوربین‌های مداربسته تحت شبکه با سفت‌افزار (Firmware) بومی تولید شده‌اند و حتی اولین ابزار امنیت شبکه ویژه سامانه نظارت تصویری نیز با نام «تتا» در کشور تولید شده است که حتی نمونه خارجی هم ندارد. این اقدامات موجب شده که حداقل در حوزهٔ نظارت تصویری، به جرات ایران جزو سه کشور برتر تکنولوژی در حوزهٔ نظارت تصویری ارزیابی گردد.

شاید قبل از برملا شدن سطح بدخواهی متجاوزان به میهن اسلامیمان، می‌شد برخی کارشکنی‌ها در توسعه تکنولوژی وطنی، الزامات و استانداردهای بومی در کشور را بجز خیانت به وطن، برخی مصلحت اندیشی به خطا و ضعف دانش و بینش ارزیابی نمود، لکن دیگر نمی‌توان تصویری جز خیانت برای هرگونه اقدامی که موجب کندی توسعه علمی و تخصصی در کشور، خصوصاً امنیت الکترونیک شود را پذیرفت.

به امید توسعهٔ هر چه بیشتر وطن عزیزمان، تا دیگر هیچ بیگانه‌ای جرات حتی خیال خام کوچکترین تجاوزی به ایران عزیزمان را نداشته باشد.

ماهواره‌های جاسوسی چشمان الکترومغناطیسی در آسمان

نویسنده:
مهسا بیگ‌رضایی

ماهواره‌های جاسوسی به‌عنوان ابزارهای پیشرفته در زمینه‌های نظامی، امنیتی و زیست‌محیطی، نقش حیاتی در نظارت و جمع‌آوری اطلاعات دارند. این ماهواره‌ها با بهره‌گیری از فناوری‌های الکترومغناطیسی مانند حسگرها و دوربین‌های پیشرفته، می‌توانند اطلاعات دقیق و ارزشمندی را از سطح زمین و فضای اطراف جمع‌آوری کنند.

ماهواره‌های جاسوسی برای پایش فعالیت‌های نظامی، شناسایی تهدیدها، نظارت بر تغییرات زیست‌محیطی و نظارت بر زیرساخت‌ها استفاده می‌شوند.

با این‌حال، استفاده از ماهواره‌های جاسوسی با چالش‌های فنی، حقوقی و اخلاقی همراه است، به‌ویژه در زمینهٔ حفاظت از حریم‌خصوصی و حفظ امنیت اطلاعات. در این مقاله، به معرفی انواع ماهواره‌های جاسوسی، فناوری‌های به‌کاررفته در آنها، و کاربردهای مختلف آنها پرداخته شده است. همچنین، چالش‌ها و محدودیت‌های موجود و چشم‌اندازهای آینده در این حوزه بررسی شده است.

ماهواره‌های جاسوسی با استفاده از پیشرفت‌های فناوری، همچنان در آینده نقش اساسی در حفظ امنیت جهانی و پیش‌بینی تهدیدها خواهند داشت.

این ماهواره‌ها با استفاده از فناوری‌های پیشرفته مانند تصویربرداری چندطیفی، رادارهای روزنهٔ مصنوعی[1](SAR) و سیستم‌های شنود الکترونیکی[2](ELINT)، توانایی شناسایی فعالیت‌های مشکوک، پایش تحرکات نظامی و ردیابی تغییرات زیست‌محیطی را دارند.

اهمیت ماهواره‌های جاسوسی در دنیای جدید نه‌تنها در نظارت بر تهدیدهای جهانی، بلکه در مدیریت بحران‌ها و کمک به تصمیم‌گیری‌های راهبردی نیز قابل توجه است.

پژوهش‌ها نشان می‌دهند که داده‌های ماهواره‌ای به افزایش دقت و سرعت در ارزیابی تهدیدها کمک می‌کنند[۱].

تاریخچهٔ توسعه و استفاده از ماهواره‌های جاسوسی

تاریخچهٔ ماهواره‌های جاسوسی به دوران جنگ سرد باز می‌گردد، زمانی که ایالات متحده و شوروی رقابت شدیدی در توسعهٔ فناوری‌های اطلاعاتی داشتند. پروژهٔ «کورونا» که در سال ۱۹۶۰ توسط ایالات متحده اجرت شد، اولین تلاش موفق برای استفاده از ماهواره‌های جاسوسی شناخته می‌شود. این پروژه امکان ثبت تصاویر باکیفیت از مناطق حساس جغرافیایی را فراهم کرد و تحولی اساسی در نظارت اطلاعاتی ایجاد نمود[۲].

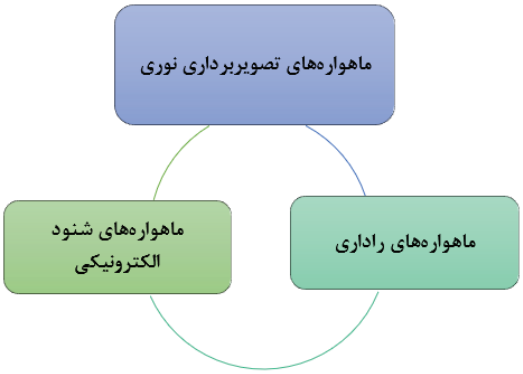
پس از آن، فناوری‌های مرتبط با ماهواره‌های جاسوسی به‌طور قابل توجهی پیشرفت کردند. رادارهای SAR امکان نظارت در شب و بر مناطق پوشیده از ابر را فراهم کردند و سیستم‌های تصویربرداری فروسرخ[۳] (مادون قرمز) (IR) به پایش مناطق با دمای بالا یا پایین کمک کردند. در دهه‌های اخیر، کشورهایی مانند چین، روسیه و اتحادیهٔ اروپا نیز در این زمینه سرمایه‌گذاری‌های کلانی انجام داده‌اند و سامانه‌های پیشرفته‌ای مانند ماهواره‌های Gaofen وLacrosse را توسعه داده‌اند[۳].

اهمیت راهبردی ماهواره‌ها در امنیت جهانی

ماهواره‌های جاسوسی نقش کلیدی در تضمین امنیت جهانی ایفا می‌کنند. این ابزارها توانایی نظارت مداوم را بر تهدیدهای بالقوه، از جمله پایگاه‌های نظامی، نقل و انتقالات تسلیحاتی و آزمایش‌های موشکی دارند. مثلاً، در جریان بحران‌های منطقه‌ای، داده‌های ماهواره‌ای به نیروهای نظامی امکان می‌دهند که تحرکات دشمن را پیش‌بینی کرده و اقدامات پیشگیرانه انجام دهند[۳]. علاوه بر کاربردهای نظامی، این ماهواره‌ها در پایش تغییرات زیست‌محیطی و مدیریت بلایای طبیعی نیز مؤثر هستند. برای مثال، در زمان وقوع زلزله یا سیل، تصاویر ماهواره‌ای به شناسایی مناطق آسیب‌دیده و برنامه‌ریزی برای امدادرسانی کمک می‌کنند[۴]. در مجموع، ماهواره‌های جاسوسی ابزارهایی راهبردی و چندمنظوره در خدمت امنیت ملی و جهانی هستند. با پیشرفت‌های جدید در هوش مصنوعی و یادگیری ماشین، انتظار می‌رود نقش این ماهواره‌ها در تحلیل داده‌ها و تصمیم‌سازی‌های راهبردی حتی بیشتر شود.

انواع ماهواره‌های جاسوسی

ماهواره‌های جاسوسی بر اساس نوع حسگرها و مأموریت‌های خود به چندین دسته تقسیم می‌شوند که هریک نقش مهمی در تأمین امنیت و جمع‌آوری اطلاعات بازی می‌کنند. در شکل ۲، سه نوع اصلی ماهواره‌های جاسوسی نشان داده شده است. در ادامه این سه نوع ماهوارهٔ جاسوسی معرفی و توضیح داده شده‌اند:



شکل ۱. انواع ماهواره‌های جاسوسی

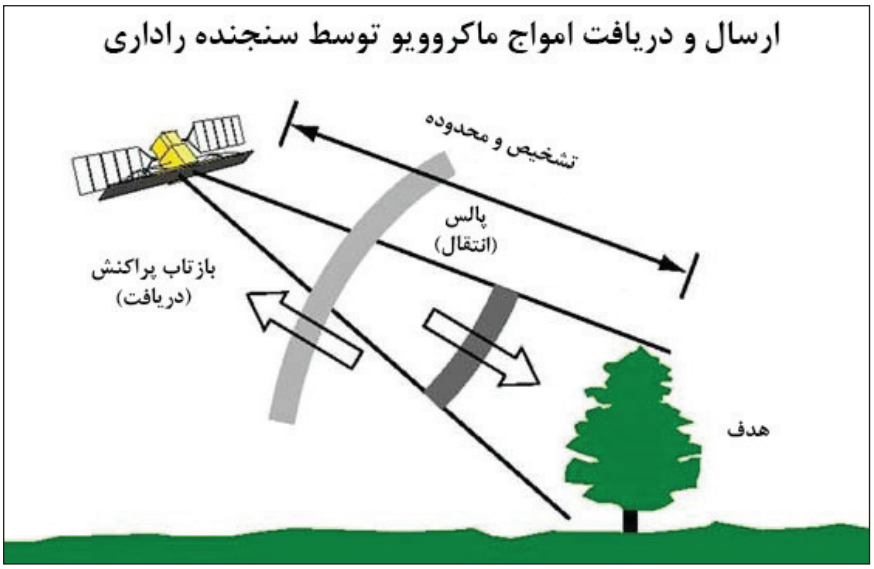
ماهواره‌های تصویربرداری نوری

ماهواره‌های تصویربرداری نوری با استفاده از دوربین‌های پیشرفته و حسگرهای تصویری تصاویری با کیفیت بالا از سطح زمین ثبت می‌کنند. این ماهواره‌ها برای نظارت بر پایگاه‌های نظامی، مرزها و فعالیت‌های مشکوک به‌کار می‌روند. شکل ۲ تصویری است که یک ماهوارهٔ جاسوسی از یک منطقهٔ حفاظت‌شده گرفته است. تصاویر ثبت‌شده توسط این ماهواره‌ها در زمان مناسب ارسال شده و با استفاده از فناوری‌های پردازش تصویر تحلیل می‌شوند. کیفیت این تصاویر به عواملی چون ارتفاع مدار و توانایی بزرگ‌نمایی بستگی دارد. مثلاً، ماهواره‌های جاسوسی جدید قادر به ثبت تصاویر با وضوح کمتر از ۳۰ سانتی‌متر هستند. این نوع ماهواره‌ها در مأموریت‌های بشردوستانه، مانند نظارت بر بلایای طبیعی و تغییرات زیست‌محیطی نیز کاربرد دارند.

شکل ۲. تصویر یک ماهوارهٔ جاسوسی امریکایی از یک منطقهٔ حفاظت‌شده

ماهواره‌های راداری

این دسته از ماهواره‌ها به رادارهای SAR مجهز هستند که قابلیت تصویربرداری در هر شرایط آب‌وهوایی و نوری را دارند. برخلاف ماهواره‌های نوری که برای تصویربرداری به نور خورشید نیاز دارند، ماهواره‌های راداری از امواج الکترومغناطیسی برای نقشه‌برداری و تصویربرداری استفاده‌می‌کنند. این ویژگی، آنها را به ابزاری بسیار کارآمد برای نظارت در شب و در مناطقی با شرایط آب‌وهوایی نامساعد تبدیل کرده‌است. به‌عنوان مثال، این ماهواره‌ها می‌توانند حرکت کشتی‌ها در دریا، تغییرات سطح زمین و حتی تردد خودروها را شناسایی کنند.
شکل ۳ عملکرد رادار SAR و شبیه‌سازی امواج راداری که از سطح زمین باز تابیده می‌شوند به تصویر کشیده است.



شکل۳. عملکرد رادار SAR و شبیه‌سازی امواج راداری که از سطح زمین باز تابیده می‌شوند.

ماهواره‌های شنود الکترونیکی

ماهواره‌های شنود الکترونیکی برای جمع‌آوری سیگنال‌های رادیویی و مخابراتی طراحی شده‌اند این ماهواره‌ها قادر به ردیابی امواج منتشرشده از رادارها، شبکه‌های مخابراتی و حتی سیستم‌های ارتباطی نظامی هستند.
هدف اصلی این ماهواره‌ها شناسایی و تحلیل الگوهای مخابراتی و تعیین مکان دقیق فرستنده‌ها است.
این اطلاعات معمولا برای مقاصد نظامی، مانند شناسایی پایگاه‌های دشمن یا استراق سمع ارتباطات حساس استفاده می‌شوند. پیشرفت‌های اخیر در هوش مصنوعی باعث بهبود توانایی این ماهواره‌ها در فیلتر و تحلیل داده‌های حجیم شده است.

جدول۱. مقایسهٔ انواع ماهواره‌های جاسوسی و کاربردهای آنها

نوع ماهواره	ویژگی‌ها	کاربردها
ماهواره‌های تصویربرداری نوری	• استفاده از دوربین‌های نوری با وضوح زیاد • وابستگی به شرایط آب‌وهوایی و نور روز	• پایش فعالیت‌های نظامی • شناسایی تغییرات محیطی • نظارت بر زیرساخت‌های حیاتی
ماهواره‌های راداری	استفاده از فناوری رادار برای تصویربرداری در تمام شرایط آب‌وهوایی و شبانه‌روز	• نظارت بر مناطق ابری یا تاریک • پایش حرکات زمینی و دریایی • کشف فعالیت‌های مخفیانه
ماهواره‌های شنود الکترونیکی	• رهگیری سیگنال‌های مخابراتی و الکترونیکی • امکان شناسایی منابع رادیویی مختلف	• شنود ارتباطات نظامی و دیپلماتیک • شناسایی امواج رادیویی از مناطق خاص • نظارت سایبری

فناوری‌های به‌کاررفته در ماهواره‌های جاسوسی

فناوری‌های به‌کاررفته در ماهواره‌های جاسوسی به سه دسته تقسیم می‌شوند.این سه دسته عبارت‌اند از: حسگرها و تجهیزات پیشرفته، سیستم‌های پردازش داده و فناوری‌های ارتباطی.

۱.حسگرها و تجهیزات پیشرفته

ماهواره‌های جاسوسی به فناوری‌های پیشرفته‌ای مجهز هستند که امکان نظارت دقیق بر فعالیت‌های زمینی را فراهم می‌کنند. حسگرهای نوری یکی از مهم‌ترین ابزارها در این ماهواره‌ها هستند که از تصویربرداری در محدودهٔ نور مرئی و فروسرخ بهره می‌برند. این حسگرها قادر به ثبت تصاویر با وضوح بالا و تحلیل جزئیاتی مانند تغییرات زیست‌محیطی و ساختاری هستند. برای مثال، ماهواره‌های KH-11 ایالات‌متحده، از فناوری نوری پیشرفته‌ای بهره می‌برند که می‌توانند تغییرات کوچک در زیرساخت‌های نظامی را شناسایی کنند. در کنار این، حسگرهای راداری مانندSAR امکان تصویربرداری دقیق در شرایط نامساعد آب‌وهوایی یا شب را فراهم می‌کنند. ماهواره‌هایRADARSAT-2 و TerraSAR-X نمونه‌هایی از این فناوری هستند که برای شناسایی فعالیت‌های نظامی یا تغییرات زمین استفاده می‌شوند. همچنین، حسگرهای حرارتی با ثبت تغییرات دمایی، فعالیت‌های مخفی انسانی و نظامی را شناسایی می‌کنند. مثلاً، این فناوری می‌تواند منابع گرمایی در زیرساخت‌های زیرزمینی یا جنگل را ردیابی کند. به‌طور مثال، ماهواره‌ی RADARSAT-2 کانادا با این فناوری توانسته است در شناسایی فعالیت‌های زمین‌شناسی و نظامی موفق عمل کند.

حسگرهای حرارتی نیز برای شناسایی تغییرات دمایی و فعالیت‌های زیرزمینی، مانند ردیابی خودروهای نظامی یا پایگاه‌های مخفی، استفاده می‌شوند.

جدول ۲. بررسی فناوری‌های به‌کاررفته در ماهواره‌های جاسوسی

فناوری	ویژگی‌ها و قابلیت‌ها	مزایا	کاربردها	نمونه ماهواره‌ها
حسگرها و تجهیزات پیشرفته	• تصویربرداری نوری (نور مرئی و فروسرخ) • SAR • حسگرهای حرارتی	• امکان ثبت تصاویر با وضوح بالا • عملکرد در شرایط آب‌وهوایی نامساعد • شناسایی تغییرات دمایی و زیست‌محیطی	• نظارت بر فعالیت‌های نظامی • ردیابی تغییرات ساختاری • شناسایی تهدیدهای مخفی در زیرساخت‌های زیرزمینی و جنگلی	• KH-11 • RADARSAT-2 • Terra SAR-X
سیستم‌های پردازش داده	• استفاده از هوش مصنوعی و یادگیری عمیق • تحلیل بی‌درنگ داده‌ها • توانایی پردازش تصاویر چندطیفی	• کاهش حجم داده‌های خام • استخراج اطلاعات دقیق • تشخیص الگوهای پنهان	• تحلیل زیست‌محیطی • شناسایی تهدیدهای فوری • مدیریت منابع طبیعی و زیرساخت‌ها	WorldView-3
فناوری‌های ارتباطی	-ارتباطات لیزری -رمزنگاری پیشرفته - انتقال داده با سرعت بالا	-امنیت بسیار بالا در انتقال داده‌ها -کاهش تاخیر در ارتباطات -مقاومت در برابر حملات سایبری	-انتقال سریع اطلاعات حساس -ارتباط ایمن با ایستگاه‌های زمینی -استفاده در عملیات نظامی و امنیتی	ماهواره‌های نظامی مدرن برنامه‌های ارتباط کوانتومی

۲. سیستم‌های پردازش داده

پس از جمع‌آوری داده‌ها، سیستم‌های پردازش داده وارد عمل می‌شوند. ماهواره‌های جاسوسی به سیستم‌های پردازش داده‌ای مجهز هستند که حجم عظیمی از اطلاعات را تحلیل و پردازش می‌کنند. این سیستم‌ها از الگوریتم‌های پیشرفتهٔ هوش مصنوعی و یادگیری عمیق بهره می‌برند تا اطلاعات خام را به داده‌های قابل فهم تبدیل کنند. برای مثال، ماهواره‌های WorldView-3 با پردازش تصاویر چندطیفی، تحلیل دقیقی از محیط ارائه می‌دهند که می‌تواند برای نظارت نظامی یا تحلیل منابع طبیعی استفاده شود. فناوری‌های پیشرفتهٔ پردازش، همچنین قابلیت‌های تحلیل بی‌درنگ را برای شناسایی تهدیدهای امنیتی فراهم می‌کنند.

۳.فناوری‌های ارتباطی

یکی از چالش‌های اصلی ماهواره‌های جاسوسی، انتقال ایمن و سریع داده‌های جمع‌آوری‌شده به مراکز زمینی است. این ماهواره‌ها از فناوری‌هایی مانند لیزرهای ارتباطی و ارتباطات رمزنگاری‌شده استفاده می‌کنند. این فناوری‌ها علاوه بر سرعت بالا، امنیت داده‌ها را در برابر حملات سایبری تضمین می‌کنند. برای مثال، ماهواره‌های جاسوسیِ جدید از سیستم‌های ارتباطی لیزری بهره می‌برند که انتقال داده‌ها را با سرعت چند گیگابیت بر ثانیه امکان‌پذیر می‌کند. همچنین، فناوری‌های ارتباطی جدید مانند ارتباطات کوانتومی در حالِ توسعه هستند که احتمال نفوذ به داده‌ها را تقریباً از بین می‌برند. فناوری‌های ارتباطی، وظیفهٔ انتقال سریع و امن اطلاعات را بر عهده دارند. فناوری ارتباطات لیزری یکی از جدیدترین نوآوری‌ها در این حوزه است که با سرعت بالا و امنیت پیشرفته، داده‌ها را به ایستگاه‌های زمینی منتقل می‌کند. پروژهٔ LCRD[۴] ناسا، نمونه‌ای از این فناوری است که انتقال داده را به سطح جدیدی ارتقا داده است. همچنین، سیستم‌های رمزنگاری پیشرفته و مقاوم در برابر نویز، امنیت اطلاعات حساس را تضمین می‌کنند و امکان استفاده از این داده‌ها را در عملیات امنیتی و نظامی فراهم می‌آورند. این فناوری‌ها، در کنار یکدیگر، ماهواره‌های جاسوسی را به ابزارهایی حیاتی در امنیت جهانی، مدیریت بحران‌ها و نظارت بر تغییرات محیطی تبدیل کرده‌اند. پیشرفت روزافزون در این حوزه، کاربردهای جدیدی را در زمینه‌های نظامی و غیرنظامی فراهم کرده و اهمیت آنها را دوچندان کرده است. در جدول ۲ فناوری‌های به‌کاررفته در ماهواره‌های جاسوسی، مزایا و کاربردهای آنها و نمونهٔ ماهواره‌هایی که از این

کاربردهای ماهواره‌های جاسوسی

در شکل ۵، چهار مورد از کاربردهای ماهواره‌های جاسوسی نشان داده شده است.

۱. نظارت نظامی

ماهواره‌های جاسوسی در حوزهٔ نظامی برای نظارت بر تحرکات نیروها، پایگاه‌های نظامی و فعالیت‌های تسلیحاتی غیروطنی به‌کار می‌روند. حسگرهای تصویربرداری با وضوح بالا و سیستم‌های راداری فعال، امکان تصویربرداری دقیق از اهداف زمینی و هوایی را در هر شرایط آب‌وهوایی فراهم می‌کنند. ماهواره‌های Keyhole [۵] که توسط ایالات متحده توسعه یافته‌اند، از فناوری‌های نوری و فروسرخ برای شناسایی تحرکات نیروهای دشمن استفاده می‌کنند. این قابلیت ارتش را قادر می‌سازد که با آگاهی دقیق از موقعیت دشمن، تصمیمات راهبردی اتخاذ کند و واکنش‌های به‌موقع نشان دهد. ایالات متحده از ماهواره‌های جاسوسی برای شناسایی فعالیت‌های هسته‌ای در کرهٔ شمالی استفاده کرده است.

این ماهواره‌ها قادرند تصاویر با دقت بالا از تأسیسات نظامی و آزمایشگاه‌های هسته‌ای ثبت کنند و تحرکات مشکوک را به‌دقت شناسایی کنند.

۲. مقابله با تروریسم و فعالیت‌های مخفیانه (کاربردهای امنیتی و اطلاعاتی)

ماهواره‌های جاسوسی در حوزهٔ امنیت‌واطلاعات برای شناسایی تهدیدهای تروریستی، پیگیری شبکه‌های قاچاق و جمع‌آوری اطلاعات حساس به‌کار می‌روند. این ماهواره‌ها می‌توانند فعالیت‌های غیرقانونی را در مناطق دورافتاده و دشوار شناسایی کنند.

به‌عنوان نمونه، ماهواره‌ها SIGINT[۵] که برای شنود و رهگیری ارتباطات الکترونیکی طراحی شده‌اند، به‌ویژه در شناسایی ارتباطات تروریستی و شبکه‌های مجرمانه مؤثر هستند[۷]. همچنین این فناوری‌ها نقش مهمی در نظارت بر مرزها و تأمین امنیت ملی دارند.

شکل ۴. کاربردهای ماهواره‌های جاسوسی

۳. پایش تغییرات زیست‌محیطی

یکی دیگر از کاربردهای اساسی ماهواره‌های جاسوسی، نظارت بر تغییرات زیست‌محیطی است. این ماهواره‌ها می‌توانند جنگل‌زدایی، تغییرات سطح دریا، ذوب یخ‌های قطبی و آلودگی اقیانوس‌ها را رصد کنند. برای مثال، ماهواره‌های Sentinel-1 که توسط آژانس فضایی اروپا (ESA) مدیریت می‌شوند، از فناوری رادار برای پایش تغییرات سطح زمین و مدیریت بلایای طبیعی بهره می‌برند[۶]، [۱]. داده‌های به‌دست‌آمده از این ماهواره‌ها به دانشمندان کمک می‌کنند اثرات تغییرات اقلیمی را بهتر درک کنند و سیاست‌های زیست‌محیطی مؤثری تدوین نمایند.

۴. مدیریت منابع طبیعی و کشاورزی

ماهواره‌های جاسوسی می‌توانند برای نظارت بر منابع طبیعی مانند جنگل‌ها، معادن و اراضی کشاورزی استفاده شوند. به‌عنوان مثال، این ماهواره‌ها می‌توانند به دولت‌ها و سازمان‌ها کمک کنند تا تغییر در پوشش گیاهی، جنگل‌زدایی و تغییر در زمین‌های کشاورزی را شناسایی کنند. ماهواره‌هایی مانند Sentinel از برنامهٔ کوپرنیکوس اتحادیهٔ اروپا، برای نظارت بر تغییرات زمین و پوشش گیاهی به‌ویژه در کشورهایی که با بحران‌های کشاورزی و زیست‌محیطی مواجه هستند، استفاده می‌کنند.

ماهواره‌های جاسوسی، با کاربردهای گسترده در نظارت نظامی، مدیریت زیست‌محیطی و امنیت اطلاعاتی، به‌عنوان ابزاری حیاتی در مدیریت چالش‌های جهانی شناخته می‌شوند. از فناوری‌های تصویربرداری پیشرفته تا سیستم‌های پردازش داده‌های راداری و شنود الکترونیکی، این ماهواره‌ها نقشی کلیدی در ارتقای امنیت و پایداری جهانی ایفا می‌کنند. اطلاعات به‌دست‌آمده از این فناوری‌ها نه‌تنها برای اهداف نظامی، بلکه برای حل مشکلات زیست‌محیطی و مدیریت بحران‌های بین‌المللی نیز حیاتی است.

چالش‌ها و محدودیت‌های ماهواره‌های جاسوسی

ماهواره‌های جاسوسی با وجود پیشرفت‌های چشمگیر، با چالش‌ها و محدودیت‌هایی در زمینه‌های فنی، حقوقی، اخلاقی و امنیتی مواجه هستند. این چالش‌ها بر نحوهٔ استفاده از این فناوری‌ها و کارایی آنها تأثیر می‌گذارند و بررسی دقیق آنها برای بهبود کاربری این سیستم‌ها ضروری است. مهم‌ترین چالش‌ها و محدودیت‌های این نوع سیستم‌ها از این قرارند:

• مسائل فنی و فناورانه:

ماهواره‌های جاسوسی به فناوری‌های پیشرفته‌ای مانند حسگرهای دقیق، پردازش سریع داده و سامانه‌های ارتباطی ایمن وابسته‌اند. اما محدودیت‌های فنی‌ای همچون توان محدود باتری، عمر کوتاه تجهیزات و چالش‌های مربوط به پردازش حجم عظیمی از داده‌های تولیدشده، مشکلات قابل‌توجهی ایجاد می‌کند. برای مثال، داده‌های تولیدشده توسط ماهواره‌های سنجش از دور مانند Landsat، نیازمند پردازش سریع و پیچیده‌ای هستند که به سخت‌افزارهای پیشرفته و الگوریتم‌های هوش مصنوعی نیاز دارد[۸]. علاوه بر این، تعمیر و به‌روزرسانی این ماهواره‌ها در فضا بسیار دشوار و پرهزینه است.

• ملاحظات حقوقی و اخلاقی:

استفاده از ماهواره‌های جاسوسی نگرانی‌های حقوقی و اخلاقی متعددی ایجاد می‌کند. این ماهواره‌ها با جمع‌آوری اطلاعات از مناطق مختلف جهان ممکن است حریم خصوصی افراد و دولت‌ها را نقض کنند. قوانین بین‌المللی، همچون «معاهدهٔ فضای ماورای جو»[۶]، به‌طور مشخص استفادهٔ نظامی از فضا را محدود می‌کند؛ اما همچنان اجرای این قوانین و نظارت بر فعالیت کشورها چالش‌برانگیز است[۹]. از نظر اخلاقی، نظارت بدون رضایت افراد یا دولت‌ها به مسئله‌ای مناقشه‌برانگیز تبدیل شده است و لازم است توازنی میان امنیت و حریم خصوصی ایجاد شود.

• تهدیدهای امنیتی و مقابله با آنها:

ماهواره‌های جاسوسی خود اهداف بالقوهٔ حملات سایبری و فیزیکی هستند. بازیگران دولتی و غیردولتی می‌توانند با نفوذ به سیستم‌های ماهواره‌ای، اطلاعات حساس را به سرقت ببرند یا سیستم‌های ارتباطی را مختل کنند. علاوه بر این، توسعهٔ فناوری‌های ضدماهواره‌ای، مانند موشک‌های ضدماهواره‌ای، تهدیدی جدی برای عملکرد این سیستم‌ها محسوب می‌شود.

برای مثال، چین در سال ۲۰۰۷ یک آزمایش موفق ضدماهواره‌ای انجام داد که نگرانی‌های زیادی راجع به امنیت ماهواره‌ها ایجاد کرد[۹]. استفاده از فناوری‌های رمزگذاری پیشرفته و ایجاد شبکه‌های مقاوم در برابر حملات سایبری از راهکارهای پیشنهادی برای مقابله با این تهدیدهاست.

با وجود پتانسیل‌های بی‌نظیر ماهواره‌های جاسوسی، این ابزارها با چالش‌های فنی، حقوقی و امنیتی‌ای مواجه هستند که مانع از بهره‌برداری بهینه از آنها می‌شود. از مسائل مرتبط با تعمیر و به‌روزرسانی این سیستم‌ها گرفته تا دغدغه‌های اخلاقی و تهدیدهای امنیتی، همه نشان‌دهندهٔ نیاز به تحقیق و توسعهٔ بیشتر در این حوزه است ارتقای فناوری‌ها، تدوین قوانین بین‌المللی جامع‌تر و ایجاد راهکارهای امنیتی نوآورانه می‌تواند این چالش‌ها را تا حد زیادی کاهش دهد.

تحولات اخیر و روندهای آینده در ماهواره‌های جاسوسی

۱. پیشرفت‌های فناوری در پنج سال گذشته

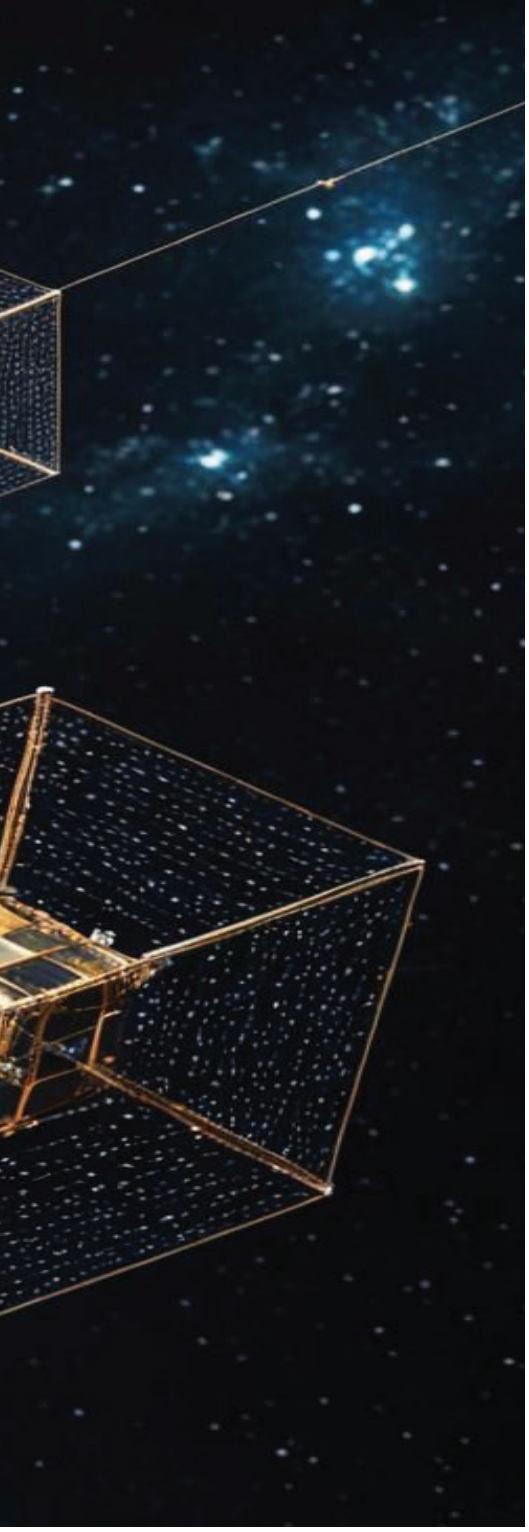
در پنج سال اخیر، فناوری‌های مرتبط با ماهواره‌های جاسوسی با سرعت بی‌سابقه‌ای پیشرفت کرده‌اند. از جملهٔ این پیشرفت‌ها، توسعهٔ حسگرهای با وضوح فوق‌العاده بالاست که امکان تصویربرداری با دقتی بی‌نظیر از سطح زمین را فراهم می‌کند.

برای مثال، ماهواره‌های مجهز به فناوری تصویربرداری هایپراسپکترال و مولتی‌اسپکترال اکنون قادر به تشخیص جزئی‌ترین تغییرات در پوشش گیاهی، خاک و آب هستند.

همچنین فناوری‌های پردازش دادهٔ مبتنی بر هوش مصنوعی (AI) و یادگیری ماشین، امکان تحلیل سریع حجم وسیعی از داده‌ها را فراهم کرده‌اند. نمونه‌ای از این پیشرفت‌ها، پروژه‌های مرتبط با شرکت‌های خصوصی مانند Planet Labs و Maxar Technologies است که توانسته‌اند خدمات پیشرفته‌ای در حوزهٔ نظارت محیطی و امنیتی ارائه دهند[۱۰].

از طرف دیگر، استفاده از رادارهای SAR که قابلیت تصویربرداری در شرایط نامساعد جوی یا در شب دارند، به‌ویژه در ماهواره‌های جدیدی مانند Sentinel-1 و ICEYE بسیار گسترش یافته‌است.

این فناوری‌ها نقش مهمی در نظارت نظامی و پایش تغییرات اقلیمی ایفا کرده‌اند.



۲. پروژه‌ها و برنامه‌های در دست اجرا

یکی از مهم‌ترین پروژه‌های جدید برنامهٔ NOR[۷] ایالات متحده است که در حال توسعهٔ نسل جدیدی از ماهواره‌های نظارتی با قابلیت‌های چندمنظوره است. این ماهواره‌ها می‌توانند به‌طور همزمان داده‌های تصویری، راداری و شنود الکترونیکی را جمع‌آوری کنند. از دیگر پروژه‌های شاخص، می‌توان به Gaofen Project چین اشاره کرد که هدف آن ایجاد شبکه‌ای گسترده از ماهواره‌های جاسوسی و نظارتی برای پوشش جهانی است. این ماهواره‌ها برای نظارت بر فعالیت‌های نظامی، مدیریت بحران‌های طبیعی و نظارت بر پروژه‌های زیربنایی، به حسگرهای پیشرفته مجهز شده‌اند. اتحادیهٔ اروپا برنامهٔ Copernicus را توسعه داده است که با تمرکز بر داده‌های زیست‌محیطی و تغییرات اقلیمی، امکان تحلیل‌های دقیق‌تر را فراهم می‌آورد. در کنار این پروژه‌ها، برنامه‌های مشابهی توسط شرکت‌های خصوصی مانند SpaceX و Amazon نیز برای توسعهٔ شبکه‌های ماهواره‌ای در حال اجرا هستند.

۳. پیش‌بینی‌ها و چشم‌اندازهای آینده

چشم‌انداز آیندهٔ ماهواره‌های جاسوسی به‌شدت به فناوری‌های پیشرفته وابسته است. یکی از مهم‌ترین روندها، استفاده از فناوری‌های کوانتومی در ارتباطات ماهواره‌ای است که امنیت داده‌ها را در برابر تهدیدهای سایبری تضمین می‌کند. همچنین، پیشرفت در مینیاتوری‌کردن ماهواره‌ها (ماهواره‌های CubeSats) امکان استفاده از ماهواره‌های کوچک‌تر و کم‌هزینه‌تر را فراهم کرده است که می‌توانند در شبکه‌های بزرگ برای پوشش جهانی استفاده شوند[۱۱]. شکل۶ تصویری انتزاعی از ماهواره‌های کوچکِ CubeSats را نشان می‌دهد که در حالِ ایجاد شبکه‌ای از ارتباطات فضایی هستند. آیندهٔ ماهواره‌های جاسوسی به‌سمت هوشمندسازی کامل و استفاده از فناوری‌های پیشرفته‌ای مانند AI، یادگیری ماشین و رایانش کوانتومی حرکت می‌کند. پیش‌بینی می‌شود که تا سال ۲۰۳۰، ماهواره‌های جاسوسی به قابلیت‌هایی نظیر تحلیل داده‌های هم‌زمان در فضا، تصویربرداری فوق دقیق با فناوری‌های کوانتومی، و استفاده از حسگرهای فوق سبک برای کاهش هزینه‌های پرتاب دست‌یابند[۸]و[۱۲].

همچنین، همکاری‌های بین‌المللی برای مقابله با تهدیدهای جهانی، مانند تغییرات اقلیمی و امنیت سایبری، نقش کلیدی در استفاده از این فناوری‌ها خواهد داشت.

در مجموع، تحولات اخیر و پیشرفت‌های آینده در زمینهٔ ماهواره‌های جاسوسی، نقش این فناوری‌ها را به‌عنوان ابزارهای کلیدی برای امنیت جهانی، مدیریت بحران و توسعهٔ پایدار تقویت می‌کند.

نتیجه‌گیری

ماهواره‌های جاسوسی از ابزارهای حیاتی در عرصهٔ امنیت جهانی و نظارت‌های مختلف در دنیای امروز هستند. این ماهواره‌ها با استفاده از فناوری‌های پیشرفته مانند حسگرها، رادارها و سیستم‌های پردازش داده، امکان جمع‌آوری اطلاعات دقیق و فوری از سطح زمین و فضای اطراف را فراهم می‌کنند. طی سال‌های اخیر، پیشرفت‌های چشمگیری در زمینه‌های تصویربرداری نوری، راداری و شنود الکترونیکی مشاهده شده است که باعث افزایش دقت، کارایی و کاربردهای این ماهواره‌ها در حوزه‌های مختلف شده است.

از یک سو، ماهواره‌های جاسوسی در نظارت‌های نظامی و امنیتی نقش اساسی ایفا می‌کنند و به کشورهای مختلف امکان می‌دهند تا از تهدیدهای بالقوه و فعالیت‌های مشکوک مطلع شوند. از سوی دیگر، این ماهواره‌ها در پایش تغییرات زیست‌محیطی، مدیریت بلایای طبیعی، نظارت بر تغییرات اقلیمی و بررسی وضعیت منابع طبیعی کاربرد دارند. با این حال، توسعهٔ ماهواره‌های جاسوسی با چالش‌های مختلفی نیز مواجه است. مسائل فنی و فناورانه، محدودیت‌های منابع و تهدیدهای امنیتی از جمله مسائلی هستند که تأثیر مستقیمی بر کارایی و استفاده از این فناوری‌ها دارند. همچنین ملاحظات حقوقی و اخلاقی در خصوص حفظ حریم خصوصی و استفاده از اطلاعات جمع‌آوری‌شده، از موضوعات حیاتی است که باید در نظر گرفته شود. در نهایت، با توجه به پیشرفت‌های اخیر در فناوری‌های ماهواره‌ای و روندهای آینده در این حوزه، می‌توان گفت که ماهواره‌های جاسوسی در آینده نقش بیشتری در تأمین امنیت، پیشگیری از تهدیدها و بهبود کیفیت زندگی انسان‌ها خواهند داشت. این ابزارها همچنان در حال تکامل هستند و تأثیراتشان بر جامعه و امنیت جهانی به‌طور مستمر گسترش خواهد یافت.

1.Synthetic Aperture Radar
2.Electronic Eavesdropping Systems
3.Infrared radiation
4.Laser Communication Relay Demonstration
5. Signal Intelligence
6.Outer Space Treaty
7.National Reconnaissance Office

شکل ۵. تصویر انتزاعی از ماهواره‌های کوچک CubeSats در حال ایجاد شبکه‌ای از ارتباطات فضایی

منابع

1. Smith, J. (2022). Synthetic Aperture Radar in Modern Satellite Systems. IEEE Transactions on Geoscience and Remote Sensing, 1195-1182 ,(5)60.
2. Jones, M., Liu, Q., & Patel, R. (2020). Historical perspectives on spy satellites: From Corona to modern systems. Space Policy, ,49 105-95.
3. Zhang, Z., Wang, Y., & Chen, X. (2021). The role of satellite surveillance in modern military strategy. Defense Technology Review, 39-25 ,(2)14.
4. Huang, R., Zhao, L., & Sun, Q. (2020). Applications of satellite imagery in disaster management: A case study. Earth Observation Journal, 17-1 ,(1)9.
5. Wilson, T., & Roberts, J. (2021). Military Applications of Spy Satellites. Journal of Military Studies, 27-15 ,(2)34.
6. Patel, R., & Kumar, V. (2023). Evolution of Electronic Intelligence Satellites: Current Trends and Future Perspectives. Journal of Military Intelligence, 62-45 ,(3)12.
7. Jones, M., Liu, Q., & Patel, R. (2020). Historical perspectives on spy satellites: From Corona to modern systems. Space Policy, ,49 105-95.
8. Brown, T., Smith, R., & Johnson, L. (2021). Technical Challenges in Satellite Operations. Journal of Space Technology, 92-78 ,(4)38.
9. Harrison, J., & Clark, M. (2019). Legal and Ethical Issues in Spy Satellite Usage. International Law Journal, 49-34 ,(2)15.
10. Lee, K. (2021). Security Challenges in Space Technology. Aerospace Security Journal, 71-56 ,(3)42.
11. Johnson, T., & Patel, S. (2023). The future of quantum communications in satellite systems. International Journal of Space Innovation, 50-34 ,(2)12.

مروری بر امنیت در اینترنت اشیا

نویسنده:
رسمیه پروانه

اینترنت اشیا به شبکه‌ای از دستگاه‌ها و سیستم‌های متصل به اینترنت اطلاق می‌شود که قادر به جمع‌آوری، ارسال و دریافت داده‌ها به‌صورت خودکار هستند. رشد سریع اینترنت اشیا در سالهای اخیر همچنان که فرصت‌های بسیاری را در زمینه‌های مختلف ایجاد کرده ، موجب چالش‌ها و مشکلات جدیدی نیز شده است. یکی از مهم‌ترینِ این چالش‌ها، مسائل امنیتی مرتبط با اینترنت اشیاست.

دستگاه‌های«اینترنت اشیا»[1] (IoT) معمولا دارای منابع محدود از نظر پردازشی و ذخیره‌سازی هستند که ممکن است موجب ضعف در پیاده‌سازی تدابیر امنیتیِ مناسب شوند. علاوه بر این، این دستگاه‌ها غالباً بدون نظارت مداوم و به‌روزرسانی‌های منظم به‌کار می‌روند. در نتیجه، دستگاه‌های اینترنت اشیا به هدفی جذاب برای حملات سایبری تبدیل شده‌اند که تهدیدهایی مانند نفوذ به سیستم‌ها، سرقت داده‌ها و حملات مبتنی بر دستکاری دستگاه‌ها را شامل می‌شود.
با توجه به چالش‌های امنیتی فوق، استانداردهای امنیتی خاصی برای اینترنت اشیا طراحی و پیاده‌سازی شده است. این استانداردها شامل مواردی همچون رمزنگاری[2] داده، احراز هویت دستگاه، نظارت بر رفتار دستگاه، و به‌روزرسانی‌های نرم‌افزاری منظم و پروتکل‌هایی برای تامین امنیت داده و حفظ یکپارچگی اطلاعات هستند. هدف این مقاله معرفی مفصل چنین مباحثی است.اینترنت به‌سرعت در حال گسترش است و تقریباً در تمامی حوزه‌های زندگی بشر نفوذ کرده است: از لوازم خانگی هوشمند مانند یخچال‌ها و ترموستات‌ها تا کاربردهای پیچیده‌تر در صنعت، بهداشت، حمل‌ونقل و کشاورزی. در تمام این کاربردها، اینترنت اشیا به بهبود کارایی، افزایش راحتی و کاهش هزینه‌ها کمک کرده است[1]. اینترنت اشیا قادر است تا محیط زندگی و کاری را هوشمندتر و کارآمدتر کند.
پیش‌بینی‌ها نشان می‌دهند که تعداد دستگاه‌های متصل به اینترنت تا سال ۲۰۲۵ به بیش از ۷۵ میلیارد دستگاه خواهد رسید، که شامل طیف وسیعی از حسگرها، دستگاه‌های پوشیدنی، ماشین‌آلات صنعتی و حتی دستگاه‌های پزشکی می‌شود[2]. این گسترش سریع باعث شده تا IoT یکی از داغ‌ترین مباحث تحقیقاتی و فناوری در چند سال اخیر باشد و به‌ویژه در زمینه‌های جدیدی همچون شهرهای هوشمند و کشاورزی دقیق تحولاتی عظیم ایجاد کرده است. به‌عنوان مثال، در حوزه‌های بهداشت، دستگاه‌های پزشکی متصل به اینترنت می‌توانند داده‌های حیاتی بیماران را بلادرنگ به پزشکان ارسال کنند و تصمیم‌گیری‌ها را بهبود ببخشند[3].
اگرچه اینترنت اشیا پتانسیل‌های عظیمی برای بهبود کیفیت زندگی بشر دارد، اما با گسترش آن، چالش‌های امنیتی و حریم خصوصی به یک نگرانی اساسی تبدیل شده‌اند. امنیت در IoT به یکی از مهم‌ترین دغدغه‌های جامعهٔ علمی و صنعتی تبدیل شده است. به این دلیل که بسیاری

از دستگاه‌های IoT دائم به اینترنت متصل هستند و غالباً قابلیت‌های امنیتی محدودی دارند یا هیچ قابلیت امنیتی ندارند. به‌علاوه، بسیاری از این دستگاه‌ها به‌طور خودکار و بدون نظارت مستقیم در حال کار هستند که می‌تواند باعث بروز آسیب‌پذیری‌های امنیتی بزرگ در آنها شود[۴].

دستگاه‌های IoT معمولا از سیستم‌عامل‌ها و سخت‌افزارهایی استفاده می‌کنند که محدودیت‌هایی از نظر منابع دارند. این مسئله باعث می‌شود که پیاده‌سازی تدابیر امنیتی پیشرفته مانند رمزنگاری پیچیده یا سیستم‌های تشخیص نفوذ دشوار باشد. علاوه بر این، این دستگاه‌ها به‌طور منظم به‌روزرسانی نمی‌شوند که این امر موجب افزایش احتمال نفوذ به سیستم‌ها و سرقت داده‌ها می‌شود[۵].

به‌طور خاص، امنیت در IoT می‌تواند در چند سطح مختلف تهدید شود:

۱.حملات سایبری: شامل حملات گسترده همچون حملات DDoS[۳] است که می‌تواند به‌راحتی در شبکه‌های IoT اجرا شود[۶].

۲. سرقت داده‌ها و حریم خصوصی دستگاه‌های IoT داده‌های حساسی همچون موقعیت جغرافیایی، وضعیت سلامت یا عادات مصرفی کاربران را جمع‌آوری می‌کنند. این داده‌ها اگر به‌درستی محافظت نشوند، می‌توانند به ابزارهایی برای نقض حریم خصوصی تبدیل شوند[۳].

۳. نقاط ضعف در پروتکل‌ها و معماری بسیاری از دستگاه‌های IoT از پروتکل‌های قدیمی و ناکارآمد برای ارتباطات استفاده می‌کنند که ممکن است در برابر حملات مقاوم نباشند [۷].

یکی از دلایل اصلی اهمیت امنیت در IoT، وابستگی روزافزون به این فناوری در زیرساخت‌های حیاتی است. به‌عنوان مثال، در صنعت تولید یا سیستم‌های حمل‌ونقل هوشمند، حملات سایبری می‌توانند باعث خرابی‌های گسترده و حتی ایجاد خطرات جانی شوند. همچنین، در حوزهٔ بهداشت، دستگاه‌های پزشکی متصل می‌توانند تحت حملات قرار گیرند و این حملات می‌توانند سلامت بیماران را به خطر بیندازند [۳].

از سوی دیگر، امنیت در IoT نه‌تنها مربوط به محافظت از دستگاه‌ها و داده‌هاست، بلکه به حفاظت از حریم خصوصی کاربران نیز مرتبط است. به دلیل ارتباط مداوم دستگاه‌ها با شبکه، اطلاعات جمع‌آوری‌شده می‌توانند برای پیگیری رفتارهای شخصی کاربران استفاده شوند، که در صورت عدم وجود تدابیر امنیتی، خطرات جدی برای حریم خصوصی افراد ایجاد خواهدکرد [۷]

با توجه به ویژگی‌های خاص دستگاه‌های IoT، چالش‌های امنیتی این حوزه پیچیده‌تر از سایر حوزه‌هاست. از جملهٔ این چالش‌ها می‌توان به موارد زیر اشاره کرد:

۱. حجم و تنوع دستگاه‌ها:
دستگاه‌های IoT از انواع مختلف سخت‌افزارها و سیستم‌عامل‌ها استفاده می‌کنند، که به‌ویژه در محیط‌های بزرگ و پیچیده، کار مدیریت امنیت را دشوار می‌کند[۱].

۲. محدودیت منابع:
بسیاری از دستگاه‌های IoT از منابع محدود پردازشی و ذخیره‌سازی استفاده می‌کنند که باعث می‌شود پیاده‌سازی تدابیر امنیتی پیچیده، همچون رمزنگاری سطح بالا یا سیستم‌های تشخیص نفوذ دشوار باشد.

۳. مدیریت و به‌روزرسانی:
بسیاری از دستگاه‌های IoT به‌ویژه در محیط‌های صنعتی و پزشکی، ممکن است از زمان تولید به‌روزرسانی نشوند که این امر موجب آسیب‌پذیری‌های امنیتی می‌شود [۳].

چالش‌ها و تهدیدهای امنیتی در اینترنت اشیا

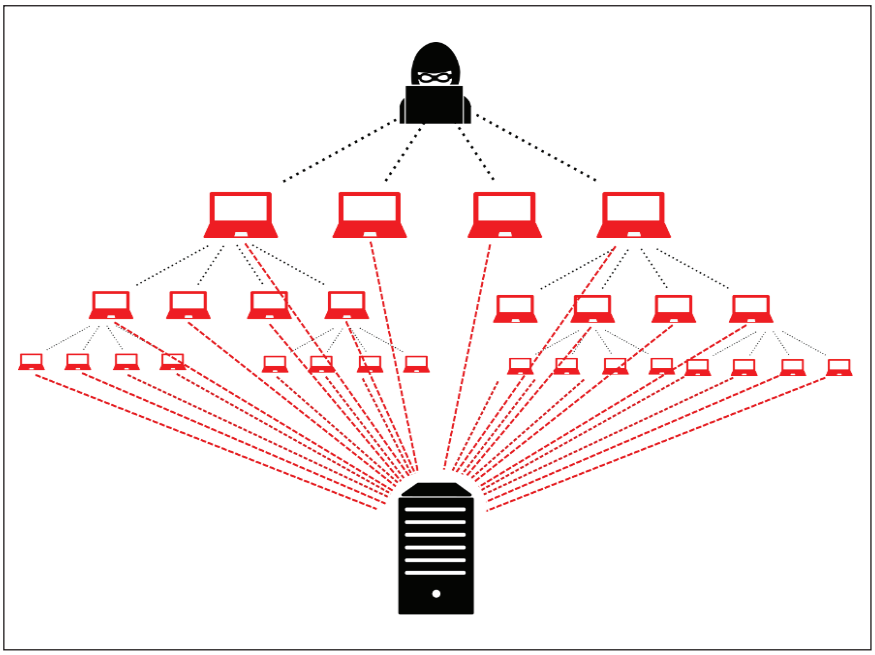
تهدیدهای امنیتی IoT به‌ویژه به‌خاطر ویژگی‌های خاص دستگاه‌های متصل، مانند منابع محدود پردازشی، ارتباط دائمی با اینترنت و تنوع در سخت‌افزار و نرم‌افزار، پیچیده‌تر از تهدیدهای امنیتی در سیستم‌های سنتی است. از جمله تهدیدها و چالش‌های متداول در این حوزه می‌توان به حملات DDoS، نفوذ به دستگاه، سرقت داده و نقض حریم خصوصی اشاره کرد که در ادامه توضیح داده می‌شوند:

۱. حملات DDoS

یکی از تهدیدهای رایج و خطرناک برای شبکه‌های IoT، حملات DDoS است که می‌تواند سیستم‌های IoT را تحت فشار قرار دهد و آنها را غیرقابل دسترس سازد. همان طور که در شکل ۱ مشاهده می‌شود، در این نوع حمله، مهاجم از تعداد زیادی دستگاه متصل به اینترنت برای ارسال حجم زیادی از داده به یک سرور یا دستگاه هدف استفاده می‌کند تا منابع آن را تخلیه کرده و سرویس را از دسترس خارج کند. دستگاه‌های IoT به‌ویژه به‌دلیل منابع محدود پردازشی خود، هدف مناسبی برای این نوع حملات هستند. به‌طور مثال، در حملهٔ Mirai که در سال ۲۰۱۶ رخ داد، هزاران دستگاه IoT، از جمله دوربین‌های مداربسته و روترهای خانگی، به‌طور هم زمان به یک شبکهٔ بزرگ حملهٔ DDoS را انجام دادند و باعث اختلال در دسترسی به خدمات آنلاین شدند[۸]

۲. نفوذ به دستگاه

یکی دیگر از تهدیدهای امنیتی مهم در IoT، نفوذ به دستگاه است. بسیاری از دستگاه‌های IoT به‌ویژه آنهایی که در خانه‌ها یا دفاتر استفاده می‌شوند، فاقد سازوکارهای امنیتی مناسب هستند و اغلب از پیش‌فرض‌های امنیتی ضعیفی مانند گذرواژه‌های ساده یا سیستم‌های احراز هویت ناکافی استفاده می‌کنند. این ضعف‌ها به مهاجمان امکان می‌دهند که به‌راحتی به دستگاه‌ها نفوذ کنند و آنها را تحت کنترل خود در آورند. نفوذ به دستگاه‌های IoT می‌تواند منجر به دسترسی به اطلاعات حساس کاربران یا حتی استفاده از دستگاه‌ها به‌عنوان ابزاری برای حملات سایبری دیگر شود[۷]. علاوه بر این، بسیاری از دستگاه‌ها به‌طور خودکار به اینترنت متصل می‌شوند و به همین دلیل می‌توانند هدف حملات با استفاده از آسیب‌پذیری‌های موجود در



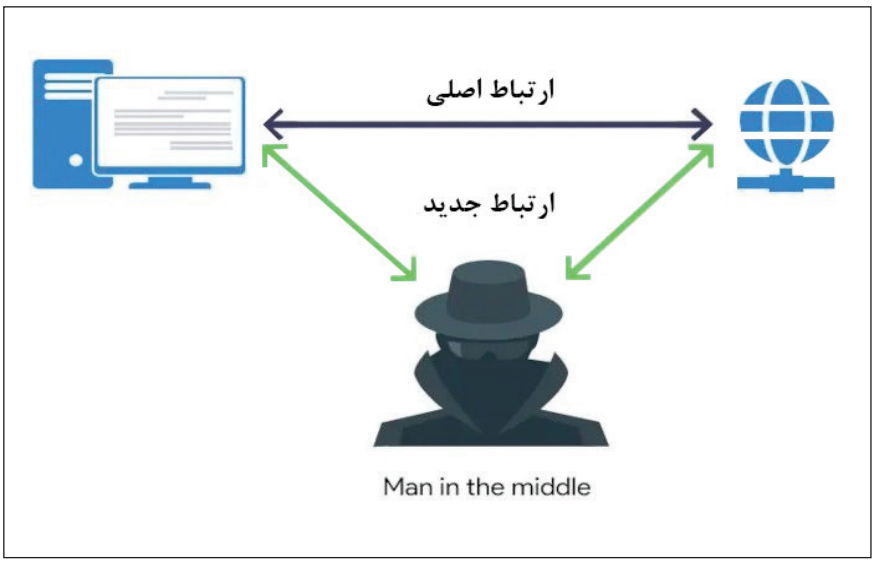
شکل ۱. حمله DDOS

نرم‌افزار یا سیستم‌عامل خود قرار گیرند.

۳. سرقت داده‌ها

یکی از اصلی‌ترین تهدیدهای امنیتی در اینترنت اشیا، سرقت داده‌هاست. دستگاه‌های IoT اغلب داده‌های حساسی مانند موقعیت جغرافیایی، وضعیت سلامت و حتی اطلاعات مربوط به رفتارهای روزمره کاربران را جمع‌آوری می‌کنند. این داده‌ها برای بهبود تجربهٔ کاربری یا تحلیل‌های تجاری استفاده به‌کار می‌آیند، اما در صورتی که به‌درستی از این داده‌ها محافظت نشود، ممکن است توسط مهاجمان به سرقت روند.

اطلاعات جمع‌آوری‌شده از دستگاه‌های پزشکی یا سیستم‌های نظارت خانگی، به‌ویژه در صورت دسترسی غیرمجاز، می‌تواند به تهدیدهای جدی برای حریم خصوصی کاربران تبدیل شود[۳]. برای مثال، نفوذ به سیستم‌های IoT در بیمارستان‌ها ممکن است داده‌های شخصی بیماران را در معرض دستبرد قرار دهد که به نوبهٔ خود می‌تواند آسیب‌های جدی به حریم خصوصی و امنیت افراد بزند.



شکل۲. حمله MITM

۴. نقض حریم خصوصی

حریم خصوصی یکی از مسائل حساس در اینترنت اشیاست. به‌دلیل جمع‌آوری و پردازش داده‌های حساس از کاربران، نقض حریم خصوصی در این حوزه می‌تواند عواقب قانونی و اجتماعی گسترده‌ای به‌دنبال داشته باشد. دستگاه‌های IoT، مانند ساعت‌های هوشمند، دوربین‌های مداربسته و سیستم‌های نظارت خانگی، به‌طور مداوم اطلاعات را از محیط اطراف خود جمع‌آوری می‌کنند. اگر این داده‌ها بدون توجه به اصول امنیتی و حریم خصوصی ذخیره شوند یا به‌درستی مدیریت نشوند، ممکن است برای اهداف تجاری یا حتی جاسوسی استفاده شوند [۷]. علاوه بر این، عدم شفافیت راجع به نحوهٔ استفاده از داده‌های جمع‌آوری‌شده و یا دسترسی به آنها توسط اشخاص ثالث می‌تواند اعتماد عمومی را خدشه‌دار کند.

۵. حملات مبتنی بر بدافزار

حملات بدافزار نیز یکی از تهدیدهای جدی در IoT است. بدافزارهایی مانند Trojans و Ransomware می‌توانند به دستگاه‌های IoT نفوذ کرده و از آنها به‌عنوان ابزاری برای گسترش حمله‌های دیگر استفاده کنند. برای مثال، بدافزارها می‌توانند به دستگاه‌های متصل نفوذ کنند و آنها را به باتنت‌هایی برای حملات DDoS یا ارسال هرزنامه تبدیل کنند[۶]. این نوع تهدیدها به‌ویژه در دستگاه‌های IoT که اغلب از سیستم‌عامل‌های ساده و بدون نظارت‌های امنیتی پیچیده استفاده می‌کنند، شایع است.

۶. حملات MitM[۴]

در حملات MitM، مهاجم به‌طور غیرمجاز ارتباطات بین دو طرف را رهگیری کرده و ممکن است آنها را تغییر دهد یا به‌دست آورد. شکل ۲ شمایی از این حمله را نمایش می‌دهد. در زمینهٔ اینترنت اشیا، این نوع حملات ممکن است هنگامی که دستگاه‌های IoT اطلاعات را از طریق شبکه‌های بی‌سیم ارسال می‌کنند، رخ دهد. به‌دلیل ضعف‌های امنیتی در بسیاری از دستگاه‌های IoT، مهاجمان می‌توانند به‌راحتی به داده‌های انتقالی دسترسی پیدا کنند و حتی آنها را تغییر دهند.

برای مثال، در سیستم‌های خانه‌های هوشمند، یک مهاجم می‌تواند به ارتباطات بین ترموستات هوشمند و برنامهٔ کنترل دما نفوذ کرده و دما را تغییر دهد یا دستورات دیگری را اجرا کند.

این نوع حمله می‌تواند به سرقت داده‌ها، تغییر اطلاعات حساس و حتی کنترل دستگاه‌ها منجر شود[۴].

۷. حملات Zero-Day

حملات Zero-Day به آسیب‌پذیری‌های ناشناخته و هنوز شناسایی‌نشدهٔ سیستم‌ها یا نرم‌افزارها حمله می‌کند. این حملات ممکن است در هر زمانی رخ دهند و معمولا هیچ‌گونه دفاعی در برابر آنها وجود ندارد، زیرا آسیب‌پذیری مورد نظر هنوز شناسایی نشده است.

در IoT، به‌دلیل استفادهٔ گسترده از سخت‌افزارها و نرم‌افزارهای متنوع، مهاجمان به‌راحتی می‌توانند از حملات Zero-Day برای نفوذ به دستگاه‌ها یا سیستم‌های شبکه‌ای استفاده کنند. یکی از مهم‌ترین چالش‌ها در مواجهه با این نوع حملات، ضعف در به‌روزرسانی‌های امنیتی منظم دستگاه‌هاست که اجازه می‌دهد آسیب‌پذیری‌ها باقی بمانند و محل سوءاستفاده قرار گیرند[۳].

۸. حملات Replay

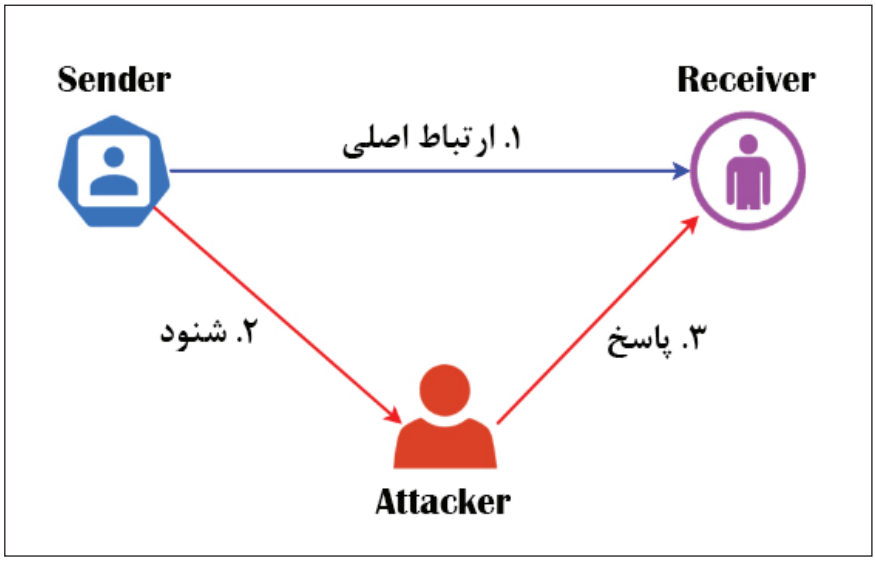
حملات Replay زمانی رخ می‌دهند که مهاجم داده‌های معتبر را ضبط کرده و سپس آنها را دوباره ارسال می‌کند تا عملیات یا درخواست‌های خاصی را در شبکه انجام دهد. در اینترنت اشیا، این نوع حملات به‌ویژه در سیستم‌های مبتنی بر پروتکل‌های ارتباطی باز یا کم‌امنیت، نظیر HTTP یا MQTT، شایع است شکل ۳ شمایی از این حمله را نشان می‌دهد.

برای مثال، اگر یک دستگاه IoT دستور احراز هویت یا تراکنش مالی ارسال کند، مهاجم می‌تواند پیام‌ها را ضبط کرده و آنها را برای انجام عملیات مجدد در زمان بعدی استفاده کند. در این صورت، اطلاعات حساس ممکن است به‌دست مهاجم بیفتد یا اقدامات غیرمجاز انجام شود[۷].

۹. حملات Brute-Force

حملات Brute-Force یکی از ساده‌ترین و رایج‌ترین حملات در دنیای امنیت سایبری است. در این حملات، مهاجم به‌طور مداوم تلاش می‌کند تا گذرواژه یا کلید امنیتی دستگاه را با استفاده از ترکیب‌های مختلف حدس بزند. به‌دلیل استفاده گسترده از گذرواژه‌های ضعیف یا پیش‌فرض در بسیاری از دستگاه‌های IoT، این حملات می‌توانند بسیار مؤثر باشند.

دستگاه‌های IoT مانند دوربین‌های مداربسته، روترهای خانگی و دستگاه‌های ذخیره‌سازی، اغلب از گذرواژه‌های ساده یا پیش‌فرض استفاده



شکل ۳. حمله Replay

می‌کنند که مهاجمان به‌راحتی می‌توانند آنها را حدس بزنند. استفاده از سیستم‌های رمزنگاری و «احراز هویت چندعاملی»[۵] می‌تواند به‌طور قابل توجهی امنیت این دستگاه‌ها را افزایش دهد[۱].

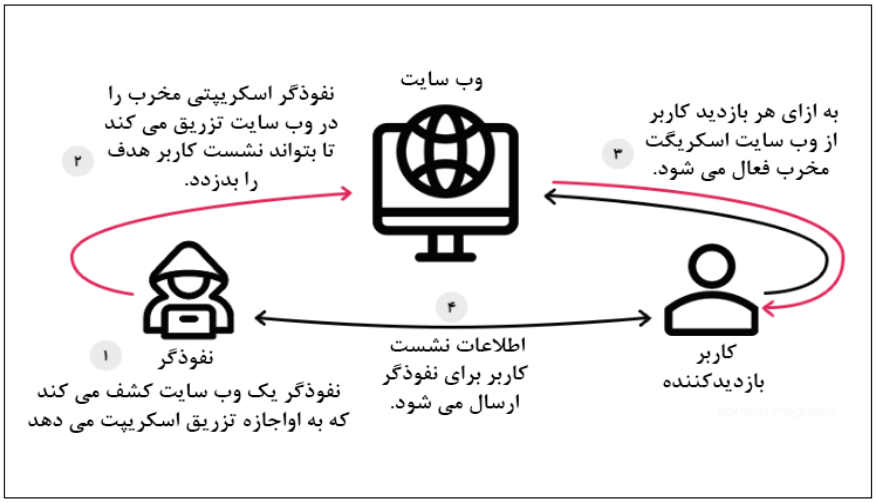
۱۰. حملات XSS[۶]

XSS به حملاتی اطلاق می‌شود که در آن مهاجم از طریق تزریق اسکریپت‌های مخرب به صفحات وب می‌تواند کاربران را فریب دهد و اطلاعات شخصی آنها را سرقت کند. در حوزهٔ اینترنت اشیا، دستگاه‌هایی که به سیستم‌های وب متصل هستند و از طریق مرورگرهای وب قابل مدیریت هستند، هدفی مناسب برای حملاتXSS به‌حساب می‌آیند. شکل ۴ شمایی از این نوع حمله را نشان می‌دهد.

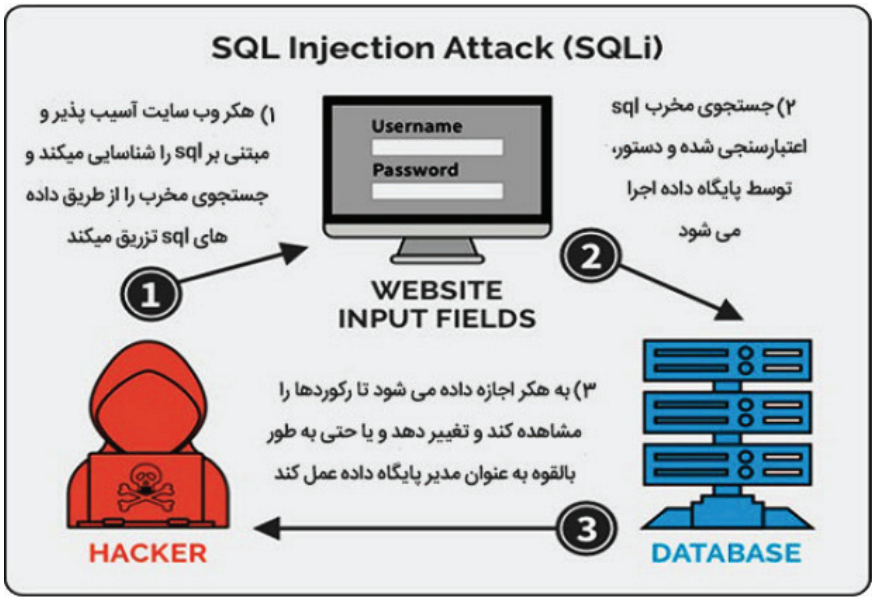
برای مثال، اگر یک دستگاه IoT از طریق یک رابط وب به کاربران اجازه دهد تا تنظیمات آن را تغییر دهند، مهاجم می‌تواند با تزریق اسکریپت‌های مخرب، به کاربران آسیب برساند و به اطلاعات خصوصی یا دسترسی‌های آنها دست یابد. این نوع حملات می‌توانند به تهدیدهای جدی امنیتی برای سیستم‌های IoT تبدیل شوند[۴].

۱۱. حملات Injection

حملات Injection زمانی رخ می‌دهند که مهاجم به ورودی‌های یک سیستم فرمان‌هایی ارسال می‌کند که می‌تواند در پایگاه داده‌ها یا سیستم‌های دیگر اجرا شود. این حملات می‌توانند از نقاط ورودی مانند فرم‌ها،URLها



شکل ۴. حمله XSS



شکل ۵. حمله Injection

یا حتی داده‌های ارسال‌شده از دستگاه‌های IoT به‌وجود آیند. شکل ۵ شمایی از این حمله را نشان می‌دهد.

در IoT، مهاجمان می‌توانند با تزریق دستوراتی به سیستم‌های پردازش داده، به اطلاعات حساس دسترسی پیدا کنند یا حتی عملکرد دستگاه‌های متصل را دستکاری کنند. این نوع حملات در صورت وجود ضعف در پردازش داده یا اعتبارسنجی ورودی‌ها می‌تواند به‌راحتی به دستگاه‌های IoT آسیب برساند[۶].

۱۲. حملات Physical Tampering

حملات فیزیکی یکی از خطرات امنیتی مهم در دنیای IoT هستند، به‌ویژه در دستگاه‌هایی که به‌راحتی در دسترس قرار دارند. مهاجم می‌تواند به‌طور فیزیکی به دستگاه دسترسی پیدا کرده و آن را دستکاری کند یا حتی سخت‌افزار آن را تغییر دهد تا به‌طور غیرمجاز به شبکه متصل شود.

به‌عنوان مثال، در سیستم‌های IoT در صنعت یا خودروها، مهاجم ممکن است به دستگاه‌های پردازش یا حسگرها دسترسی پیدا کند و از آنها برای تغییر داده‌ها یا به‌دست آوردن اطلاعات حساس استفاده کند.

این نوع حملات به‌ویژه زمانی خطرناک می‌شوند که دستگاه‌ها به‌درستی محافظت نشده یا سازوکارهای امنیتی سخت‌افزاری نداشته باشند[۷].

راهبردها و شگردهای تقویت امنیت

با توجه به اینکه اینترنت اشیا به‌سرعت در حال گسترش است و دستگاه‌ها و حسگرهای هوشمند به‌طور فزاینده‌ای در زندگی روزمرهٔ ما حضور دارند، محافظت از این دستگاه‌ها در برابر تهدیدهای امنیتی به یکی از مهم‌ترین چالش‌ها تبدیل شده است. امنیت در اینترنت اشیا به‌ویژه به‌دلیل تعداد زیاد دستگاه‌ها، تنوع فناوری‌ها و پروتکل‌ها، محدودیت‌های منابع سخت‌افزاری و نیاز به ارتباط مداوم بین دستگاه‌ها و شبکه‌ها، نیازمند رویکردهای پیچیده و چندلایه است. برخی از مهم‌ترین راهبردراهبردها و شگردشگردهای امنیتی برای تقویت امنیت دستگاه‌ها و شبکه‌های IoT از قرار ادامه‌اند.

۱. رمزنگاری

یکی از اساسی‌ترین و مهم‌ترین ابزارها برای حفظ امنیت در اینترنت اشیا، رمزنگاری داده‌هاست. رمزنگاری به‌طور مؤثر از دسترسی غیرمجاز به داده‌های حساس و اطلاعات شخصی جلوگیری می‌کند و امکان محافظت از داده‌ها را در حین انتقال از یک دستگاه به دستگاه دیگر فراهم می‌آورد. در IoT، داده‌ها معمولا از دستگاه‌های هوشمند به شبکه‌های ابری یا دستگاه‌های دیگر منتقل می‌شوند و این ارتباطات می‌توانند در معرض حملات قرار گیرند. بنابراین، رمزنگاری داده‌ها اهمیت ویژه‌ای دارد.

رمزنگاری داده‌ها در حین انتقال، مانند استفاده از پروتکل‌هایTLS/SSL ، و رمزنگاری داده‌های ذخیره‌شده و استفاده از الگوریتم‌های رمزنگاری جدیدی مانند AES می‌تواند به‌طور مؤثری از اطلاعات حساس محافظت کنند. به‌ویژه در شبکه‌های بی‌سیم که ممکن است مهاجمان بتوانند داده‌ها را رهگیری کنند، رمزنگاری اهمیت زیادی دارد. برای تقویت بیشتر امنیت، می‌توان از «رمزنگاری سرتاسری»[۷] استفاده کرد که در آن تنها گیرنده و فرستندهٔ مجاز، قادر به رمزگشایی داده‌ها خواهند بود[۳].

۲. احراز هویت و کنترل دسترسی

یکی از بزرگ‌ترین تهدیدهای در حوزهٔ اینترنت اشیا، دسترسی غیرمجاز به دستگاه‌ها و داده‌هاست. بنابراین، احراز هویت قوی و کنترل دسترسی مناسب اهمیت زیادی دارد. دستگاه‌ها و سیستم‌های IoT باید قادر باشند تا هویت دستگاه‌ها و کاربران را به‌درستی تأیید کنند و به آنها فقط در صورتی اجازهٔ دسترسی به منابع یا داده‌های حساس را بدهند که هویتشان معتبر باشد.

برای این منظور، استفاده از سیستم‌های احراز هویت چندعاملی یکی از بهترین روش‌هاست. MFA فرایند احراز هویت را با ترکیب چندین روش مختلف مانند کدهای یک‌بارمصرف (OTP)، گذرواژه، بیومتریک‌ها یا حتی ایجاد هویت از طریق دستگاه‌های فیزیکی مانند کارت‌های هوشمند یا توکن‌ها، تقویت می‌کند. این روش به‌طور قابل توجهی احتمال دسترسی غیرمجاز به سیستم‌ها را کاهش می‌دهد.

علاوه بر این، کنترل دسترسی به منابع نیز باید به‌طور دقیق تنظیم شود. استفاده از مدل‌های کنترل دسترسی مبتنی بر نقش (RBAC) یا کنترل دسترسی مبتنی بر سیاست (ABAC) می‌تواند به مدیریت دقیق دسترسی‌های مختلف در سطح دستگاه‌ها و کاربران کمک کند. این سیاست‌ها به‌طور مؤثر کنترل می‌کنند که کدام دستگاه‌ها یا کاربران به چه منابعی دسترسی دارند و چه عملیاتی را می‌توانند انجام دهند[۴].

۳. مدیریت دستگاه‌ها

از آنجا که اینترنت اشیا شامل تعداد زیادی دستگاه است که همگی ممکن است به شبکه متصل شوند، مدیریت دستگاه‌ها به‌ویژه در مقیاس‌های بزرگ، یکی از چالش‌های امنیتی اصلی است. هر دستگاه IoT باید به‌دقت شناسایی، نظارت و مدیریت شود تا از بروز تهدیدهای امنیتی جلوگیری شود. سیستم‌های

مدیریت دستگاه باید قادر باشند تا دستگاه‌ها را به‌طور متمرکز شناسایی کرده و وضعیت آنها را به‌صورت بلادرنگ نظارت کنند.
به‌ویژه در شبکه‌های IoT که دائماً دستگاه‌های جدید به شبکه اضافه می‌شوند، استفاده از پروتکل‌های خودکار برای شناسایی و تأیید دستگاه‌های جدید بسیار اهمیت دارد. به این ترتیب، هر دستگاه جدید که به شبکه متصل می‌شود، به‌طور خودکار شناسایی و تأیید می‌شود تا از دسترسی دستگاه‌های مخرب جلوگیری شود.
یکی دیگر از نکات مهم در مدیریت دستگاه‌ها، آسیب‌پذیری‌های دستگاه‌هاست. بسیاری از دستگاه‌های IoT ممکن است با آسیب‌پذیری‌های شناخته‌شده‌ای مواجه شوند. بنابراین، نظارت مستمر بر وضعیت دستگاه‌ها و اعمال به‌روزرسانی‌های امنیتیِ به‌موقع بسیار حائز اهمیت است. پلتفرم‌های مدیریت IoT باید قادر باشند پچ‌های امنیتی را برای دستگاه‌های آسیب‌پذیر اعمال کنند و به‌طور خودکار دستگاه‌ها را به‌روزرسانی کنند[۷].

۴. به‌روزرسانی‌های نرم‌افزاری و پچ‌ها

به‌روزرسانی‌های نرم‌افزاری و اعمال پچ‌های امنیتیِ به‌موقع، روش مهمی برای مقابله با تهدیدهای امنیتی شناخته‌شده در دستگاه‌های IoTاست. بسیاری از دستگاه‌های IoT از طریق آسیب‌پذیری‌های امنیتی خودشان است که توسط مهاجمان مورد سوءاستفاده قرار می‌گیرند. یکی از مهم‌ترین راهکارهای امنیتی، اعمال سریع پچ‌های امنیتی به دستگاه‌هاست.
اگر دستگاه‌های IoT مداوم به‌روز نشوند، در معرض تهدیدهای جدید و شناخته‌شده قرار می‌گیرند. به‌ویژه زمانی که آسیب‌پذیری‌ها از سوی تولیدکنندگان شناسایی شده و پچ‌های مربوطه ارائه می‌شوند، عدم به‌روزرسانیِ دستگاه‌ها می‌تواند به شکلی جدی امنیت را به‌خطر بیندازد. در نتیجه، فرایند به‌روزرسانی باید به‌طور خودکار و ایمن انجام شود.
در این راستا، استفاده از سیستم‌های مدیریت پچ‌های خودکار و به‌روزرسانی‌های توزیع‌شده می‌تواند به تضمین امنیت کمک کند. به‌علاوه، دستگاه‌ها باید قادر به دریافت به‌روزرسانی‌های ایمن از منابع معتبر و تأسیس‌شده باشند[۱].

۵. شبکه‌های امن و نظارت بر ترافیک

در بسیاری از حملات، مهاجمان سعی می‌کنند تا شبکه‌های دستگاه‌های IoT را هدف قرار دهند و به داده‌های حساس دسترسی پیدا کنند. برای مقابله با این تهدیدها، استفاده از شبکه‌های امن و نظارت بر ترافیک شبکه اهمیت ویژه‌ای دارد.
یکی از روش‌های مؤثر برای تأمین امنیت شبکه، استفاده از VPN (شبکهٔ خصوصی مجازی) و فایروال‌هاست که می‌توانند از دستگاه‌ها در برابر دسترسی‌های غیرمجاز محافظت کنند. به‌علاوه، استفاده از «سیستم‌های تشخیص نفوذ» (IDS)[۸] و «سیستم‌های پیشگیری از نفوذ» (IPS)[۹] به شناسایی و جلوگیری از حملات سایبری در شبکه‌های IoT کمک می‌کنند. این سیستم‌ها می‌توانند فعالیت‌های مشکوک را شناسایی کرده و برای متوقف‌کردن حملات اقدامات فوری انجام دهند.
نظارت بر ترافیک شبکه و تشخیص رفتار غیرمعمول (UBA) می‌تواند به شناسایی حملات از نوع MitM، DDoS و سایر تهدیدها کمک کند. به این ترتیب، سیستم‌های نظارتی می‌توانند به‌طور مؤثر به شناسایی و پیشگیری از تهدیدهای شبکه‌ای در دستگاه‌های IoT کمک‌کنند [۶]

۶. آموزش کاربران و آگاه‌سازی

آموزش کاربران و آگاه‌سازی آنان از خطرات امنیتی یکی از مؤثرترین راه‌ها برای پیشگیری از تهدیدها در حوزهٔ IoT است. بسیاری از حملات سایبری از طریق خطاهای انسانی مانند استفاده از گذرواژه‌های ضعیف یا اشتباهات کاربران صورت می‌گیرد. بنابراین، باید به آموزش و آگاه‌سازی کاربران دربارهٔ چگونگی استفادهٔ امن از دستگاه‌های IoT توجه ویژه‌ای داشت.
آموزش کاربران دربارهٔ ایجاد گذرواژه‌های قوی، تشخیص ایمیل‌های فیشینگ و استفاده از ویژگی‌های امنیتی مانند احراز هویت چندعاملی می‌تواند کمک شایانی به تقویت امنیت دستگاه‌ها و شبکه‌ها کند. برگزاری دوره‌های آموزشی و ارتقای سطح آگاهی در این زمینه به‌ویژه در شرکت‌ها و سازمان‌ها ضروری است [۴].

پروتکل‌ها و استانداردهای امنیتی

در دنیای اینترنت اشیا، استانداردها و پروتکل‌های امنیتی نقش بسیار مهمی در حفظ امنیت داده‌ها، ارتباطات و دستگاه‌ها دارند. با توجه به رشد سریع این فناوری و نیاز به ارتباط میان تعداد زیادی دستگاه، استفاده از پروتکل‌های امنیتی معتبر و طراحی‌شده برای IoT می‌تواند از بسیاری از تهدیدهای امنیتی جلوگیری کند. این استانداردها و پروتکل‌ها برای تأمین امنیت داده‌ها، احراز هویت و حفظ یکپارچگی اطلاعات طراحی شده‌اند. در این بخش به معرفی برخی از پروتکل‌ها و استانداردهای امنیتی پرکاربرد در این حوزه می‌پردازیم.

۱. پروتکل TLS[۱۰]

TLS یکی از رایج‌ترین و مؤثرترین پروتکل‌های امنیتی برای ارتباطات اینترنتی است. این پروتکل برای حفاظت از داده‌های منتقل‌شده در شبکه‌های ناامن طراحی شده است و به‌طور گسترده‌ای در IoT برای تأمین امنیت ارتباطات بین دستگاه‌ها و سرورها استفاده می‌شود. TLS به‌طور خاص برای رمزگذاری داده‌ها و احراز هویت سرورها به‌منظور جلوگیری از شنود و حملات MITM استفاده می‌شود.
در IoT با توجه به اتصال دستگاه‌های مختلف به یکدیگر انتقال دائم داده‌ها بین دستگاه‌ها و سرورها، استفاده از TLS برای جلوگیری از دسترسی‌های غیرمجاز و محافظت از اطلاعات حساس ضروری است. TLS به دستگاه‌ها و سرورها امکان می‌دهد تا ارتباطات امنی برقرار کنند و مطمئن باشند که اطلاعات تنها توسط مقاصد معتبر قابل دسترسی است[۹].
TLS به‌ویژه در پروتکل‌های HTTP و MQTT در محیط‌های IoT استفاده می‌شود. این پروتکل‌ها به‌طور گسترده در خدمات مبتنی بر وب و ارتباطات «دستگاه به دستگاه»[۱۱] (D۲D) استفاده می‌شوند و از TLS برای رمزگذاری داده‌ها و محافظت از کانال‌های ارتباطی استفاده می‌کنند[۷].

۲. پروتکل IPSec[۱۲]

IPSec یکی دیگر از پروتکل‌های امنیتی است که برای تأمین امنیت ارتباطات شبکه‌ای در لایهٔ شبکه طراحی شده است. این پروتکل به‌ویژه در شبکه‌های مبتنی بر پروتکل IP کاربرد دارد و برای رمزگذاری بسته‌های داده و احراز هویت ارتباطات بین دو نقطه از شبکه استفاده می‌شود.
در IoT، استفاده از IPSec می‌تواند به تأمین امنیت ارتباطات میان دستگاه‌ها، سرورها و شبکه‌ها کمک کند. IPSec از دو حالت اصلی استفاده می‌کند:
۱. حالت تونل[۱۳] که برای ایجاد VPNها بین دستگاه‌ها و شبکه‌ها استفاده می‌شود.
۲. حالت حمل‌ونقل[۱۴] که برای رمزگذاری تنها بخشی از داده‌های IP استفاده می‌شود و معمولا در ارتباطات مستقیم بین دستگاه‌ها کاربرد دارد.
این پروتکل به‌ویژه برای ایجاد شبکه‌های

امن در دستگاه‌های IoT که نیاز به تبادل داده‌های حساس دارند، مانند سیستم‌های نظارت بر سلامت و خانه‌های هوشمند، استفاده می‌شود[۱۰]. به‌کارگیری IPSec در لایهٔ شبکه به افزایش امنیت در برابر حملات MitM و فیشینگ کمک می‌کند.

۳. پروتکل MQTT [۱۵]

پروتکل MQTT یکی از پروتکل‌های محبوب در اینترنت اشیاست که برای ارتباطات کم‌مصرف و پیام‌رسانی به‌کار می‌رود. این پروتکل به‌ویژه برای محیط‌هایی که نیاز به ارسال داده‌های کم‌حجم و سریع دارند، مناسب است. با اینکه MQTT خود به‌طور پیش‌فرض از امنیت برخوردار نیست، اما امکان پیاده‌سازی TLS برای رمزگذاری داده‌ها و احراز هویت در آن وجود دارد.

استفاده از TLS در MQTT به دستگاه‌ها کمک‌می‌کند که ارتباطات ایمن و محافظت‌شده‌ای، حتی در محیط‌های ناامن، داشته باشند. علاوه بر این، می‌توان از احراز هویت برای تعیین هویت دستگاه‌ها و سرورها استفاده کرد تا فقط دستگاه‌های مجاز بتوانند به شبکه متصل شوند[۱۱]. در این راستا، استانداردهای جدیدتر مانند OAuth 2.0 می‌توانند به پیاده‌سازی سیاست‌های دسترسی و امنیت در محیط‌های MQTT کمک کنند.

۴. پروتکل CoAP [۱۶]

CoAP یک پروتکل کم‌هزینه و کم‌مصرف است که برای دستگاه‌های IoT با منابع محدود طراحی شده است. این پروتکل به‌ویژه در شرایطی که دستگاه‌ها پهنای باند پایین دارند و کم انرژی مصرف می‌کنند، استفاده می‌شود. CoAP از پروتکل UDP به‌جای TCP برای کاهش overhead ارتباطات استفاده می‌کند و از همین رو به‌طور گسترده در دستگاه‌های هوشمند و شبکه‌های IoT که نیاز به مصرف انرژی پایین دارند، کاربرد دارد.

برای افزایش امنیت در CoAP، استاندارد DTLS به‌کار می‌رود.[۱۷] DTLS همانند TLS است، با این تفاوت که برای ارتباطات مبتنی بر UDP طراحی شده و می‌تواند برای رمزگذاری داده‌ها، جلوگیری از دستکاری و احراز هویت دستگاه‌ها استفاده شود. این پروتکل به‌طور مؤثری از اطلاعات حساس در شبکه‌های IoT محافظت می‌کند و امنیت ارتباطات در محیط‌های غیرامن را تضمین می‌کند[۱۲].

۵. پروتکل LoWPAN۶ [۱۸]

LoWPAN۶ یکی دیگر از پروتکل‌های پرکاربرد در IoT است که برای انتقال IPv۶ روی شبکه‌های بی‌سیم کم‌مصرف طراحی شده است. این پروتکل به دستگاه‌های IoT اجازه می‌دهد تا به اینترنت متصل شوند و از آدرس‌دهی IP برای ارتباطات استفاده کنند. برای تأمین امنیت در این پروتکل، معمولا از IPSec و همچنین DTLS استفاده می‌شود تا ارتباطات رمزگذاری‌شده و امن بین دستگاه‌ها برقرار شود. LoWPAN۶ معمولا در شبکه‌های مقیاس بزرگ که نیاز به پشتیبانی از تعداد زیادی دستگاه دارند، مانند خانه‌های هوشمند و کشاورزی هوشمند استفاده می‌شود. امنیت این پروتکل می‌تواند از طریق رمزنگاری، احراز هویت و کنترل دسترسی تقویت شود[۱۳].

۶. استانداردهای جدیدتر در امنیت IoT

با پیشرفت فناوری و نیاز به امنیت بیشتر در اینترنت اشیا، استانداردهای جدیدتری برای بهبود امنیت طراحی شده‌اند. یکی از این استانداردها IoTSF (IoT Security Foundation) است که مجموعه‌ای از دستورالعمل‌ها و شیوه‌ها را برای طراحی امن دستگاه‌های IoT و شبکه‌های متصل ارائه می‌دهد. این استانداردها شامل مدیریت دستگاه‌ها، رمزنگاری، احراز هویت و کنترل دسترسی است که به‌طور خاص برای دستگاه‌های IoT طراحی شده‌اند[۱۴].

EU Cybersecurity Act نیز یکی دیگر از اقدامات مهم اتحادیهٔ اروپا برای افزایش امنیت در IoT است. این قانون به بررسی و تضمین استانداردهای امنیتی در دستگاه‌ها و سیستم‌های IoT پرداخته و الزامات جدیدی را برای تولیدکنندگان دستگاه‌های هوشمند و سیستم‌های IoT ایجاد کرده‌است

چالش‌ها و راهکارهای پیش رو

با گسترش و پیچیده‌تر شدن این فناوری و تعداد دستگاه‌های متصل به اینترنت، نگرانی‌ها دربارهٔ تهدیدهای امنیتی نیز افزایش یافته است. امنیت IoT باید توجه ویژه‌ای به روندهای نوظهور، چالش‌های جدید و راهکارهای پیشرفته برای مقابله با این تهدیدها داشته باشد. این روندها و چالش‌ها از قرار ادامه‌اند:

۱. افزایش پیچیدگی شبکه‌های IoT و نیاز به امنیت مقیاس‌پذیر

با افزایش تعداد دستگاه‌های متصل به اینترنت، به‌ویژه در محیط‌هایی که دستگاه‌های IoT به‌صورت گسترده و در مقیاس‌های بزرگ و متنوع عمل می‌کنند، امنیت باید به شکلی مقیاس‌پذیر طراحی شود. به‌عنوان مثال، در خانه‌های هوشمند و شهرهای هوشمند، میلیون‌ها دستگاه به یکدیگر متصل می‌شوند که این امر نیازمند راهکارهای امنیتی است که بتوانند از تعداد بسیار زیاد دستگاه‌ها و داده‌ها به طور هم‌زمان پشتیبانی کنند.

چالش‌ها	**• مدیریت هویت دستگاه‌ها:** با افزایش تعداد دستگاه‌های متصل، مدیریت هویت و دسترسی به این دستگاه‌ها به چالشی بزرگ تبدیل می‌شود. **•کنترل دسترسی:** کنترل دسترسی به داده‌ها و منابع برای میلیون‌ها دستگاه ممکن است به‌ویژه در مقیاس‌های بزرگ مشکل‌ساز باشد
راهکارها	**• مدیریت خودکار دستگاه‌ها و احراز هویت مبتنی بر اعتماد:** در آینده، استفاده از راهکارهای احراز هویت مبتنی بر بلاک‌چین و مدیریت هویت غیرمتمرکز می‌تواند به‌طور مؤثری امنیت مقیاس‌پذیر را فراهم کند. **• استفاده از روش‌های یادگیری ماشین:** استفاده از الگوریتم‌های یادگیری ماشین برای شناسایی رفتارهای مشکوک و مدیریت خودکار تهدیدها در سطح شبکه به‌ویژه در مقیاس‌های بزرگ در آینده اهمیت بالایی خواهد داشت.

۲. اهمیت پردازش داده‌ها در لبه و امنیت آن

یکی از روندهای نوظهور در IoT، پردازش داده‌ها در لبه است. به‌جای ارسال تمام داده‌ها به سرورها برای پردازش، در مدل لبه، داده‌ها در نزدیکی منبع تولید، یعنی در دستگاه یا گره‌های نزدیک به دستگاه‌ها، پردازش می‌شوند. این فناوری تأخیر و بار شبکه را کاهش می‌دهد و باعث افزایش سرعت پردازش می‌شود.

چالش‌ها	**• امنیت داده‌ها در لبه:** در محیط‌های لبه، دستگاه‌ها معمولا به‌طور مستقیم در معرض حملات هستند. بنابراین، امنیت داده‌ها و اطمینان از یکپارچگی آنها در این محیط‌ها اهمیت زیادی دارد. **• نبود سیاست‌های یکپارچهٔ امنیتی:** استانداردهای امنیتی یکپارچه برای تمام دستگاه‌های متصل در شبکه‌های لبه‌ای وجود ندارد و این امر به تهدیدهای امنیتی جدید منجر می‌شود
راهکارها	**• رمزگذاری در لبه:** یکی از مهم‌ترین راهکارها برای تأمین امنیت در پردازش داده در لبه، استفاده از رمزگذاری داده‌ها در دستگاه‌ها قبل از ارسال آنها به شبکه است. این امر از دسترسی غیرمجاز به داده جلوگیری می‌کند. **• پردازش هوشمند و خودکار تهدیدها:** با استفاده از فناوری‌های نوین مانند هوش مصنوعی و یادگیری ماشین می‌توان تهدیدها را در مراحل ابتدایی شناسایی کرده و به‌طور خودکار واکنش‌های امنیتی مناسب را پیاده‌سازی کرد.

۳.حفظ حریم خصوصی درعصرIoT وپردازش داده‌های شخصی

چالش‌ها	**• جمع‌آوری حجم عظیم داده‌های شخصی:** با افزایش تعداد دستگاه‌های IoT، حجم داده‌های شخصی که جمع‌آوری می‌شود نیز افزایش می‌یابد که این امر تهدیدهای جدیدی برای حریم خصوصی ایجاد می‌کند. **• مدیریت داده‌ها و پیروی از مقررات قانونی:** رعایت قوانین و مقررات حریم خصوصی مانند مقررات عمومی حفاظت از داده‌ها در اتحادیه‌اروپا (GDPR) می‌تواند در شرایط پیچیدهٔ IoT مشکل‌ساز باشد.
راهکارها	**• استفاده از شگردهای حفظ حریم خصوصی:** شگردهای نوینی همچون «پوشش‌دهی داده‌ها»[۱۹] و حفظ حریم خصوصی از طریق رمزنگاری داده‌ها می‌توانند از داده‌های شخصی محافظت کنند و دسترسی غیرمجاز به آنها را محدود نمایند. **• مدیریت داده‌ها مبتنی بر بلاک‌چین:** استفاده از فناوری بلاک‌چین برای مدیریت داده‌های شخصی و فراهم آوردن تراکنش‌های امن و غیر قابل تغییر می‌تواند به حفاظت از حریم خصوصی کاربران کمک کند.

۴. حملات جدید و پیچیده در حوزهٔ امنیت IoT

با پیشرفت فناوری‌های حملات سایبری، تهدیدهای جدیدی در حوزهٔ امنیت IoT به‌وجود خواهد آمد. حملات سایبری ممکن است حتی پیچیده‌تر از حملات DDoS و نفوذ به دستگاه‌ها شوند و شامل تهدیدهایی مانند حملات مبتنی بر هوش مصنوعی و حملات مبتنی بر 5G باشند.

چالش‌ها	**• حملات هوش مصنوعی و یادگیری ماشین:** استفاده از الگوریتم‌های یادگیری ماشین برای ایجاد حملات هوشمند که قادر به دور زدن سیستم‌های امنیتی هستند، به یک تهدید بزرگ تبدیل می‌شود. **• امنیت شبکه‌های 5G:** با ورود به دوران 5G و به‌ویژه پیوند آن با IoT ، تهدیدهای امنیتی جدیدی مانند حملات به زیرساخت‌های شبکه 5G و بهره‌برداری از آسیب‌پذیری‌های این شبکه می‌تواند به امنیت دستگاه‌ها و داده‌ها آسیب وارد کند.
راهکارها	**• پایش و واکنش خودکار به تهدیدها:** استفاده از ابزارهای پیشرفته برای شناسایی بلادرنگ تهدیدها و پاسخ سریع به آنها می‌تواند به مقابله با حملات پیچیده کمک کند. **•توسعهٔ پروتکل‌های امنیتی خاص 5G:** طراحی پروتکل‌ها و استانداردهای امنیتی خاص برای 5G و ارتباطات مبتنی بر IoT می‌تواند از بروز تهدیدهای امنیتی جدید جلوگیری کند.

۵. استانداردها و چارچوب‌های امنیتی جهانی

در نهایت، به‌منظور مقابله با چالش‌های امنیتی جدید، توسعه و پذیرش استانداردهای جهانی برای امنیت IoT ضرورت دارد. این استانداردها باید شامل دستورالعمل‌هایی برای طراحی امن دستگاه‌ها، حفاظت از داده‌ها و تعامل امن دستگاه‌ها با یکدیگر باشند.

چالش‌ها	**• نبود استانداردهای یکپارچه:** در حال حاضر، بسیاری از استانداردهای امنیتی IoT پراکنده و غیرمتمرکز هستند، و این امر می‌تواند منجر به ناهماهنگی در طراحی امنیت دستگاه‌ها و شبکه‌ها شود.
راهکارها	**•توسعهٔ استانداردهای جهانی:** ایجاد چارچوب‌های امنیتی جهانی مانندIoT Cybersecurity Improvement Act و همکاری‌های بین‌المللی برای پذیرش این استانداردها، می‌تواند به ارتقای سطح امنیت در IoT کمک کند.

این چشم‌انداز نشان‌دهندهٔ نیاز به اتخاذ رویکردهای نوآورانه و هوشمندانه برای تأمین امنیت اینترنت اشیا در برابر تهدیدهای آینده است. روندهای نوظهور، چالش‌های جدید و راهکارهای پیشرفته در این زمینه باید به‌طور مستمر مورد توجه قرار گیرند تا بتوان از این فناوری به‌صورت امن و مطمئن بهره‌برداری کرد.

نتیجه‌گیری

امنیت در اینترنت اشیا یکی از مهم‌ترین چالش‌ها و دغدغه‌های امروزی در دنیای فناوری اطلاعات است. با گسترش روزافزون تعداد دستگاه‌های متصل و پیچیدگی‌های شبکه‌های اینترنت اشیا، تهدیدهای امنیتی جدید و پیچیده‌ای ظهور کرده است که نیازمند راهکارهای نوآورانه و پیشرفته است. این تهدیدها شامل حملات DDoS، نفوذ به دستگاه‌ها، سرقت داده‌ها، حملاتMitM و بسیاری از تهدیدهای دیگر است که می‌توانند به اطلاعات حساس و سیستم‌های حیاتی آسیب بزنند.

با توجه به این تهدیدها، اتخاذ راهبردهای امنیتی مؤثر ضروری است. از جملهٔ این راهبردها می‌توان به استفاده از رمزنگاری برای حفاظت از داده‌ها، احراز هویت قوی برای اطمینان از صحت و اعتبار دستگاه‌ها و مدیریت به‌روزرسانی‌های نرم‌افزاری برای مقابله با آسیب‌پذیری‌های جدید اشاره کرد. همچنین، پروتکل‌های امنیتی مانند IPSec، TLS و CoAP در طراحی شبکه‌های امن و حفاظت از داده‌ها در بستر اینترنت اشیا نقش حیاتی ایفا می‌کنند.

در آینده، روندهای جدیدی همچون پردازش داده‌ها در لبه، هوش مصنوعی و یادگیری ماشین و همچنین توسعهٔ شبکه‌های 5G چالش‌های امنیتی جدیدی را ایجاد خواهند کرد. بنابراین، به‌کارگیری راهکارهای امنیتی مقیاس‌پذیر و مبتنی بر هوش مصنوعی می‌تواند به شناسایی و پیشگیری از تهدیدهای پیچیده کمک کنند. علاوه بر این، حفظ حریم خصوصی و مدیریت داده‌های شخصی از دیگر اولویت‌های امنیتی در IoT به‌شمار می‌روند.

به‌طور کلی، با توجه به سرعت پیشرفت فناوری اینترنت اشیا و گسترش روزافزون آن، توجه به استانداردهای جهانی و چارچوب‌های امنیتی یکپارچه ضروری است. این استانداردها می‌توانند به ایجاد امنیت پایدار و محافظت از داده‌ها در برابر تهدیدهای جدید کمک کنند. در نهایت، برای دستیابی به امنیت کامل در اینترنت اشیا، همکاری میان محققان، توسعه‌دهندگان و تولیدکنندگانِ دستگاه‌ها ضروری است تا بتوان در برابر چالش‌های امنیتی پیچیدهٔ آینده مقاومت کرد.

1.Internet of Thing
2.encryption
3.Distributed Denial of Service
4.Man-in-the-Middle
5. Multi-Factor Authentication
6.Cross-Site Scripting
7.End-to-End Encryption
8.Intrusion Detection System
9.Intrusion prevention System
10.Transport Layer Security
11.Device To Device
12.Internet Protocol Security
13.Tunnel
14.Transport
15. Message Queuing Telemetry Transport
16.Constrained Application Protocol
17.Datagram Transport Layer Security
18.IPv6 over Low Power Wireless. Personal Area Networks
19.Data Masking

منابع

1. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems, 1660-1645 ,(7)29.
2. Statista. (2021). "Number of IoT devices worldwide from 2015 to 2025." Retrieved from Statista
3. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). "Security, privacy and trust in Internet of Things: The road ahead." Computer Networks, 164-146 ,76.
4. Roman, R., Zhou, J., & Lopez, J. (2013). "On the security of Internet of Things." International Journal of Computer Science and Network Security, 10-1 ,(6)13.
5. Atzori, L., Iera, A., & Morabito, G. (2010). "The Internet of Things: A survey." Computer Networks, 2805-2787 ,(15)54.
6. Zhang, Y., Deng, R., & Liu, L. (2014). "Security and privacy in the Internet of Things." Securityand Privacy, 12-1 ,(4)12.
7. Zhou, J., Liu, L., & Yang, L. (2015). "Security and privacy in the Internet of Things." International Journal of Computer Applications, 40-33 ,(13)113.
8. Kumar, S., & Kapoor, A. (2016). "IoT-based DDoS attack detection: A survey." Proceedings of the 2016 International Conference on Computer Communication and Networks (ICCCN), 8-1.
9. Housley, R., Ford, W. E., Polk, W. T., & Solo, D. (2002). RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1. IETF.
10. Kent, S., & Atkinson, R. (2005). RFC 4301: Security Architecture for the Internet Protocol. IETF.
11.Rodriguez, P., & Saqib, S. (2014). "Security in the Internet of Things: A Survey." International Journal of Computer Applications, 30-24 ,(9)96.
12.Shelby, Z., Hartke, K., & Bormann, C. (2014). RFC 7252: Constrained Application Protocol (CoAP). IETF.
13. Montenegro, G., Kushalnagar, N., Hui, J., & Culler, D. (2007). RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks. IETF.
14. IoT Security Foundation (2020). IoT Security Foundation: Security by Design. Available at: www.iotsecurityfoundation.org.
15. Zhang, Y., Deng, R., & Liu, X. (2021). "Blockchain-Based Authentication for IoT Security: A Survey." IEEE Internet of Things Journal, 7398-7386 ,(9)8.
16. Yang, K., Li, H., & Xu, L. (2020). "Artificial Intelligence in IoT Security: A Review." IEEE Access, 147178-147165 ,8.
17.Zheng, Z., Xie, S., & Dai, H. (2020). "Blockchain for IoT Security and Privacy: Theories, Challenges, and Solutions." IEEE Internet of Things Journal, 95-77 ,(1)7.

تحلیل پیش‌بینانه با استفاده از تصاویر نظارتی

نویسنده:
مهسا بیگ‌رضایی

تحلیل پیش‌بینانه داده‌های تصویری یکی از حوزه‌های پیشرفته و حیاتی در علوم داده و هوش مصنوعی است که از تصاویر نظارتی برای پیش‌بینی رخدادها و رفتارهای آینده استفاده می‌کند.

فرایند«تحلیل پیش‌بینانه»[1] شامل مراحل جمع‌آوری، پیش‌پردازش داده‌ها، استخراج ویژگی‌ها، مدل‌سازی پیش‌بینانه، ارزیابی مدل و بهره‌برداری از پیش‌بینی‌ها در تصمیم‌گیری است. تکنیک‌هایی مانند «یادگیری ماشین» [2] و یادگیری عمیق، نقش کلیدی در استخراج ویژگی‌های تصویری و بهبود دقت پیش‌بینی دارند. با وجود مزایای متعدد، چالش‌هایی نظیر کیفیت پایین تصاویر، حجم بالای داده‌ها، حریم خصوصی و پیچیدگی تفسیر مدل‌ها در این زمینه وجود دارد. پیشرفت‌هایی مانند استفاده از مدل‌هایTransformer، پردازش بلادرنگ و سیستم‌های ترکیبی انسان–ماشین، افق‌های جدیدی را در این حوزه گشوده‌اند. این مقاله به بررسی مراحل، چالش‌ها و فرصت‌های آیندهٔ تحلیل پیش‌بینانهٔ داده‌های تصویری پرداخته و راه‌کارهایی برای بهبود این فرایند ارائه‌می‌دهد تحلیل پیش‌بینانه به‌عنوان یکی از نوآوری‌های کلیدی در علم داده و یادگیری ماشین، توانایی استفاده از داده‌های موجود برای پیش‌بینی رویدادهای آینده را فراهم می‌کند. داده‌های تصویری حاصل از سیستم‌های نظارتی، یکی از غنی‌ترین منابع برای این نوع تحلیل‌ها هستند. این داده‌ها اطلاعات بسیار دقیقی دربارهٔ محیط، رفتار افراد و تعاملات اجتماعی ارائه می‌دهند و می‌توانند به شناسایی الگوها و روندهای پیچیده کمک کنند. با پیشرفت در فناوری‌های نظارت تصویری، از جمله دوربین‌های هوشمند و سیستم‌های ذخیره‌سازیِ کلان‌داده، تحلیل این تصاویر به حوزه‌ای بسیار پرکاربرد در امنیت، حمل‌ونقل و مدیریت شهری تبدیل شده است. مطالعات متعددی نشان داده‌اند که تحلیل پیش‌بینانه با استفاده از تصاویر نظارتی، ابزار قدرتمندی برای جلوگیری از وقوع حوادث ناگوار و بهینه‌سازی فرایندهای مختلف ارائه می‌دهد.

اهمیت تصاویر نظارتی در تحلیل پیش‌بینانه

تصاویر نظارتی نقش مهمی در جمع‌آوری داده‌های دقیق و واقعی ایفا می‌کنند. این تصاویر به‌طور گسترده در مکان‌های عمومی، جاده‌ها، فرودگاه‌ها و مراکز خرید استفاده می‌شوند و داده‌های بصری ارزشمندی از تعاملات انسانی، حرکت وسایل نقلیه و رفتار محیطی ارائه می‌دهند. اهمیت این تصاویر زمانی برجسته‌تر می‌شود که از آنها برای تحلیل پیش‌بینانه استفاده شود. با کمک الگوریتم‌های یادگیری عمیق، مانند «شبکه‌های‌عصبی پیچشی»[3](CNNs)، می‌توان از داده‌های خام تصویری، الگوهای رفتاری یا رویدادهای بالقوه را استخراج کرد. به عنوان مثال، در حوزهٔ امنیت عمومی، دوربین‌های نظارتی با استفاده از تحلیل پیش‌بینانه می‌توانند رفتارهای غیرعادی مانند رفتارهای پیشامجرمانه را شناسایی کرده و به جلوگیری از جرایم کمک کنند. در عین حال، این فناوری‌ها امکان تحلیل بلادرنگ داده‌ها را فراهم کرده و واکنش سریع به موقعیت‌های اضطراری را امکان‌پذیر می‌سازند.

نقش تحلیل پیش‌بینانه در مسائل دنیای واقعی

تحلیل پیش‌بینانه با استفاده از تصاویر نظارتی کاربردهای فراوانی در دنیای واقعی دارد. یکی از اصلی‌ترین کاربردها در حوزهٔ امنیت است، جایی که شناسایی رفتارهای مشکوک یا غیرمعمول می‌تواند از وقوع حوادث جلوگیری کند. به‌عنوان مثال، در فرودگاه‌ها و ایستگاه‌های قطار، سیستم‌های مبتنی بر تحلیل تصاویر نظارتی

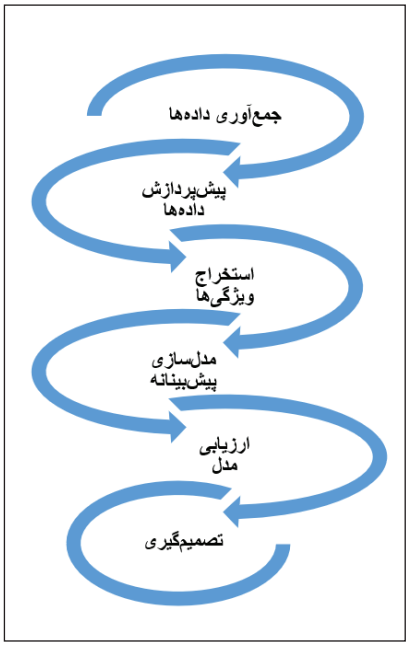
می‌توانند رفتار افراد را زیر نظر گرفته و اقدامات بالقوه‌خطرناک را پیش‌بینی کنند.
در حوزهٔ حمل‌ونقل شهری، این فناوری می‌تواند به بهینه‌سازی جریان ترافیک کمک‌کند. تصاویر نظارتی از جاده‌ها و تقاطع‌ها می‌توانند به شناسایی گلوگاه‌های ترافیکی و پیش‌بینی تراکم کمک کنند.
مطالعه‌ای توسط وانگ نشان داده است که استفاده از مدل‌های یادگیری عمیق برای تحلیل تصاویر ترافیکی، می‌تواند زمان سفر و مصرف انرژی را کاهش دهد. علاوه بر این، تحلیل پیش‌بینانه در حوزهٔ خرده‌فروشی نیز تأثیر قابل توجهی داشته است. با تحلیل تصاویر دوربین‌های نظارتی در فروشگاه‌ها، الگوهای خرید مشتریان شناسایی شده و استراتژی‌های بازاریابی هدفمند ارائه می‌شود. این کاربردها نشان می‌دهند که تصاویر نظارتی می‌توانند نقش کلیدی در بهبود بهره‌وری و امنیت در دنیای واقعی ایفا کنند.
هدف اصلی این مقاله ارائهٔ دیدگاهی جامع و به‌روز از تحلیل پیش‌بینانه با استفاده از تصاویر نظارتی است. با تمرکز بر پیشرفت‌های اخیر در الگوریتم‌های یادگیری عمیق، کاربردهای عملی این فناوری در زمینه‌های مختلف بررسی‌می‌شود. علاوه بر این، چالش‌ها و محدودیت‌های موجود، از جمله نیاز به پردازش حجم بالای داده‌ها و مسائل اخلاقی مانند حفظ حریم خصوصی، بررسی می‌شود.

مبانی نظری و مفاهیم پایه

تحلیل پیش‌بینانه فرایند با استفاده از تکنیک‌های آماری پیشرفته و الگوریتم‌های یادگیری ماشین به شناسایی الگوها در داده‌های موجود و پیش‌بینی رویدادهای آینده می‌پردازد. در حوزهٔ تصاویر نظارتی، این تحلیل با استفاده از داده‌های تصویریِ جمع‌آوری‌شده توسط دوربین‌ها و سیستم‌هایِ ضبط ویدئویی، توانسته است به بهبود امنیت، مدیریت ترافیک و حتی نظارت بر محیط زیست کمک کند. سیستم‌های نظارتی جدید که مجهز به فناوری‌های هوش مصنوعی و یادگیری عمیق هستند، می‌توانند حجم عظیمی از داده‌های بصری را پردازش کرده و اطلاعات مفیدی برای تصمیم‌گیری‌های پیشگیرانه فراهم کنند. یکی از فناوری‌های اصلی استفاده‌شده در تحلیل داده‌های تصویری CNNs است. علاوه بر این، استفاده از مدل‌های پیشرفته مانند «شبکه‌های بازگشتی» (RNNs)[۴] و یادگیری تقویتی، امکان تحلیل رفتارها و پیش‌بینی نتایج پیچیده‌تر را فراهم می‌کند.

تحلیل پیش‌بینانه و تصاویر نظارتی

تحلیل پیش‌بینانه رویکردی است که از داده‌های تاریخی و فعلی برای شناسایی روندها و پیش‌بینی رویدادهای آتی استفاده می‌کند. این تحلیل با ترکیب روش‌های آماری و یادگیری ماشین، ابزار قدرتمندی برای مدل‌سازی سناریوهای آینده ارائه می‌دهد. در حوزهٔ تصاویر نظارتی، داده‌ها به‌صورت تصویری یا ویدئویی از طریق سیستم‌های نظارتی مختلف جمع‌آوری می‌شوند. این تصاویر که شامل رفتار انسان‌ها، حرکت وسایل نقلیه و تغییرات محیطی هستند، پایه‌ای برای تحلیل‌های پیش‌بینانه فراهم می‌کنند. تصاویر نظارتی عمدتاً از دوربین‌های ثابت مانند دوربین‌های مداربسته[۵](CCTV)، ویدئوهای پهپادها و حتی تصاویر ماهواره‌ای تأمین می‌شوند. این داده‌ها یا به‌صورت پیوسته ضبط می‌شوند یا در شرایط خاص، از لحظات کلیدی تصاویر ثابت ثبت‌می‌شود. تحلیل این داده‌ها می‌تواند به شناسایی تهدیدهای امنیتی، بهبود مدیریت شهری و حتی نظارت بر فرایندهای صنعتی کمک کند.
تحلیل پیش‌بینانهٔ داده‌های تصویری فرایندی چندمرحله‌ای است. این مراحل در شکل ۱ نشان داده شده است.
این فرایند با جمع‌آوری داده‌های تصویری از منابعی مانند دوربین‌های نظارتی و پهپادها آغاز می‌شود. سپس تصاویر در مرحلهٔ پیش‌پردازش با حذف نویز، نرمال‌سازی و تقویت داده‌ها آماده می‌شوند. در گام بعد، استخراج ویژگی‌ها با استفاده از روش‌های سنتی یا CNN انجام می‌شود تا ویژگی‌های مهم تصاویر شناسایی شوند. در مرحلهٔ مدل‌سازی پیش‌بینانه، از الگوریتم‌های یادگیری عمیق یا مدل‌های Transformer برای پیش‌بینی الگوها و رفتارها استفاده می‌شود.
عملکرد مدل‌ها با معیارهایی نظیر دقت و حساسیت ارزیابی شده و در نهایت، پیش‌بینی‌های مدل برای تصمیم‌گیری‌های هوشمند، مانند شناسایی رفتارهای مشکوک یا مدیریت ترافیک، به‌کارگرفته می‌شوند.
این فرایند نیازمند به‌روزرسانی مداوم مدل‌ها و مدیریت تغییرات محیطی برای حفظ دقت و کارایی آن است.



شکل ۱. فرایند تحلیل پیش‌بینانه.

انواع داده‌های تصویری در سیستم‌های نظارتی

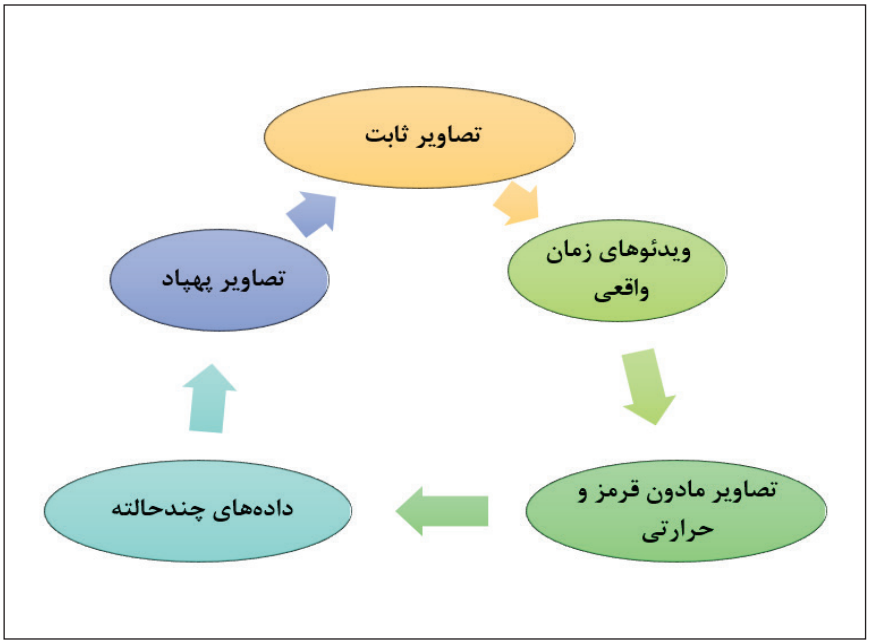
سیستم‌های نظارتی، داده‌های تصویری متنوعی تولید می‌کنند که هر نوع برای اهداف خاصی استفاده می‌شود. این داده‌ها مطابق شکل ۲ به دسته‌های زیر تقسیم می‌شوند:

۱. «تصاویر ثابت»[۶]:
این نوع داده‌ها به‌صورت عکس‌های جداگانه ثبت می‌شوند و معمولا برای شناسایی اشیا یا افراد به‌کار می‌روند؛ مثلا در شناسایی چهره کاربرد فراوانی دارند[۴].

۲. «ویدئوهای زمان واقعی»[۷]:
این داده‌ها به‌صورت پیوسته و زنده ضبط می‌شوند و برای تحلیل رفتارها، الگوهای حرکتی و تشخیص رویدادهای غیرعادی در محیط‌های مختلف به‌کار می‌روند. این ویدئوها به دلیل پویایی و غنی بودن داده‌ها، در تحلیل پیش‌بینانه بسیار مفید هستند[۵].

۳. تصاویر مادون قرمز و حرارتی:
این تصاویر در شرایطی که نور محیط ناکافی است، مانند شب یا محیط‌های مه‌آلود، اهمیت بالایی دارند و در سیستم‌های امنیتی برای شناسایی افراد یا اشیا در تاریکی استفاده می‌شوند[۶].

۴. «داده‌های چندحالته»[۸]:
این داده‌ها ترکیبی از اطلاعات بصری با دیگر انواع داده‌ها، مانند داده‌های صوتی یا حسگرهای محیطی، هستند[۷].



شکل ۲. انواع داده‌های تصویری در سیستم‌های نظارتی

۵. «تصویرسازی از طریق پهپاد»[۹]:

تصاویر جمع‌آوری‌شده توسط پهپادها به دلیل پوشش گسترده و زوایای دید متنوع، در مدیریت ترافیک، نظارت محیطی و کنترل بلایای طبیعی بسیار مؤثر هستند[۸].

این داده‌ها، با بهره‌گیری از تکنیک‌های پیشرفتهٔ یادگیری ماشین، برای کاربردهای امنیتی، بهینه‌سازی شهری و پیش‌بینی‌های محیطی به‌کار می‌روند. به‌عنوان مثال، تصاویر ویدئویی زمان واقعی از تقاطع‌های شهری، امکان پیش‌بینی تراکم ترافیک و بهبود جریان تردد را فراهم می‌کنند.

پیشرفت‌های اخیر در تحلیل داده‌های تصویری

تحلیل داده‌های تصویری در سال‌های اخیر به لطف پیشرفت در الگوریتم‌های یادگیری عمیق، به‌طور قابل توجهی بهبود یافته است. یکی از پیشرفت‌های کلیدی در این زمینه، توسعهٔ «شبکه‌های عصبی پیچشی عمیق»[۱۰] است که قابلیت استخراج ویژگی‌های پیچیده را از داده‌های تصویری دارند[۹]. علاوه بر این، تکنیک‌های ترکیبی مانند استفاده از یادگیری تقویتی برای پیش‌بینی رفتارهای بلندمدت، امکان تحلیل‌های پیچیده‌تر را فراهم کرده است.

پیشرفت در سیستم‌های «پردازش لبه»[۱۱] نیز به تحلیل سریع‌تر داده‌ها کمک کرده است. با استفاده از این فناوری، تحلیل داده‌ها مستقیماً در نزدیکی منبع تولید (مانند دوربین‌های نظارتی) انجام می‌شود که به کاهش تأخیر زمانی و افزایش سرعت تصمیم‌گیری کمک می‌کند[۱۰]. همچنین، «مدل‌های مبتنی بر توجه»[۱۲]، مانندTransformerها، در استخراج روابط پیچیده در داده‌های تصویری بسیار مؤثر بوده‌اند و کاربردهای پیش‌بینانه را بهبود بخشیده‌اند [۷].

روش‌ها و تکنیک‌های تحلیل پیش‌بینانه

۱. یادگیری ماشین

یادگیری ماشین به‌عنوان یکی از زیرشاخه‌های هوش مصنوعی، نقش کلیدی در تحلیل تصاویر نظارتی دارد. این روش با استفاده از الگوریتم‌های یادگیریِ نظارت‌شده و بدون نظارت، به سیستم‌های نظارتی امکان شناسایی الگوها و رفتارهای خاص داده می‌شود. الگوریتم‌هایی مانند «ماشین‌های بردار پشتیبان» [۱۳] (SVM) ، «جنگل تصادفی» [۱۴] و «دسته‌بندی کی-میانگین» [۱۵] به‌طور گسترده برای دسته‌بندی، رگرسیون و خوشه‌بندی داده‌های تصویری استفاده می‌شوند. به‌عنوان مثال، ازSVM برای شناسایی اشیا یا تشخیص فعالیت‌های مشکوک در ویدئوها استفاده می‌شود[۸].

یکی دیگر از کاربردهای یادگیری ماشین در تحلیل تصاویر، استفاده از تکنیک‌های کاهش ابعاد داده مانند تحلیل مؤلفه‌های اصلی[۱۶] (PCA) برای بهبود کارایی و سرعت سیستم‌های نظارتی است. این روش‌ها به سیستم‌ها کمک می‌کنند تا حجم داده‌های ویدئویی بزرگ را مدیریت کنند و تنها اطلاعات مهم و مرتبط را استخراج کنند[۱۰].

۲. یادگیری عمیق

یادگیری عمیق به‌عنوان یکی از پیشرفته‌ترین فناوری‌های هوش مصنوعی، تحول بزرگی در تحلیل تصاویر نظارتی ایجاد کرده است. این فناوری از مدل‌های پیچیده مانند CNNs و شبکه‌های LSTM [۱۷] بهره می‌برد تا الگوهای پیچیده‌تر و جزئیات دقیق‌تری را از داده‌های تصویری استخراج کند. به‌عنوان مثال، CNNها می‌توانند با تحلیل پیکسل‌های تصویر، اشیای مختلف مانند خودروها، افراد یا کیف‌های مشکوک را با دقت بسیار بالا شناسایی کنند [۱۱].

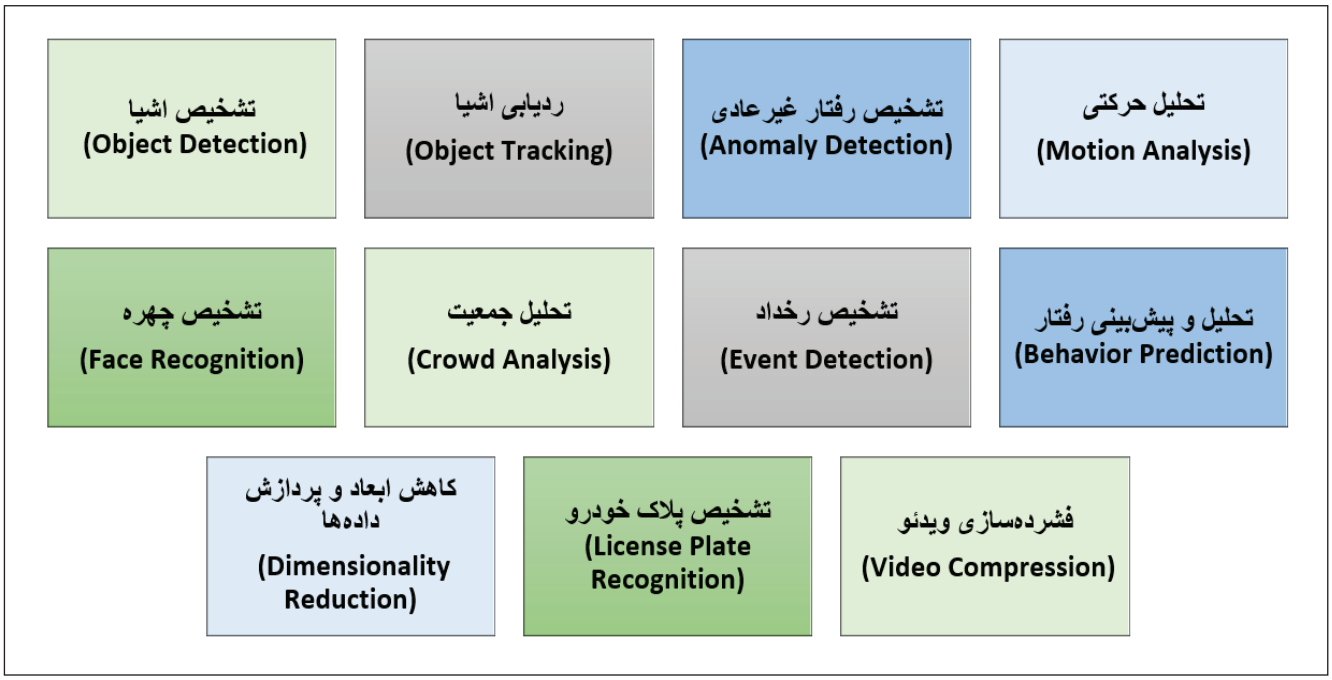
علاوه بر این، مدل‌های ترکیبی مانند CNN-LSTM برای تحلیل توالی‌های زمانی در داده‌های ویدئویی، مانند تشخیص رفتارهای غیرعادی یا پیش‌بینی حوادث، بسیار مؤثر هستند. این ترکیب امکان تحلیل هم‌زمان ویژگی‌های فضایی و زمانی را فراهم کرده و عملکرد سیستم‌های نظارتی را بهبود می‌بخشد[۹].

۳. تکنیک‌های پرکاربرد در تحلیل داده‌های تصویری

تحلیل داده‌های تصویری در سیستم‌های نظارتی، از تکنیک‌های پیشرفتهٔ هوش مصنوعی و یادگیری ماشین بهره می‌برد تا اطلاعات مفیدی را از تصاویر و ویدئوها استخراج کند. این تکنیک‌ها به شناسایی، ردیابی، تحلیل رفتارها و الگوهای حرکتی کمک می‌کنند. در شکل ۳ انواع این تکنیک‌ها خلاصه شده است. در ادامه، اصلی‌ترین تکنیک‌ها در این حوزه معرفی خواهد شد.

- **«تشخیص اشیا»[۱۸]:**

تشخیص اشیا فرایندی است که در آن اشیای مختلف در یک تصویر یا ویدئو شناسایی و مکان آنها مشخص می‌شود. تکنیک‌هایی مانند YOLO [۱۹] وFaster R-CNN از



شکل ۳. انواع تکنیک‌های تحلیل پیش‌بینانه در سیستم‌های نظارت تصویری

پیشرفته‌ترین روش‌ها در این زمینه هستند. این تکنیک برای شناسایی اشیای مشکوک، خودروها یا افراد در محیط‌های نظارتی بسیار مؤثر است. به‌عنوان مثال، در یک ایستگاه قطار، با استفاده از این روش می‌توان کیف‌های رهاشده یا اشیای غیرعادی را شناسایی کرد.

• **«ردیابی اشیا»** [۲۰]

ردیابی اشیا به فرایند دنبال‌کردن مسیر حرکت یک یا چند شیء در طول یک ویدئو گفته می‌شود. الگوریتم‌های رایجی مانند Kalman Filter، DeepSORT و Optical Flow در این تکنیک استفاده می‌شوند. این روش در مدیریت ترافیک برای پیگیری خودروها یا در سیستم‌های امنیتی برای ردیابی افراد مظنون کاربرد دارد. این تکنیک، اطلاعات ارزشمندی مانند سرعت، جهت حرکت و تعامل اشیا را فراهم می‌کند.

• **«تشخیص رفتارهای غیرعادی»** [۲۱]

تشخیص رفتارهای غیرعادی یکی از کاربردی‌ترین تکنیک‌ها در تحلیل داده‌های تصویری است که برای شناسایی فعالیت‌های ناهنجار در محیط استفاده می‌شود. این روش معمولا از مدل‌های یادگیری بدون نظارت مانند Autoencoders یا Gaussian Mixture Models بهره می‌برد. برای مثال، سیستم‌های نظارتی می‌توانند با این تکنیک رفتارهایی مانند توقف ناگهانی یک فرد یا حرکت غیرعادی خودروها را در خیابان شناسایی کنند.

• **تحلیل حرکت و جریان جمعیت**

تحلیل حرکت و جریان جمعیت به بررسی و پیش‌بینی رفتارهای گروهی در ویدئوها می‌پردازد. تکنیک‌هایی مانند Optical Flow و مدل‌های یادگیری عمیق مانند ConvLSTM برای این منظور به‌کار می‌روند. این روش در محیط‌های عمومی مانند استادیوم‌ها، ایستگاه‌های مترو و مراکز خرید برای مدیریت ازدحام و پیشگیری از خطرات کاربرد دارد. به‌عنوان مثال، می‌توان از این تکنیک برای شناسایی تراکم بیش از حد جمعیت در یک نقطه استفاده کرد و با اقدامات سریع از وقوع حوادث جلوگیری کرد.

این تکنیک‌ها پایه و اساس سیستم‌های جدید نظارت تصویری را تشکیل می‌دهند و نقش کلیدی در بهبود امنیت و کارایی دارند. در جدول ۱ به‌طور خلاصه روش‌ها و تکنیک‌های تحلیل پیش‌بینانه در سیستم‌های نظارت تصویری ارائه شده‌اند.

ترکیب داده‌های تصویری با سایر منابع داده

یکی از رویکردهای نوین در تحلیل پیش‌بینانه، استفاده از داده‌های چندحالته است. این روش با ترکیب داده‌های تصویری و اطلاعات جمع‌آوری‌شده از حسگرهای دیگر، نتایج دقیق‌تری ارائه می‌دهد. برای مثال، ترکیب تصاویر ویدئویی با داده‌های صوتی یا داده‌های حسگرهای محیطی می‌تواند برای شناسایی سریع‌تر حوادث به‌کار رود. به عنوان نمونه، در یک ایستگاه مترو، ترکیب تصاویر دوربین‌های نظارتی با داده‌های صوتی مربوط به افزایش صداهای ناگهانی می‌تواند وقوع درگیری را پیش‌بینی کند[۷].

کاربردهای تصاویر نظارتی در تحلیل پیش‌بینانه

برخی از مهم‌ترین کاربردهای تصاویر نظارتی در تحلیل پیش‌بینانه در ادامه معرفی شده‌اند:

•کاربردهای امنیتی و پیش‌بینی جرایم:

تصاویر نظارتی به کمک تکنیک‌های پیشرفته‌ای مانند تشخیص رفتارهای غیرعادی و تحلیل الگوهای حرکتی می‌توانند رفتارهای مشکوک را شناسایی کرده و احتمال وقوع جرایم را کاهش دهند.

برای مثال، در یک ایستگاه مترو، تحلیل تصاویر نظارتی می‌تواند فردی را که به‌طور غیرعادی در یک منطقه تردد می‌کند شناسایی کند و هشدارهای لازم را به نیروی امنیتی ارسال کند[۱۲].

جدول ۱. روش‌ها و تکنیک‌های تحلیل پیش‌بینانه در سیستم‌های نظارت تصویری به‌همراه کاربردهای اصلی و تکنیک‌های استفاده‌شده

روش/ تکنیک	توضیحات	کاربردها
تشخیص اشیا	شناسایی و دسته‌بندی اشیا با استفاده از مدل‌های یادگیری عمیق مانند YOLO، Faster R-CNN و SSD	شناسایی افراد، خودروها، اشیای مشکوک، نظارت بر مناطق حساس
ردیابی اشیا	دنبال‌کردن اشیای متحرک در ویدئو با الگوریتم‌هایی مانند DeepSORT و Kalman Filter	ردیابی افراد یا وسایل نقلیه، شناسایی حرکات غیرعادی
تشخیص رفتار غیرعادی	شناسایی رفتارهای غیرعادی با استفاده از Autoencoders، One-Class SVM و GAN	تشخیص رفتارهای مشکوک، ورود غیرمجاز یا رفتارهای پرخطر
تحلیل حرکتی	تحلیل جهت و سرعت حرکت با تکنیک‌هایی مانند Optical Flow و Background Subtraction	شناسایی حرکات غیرطبیعی، تحلیل رفتار افراد یا وسایل نقلیه
تشخیص چهره	شناسایی و تطبیق چهره با مدل‌هایی مانند FaceNet، DeepFace، ArcFace	شناسایی افراد مجاز یا مظنون، جلوگیری از ورود غیرمجاز.
تحلیل جمعیت	تخمین تراکم جمعیت و تحلیل جریان حرکت با استفاده از Crowd Density Estimation و Crowd Flow Analysis	پیش‌بینی ازدحام، جلوگیری از حوادث، شناسایی تجمعات مشکوک
تشخیص رخداد	شناسایی رخدادها و توالی‌های مهم با مدل‌هایی مانند LSTM و Spatio-Temporal Networks	پیش‌بینی تصادف‌ها، شناسایی رفتارهای خطرناک
تحلیل و پیش‌بینی رفتار	پیش‌بینی رفتارهای آینده با استفاده از Behavior Clustering و Reinforcement Learning.	پیش‌بینی رفتارهای مجرمانه، تحلیل حرکات در محیط‌های حساس
کاهش ابعاد و پردازش داده‌ها	کاهش پیچیدگی داده‌ها با PCA و t-SNE برای پردازش سریع‌تر	افزایش سرعت پردازش، کاهش حجم داده‌های ویدئویی
تشخیص پلاک خودرو	شناسایی پلاک خودروها با OCR و Segmentation Models	شناسایی خودروهای مشکوک یا مجاز، نظارت بر ترافیک
فشرده‌سازی ویدئو	استفاده از تکنیک‌هایی مانند H.264 و نمونه‌گیری فریم برای کاهش حجم داده	ذخیره‌سازی بهینه، افزایش سرعت تحلیل و پردازش

•مدیریت ترافیک شهری:

در شهرهای هوشمند، تصاویر نظارتی برای تحلیل الگوهای ترافیکی و پیش‌بینی جریان خودروها به‌کار می‌روند. الگوریتم‌هایی مانند CNN وOptical Flow می‌توانند تراکم ترافیک را پیش‌بینی کرده و زمان بهینه برای تغییر چراغ‌های راهنمایی یا مدیریت ترافیک را تعیین کنند.

همچنین، این تصاویر برای شناسایی تصادف‌ها یا وسایل نقلیه‌ای که به‌طور غیرقانونی متوقف شده‌اند، استفاده می‌شوند[۱۳].

•مدیریت بحران و ایمنی عمومی:

تصاویر نظارتی در شناسایی و پیش‌بینی شرایط اضطراری مانند ازدحام بیش از حد جمعیت، حوادث آتش‌سوزی یا حوادث طبیعی مفید هستند. با استفاده از تحلیل پیش‌بینانه، می‌توان مناطق پرخطر را پیش از وقوع بحران شناسایی کرد و اقدامات پیشگیرانه انجام داد.

به‌عنوان مثال، در رویدادهای بزرگ، تحلیل جریان جمعیت از تصاویر نظارتی می‌تواند از وقوع ازدحام و آسیب‌های ناشی از آن جلوگیری کند [۷].

• کاربردهای صنعتی و تجاری:

در صنایع و فروشگاه‌ها، تصاویر نظارتی برای پیش‌بینی رفتار مشتریان، شناسایی الگوهای خرید و مدیریت بهتر منابع انسانی استفاده می‌شوند.به‌عنوان مثال، یک فروشگاه بزرگ می‌تواند از تصاویر نظارتی برای پیش‌بینی تراکم مشتریان در ساعات خاص استفاده کند و تعداد کارکنان خود را بهینه کند.

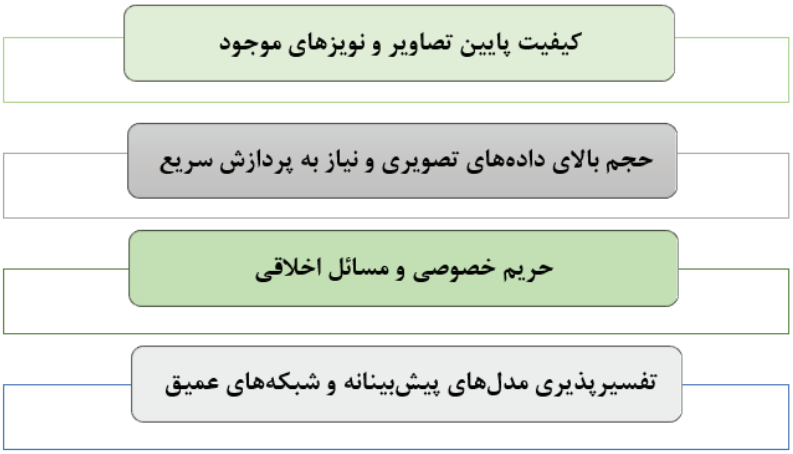
• بهینه‌سازی سیستم‌های حمل‌ونقل‌عمومی

در ایستگاه‌های مترو، فرودگاه‌ها و پایانه‌های اتوبوسرانی، تصاویر نظارتی می‌توانند برای

پیش‌بینی جریان مسافران و بهبود خدمات استفاده شوند. تحلیل داده‌های تصویری می‌تواند ازدحام را پیش‌بینی کرده و برنامهٔ حرکت وسایل حمل‌ونقل عمومی را بهینه کند[۱۴].
این کاربردها نشان‌دهندهٔ توانایی بالای کاربرد تصاویر نظارتی در بهبود مدیریت شهری، امنیت عمومی و خدمات تجاری است و با پیشرفت فناوری، این حوزه پتانسیل رشد بیشتری خواهد داشت.

چالش‌ها و محدودیت‌ها

در شکل ۴ فهرستی از مهم‌ترین چالش‌ها نشان داده شده است. در ادامه، مهم‌ترین چالش‌ها و محدودیت‌ها در این حوزه را بررسی می‌کنیم:



شکل ۴. چالش‌ها و محدودیت‌ها در تحلیل پیش‌بینانه مبتنی بر تصاویر نظارتی

• کیفیت پایین تصاویر و نویزهای موجود:

کیفیت تصاویر نظارتی به عوامل متعددی از جمله شرایط نوری، تفکیک‌پذیریِ دوربین‌ها و نویزهای محیطی وابسته است. در تصاویر با کیفیت پایین ممکن است جزئیات مهمی از دست برود و دقت الگوریتم‌های تحلیل پیش‌بینانه کاهش یابد. به‌عنوان مثال، در محیط‌هایی با نور کم یا در هوای بارانی، مدل‌های یادگیری عمیق ممکن است در شناسایی اشیا و رفتارها با خطا مواجه شوند[۴].

• حجم بالای داده‌های تصویری و نیاز به پردازش سریع:

سیستم‌های نظارتی معمولا حجم زیادی داده‌های تصویری تولید می‌کنند که نیازمند ذخیره‌سازی و پردازش سریع هستند. مدیریت این حجم از داده، به‌ویژه در زمان واقعی ، یک چالش اساسی است. استفاده از زیرساخت‌های محاسباتی قدرتمند مانند پردازش‌های ابری یا فناوری لبه از جمله راه‌حل‌های ممکن است، اما این موارد هزینه‌بر هستند و به منابع قابل توجهی نیاز دارند[۱۲].

•حریم خصوصی و مسائل اخلاقی:

استفادهٔ گسترده از تصاویر نظارتی نگرانی‌های عمده‌ای در مورد حریم خصوصی و مسائل اخلاقی ایجاد می‌کند. ضبط و تحلیل مداوم فعالیت‌های افراد ممکن است با قوانین حفظ حریم خصوصی در تضاد باشد. برای کاهش این نگرانی‌ها، استفاده از تکنیک‌های «ناشناس‌سازی داده‌ها»[۲۲] یا رمزنگاری می‌تواند تا حدی این چالش‌ها را برطرف کند، اما همچنان چالش‌های قانونی و اجتماعی قابل توجهی در این مسیر باقی می‌مانند[۷].

•تفسیرپذیری مدل‌های پیش‌بینانه و شبکه‌های عمیق:

بسیاری از مدل‌های یادگیری عمیق که در تحلیل تصاویر نظارتی به‌کار می‌روند، به دلیل پیچیدگی ساختار خود، به‌سختی قابل تفسیر هستند. این موضوع می‌تواند مانع از اعتماد کامل به نتایج پیش‌بینی شود، به‌ویژه در سیستم‌هایی که تصمیم‌گیری‌های حساس (مانند امنیت عمومی) را تحت تأثیر قرار می‌دهند. توسعهٔ «مدل‌های تفسیرپذیرتر»[۲۳] و ارائهٔ ابزارهایی برای توضیح خروجی مدل‌ها از جمله راهکارهای پیشنهادی در این زمینه است[۱۶].
با وجود این چالش‌ها، تلاش‌های پژوهشی و فناورانه در جهت بهبود کیفیت تصاویر، افزایش سرعت پردازش و تضمین حریم خصوصی می‌تواند گامی مؤثر برای توسعهٔ تحلیل پیش‌بینانه در سیستم‌های نظارتی باشد.

پیشرفت‌ها و فرصت‌های آینده

تحلیل پیش‌بینانه مبتنی بر تصاویر نظارتی با پیشرفت‌های اخیر در حوزهٔ هوش مصنوعی و یادگیری ماشین، فرصت‌های جدیدی برای ارتقای عملکرد و گسترش کاربردهای خود ایجاد کرده است. در ادامه، به بررسی مهم‌ترین پیشرفت‌ها و فرصت‌های آینده در این حوزه می‌پردازیم:

• استفاده از مدل‌های پیشرفته‌تر مانند Transformerها:

مدل‌های مبتنی بر Transformer که در ابتدا برای پردازش زبان طبیعی توسعه یافتند، اکنون به دلیل توانایی بالای آنها در شناسایی الگوهای پیچیده و روابط بلندمدت، به حوزهٔ تحلیل تصاویر نیز گسترش یافته‌اند. مدل‌هایی مانندViT[۲۴] به‌طور موفقیت‌آمیزی در وظایفی مانند تشخیص اشیا و طبقه‌بندی تصاویر مورد استفاده قرار گرفته‌اند. این مدل‌ها به دلیل معماری خود، قابلیت ترکیب با دیگر روش‌ها برای ایجاد پیش‌بینی‌های دقیق‌تر را فراهم می‌کنند[۱۵].

• بهبود پردازش بلادرنگ:

یکی از بزرگ‌ترین چالش‌های سیستم‌های نظارتی، توانایی پردازش حجم بالای داده در زمان واقعی است. پیشرفت فناوری‌های سخت‌افزاری مانند پردازنده‌های گرافیکی (GPUs) و تکنیک‌های پردازش لبه‌ای این امکان را فراهم کرده تا سیستم‌های نظارتی بتوانند در لحظه، رفتارها و حوادث را تحلیل کنند. به‌عنوان مثال، در محیط‌هایی مانند فرودگاه‌ها یا مراکز خرید، پردازش بلادرنگ می‌تواند در پیشگیری از ازدحام یا شناسایی رفتارهای مشکوک نقش حیاتی ایفا کند[۱۶].

• افزایش امنیت و حفظ حریم خصوصی در تحلیل تصاویر:

نگرانی‌های مربوط به امنیت داده‌ها و حریم خصوصی در سیستم‌های نظارتی باعث شده تا پژوهشگران به توسعهٔ تکنیک‌هایی مانند رمزنگاری داده‌ها و ناشناس‌سازی تصاویر روی آورند. روش‌هایی مانند «یادگیری فدرال»[۲۵] که بدون نیاز به انتقال داده‌ها امکان یادگیری از اطلاعات توزیع‌شده را فراهم می‌کند، به‌عنوان راهکاری مؤثر برای حفظ حریم خصوصی و امنیت مطرح شده‌اند.

•توسعه سیستم‌های ترکیبی انسان-ماشین در تحلیل پیش‌بینانه:

سیستم‌های ترکیبی که از تعامل انسان و ماشین بهره می‌برند، پتانسیل بالایی برای بهبود تحلیل پیش‌بینانه دارند. در این سیستم‌ها، الگوریتم‌های هوش مصنوعی مسئول تحلیل اولیهٔ داده‌ها هستند، در حالی که انسان‌ها برای تأیید و تفسیر نتایج وارد عمل می‌شوند. این رویکرد می‌تواند دقت پیش‌بینی‌ها را افزایش دهد و احتمال خطاهای ناشی از تفسیر نادرست مدل‌ها را کاهش دهد [۱۷]. این پیشرفت‌ها، همراه با فرصت‌های آینده می‌تواند بهبود قابل‌توجهی در کارایی و قابلیت اطمینان تحلیل پیش‌بینانه مبتنی بر تصاویر نظارتی ایجاد کند و حوزه‌های جدیدی برای تحقیق و توسعه باز کند

شکل ۵. پیشرفت‌ها و فرصت‌های آینده در حوزهٔ تحلیل پیش‌بینانه

نتیجه‌گیری

تحلیل پیش‌بینانه مبتنی بر تصاویر نظارتی، به‌عنوان یکی از کاربردهای کلیدی هوش مصنوعی و یادگیری ماشین، توانسته است تأثیر چشمگیری در بهبود امنیت، مدیریت ترافیک و نظارت محیطی داشته باشد. پژوهشگران با بهره‌گیری از الگوریتم‌های پیشرفته‌ای مانند CNN، مدل‌های Transformer و روش‌های یادگیری ترکیبی، نه‌تنها توانسته‌اند دقت پیش‌بینی‌ها را در این فناوری افزایش دهند، بلکه ظرفیت تحلیل داده‌های پیچیده را نیز گسترش داده‌اند.

با این حال، چالش‌هایی مانند کیفیت پایین تصاویر، حجم بالای داده‌های تصویری، نیاز به پردازش در زمان واقعی و مسائل مربوط به حریم خصوصی همچنان به‌عنوان موانع اساسی در این مسیر مطرح هستند. برای غلبه بر این چالش‌ها، نیاز به توسعهٔ فناوری‌های جدیدی مانند پردازش لبه‌ای، یادگیری فدرال و روش‌های رمزنگاری داده وجود دارد. در نهایت، با توجه به پیشرفت‌های سریع در فناوری و افزایش آگاهی از مسائل اخلاقی و حریم خصوصی، فرصت‌های گسترده‌ای برای بهبود و نوآوری در تحلیل پیش‌بینانه وجود دارد. این فناوری می‌تواند در آینده به‌عنوان ابزاری قدرتمند برای ایجاد سیستم‌های هوشمند و کارآمد، نقشی تعیین‌کننده ایفا کند.

منابع

1.Wang, Y., Liu, F., & Zhang, Z. (2020). Leveraging deep neural networks for predictive traffic analysis using surveillance data. Journal of Urban Computing, 138-123 ,(2)10.
2.Zhang, Z., Wang, Y., & Chen, X. (2021). Predictive analytics using surveillance images: A review of methods and applications. IEEE Transactions on Image Processing, 17-1 ,30.
3.Wang, Y., Liu, F., & Zhang, Z. (2020). Leveraging deep neural networks for predictive traffic analysis using surveillance data. Journal of Urban Computing, 138-123 ,(2)10.
4.Zhang, Z., Wang, Y., & Chen, X. (2021). Predictive analytics using surveillance images: A review of methods and applications. IEEE Transactions on Image Processing, 17-1 ,30.
5.Li, H., Xu, J., & Yang, W. (2020). Deep learning approaches for surveillance video analysis: Advances and challenges. Computer Vision and Pattern Recognition (CVPR), 62-45 ,(3)15.
6.Chen, X., Zhang, Y., & Li, J. (2020). Thermal imaging for surveillance: Advances in feature extraction and behavior analysis. IEEE Transactions on Image Processing, 10358-10347 ,29.
7.Yang, H., Xu, L., & Li, W. (2023). Multimodal data fusion for predictive analysis in urban surveillance. Pattern Recognition Letters, 102-89 ,155.
8.Xu, G., Zhao, T., & Wang, Z. (2021). Drone-based surveillance and its implications for predictive analytics: A review. Journal of Visual Communication and Image Representation, ,75 103207.
9.Huang, J., Zhang, Y., & Li, W. (2022). Advances in CNN-based image analysis for smart surveillance systems. IEEE Transactions on Image Processing, 4435-4421 ,31.
10.Zhao, L., Huang, R., & Sun, Q. (2021). Intelligent traffic management with predictive analysis: A case study in smart cities. Journal of Transportation Research Part C, 103083 ,125.
11.Goodfellow, I., Bengio, Y., & Courville, A. (2020). Deep Learning. MIT Press.
12.Cheng, D., Luo, H., & Fan, X. (2020). Anomaly detection in surveillance videos using deep learning methods: A review. Pattern Recognition Letters, 119-112 ,140.
13.Zhang, P., Wang, D., & Hu, X. (2019). Crowd movement prediction in large-scale public events using deep learning models. IEEE Transactions on Intelligent Transportation Systems.
14.Wang, Y., Liu, F., & Zhang, Z. (2021). Leveraging deep neural networks for predictive traffic analysis using surveillance data. Journal of Urban Computing, 138-123 ,(2)10.
15.Dosovitskiy, A., Beyer, L., Kolesnikov, A., et al. (2021). An image is worth 16x16 words: Transformers for image recognition at scale. International Conference on Learning Representations (ICLR).
16.Han, K., Wang, Y., & Tian, Q. (2020). Real-time video analysis: Challenges and advances. IEEE Transactions on Multimedia, 1142-1128 ,(4)22.
17.Amershi, S., Weld, D., Vorvoreanu, M., et al. (2019). Guidelines for human-AI interaction. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

1.predictive analysis
2.machine learning
3.Convolutional Neural Networks
4.Returned Neural Networks
5.Closed-Circuit Television
6.still images
7.real-time videos
8.multimodal data
9.drone imagery
10.deep CNNs
11.edge computing
12.Attention-Based Models
13.Support Vector Machine
14.random forest
15.k-means clustering
16.Principal Component Analysis
17.Long short-term memory
18.object detection
19.You Only Look Once
20.object tracking
21.anomaly detection
22.data anonymization
23.interpretable AI
24.Vision Transformer
25.federated learning

هاردنینگ امنیتی نظارت تصویری رویکردی جامع به حفاظت از زیرساخت‌های حیاتی

نویسنده:
سید علی صموتی

این مقاله به بررسی جامع روش‌های هاردنینگ امنیتی در نظارت تصویری می‌پردازد. با توجه به اهمیت روزافزون امنیت سایبری و حفاظت از داده‌های حساس، ارائه راهکارهای عملی برای افزایش امنیت این سیستم‌ها ضروری است. در این مقاله، رویکردی لایه‌ای به هاردنینگ امنیتی معرفی شده و راهکارهای عملی در چهار سطح پایه، محافظتی، امن و بسیار امن ارائه می‌گردد.

امروزه نظارت تصویری تحت شبکه به عنوان ابزارهای کلیدی در حفاظت از دارایی‌ها و اطلاعات شخصی افراد شناخته می‌شوند. این سیستم‌ها با ارائه قابلیت‌های پیشرفته، به کاربران امکان می‌دهند تا به طور مؤثری از محیط‌های خود مراقبت کنند و امنیت را در سطوح مختلف تضمین نمایند. با این حال، یک پارادوکس در حال ظهور است که نشان می‌دهد این سیستم‌ها، که به منظور محافظت طراحی شده‌اند، ممکن است خود به ابزاری برای نقض حریم خصوصی تبدیل شوند. نگرانی‌های فزاینده‌ای درباره استفاده نادرست از داده‌های تصویری و نظارت غیرمجاز بر افراد وجود دارد که می‌تواند به مشکلات جدی قانونی و اخلاقی منجر شود. این سیستم‌ها به دلیل پردازش و مدیریت داده‌های تصویری حساس، همواره در معرض تهدیدات سایبری قرار دارند. قابلیت دسترسی از راه دور به این سیستم‌ها، خطراتی را به همراه دارد که می‌تواند به سوءاستفاده از اطلاعات حساس و نفوذ به حریم خصوصی افراد منجر شود. بنابراین، ضروری است که اقدامات امنیتی مؤثری در طراحی و پیاده‌سازی این سیستم‌ها لحاظ شود. هاردنینگ امنیتی و به‌کارگیری بهترین شیوه‌ها می‌تواند به کاهش خطرات و حفاظت از اطلاعات شخصی کمک کند و اطمینان حاصل کند که این سیستم‌ها به جای تهدید، به ابزاری برای امنیت تبدیل شوند.

سطوح امنیتی در هاردنینگ نظارت تصویری

۱. سطح پایه (Default Level)

این سطح شامل قابلیت‌های امنیتی پایه است که بدون نیاز به تنظیمات اضافی در دسترس کاربران قرار دارد. یکی از مهم‌ترین ویژگی‌ها، سیاست‌های پیچیده رمز عبور است که الزام استفاده از رمزهای عبور حداقل ۸ کاراکتری با ترکیبی از حروف، اعداد و نمادها را فراهم می‌کند. این اقدام به جلوگیری از حملات مختلف مانند حملات دیکشنری و بروت‌فورس کمک می‌کند و امنیت اولیه سیستم را افزایش می‌دهد. همچنین، حذف رمز عبور پیش‌فرض یکی دیگر از ویژگی‌های مهم این سطح است که به کاربران این امکان را می‌دهد تا در اولین دسترسی خود، رمز عبور شخصی تنظیم کنند و از وجود رمز عبور اولیه که ممکن است به راحتی قابل حدس باشد، جلوگیری کنند.

محدودیت تلاش‌های ناموفق نیز از جمله ویژگی‌های کلیدی این سطح است که به مسدود کردن ورود پس از ۵ بار تلاش ناموفق در مدت ۳۰ ثانیه می‌پردازد. این ویژگی به کاهش خطر حملات بروت‌فورس کمک می‌کند و از دسترسی غیرمجاز به سیستم جلوگیری می‌کند. علاوه بر این، عدم استفاده از سرویس‌های راه دور، از جمله حذف سرویس‌های Telnet و SSH به امنیت سیستم کمک می‌کند و از نقاط ضعف بالقوه در ارتباطات شبکه‌ای جلوگیری می‌کند. این اقدامات، به ویژه در محیط‌هایی که به امنیت بالایی نیاز دارند، بسیار حیاتی هستند.

رمزنگاری تنظیمات نیز یکی دیگر از قابلیت‌های امنیتی این سطح است که به محافظت از فایل‌های پشتیبان تنظیمات کمک می‌کند. این ویژگی اطمینان می‌دهد که اطلاعات حساس مربوط به تنظیمات سیستم در برابر دسترسی غیرمجاز محافظت شده و در صورت بروز هرگونه مشکل، امکان بازیابی امن آنها وجود دارد. همچنین، امنیت فریمور با رمزنگاری و به‌روزرسانی امن فریمور، به حفظ یکپارچگی و عملکرد صحیح سیستم کمک می‌کند و از نفوذ به سیستم از طریق آسیب‌پذیری‌های فریمور جلوگیری می‌کند [۳].

در نهایت، اضافه‌کردن قابلیت‌هایی مانند واترمارک و رمزنگاری ویدئوها به این سطح، به حفاظت از محتوای تصویری و جلوگیری از سوءاستفاده از اطلاعات تصویری کمک می‌کند. این ویژگی‌ها به ویژه در محیط‌های نظارتی که اطلاعات حساس و حیاتی وجود دارد، اهمیت بالایی دارند و به کاربران این امکان را می‌دهند که اطمینان حاصل کنند که محتوای آنها به درستی محافظت شده و از دسترسی غیرمجاز جلوگیری می‌شود. در مجموع، این سطح پایه امنیتی به عنوان یک نقطه شروع مؤثر برای حفاظت از سیستم‌های نظارت تصویری تحت شبکه عمل می‌کند و می‌تواند به عنوان مبنایی برای توسعه و بهبود امنیت در سطوح بالاتر مورد استفاده قرار گیرد [۴].

۲. سطح محافظتی (Protective Level)

این سطح شامل تنظیمات امنیتی پیش‌فرض دستگاه پس از خرید یا بازگشت به تنظیمات کارخانه است که به منظور ایجاد یک محیط امن برای کاربران طراحی شده است. یکی از اولین اقداماتی که در این سطح انجام می‌شود، بازگشت به تنظیمات کارخانه است. این فرآیند شامل پاک‌سازی اطلاعات موجود در دستگاه می‌باشد که به حذف هرگونه تنظیمات یا داده‌های شخصی کمک می‌کند. این اقدام نه تنها به جلوگیری از دسترسی غیرمجاز به اطلاعات حساس کمک می‌کند، بلکه به کاربران این امکان را می‌دهد که از یک نقطه شروع امن برای پیکربندی مجدد دستگاه خود برخوردار شوند [۴،۳،۲،۱].

• غیرفعال‌سازی ورود مهمان یکی دیگر از ویژگی‌های مهم این سطح است که به محافظت از دسترسی غیرمجاز به جریان ویدیو کمک می‌کند. با غیرفعال کردن این گزینه، کاربران می‌توانند اطمینان حاصل کنند که تنها افراد مجاز به مشاهده و دسترسی به محتوای ویدیویی موجود در سیستم دسترسی دارند. این اقدام به‌ویژه در محیط‌های نظارتی که امنیت اطلاعات بسیار حیاتی است، اهمیت دارد و از سوءاستفاده‌های احتمالی جلوگیری می‌کند [۳،۲].

•غیرفعال‌سازی اتصالات RTSP بدون احراز هویت نیز از دیگر ویژگی‌های کلیدی این سطح است. این اقدام به حفاظت از جریان RTSP کمک می‌کند و اطمینان می‌دهد که تنها کاربران مجاز می‌توانند به محتوای ویدیویی دسترسی پیدا کنند.

RTSP (Real-Time Streaming Protocol) پروتکلی است که برای کنترل جریان‌های ویدیویی و صوتی در شبکه‌ها استفاده می‌شود و به ویژه در سیستم‌های نظارتی که به طور مداوم در حال انتقال داده‌ها هستند، اهمیت دارد [۳،۲].

•غیرفعال‌سازی سرویس‌های غیرضروری نیز از دیگر اقدامات امنیتی این سطح است که به کاهش سطح حمله و نقاط ضعف بالقوه کمک می‌کند. سرویس‌هایی مانند [۴]:

➢ Multicast

پروتکلی که برای ارسال داده‌ها به گروهی از کاربران به طور همزمان استفاده می‌شود. این روش به ویژه در پخش ویدیو و صوت به صورت زنده کاربرد دارد.

➢DDNS (Dynamic Domain Name System)

پروتکلی که برای ترجمه نام دامنه به آدرس IP متغیر به کار می‌رود. این پروتکل به دستگاه‌ها اجازه می‌دهد که با تغییر آدرس IP خود، همچنان با یک نام دامنه ثابت قابل دسترسی باشند.

➢ QoS (Quality of Service)

پروتکلی برای مدیریت ترافیک شبکه و تضمین کیفیت خدمات. این پروتکل به تخصیص پهنای باند به برنامه‌ها و خدمات مختلف کمک می‌کند

➢ FTP (File Transfer Protocol)

پروتکلی برای انتقال فایل‌ها بین دستگاه‌ها در شبکه. این پروتکل به کاربران این امکان را می‌دهد که فایل‌ها را به آسانی بارگذاری و دانلود کنند.

➢ SNMP (Simple Network Management Protocol)

پروتکلی برای نظارت و مدیریت دستگاه‌های شبکه. این پروتکل به مدیران شبکه این امکان را می‌دهد که وضعیت دستگاه‌ها را بررسی کنند و به صورت خودکار هشدارهایی در صورت بروز مشکلات دریافت کنند.

➢Link-Local IPv۴

پروتکلی برای ارتباطات محلی بین دستگاه‌ها در یک شبکه محلی. این پروتکل به دستگاه‌ها اجازه می‌دهد که بدون نیاز به سرور DHCP، آدرس‌های IP محلی اختصاص دهند.

➢UPnP (Universal Plug and Play)

پروتکلی برای شناسایی و ارتباط دستگاه‌ها در یک شبکه محلی. این پروتکل به دستگاه‌ها اجازه می‌دهد که به طور خودکار با یکدیگر ارتباط برقرار کنند.

➢ Bonjour

پروتکلی برای شناسایی و اتصال دستگاه‌ها در شبکه‌های محلی. این پروتکل به کاربران این امکان را می‌دهد که بدون نیاز به پیکربندی دستی، دستگاه‌ها را شناسایی و به آن‌ها متصل شوند.

➢MQTT (Message Queuing Telemetry Transport)

پروتکلی سبک برای انتقال پیام‌ها بین دستگاه‌ها در شبکه‌های IoT. این پروتکل به ویژه برای ارتباطات کم‌عرض باند و در شرایطی که اتصال ناپایدار است، مناسب است.

غیرفعال‌سازی این سرویس‌ها نه تنها به کاهش خطرات مرتبط با حملات سایبری کمک می‌کند بلکه به بهبود عملکرد کلی دستگاه نیز کمک می‌کند. با حذف سرویس‌های غیرضروری، بار ترافیکی سیستم کاهش می‌یابد و منابع بیشتری برای پردازش داده‌های مهم و ضروری در دسترس قرار می‌گیرد. این ویژگی به کاربران این امکان را می‌دهد که از حداکثر ظرفیت دستگاه خود بهره‌برداری کنند و در عین حال امنیت آن را حفظ نمایند. در نهایت، این سطح محافظتی

به عنوان یک نقطه شروع مؤثر برای ایجاد یک محیط امن در سیستم‌های نظارتی تحت شبکه عمل می‌کند. با اجرای این تنظیمات پیش‌فرض، کاربران می‌توانند اطمینان حاصل کنند که دستگاه آن‌ها به طور مؤثری در برابر تهدیدات خارجی محافظت شده است و از اطلاعات حساس خود به خوبی نگهداری می‌شود. این اقدامات نه تنها به حفاظت از اطلاعات شخصی کمک می‌کند بلکه به افزایش اعتماد کاربران به سیستم‌های نظارتی و امنیتی نیز منجر می‌شود.

۳. سطح امن (Secure Level)

این سطح شامل تنظیمات پیشرفته‌تر برای افزایش امنیت است که به کاربران این امکان را می‌دهد که از سیستم‌های خود در برابر تهدیدات سایبری محافظت کنند. یکی از اولین اقدامات، به‌روزرسانی فریمور است. این فرآیند شامل نصب آخرین نسخه‌های فریمور دستگاه می‌شود تا از بهبودهای امنیتی و رفع آسیب‌پذیری‌های شناخته‌شده بهره‌مند شوند. به‌روزرسانی‌های منظم نه تنها امنیت دستگاه را افزایش می‌دهند، بلکه عملکرد کلی آن را نیز بهبود می‌بخشند. با توجه به اینکه بسیاری از حملات سایبری از آسیب‌پذیری‌های قدیمی استفاده می‌کنند، اطمینان از به‌روزرسانی فریمور به عنوان یک اقدام اولیه و حیاتی در نظر گرفته می‌شود [۶،۵،۳،۲،۱].

تنظیم دقیق تاریخ و زمان دستگاه نیز یکی دیگر از اقدامات مهم در این سطح است. عدم دقت در زمان می‌تواند به تحلیل نادرست لاگ‌ها و مشکلات دیگر منجر شود. برای مثال، اگر زمان دستگاه به درستی تنظیم نشده باشد، ممکن است رویدادها به اشتباه ثبت شوند و در نتیجه، شناسایی حوادث امنیتی دشوار شود. با تنظیم صحیح تاریخ و زمان، کاربران می‌توانند اطمینان حاصل کنند که اطلاعات موجود در لاگ‌ها دقیق و قابل اعتماد هستند. این امر به تحلیل‌گران امنیتی کمک می‌کند تا به راحتی الگوهای مشکوک را شناسایی کرده و واکنش مناسب را نشان دهند [۳].

یکی دیگر از ویژگی‌های کلیدی در این سطح، استفاده از پروتکل‌های امن ارتباطی است. پروتکل‌هایی مانند HTTPS برای وب و RTSP امن برای انتقال ویدیو، به کاربران این امکان را می‌دهند که داده‌های خود را به صورت رمزنگاری‌شده منتقل کنند. HTTPS با استفاده از SSL/TLS، ارتباطات وب را امن می‌کند و از حملات MITM جلوگیری می‌کند. این پروتکل به ویژه برای وب‌سایت‌هایی که اطلاعات حساس را منتقل می‌کنند، ضروری است. درعین‌حال، RTSP امن به انتقال ویدیو به صورت رمزنگاری‌شده کمک می‌کند و از دسترسی غیرمجاز به محتوای ویدیویی جلوگیری می‌کند[۴،۳].

تغییر پورت‌های پیش‌فرض یکی دیگر از اقداماتی است که می‌تواند به جلوگیری از حملات اسکن کمک کند. بسیاری از حملات سایبری به سادگی با شناسایی پورت‌های پیش‌فرض سرویس‌ها آغاز می‌شوند. با تغییر این پورت‌ها، کاربران می‌توانند احتمال شناسایی و دسترسی غیرمجاز به سیستم‌های خود را کاهش دهند. این اقدام به ویژه در محیط‌های حساس که امنیت اطلاعات بسیار مهم است، اهمیت دارد. با استفاده از پورت‌های غیرمعمول، مهاجمان باید تلاش بیشتری برای شناسایی نقاط ضعف انجام دهند، که این می‌تواند به کاهش خطرات کمک کند [۴،۳،۲].

فیلترینگ IP نیز یکی دیگر از ویژگی‌های مهم در این سطح است. این اقدام به کاربران این امکان را می‌دهد که دسترسی به دستگاه را بر اساس آدرس IP محدود کنند. با ایجاد لیست‌های مجاز و محدود کردن دسترسی به آدرس‌های غیرمجاز، کاربران می‌توانند از حملات سایبری و دسترسی غیرمجاز جلوگیری کنند. این روش به ویژه در محیط‌های سازمانی که نیاز به کنترل دقیق دسترسی دارند، بسیار مؤثر است. فیلترینگ IP به کاربران این امکان را می‌دهد که تنها به آدرس‌های مشخص اجازه دسترسی دهند و از این طریق امنیت سیستم را افزایش دهند [۶،۵،۱].

استفاده امن از SNMP که اختصاریست از (Simple Network Management Protocol) نیز در این سطح توصیه می‌شود. تنها استفاده از نسخه ۳ این پروتکل به دلیل قابلیت‌های امنیتی بهتر آن، از جمله احراز هویت و رمزنگاری، بسیار مهم است.

SNMP به مدیران شبکه این امکان را می‌دهد که وضعیت دستگاه‌ها را نظارت کنند و به صورت خودکار هشدارهایی در صورت بروز مشکلات دریافت کنند. با استفاده از نسخه ۳، اطلاعات حساس مدیریت شبکه به طور مؤثری محافظت می‌شود و از دسترسی غیرمجاز جلوگیری می‌شود. این اقدام به بهبود امنیت کلی شبکه کمک می‌کند و از سوءاستفاده‌های احتمالی جلوگیری می‌کند [۷،۴].

مدیریت کاربران نیز یکی دیگر از جنبه‌های کلیدی در این سطح است. ایجاد حساب‌های کاربری با حداقل دسترسی به کاربران این امکان را می‌دهد که تنها به منابع مورد نیاز خود دسترسی داشته باشند. این اقدام به کاهش خطرات ناشی از دسترسی غیرمجاز کمک می‌کند و اطمینان می‌دهد که کاربران تنها به اطلاعات و منابع ضروری دسترسی دارند. با مدیریت دقیق کاربران، سازمان‌ها می‌توانند از سوءاستفاده‌های داخلی جلوگیری کنند و امنیت اطلاعات را بهبود بخشند. این روش به ویژه در محیط‌های حساس که اطلاعات محرمانه وجود دارد، اهمیت دارد [۳].

رمزنگاری داده‌های ذخیره شده نیز از دیگر اقداماتی است که در این سطح توصیه می‌شود. استفاده از LUKS (Linux Unified Key Setup) برای رمزنگاری داده‌های ذخیره شده بر روی دیسک، به حفاظت از اطلاعات حساس در صورت سرقت یا دسترسی غیرمجاز کمک می‌کند. این اقدام اطمینان می‌دهد که حتی در صورت دسترسی فیزیکی به دستگاه، اطلاعات حساس قابل دسترسی نخواهند بود. رمزنگاری داده‌ها به عنوان یک لایه اضافی امنیتی عمل می‌کند و به کاربران این امکان را می‌دهد که از اطلاعات خود به طور مؤثری محافظت کنند. در نهایت، رمزنگاری داده‌های پشتیبان نیز از اهمیت بالایی برخوردار است. استفاده از فایل‌های ZIP رمزنگاری شده برای پشتیبان‌گیری از داده‌ها اطمینان می‌دهد که حتی در صورت دسترسی غیرمجاز به فایل‌های پشتیبان، اطلاعات حساس محافظت شده باقی می‌مانند. این اقدام به کاربران این امکان را می‌دهد که از اطلاعات خود در برابر از دست رفتن یا سرقت محافظت کنند و به راحتی آن‌ها را بازیابی کنند. رمزنگاری پشتیبان‌ها به عنوان یک استراتژی امنیتی مهم، به افزایش اعتماد کاربران به سیستم‌های خود کمک می‌کند و از تهدیدات سایبری جلوگیری می‌کند [۷،۳،۱].

با اجرای این تنظیمات پیشرفته، کاربران می‌توانند اطمینان حاصل کنند که سیستم‌های نظارتی و امنیتی آن‌ها به طور مؤثری در برابر حملات محافظت شده‌اند. این اقدامات نه تنها به حفاظت از اطلاعات شخصی کمک می‌کند بلکه به افزایش اعتماد کاربران به سیستم‌های خود نیز منجر می‌شود. به طور کلی، این سطح امن به عنوان یک نقطه شروع مؤثر برای ایجاد یک محیط امن در سیستم‌های نظارتی تحت شبکه عمل می‌کند [۴].

۴.سطح بسیار امن (Very Secure Level)

این سطح بالاترین سطح امنیتی است که با ترکیب قابلیت‌های امنیتی دستگاه و راهکارهای امنیتی خارجی حاصل می‌شود. یکی از ویژگی‌های کلیدی این سطح، کنترل دسترسی مبتنی بر گواهی X 802.1 است. این پروتکل به سازمان‌ها این امکان را می‌دهد که دسترسی به شبکه را به صورت دقیق مدیریت کنند. با پیاده‌سازی کنترل دسترسی مبتنی بر پورت، تنها دستگاه‌های مجاز می‌توانند به شبکه متصل شوند. این روش به ویژه در محیط‌های سازمانی که نیاز به امنیت بالا دارند، بسیار مؤثر است. با این سیستم، هر دستگاهی که تلاش می‌کند به شبکه متصل شود، باید گواهی معتبر را ارائه دهد تا اجازه دسترسی دریافت کند [۴،۳،۲،۱].

احراز هویت متقابل دستگاه نیز یکی دیگر از ویژگی‌های مهم در این سطح است. این فرآیند شامل استفاده از گواهی‌نامه‌های دیجیتال برای شناسایی و تأیید هویت دستگاه‌ها می‌شود. با استفاده از این روش، هر دستگاه قبل از برقراری ارتباط با سایر دستگاه‌ها باید هویت خود را تأیید کند. این اقدام به جلوگیری از حملات سایبری و دسترسی غیرمجاز کمک می‌کند. احراز هویت متقابل به افزایش اعتماد در ارتباطات شبکه‌ای کمک می‌کند و اطمینان می‌دهد که تنها دستگاه‌های معتبر قادر به برقراری ارتباط هستند. این ویژگی به ویژه در محیط‌های حساس که امنیت اطلاعات بسیار مهم است، اهمیت دارد [۴،۳].

امنیت فیزیکی نیز از دیگر جنبه‌های حیاتی در این سطح است. محافظت از دستگاه‌ها در برابر دستکاری فیزیکی می‌تواند از حملات مستقیم و دسترسی غیرمجاز جلوگیری کند. این اقدام شامل استفاده از قفل‌های فیزیکی، دوربین‌های نظارتی و سیستم‌های هشدار است. با ایجاد محیطی امن برای دستگاه‌ها، سازمان‌ها می‌توانند از سرقت یا آسیب به تجهیزات خود جلوگیری کنند. امنیت فیزیکی به عنوان یک لایه اضافی از امنیت، به حفاظت از اطلاعات حساس و زیرساخت‌های حیاتی کمک می‌کند. این اقدام به ویژه در مکان‌هایی که دستگاه‌ها در معرض خطر هستند، اهمیت دارد [۴،۳].

در این سطح، مدیریت جامع امنیت نیز اهمیت ویژه‌ای دارد. این مدیریت شامل نظارت مستمر بر سیستم‌ها و ارزیابی تهدیدات بالقوه است. با استفاده از ابزارهای پیشرفته، سازمان‌ها می‌توانند به سرعت به تهدیدات واکنش نشان دهند و از بروز حوادث امنیتی جلوگیری کنند. این مدیریت به کاربران این امکان را می‌دهد که نقاط ضعف سیستم‌های خود را شناسایی کرده و اقدامات لازم را برای بهبود امنیت انجام دهند. همچنین، آموزش مداوم کارکنان در زمینه امنیت سایبری می‌تواند به کاهش خطرات ناشی از خطاهای انسانی کمک کند.

استفاده از رمزنگاری پیشرفته نیز در این سطح توصیه می‌شود. رمزنگاری داده‌ها به کاربران این امکان را می‌دهد که اطلاعات حساس خود را از دسترسی غیرمجاز محافظت کنند. با استفاده از الگوریتم‌های رمزنگاری قوی، داده‌ها به صورت نامفهوم ذخیره می‌شوند و تنها افراد مجاز می‌توانند به آن‌ها دسترسی پیدا کنند. این اقدام به ویژه در انتقال اطلاعات حساس بین دستگاه‌ها و سرورها اهمیت دارد. رمزنگاری نه تنها به حفاظت از داده‌ها کمک می‌کند، بلکه به افزایش اعتماد کاربران به سیستم‌های امنیتی نیز منجر می‌شود.

نظارت و تحلیل ترافیک شبکه نیز از دیگر ویژگی‌های مهم در این سطح است. با استفاده از ابزارهای پیشرفته، سازمان‌ها می‌توانند ترافیک شبکه را به صورت لحظه‌ای تحلیل کنند و فعالیت‌های مشکوک را شناسایی کنند. این نظارت به کاربران این امکان را می‌دهد که به سرعت به تهدیدات واکنش نشان دهند و از بروز حملات جلوگیری کنند. همچنین، تحلیل ترافیک می‌تواند به شناسایی الگوهای غیرعادی و رفتارهای مشکوک کمک کند. این اقدام به طور کلی به بهبود امنیت شبکه و حفاظت از اطلاعات حساس منجر می‌شود.

ایجاد سیاست‌های امنیتی جامع نیز در این سطح ضروری است. این سیاست‌ها باید شامل دستورالعمل‌های واضح برای مدیریت امنیت، دسترسی و استفاده از منابع باشد. با تدوین سیاست‌های امنیتی، سازمان‌ها می‌توانند اطمینان حاصل کنند که تمامی کارکنان از رویه‌های امنیتی پیروی می‌کنند. این سیاست‌ها باید به طور منظم بازنگری و به‌روز شوند تا با تغییرات فناوری و تهدیدات جدید هم‌راستا باشند. ایجاد یک فرهنگ امنیتی در سازمان به کاهش خطرات و افزایش آگاهی کارکنان کمک می‌کند [۴،۳].

پشتیبان‌گیری منظم و امن نیز از دیگر جنبه‌های حیاتی در این سطح است. با ایجاد نسخه‌های پشتیبان از داده‌های حساس و ذخیره‌سازی آن‌ها در مکان‌های امن، سازمان‌ها می‌توانند از از دست رفتن اطلاعات در صورت بروز حوادث امنیتی جلوگیری کنند. این نسخه‌های پشتیبان باید به صورت رمزنگاری شده و در مکان‌های جداگانه نگهداری شوند. این اقدام به کاربران این امکان را می‌دهد که در صورت بروز مشکل، به سرعت به اطلاعات خود دسترسی پیدا کنند و آن‌ها را بازیابی کنند. پشتیبان‌گیری منظم به عنوان یک استراتژی امنیتی مهم، به افزایش اعتماد کاربران به سیستم‌های خود کمک می‌کند [۴،۲].

در نهایت، آزمون و ارزیابی امنیتی منظم نیز از اهمیت بالایی برخوردار است. با انجام تست‌های نفوذ و ارزیابی‌های امنیتی، سازمان‌ها می‌توانند نقاط ضعف سیستم‌های خود را شناسایی کرده و اقدامات لازم را برای بهبود امنیت انجام دهند. این ارزیابی‌ها باید به صورت دوره‌ای انجام شوند تا اطمینان حاصل شود که سیستم‌ها در برابر تهدیدات جدید مقاوم هستند. با توجه به تغییرات مداوم در فناوری و تهدیدات سایبری، این ارزیابی‌ها به عنوان بخشی از استراتژی امنیتی کلی سازمان باید در نظر گرفته شوند. این اقدام به کاربران این امکان را می‌دهد که از امنیت سیستم‌های خود اطمینان حاصل کنند و در برابر حملات سایبری محافظت شوند [۷،۵،۳].

۳. بهترین شیوه‌های پیاده‌سازی

۳-۱- مدیریت رمزهای عبور

مدیریت رمزهای عبور یکی از جنبه‌های کلیدی امنیت اطلاعات است و پیاده‌سازی بهترین شیوه‌ها در این زمینه می‌تواند به طور قابل توجهی از خطرات ناشی از دسترسی غیرمجاز جلوگیری کند. اولین و مهم‌ترین اقدام، استفاده از رمزهای عبور پیچیده است. رمزهای عبور باید شامل ترکیبی از حروف بزرگ و کوچک، اعداد و نمادها باشند و حداقل ۱۲ تا ۱۶ کاراکتر طول داشته باشند. این نوع رمزهای عبور به سختی قابل حدس زدن هستند و به همین دلیل امنیت بیشتری را فراهم می‌کنند. همچنین، استفاده از عبارات عبور (passphrases) به جای رمزهای عبور ساده می‌تواند به افزایش امنیت کمک کند. به عنوان مثال، استفاده از یک جمله یا عبارت تصادفی که برای کاربر معنی دارد، می‌تواند به یادآوری آسان‌تر و در عین حال پیچیدگی بیشتر منجر شود [۸،۴،۲].

بهترین شیوه دیگر در این بخش، تغییر منظم رمزهای عبور است. سازمان‌ها باید سیاست‌هایی را برای تغییر دوره‌ای رمزهای عبور تعیین کنند. این تغییر می‌تواند هر سه تا شش ماه یک بار انجام شود. با تغییر منظم رمزهای عبور، احتمال دسترسی غیرمجاز به حساب‌ها کاهش می‌یابد،

به ویژه اگر رمز عبور قبلاً به خطر افتاده باشد. این اقدام به کاربران یادآوری می‌کند که به امنیت حساب‌های خود توجه کنند و از استفاده طولانی‌مدت از یک رمز عبور خاص جلوگیری کنند. همچنین، آموزش کارکنان درباره اهمیت تغییر منظم رمزهای عبور و تأثیر آن بر امنیت کلی سازمان، می‌تواند به افزایش آگاهی و رعایت این سیاست‌ها کمک کند [۸].

سومین اقدام مهم، عدم استفاده از رمزهای عبور پیش‌فرض است. بسیاری از دستگاه‌ها و نرم‌افزارها با رمزهای عبور پیش‌فرض عرضه می‌شوند که معمولا در دسترس عموم قرار دارند. این رمزهای عبور به راحتی قابل شناسایی و سوءاستفاده هستند. بنابراین، کاربران باید بلافاصله پس از نصب یا راه‌اندازی دستگاه، رمز عبور پیش‌فرض را تغییر دهند. این اقدام به ویژه در مورد دستگاه‌های متصل به شبکه و سیستم‌های مدیریتی اهمیت دارد، زیرا عدم تغییر رمز عبور پیش‌فرض می‌تواند به راحتی منجر به دسترسی غیرمجاز شود. سازمان‌ها باید سیاست‌های سخت‌گیرانه‌ای را برای تغییر این رمزهای عبور پیش‌فرض پیاده‌سازی کنند و از کاربران بخواهند که این تغییرات را به عنوان بخشی از فرآیند راه‌اندازی انجام دهند [۸,۲].

شیوه دیگر، پیاده‌سازی سیاست قفل حساب است. این سیاست به کاربران این امکان را می‌دهد که پس از چند تلاش ناموفق برای ورود به سیستم، حساب کاربری قفل شود. این اقدام به جلوگیری از حملات brute force کمک می‌کند، جایی که مهاجم تلاش می‌کند تا با امتحان کردن رمزهای عبور مختلف به حساب‌ها دسترسی پیدا کند. معمولا، پس از چند تلاش ناموفق (مثلاً ۵ تلاش)، حساب به مدت مشخصی قفل می‌شود و کاربر باید برای بازگشایی آن مراحل احراز هویت را طی کند. این سیاست نه تنها از دسترسی غیرمجاز جلوگیری می‌کند، بلکه به کاربران یادآوری می‌کند که امنیت حساب‌های خود را جدی بگیرند و از رمزهای عبور قوی استفاده کنند. به علاوه، اطلاع‌رسانی به کاربران در مورد قفل شدن حساب و مراحل لازم برای بازیابی آن، می‌تواند به افزایش امنیت و آگاهی کاربران کمک کند [۸,۴,۲].

۳-۲- مدیریت دسترسی

مدیریت دسترسی یکی از ارکان اساسی امنیت اطلاعات است و پیاده‌سازی بهترین شیوه‌ها در این زمینه می‌تواند به جلوگیری از دسترسی غیرمجاز و حفاظت از اطلاعات حساس کمک کند. اولین اصل مهم در این زمینه، اعمال اصل حداقل دسترسی است. این اصل به این معناست که کاربران تنها باید به اطلاعات و منابعی دسترسی داشته باشند که برای انجام وظایف خود به آن‌ها نیاز دارند. با پیاده‌سازی این اصل، سازمان‌ها می‌توانند خطرات ناشی از دسترسی غیرمجاز را کاهش دهند و از سوءاستفاده‌های احتمالی جلوگیری کنند. این اقدام به ویژه در محیط‌های سازمانی که اطلاعات حساس و حیاتی وجوددارد، اهمیت ویژه‌ای دارد [۲,۹,۸,۴]

دومین اقدام مهم در مدیریت دسترسی، ایجاد حساب‌های کاربری جداگانه برای هر کاربر است. استفاده از حساب‌های مشترک می‌تواند منجر به مشکلاتی در شناسایی و ردیابی فعالیت‌ها شود. با ایجاد حساب‌های کاربری منحصر به فرد، سازمان‌ها می‌توانند به راحتی فعالیت‌های هر کاربر را نظارت کنند و در صورت بروز مشکلات امنیتی، به سرعت به شناسایی منبع مشکل بپردازند. این اقدام همچنین به افزایش مسئولیت‌پذیری کاربران کمک می‌کند، زیرا هر کاربر می‌داند که فعالیت‌های او قابل شناسایی است و باید در استفاده از منابع سازمانی دقت کند [۹,۸].

استفاده از احراز هویت دو عاملی (FA2) نیز یکی دیگر از بهترین شیوه‌های مدیریت دسترسی است. این روش به کاربران این امکان را می‌دهد که برای ورود به سیستم، علاوه بر رمز عبور، یک عامل دوم شناسایی (مانند کد ارسال شده به تلفن همراه یا ایمیل) را وارد کنند. این اقدام به طور قابل توجهی امنیت حساب‌های کاربری را افزایش می‌دهد و حتی در صورت به خطر افتادن رمز عبور، دسترسی غیرمجاز به سیستم‌ها و اطلاعات حساس را دشوارتر می‌کند. پیاده‌سازی FA2 به ویژه در حساب‌های کاربری با دسترسی به اطلاعات حساس و حیاتی توصیه می‌شود [۹,۴].

بازنگری منظم دسترسی‌ها نیز از دیگر جنبه‌های مهم در مدیریت دسترسی است. سازمان‌ها باید به طور دوره‌ای دسترسی‌های کاربران را بررسی کنند و اطمینان حاصل کنند که تنها افرادی که به اطلاعات خاص نیاز دارند، به آن‌ها دسترسی دارند. این بازنگری‌ها می‌توانند شامل حذف دسترسی‌های غیرضروری برای کارمندانی باشند که به دلایل مختلف (مانند تغییر شغل یا ترک سازمان) دیگر نیازی به دسترسی ندارند. با این اقدام، سازمان‌ها می‌توانند از خطرات ناشی از دسترسی‌های غیرمجاز جلوگیری کنند و امنیت کلی سیستم‌های خود را افزایش‌دهند [۹,۸,۴ ,۲]

آموزش کاربران در مورد اهمیت مدیریت دسترسی و شیوه‌های صحیح استفاده از آن نیز بسیار حیاتی است. سازمان‌ها باید برنامه‌های آموزشی منظم برای کارکنان خود برگزار کنند تا آن‌ها را با بهترین شیوه‌های امنیتی آشنا کنند. این آموزش‌ها می‌توانند شامل آگاهی از خطرات ناشی از دسترسی غیرمجاز و نحوه استفاده صحیح از حساب‌های کاربری باشند. با افزایش آگاهی کارکنان، احتمال بروز خطاهای انسانی و سوءاستفاده‌های ناخواسته کاهش می‌یابد و امنیت کلی سازمان بهبود می‌یابد [۹,۴,۳].

استفاده از نرم‌افزارهای مدیریت دسترسی نیز می‌تواند به بهبود فرآیند مدیریت دسترسی کمک کند. این نرم‌افزارها به سازمان‌ها این امکان را می‌دهند که به راحتی دسترسی‌های کاربران را مدیریت کنند و گزارش‌های دقیقی از فعالیت‌های کاربران ارائه دهند. این ابزارها می‌توانند به شناسایی رفتارهای مشکوک و دسترسی‌های غیرمجاز کمک کنند و امکان نظارت مستمر بر امنیت سیستم‌ها را فراهم آورند. با استفاده از این نرم‌افزارها، سازمان‌ها می‌توانند به صورت مؤثرتری به مدیریت دسترسی‌ها و حفاظت از اطلاعات حساس بپردازند.

در نهایت، ایجاد سیاست‌های امنیتی واضح و جامع در زمینه مدیریت دسترسی نیز از اهمیت بالایی برخوردار است. این سیاست‌ها باید شامل دستورالعمل‌های مشخصی برای مدیریت دسترسی، احراز هویت و استفاده از منابع باشد. با تدوین این سیاست‌ها و اطلاع‌رسانی به کارکنان، سازمان‌ها می‌توانند اطمینان حاصل کنند که تمامی اعضای تیم از رویه‌های امنیتی پیروی می‌کنند. این سیاست‌ها باید به طور منظم بازنگری و به‌روز شوند تا با تغییرات فناوری و تهدیدات جدید هم‌راستا باشند. این اقدام به افزایش امنیت و حفاظت از اطلاعات حساس سازمان کمک می‌کند [۹,۴,۳].

۳-۳- امنیت شبکه

امنیت شبکه یکی از جنبه‌های حیاتی در حفاظت از اطلاعات و سیستم‌های سازمانی است. با افزایش تهدیدات سایبری و حملات به شبکه‌ها، پیاده‌سازی بهترین شیوه‌ها در این زمینه ضروری است. یکی از مهم‌ترین اقدامات در این راستا، جداسازی شبکه دوربین‌ها است. این جداسازی به معنای ایجاد یک شبکه مستقل برای دوربین‌های مداربسته و تجهیزات نظارتی است. با این کار، می‌توان از دسترسی غیرمجاز به تصاویر و داده‌های حساس جلوگیری کرد. همچنین، این

اقدام باعث کاهش بار ترافیکی روی شبکه اصلی می‌شود و عملکرد کلی سیستم‌های نظارتی را بهبود می‌بخشد. جداسازی شبکه دوربین‌ها به سازمان‌ها این امکان را می‌دهد که امنیت بیشتری را برای اطلاعات حساس خود فراهم کنند [۹،۸،۴،۲].

دومین شیوه موثر، استفاده از VLAN (شبکه‌های محلی مجازی) است. با ایجاد VLAN، می‌توان گروه‌های مختلفی از کاربران و دستگاه‌ها را در شبکه تفکیک کرد. این تفکیک به سازمان‌ها این امکان را می‌دهد که دسترسی به منابع خاص را بر اساس نیاز کاربران مدیریت کنند. به عنوان مثال، می‌توان VLANهای جداگانه‌ای برای بخش‌های مختلف سازمان ایجاد کرد و به این ترتیب، امنیت و کنترل بیشتری بر روی ترافیک شبکه اعمال کرد. همچنین، استفاده از VLAN می‌تواند به کاهش خطرات ناشی از حملات داخلی کمک کند و امکان نظارت دقیق‌تری بر روی ترافیک داده‌ها را فراهم آورد.

پیاده‌سازی فایروال نیز یکی دیگر از اقدامات کلیدی در امنیت شبکه است. فایروال‌ها به عنوان یک خط دفاعی اولیه در برابر تهدیدات خارجی عمل می‌کنند و ترافیک ورودی و خروجی شبکه را بررسی و کنترل می‌کنند. با تنظیم قوانین مناسب برای فایروال، سازمان‌ها می‌توانند به راحتی از دسترسی‌های غیرمجاز جلوگیری کنند و ترافیک مشکوک را شناسایی کنند. فایروال‌ها می‌توانند به صورت سخت‌افزاری یا نرم‌افزاری پیاده‌سازی شوند و بسته به نیاز سازمان، می‌توانند قابلیت‌های مختلفی را ارائه دهند. این ابزارها به عنوان یک لایه امنیتی اضافی، امنیت کلی شبکه را افزایش می‌دهند.

رمزنگاری ارتباطات یکی دیگر از شیوه‌های مهم در امنیت شبکه است. با رمزنگاری داده‌ها، اطلاعات حساس در حین انتقال بین دستگاه‌ها محافظت می‌شود و حتی در صورت دسترسی غیرمجاز به داده‌ها، اطلاعات قابل خواندن نخواهند بود. استفاده از پروتکل‌های رمزنگاری مانند SSL/TLS برای ارتباطات اینترنتی و VPN برای ارتباطات داخلی، می‌تواند به افزایش امنیت کمک کند. این اقدام به ویژه در محیط‌های سازمانی که اطلاعات حساس و حیاتی وجود دارد، بسیار ضروری است. با رمزنگاری ارتباطات، سازمان‌ها می‌توانند از حریم خصوصی و امنیت اطلاعات خود محافظت کنند [۸،۳،۲].

نظارت مستمر بر شبکه نیز از دیگر جنبه‌های مهم امنیت شبکه است. با استفاده از ابزارهای نظارتی، سازمان‌ها می‌توانند به طور مداوم فعالیت‌های شبکه را زیر نظر داشته باشند و هرگونه رفتار مشکوک یا غیرمعمول را شناسایی کنند. این نظارت می‌تواند شامل تجزیه و تحلیل ترافیک شبکه، شناسایی الگوهای غیرعادی و بررسی لاگ‌های فعالیت‌ها باشد. با شناسایی زودهنگام تهدیدات، سازمان‌ها می‌توانند اقدامات لازم را برای مقابله با حملات انجام دهند و از بروز آسیب‌های جدی جلوگیری کنند. این اقدام به افزایش توان دفاعی سازمان در برابر تهدیدات سایبری کمک می‌کند.

آموزش کارکنان در زمینه امنیت شبکه نیز بسیار حیاتی است. سازمان‌ها باید برنامه‌های آموزشی منظم برای کارکنان خود برگزار کنند تا آن‌ها را با بهترین شیوه‌های امنیتی آشنا کنند. این آموزش‌ها می‌توانند شامل آگاهی از خطرات ناشی از حملات سایبری، نحوه شناسایی ایمیل‌های فیشینگ و استفاده صحیح از شبکه باشند. با افزایش آگاهی کارکنان، احتمال بروز خطاهای انسانی و سوءاستفاده‌های ناخواسته کاهش می‌یابد. همچنین، کارکنان باید بدانند که در صورت شناسایی هرگونه رفتار مشکوک، باید به سرعت به مسئولان امنیتی گزارش دهند۴،۳.

استفاده از سیستم‌های تشخیص نفوذ(IDS) نیز می‌تواند به بهبود امنیت شبکه کمک کند. این سیستم‌ها به شناسایی و تجزیه و تحلیل ترافیک شبکه پرداخته و هرگونه فعالیت مشکوک را شناسایی می‌کنند. با استفاده از IDS، سازمان‌ها می‌توانند به سرعت به تهدیدات پاسخ دهند و اقدامات لازم را برای جلوگیری از نفوذ انجام دهند. این سیستم‌ها می‌توانند به صورت خودکار هشدارهایی به مسئولان امنیتی ارسال کنند و به آن‌ها کمک کنند تا به موقع اقدامات لازم را انجام دهند. استفاده از IDS به عنوان یک لایه امنیتی اضافی، به بهبود امنیت کلی شبکه کمک می‌کند.

پیاده‌سازی سیاست‌های امنیتی جامع نیز از اهمیت بالایی برخوردار است. این سیاست‌ها باید شامل دستورالعمل‌های مشخصی برای امنیت شبکه، مدیریت دسترسی و استفاده از منابع باشد. با تدوین این سیاست‌ها و اطلاع‌رسانی به کارکنان، سازمان‌ها می‌توانند اطمینان حاصل کنند که تمامی اعضای تیم از رویه‌های امنیتی پیروی می‌کنند. این سیاست‌ها باید به طور منظم بازنگری و به‌روز شوند تا با تغییرات فناوری و تهدیدات جدید هم‌راستا باشند. این اقدام به افزایش امنیت و حفاظت از اطلاعات حساس سازمان کمک می‌کند. چارچوب‌ها و چک لیست‌های متعددی توسط ارگان‌های بین المللی و ملی تصویب شده است که میتواند راهکار مناسب در این حوزه باشد.

استفاده از به‌روزرسانی‌های منظم نرم‌افزار نیز یکی دیگر از شیوه‌های مهم در امنیت شبکه است. نرم‌افزارها و سیستم‌عامل‌ها باید به‌طور منظم به‌روز شوند تا از آسیب‌پذیری‌های شناخته‌شده جلوگیری شود. این به‌روزرسانی‌ها معمولا شامل وصله‌های امنیتی هستند که به رفع مشکلات و آسیب‌پذیری‌های موجود کمک می‌کنند. سازمان‌ها باید یک برنامه منظم برای به‌روزرسانی نرم‌افزارهای خود داشته باشند و اطمینان حاصل کنند که تمامی دستگاه‌ها و سیستم‌ها به آخرین نسخه‌های امنیتی مجهز هستند. این اقدام به کاهش خطرات ناشی از حملات سایبری کمک می‌کند و امنیت کلی شبکه را بهبود می‌بخشد [۶،۴،۳].

در نهایت، ایجاد یک برنامه پاسخ به حادثه نیز از اهمیت بالایی برخوردار است. این برنامه باید شامل مراحل مشخصی برای شناسایی، تجزیه و تحلیل و پاسخ به حملات سایبری باشد. با داشتن یک برنامه پاسخ به حادثه، سازمان‌ها می‌توانند به سرعت به تهدیدات پاسخ دهند و آسیب‌های احتمالی را کاهش دهند. این برنامه باید به‌طور منظم آزمایش و به‌روز شود تا اطمینان حاصل شود که در صورت بروز حمله، تیم‌های امنیتی آماده و مجهز به پاسخگویی هستند. با این اقدام، سازمان‌ها می‌توانند امنیت شبکه خود را بهبود بخشند و از اطلاعات حساس خود محافظت کنند [۹،۷،۶،۴،۱].

۳-۴- نظارت و ثبت رویدادها

نظارت و ثبت رویدادها یکی از جنبه‌های حیاتی در امنیت اطلاعات است که به سازمان‌ها کمک می‌کند تا فعالیت‌های مشکوک را شناسایی و به موقع واکنش نشان دهند. اولین اقدام در این زمینه، فعال‌سازی ثبت رویدادها است. با فعال کردن این ویژگی، تمامی فعالیت‌های کاربران و سیستم‌ها در یک پایگاه داده ثبت می‌شود. این اطلاعات می‌توانند شامل ورود و خروج کاربران، تغییرات در فایل‌ها و دسترسی به منابع باشند. ثبت دقیق این رویدادها به سازمان‌ها این امکان را می‌دهد که در صورت بروز مشکلات، به سادگی به شناسایی منبع مشکل بپردازند و اقدامات لازم را انجام دهند [۹،۷،۵،۲].

دومین اقدام مهم، بررسی منظم لاگ‌ها است. سازمان‌ها باید به طور دوره‌ای لاگ‌های

ثبت‌شده را مورد بررسی قرار دهند تا هرگونه رفتار غیرمعمول یا مشکوک را شناسایی کنند. این بررسی‌ها می‌توانند شامل تجزیه و تحلیل الگوهای دسترسی، شناسایی ورودهای غیرمجاز و پیگیری تغییرات غیرمنتظره در سیستم‌ها باشند. با شناسایی زودهنگام تهدیدات، سازمان‌ها می‌توانند اقدامات لازم را برای مقابله با حملات انجام دهند و از بروز آسیب‌های جدی جلوگیری کنند. این فرآیند بررسی باید به صورت مستمر و با استفاده از ابزارهای مناسب انجام شود [۹،۷،۶،۱].

ذخیره‌سازی امن لاگ‌ها نیز از دیگر جنبه‌های مهم نظارت و ثبت رویدادها است. لاگ‌ها باید در محیطی امن ذخیره‌سازی شوند تا از دسترسی غیرمجاز و تغییرات ناخواسته محافظت شوند. استفاده از رمزنگاری برای ذخیره‌سازی لاگ‌ها و همچنین تعیین سیاست‌های دسترسی مناسب می‌تواند به حفاظت از این اطلاعات کمک کند. همچنین، سازمان‌ها باید اطمینان حاصل کنند که لاگ‌ها برای مدت زمان معین و مطابق با قوانین و مقررات مربوطه نگهداری می‌شوند. این اقدام به سازمان‌ها این امکان را می‌دهد که در صورت نیاز، به سادگی به اطلاعات ثبت‌شده دسترسی داشته باشند و از آن‌ها برای تحلیل‌های بعدی استفاده کنند [۹،۶،۴،۲].

هشدار خودکار رویدادهای مشکوک یکی دیگر از بهترین شیوه‌ها در نظارت و ثبت رویدادها است. با پیاده‌سازی سیستم‌های هشداردهنده، سازمان‌ها می‌توانند به سرعت به فعالیت‌های مشکوک واکنش نشان دهند. این سیستم‌ها می‌توانند به صورت خودکار رویدادهای غیرمعمول را شناسایی کرده و هشدارهایی به مسئولان امنیتی ارسال کنند. این اقدام به سازمان‌ها این امکان را می‌دهد که در زمان واقعی به تهدیدات پاسخ دهند و از بروز آسیب‌های جدی جلوگیری کنند. همچنین، این سیستم‌ها می‌توانند به کاهش زمان واکنش به تهدیدات کمک کنند و امنیت کلی شبکه را بهبود بخشند [۹،۶،۴،۲].

در نهایت، آموزش کارکنان در زمینه اهمیت نظارت و ثبت رویدادها نیز بسیار حیاتی است. سازمان‌ها باید برنامه‌های آموزشی منظم برای کارکنان خود برگزار کنند تا آن‌ها را با بهترین شیوه‌های امنیتی آشنا کنند. این آموزش‌ها می‌توانند شامل نحوه شناسایی رفتارهای مشکوک و اهمیت گزارش‌دهی به موقع باشند. با افزایش آگاهی کارکنان، احتمال بروز خطاهای انسانی و سوءاستفاده‌های ناخواسته کاهش می‌یابد. همچنین، کارکنان باید بدانند که در صورت شناسایی هرگونه رفتار مشکوک، باید به سرعت به مسئولان امنیتی گزارش دهند. این اقدام به تقویت فرهنگ امنیتی در سازمان و حفاظت از اطلاعات حساس کمک می‌کند [۲، ۹،۶،۴].

۴.چالش‌ها و راهکارها

۴-۱- چالش‌های فنی

چالش‌های فنی در امنیت اطلاعات می‌توانند به طور قابل توجهی بر عملکرد و کارایی سیستم‌ها تأثیر بگذارند. یکی از این چالش‌ها، پیچیدگی پیکربندی است. بسیاری از سیستم‌ها و ابزارهای امنیتی نیاز به پیکربندی دقیق دارند تا به درستی عمل کنند.این پیچیدگی ممکن است منجر به خطاهای انسانی شود که در نهایت به نقاط ضعف امنیتی منجر می‌شود.

به همین دلیل، سازمان‌ها باید به دقت مراحل پیکربندی را دنبال کنند و از ابزارهای خودکار برای کاهش احتمال خطا استفاده کنند [۹،۸،۵،۲].

چالش دیگری که سازمان‌ها با آن مواجه هستند، محدودیت‌های سخت‌افزاری است.بسیاری از سیستم‌های امنیتی نیاز به منابع سخت‌افزاری بالا دارند که ممکن است در دسترس نباشند. این محدودیت‌ها می‌توانند عملکرد کلی سیستم را تحت تأثیر قرار دهند و در برخی موارد، منجر به ناتوانی در پیاده‌سازی راهکارهای امنیتی مناسب شوند. سازمان‌ها باید به این موضوع توجه داشته باشند و منابع لازم برای پشتیبانی از سیستم‌های امنیتی خود را تأمین کنند [۹،۸،۵،۲].

تداخل با عملکرد نیز یکی دیگر از چالش‌های فنی است. ابزارهای امنیتی ممکن است باعث کاهش سرعت سیستم‌ها و تأثیر منفی بر تجربه کاربری شوند. این تداخل می‌تواند موجب نارضایتی کارکنان و کاهش بهره‌وری شود. برای مقابله با این چالش، سازمان‌ها باید به دنبال راهکارهایی باشند که امنیت را بدون تأثیر منفی بر عملکرد سیستم‌ها حفظ کنند. این اقدام شامل انتخاب ابزارهای بهینه و تنظیمات مناسب برای کاهش بار اضافی بر روی سیستم‌ها است [۹،۸،۵،۳،۲].

چالش دیگر، نیاز به تخصص فنی است. بسیاری از راهکارهای امنیتی نیاز به دانش و تخصص بالا دارند که ممکن است در دسترس همه سازمان‌ها نباشد.کمبود کارشناسان ماهر در زمینه امنیت اطلاعات می‌تواند منجر به ضعف در پیاده‌سازی و مدیریت سیستم‌های امنیتی شود. به همین دلیل، سازمان‌ها باید به جذب و آموزش نیروی انسانی متخصص در این حوزه توجه ویژه‌ای داشته باشند و از منابع خارجی نیز در صورت نیاز استفاده کنند [۹،۷،۵].

۴-۲- راهکارها

برای مقابله با چالش‌های فنی، آموزش مستمر تیم فنی یکی از بهترین راهکارها است. با برگزاری دوره‌های آموزشی منظم، تیم‌های فنی می‌توانند با آخرین تکنولوژی‌ها و به‌روزترین روش‌های امنیتی آشنا شوند. این آموزش‌ها به کارکنان این امکان را می‌دهد که توانایی‌های خود را افزایش دهند و به طور مؤثری با چالش‌ها مقابله کنند. همچنین، این اقدام به تقویت فرهنگ امنیتی در سازمان کمک می‌کند و باعث می‌شود که تیم فنی با اعتماد به نفس بیشتری عمل کند [۹،۷،۶].

مستندسازی دقیق نیز یکی دیگر از راهکارهای مؤثر در مدیریت چالش‌های فنی است. با ایجاد مستندات جامع و دقیق برای فرآیندها و پیکربندی‌ها، سازمان‌ها می‌توانند از بروز خطاهای انسانی جلوگیری کنند. این مستندات باید شامل دستورالعمل‌های واضح و مراحل اجرایی باشند تا هر فردی بتواند به راحتی از آن‌ها استفاده کند. همچنین، مستندسازی به تسهیل فرآیند آموزش و انتقال دانش کمک می‌کند و در مواقعی که اعضای تیم تغییر می‌کنند، اطلاعات حیاتی را حفظ می‌کند.

تست منظم امنیتی نیز یکی از راهکارهای کلیدی برای شناسایی نقاط ضعف و مشکلات احتمالی در سیستم‌ها است.

با انجام تست‌های امنیتی دوره‌ای، سازمان‌ها می‌توانند به شناسایی آسیب‌پذیری‌ها و نقاط ضعف سیستم‌های خود بپردازند و اقدامات لازم را برای رفع آن‌ها انجام دهند.این تست‌ها می‌توانند شامل ارزیابی‌های نفوذ، تحلیل‌های خطر و بررسی‌های امنیتی باشند. با شناسایی زودهنگام مشکلات، سازمان‌ها می‌توانند از بروز حملات و آسیب‌های جدی جلوگیری کنند [۹،۷،۵]. به‌روزرسانی مداوم نرم‌افزارها و سیستم‌ها نیز از اهمیت بالایی برخوردار است.

با توجه به اینکه تهدیدات سایبری به سرعت در حال تغییر و تحول هستند، سازمان‌ها باید به‌روزرسانی‌های امنیتی را به طور منظم انجام دهند.

این به‌روزرسانی‌ها معمولا شامل وصله‌های امنیتی هستند که به رفع مشکلات و آسیب‌پذیری‌های شناخته‌شده کمک می‌کنند. سازمان‌ها باید یک برنامه منظم برای به‌روزرسانی نرم‌افزارهای خود

داشته باشند و اطمینان حاصل کنند که تمامی دستگاه‌ها و سیستم‌ها به آخرین نسخه‌های امنیتی مجهز هستند [۹،۶،۴،۲،۱].
در نهایت، ایجاد یک برنامه مدیریت ریسک نیز می‌تواند به سازمان‌ها در مقابله با چالش‌های فنی کمک کند. این برنامه باید شامل شناسایی، ارزیابی و اولویت‌بندی ریسک‌ها باشد.
با داشتن یک برنامه مدیریت ریسک، سازمان‌ها می‌توانند به طور مؤثری به چالش‌ها پاسخ دهند و منابع خود را به بهترین شکل تخصیص دهند. این اقدام به سازمان‌ها این امکان را می‌دهد که با آگاهی از ریسک‌ها، تصمیمات بهتری در زمینه امنیت اطلاعات اتخاذ کنند و از بروز مشکلات جدی جلوگیری نمایند [۹،۶،۴،۲،۱].

نتیجه‌گیری

هاردنینگ امنیتی سیستم‌های نظارت تصویری به عنوان یک رویکرد جامع برای حفاظت از زیرساخت‌های حیاتی، نیازمند توجه ویژه به چالش‌های فنی و راهکارهای مؤثر است.
با شناسایی چالش‌هایی مانند پیچیدگی پیکربندی، محدودیت‌های سخت‌افزاری و نیاز به تخصص فنی، سازمان‌ها می‌توانند با برنامه‌ریزی دقیق و پیاده‌سازی بهترین شیوه‌ها، امنیت سیستم‌های خود را بهبود بخشند.
همچنین، توجه به آموزش مستمر تیم فنی و مستندسازی دقیق فرآیندها، به افزایش توانایی‌های کارکنان و کاهش خطاهای انسانی کمک می‌کند.
در کنار این چالش‌ها، راهکارهایی همچون به‌روزرسانی مداوم نرم‌افزارها و سیستم‌ها، تست‌های امنیتی منظم و ایجاد برنامه‌های مدیریت ریسک، می‌توانند به سازمان‌ها در مقابله با تهدیدات سایبری یاری رسانند.
با اتخاذ این رویکردهای جامع، سازمان‌ها قادر خواهند بود تا با اطمینان بیشتری به حفاظت از داده‌های حساس و زیرساخت‌های حیاتی خود بپردازند و از بروز آسیب‌های جدی جلوگیری کنند.
در نهایت، ایجاد یک فرهنگ امنیتی در سازمان و آگاهی کارکنان از اهمیت هاردنینگ امنیتی، به تحقق این اهداف کمک می‌کند.

منابع

1.Dahua, "Product Security Hardening Guide." [Online]. Available: https://material.dahuasecurity.com/download/20180817/Dahua-Product-Security-Hardening-Guide-V01_0_2.pdf
2.Pelco, "Pelco Camera Hardening Guide." [Online]. Available: https://www.hanwhavision.com/wp-content/uploads/10/2021/IPCameraNetwork_Hardening_Guide_En_20230418.pdf
3.H. vision, "IP Camera Network Hardening Guide." [Online]. Available: https://www.hanwhavision.com/wp-content/uploads/10/2021/IPCameraNetwork_Hardening_Guide_En_20230418.pdf
4.Wisenet, "Network Hardening Guide," 2021. [Online]. Available: https://hanwhavisionamerica.com/wp-content/uploads/Graphics/Whitepapers/Cybersecurity_Whitepapers/nvr_network_hardening_guide_en_200724.pdf
5.Avigilon, "Avigilon System Hardening Guide," 2024. [Online]. Available: https://d8eqw8u9b6kgn.cloudfront.net/documents/avigilon-system-hardening-guide-en.pdf.
6.A. Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations," presented at the Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, 2016. [Online]. Available: https://doi.org/2995289.2995290/10.1145.
7.Axis. "AXIS OS Hardening Guide." https://help.axis.com/en-us/axis-os-hardening-guide (accessed.
8.Eagle. "Cybersecurity: 12 Ways to Keep Your Security Cameras Safe." https://www.een.com/security-camera-system-cyber-best-practices/ (accessed.
9.A. C. defense, "Enhanced Visibility and Hardening Guidance for Communications Infrastructure
Publish DateDecember 2024 ",2024 ,04. [Online]. Available: https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure.

تاکید رئیس پلیس نظارت بر اماکن عمومی فراجا بر الزام نصب دوربین‌های مداربسته مورد تایید آزمایشگاه تجهیزات نظارت تصویری در تمامی واحدهای صنفی کشور

سردار نوروزی، رئیس پلیس نظارت بر اماکن عمومی فراجا در حاشیه برگزاری یازدهمین اجلاس هشتمین دوره هیأت نمایندگان اتاق اصناف ایران، بر لزوم نصب دوربین‌های نظارت تصویری مورد تایید آزمایشگاه تجهیزات نظارت تصویری در تمامی واحدهای صنفی تاکید کرد.

طی مصوبه ابلاغی پلیس نظارت بر اماکن عمومی فراجا به اتاق اصناف ایران، اجرای سند «الزامات پایش تصویری اماکن عمومی و صنوف» برای تمامی واحدهای صنفی با شرایط خاصی الزامی شده است. طبق این مصوبه، تمامی اصناف و اماکن عمومی کشور به چهار سطح امنیتی (با نام های SL1 تا SL۴ که SL۴ بالاترین سطح امنیتی است) تقسیم بندی شده‌اند. شایان ذکر است با توجه به حساسیت واحدهای صنفی و اماکن عمومی، هیچکدام در سطح امنیتی SL۰ قرار نمی‌گیرند. تمامی تجهیزات نظارت تصویری مطابق «الزامات پایش تصویری اماکن عمومی و صنوف»، باید متناسب سطح امنیتی مورد بهره برداری قرار گیرند. به بیان دیگر، تجهیزاتی که در SL1 قرار دارند، باید حداقل شاخص های این سطح را رعایت کرده باشند. کلا تجهیزات در سطح امنیتی بالاتر، کیفیت بهتری نسبت به تجهیزات در سطح امنیتی پایین‌تر دارند، به عنوان مثال تجهیزات SL۳، قابلیت های بیشتری نسبت به تجهیزات SL1 خواهند داشت. درگاه استعلام تجهیزات نظارت تصویری به نشانی https://egovahi.ir مرجع استعلام سطح بندی تجهیزات نظارت تصویری است و همگان می‌توانند قبل از خرید تجهیزات، تطابق سطح تجهیزات را با سطح امنیتی مکان خود بررسی کنند. تمامی تولیدکنندگان و واردکنندگان نیز می‌توانند با ارایه نتایج آزمایشگاه تجهیزات نظارت تصویری، سطح امنیتی تجهیزات خود را به اطلاع عمومی برسانند.

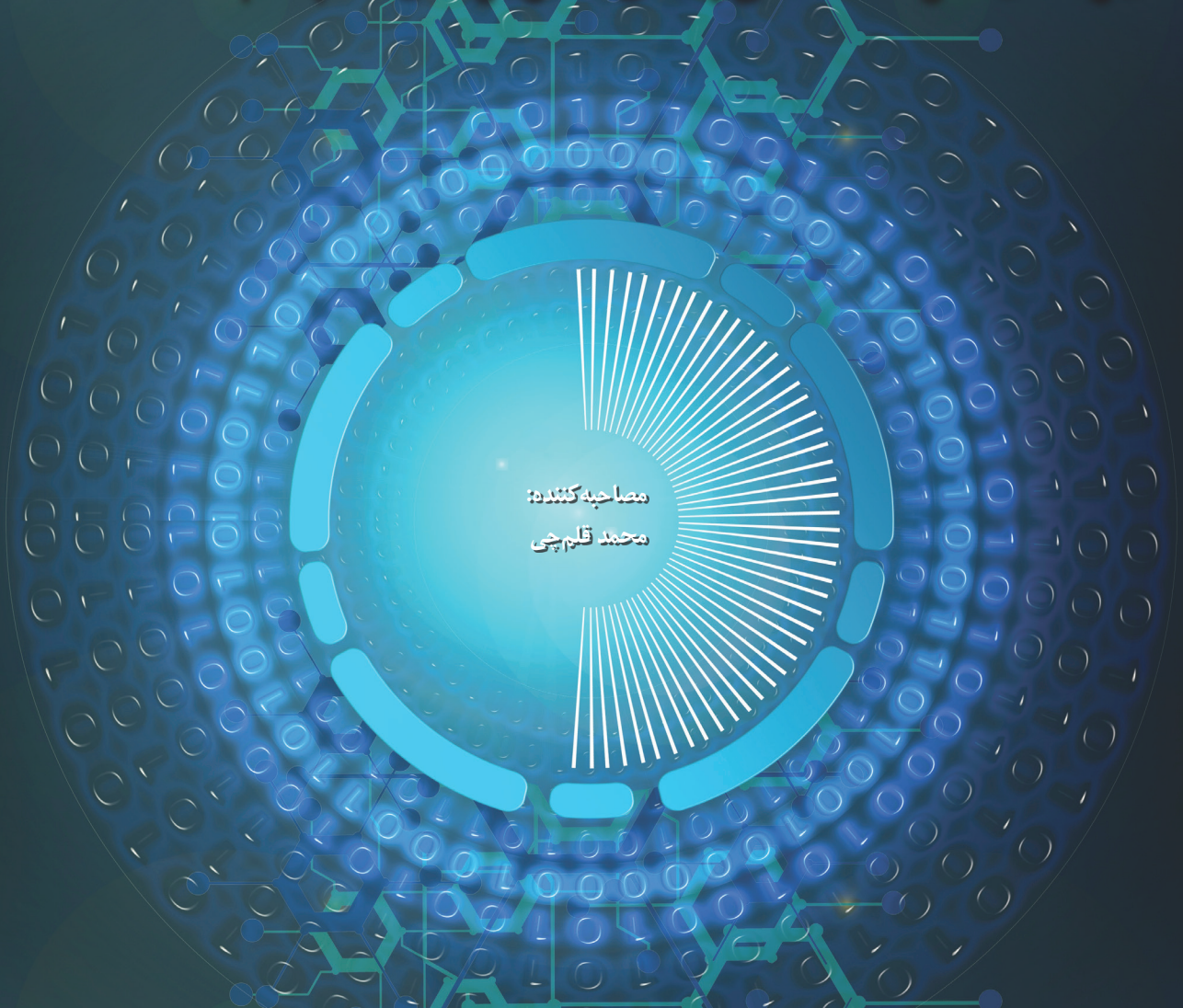
طبق سند «الزامات پایش تصویری اماکن عمومی و صنوف»، درگاه «سامانه پایش تصویری اماکن (سپتام)» پل ارتباطی میان آزمایشگاه‌های تخصصی نظارت تصویری و مقتضایان دریافت تاییدیه سامانه نظارت تصویری اصناف و اماکن عمومی است. به روزرسانی‌های بعدی این سند نیز از همین طریق به اطلاع عموم خواهد رسید.

سامانه‌های نظارت تصویری سنتی ریسک‌های متعددی از جمله سرقت ذخیره‌ساز، از کار افتادن و عدم اطلاع رسانی در لحظه به بهره‌بردار دارند که به همین دلیل در الزامات پایش تصویری اماکن، اصناف و اماکن عمومی که در سطح SL۲ یا بالاتر قرار می‌گیرند، بنا به سناریوی صنف خود (که در سند الزامات آمده است)، نیازمند تامین دوربین ابری از اپراتورهای نظارت تصویری ابری هستند.

از سوی دیگر، در صورتیکه در سطوح امنیتی مهم (SL۲ به بالا)، واحد صنفی یا مکان عمومی فاقد نگهبان باشد، نیازمند دریافت خدمات نگهبان هوشمند که معمولا ۱۰ برابر هزینه کمتری نسبت به نگهبان سنتی هستند و ریسک‌های نگهبان سنتی را ندارند می‌باشند.

نشست با جناب آقای روح الامین دادگر

مدیرعامل شرکت سامان پایش تصویر امن (سپتام)



مصاحبه کننده:
محمد قلم‌چی

روح‌الامین دادگر، مدیرعامل محترم شرکت سامان پایش تصویر امن (سپتام)، میهمان این شماره مجله امنیت الکترونیک هستند تا توضیحات بیشتری درخصوص سپتام از ایشان بشنویم.

۱.درخصوص شرکت سامان پایش تصویر امن (سپتام)، حوزه وظایف و لزوم تاسیس آن توضیحاتی ارائه فرمایید.

شرکت سامان پایش تصویر امن مجری طرح سپتام (مخفف «سامانه پایش تصویری اماکن») که یک طرح ملی است که با همکاری پلیس اماکن در سراسر کشور عزیزمان ایران راه‌اندازی شده است و هدف اصلی آن نظارت بر کیفیت و استاندارد دوربین‌های مداربسته و سیستم‌های حفاظتی در اماکن عمومی و واحدهای صنفی می‌باشد. به طوری که دریافت تأییدیه سپتام در حال حاضر پیش‌نیاز صدور مجوزهای تایید محور است.

شرکت سپتام بر اساس ماموریت های محوله از سوی پلیس نظارت بر اماکن عمومی فراجا حوزه فعالیت خود را در دو بخش مهم تعریف کرده است که عبارتند از:

الف) صدور گواهی تأییدیه: فعالیت‌های این بخش شامل ارزیابی تخصصی تجهیزات نظارت تصویری و سیستم‌های مداربسته واحدها از نظر کیفیت فنی، بررسی شیوه نصب و عملکرد ایمن و تطبیق همه موارد با الزامات و استانداردهای ملی و بین المللی در آزمایشگاه های تخصصی است.

ب) پایش و تضمین امنیتی: این بخش شامل ایجاد امکان دسترسی پلیس به تصاویر دوربین برای ارتقای امنیت عمومی، نظارت بر عملکرد دوربین‌ها و پشتیبانی از فعالیت‌های امنیتی تجهیزات نظارت تصویری اماکن است.

همچنین لزوم تاسیس و راه اندازی سپتام نیز در چهار بخش خلاصه می‌شود:

الف) استانداردسازی تجهیزات حفاظتی:

استانداردسازی به منظور جلوگیری از استفاده از دوربین‌های غیر استاندارد و آسیب‌پذیر با تضمین کیفیت از طریق آزمایشگاه و صدور گواهی انجام می‌گیرد.

ب) ارتقای امنیت عمومی:

با دسترسی به تصاویر سیستم‌های نظارتی، پلیس می‌تواند واکنش سریع‌تری به حوادث داشته باشد.

ج) اعتماد مخاطبان و کسب‌وکارها:

داشتن گواهی سپتام در بنگاه‌های اقتصادی و همه کسب و کارها نشان‌دهنده این است که سیستم حفاظتی آن‌ها مورد تأیید رسمی است و این اماکن دارای گواهی، در جذب مشتری بیشتر و آرامش خاطر عمومی به مراتب از اماکن فاقد گواهی جلوتر خواهند بود.

۲. تعامل سپتام با پلیس نظارت بر اماکن و شرکت مخابرات به چه نحوی است؟

تعامل سپتام (سامانه پایش تصویری اماکن) با پلیس نظارت بر اماکن عمومی فراجا (فرماندهی انتظامی جمهوری اسلامی ایران) بسیار نزدیک، ساختاریافته و هدفمند است. سپتام بازوی فنی پلیس برای اطمینان از امنیت محل کسب وکار متقاضیان و نیز سایر اماکن عمومی می باشد. بر کسی پوشیده نیست که پلیس اماکن عمومی، بخشی از فراجا است که بر اصناف، مشاغل و اماکن عمومی با اهمیت امنیتی و اجتماعی بالا نظارت می‌کند و وظیفه دارد صرافی‌ها، طلافروشی‌ها، فروشگاه‌های تجهیزات نظامی، دارویی و نیز اماکن پرتردد یا حساس پلیس را از نظر امنیتی بررسی کند و برای آن‌ها مجوز فعالیت یا تمدید مجوز صادر کند که پیش نیاز صدور و یا تمدید هر جوازی ابتدا نیاز به اخذ گواهی سپتام از سامانه saptam.ir است و همانطور که پیش‌تر گفته شد سپتام سامانه‌ای است که برای استانداردسازی و پایش تصویری (دوربین مداربسته) اماکن حساس طراحی شده است. این سامانه ایجاد شده است تا نصب دوربین‌ها بر اساس استاندارد واحد باشد. تصاویر دوربین‌ها قابل ضبط، پایش و بررسی قضایی باشند. گواهی تأییدیه‌ای برای تطابق کسب‌وکار با مقررات امنیتی صادر شود.

در خصوص تعامل سپتام و پلیس اماکن شامل مراحل ذیل است:

مرحله ۱: متقاضی کسب‌وکار در سامانه سپتام ثبت‌نام می‌کند.

مرحله ۲: متقاضی پس از خرید تجهیزات سامانه نظارت تصویری محل کسب خود از هر مرکز معتبری که تجهیزات آن مورد تایید سامانه egovahi.ir است نسبت به نصب آنها توسط نصابی دانا و توانا و مورد وثوق خودش اقدام می نماید.

مرحله ۳: کارشناس رسمی سپتام پروژه را ارزیابی و تأیید می‌کند. پلیس فقط در صورت دریافت گواهی تأییدیه سپتام، مجوز نهایی را صادر می‌کند.

مرحله ۴: گواهی سپتام در سامانه برای پلیس قابل مشاهده می‌شود. پلیس با مشاهده گواهی، مجوز صنفی یا تمدید آن را صادر می‌کند.

اگر که متقاضی نسبت به دریافت گواهی اقدام نکند، مجوز فعالیت برای مشاغل و کسب و کارهای تایید محور صادر یا تمدید نخواهد شد. به همین دلیل، نصب دوربین و دریافت گواهی از سپتام عملاً یکی از شروط پلیس برای صدور یا تمدید جواز است.

۳. چه کسانی برای اخذ تاییدیه سپتام اقدام می‌کنند و متقاضی چه مدارک و اطلاعاتی را برای ثبت نام باید ارائه دهد؟

کسب و کارها به دو دسته تایید محور و ثبت محور تقسیم می‌شوند و همانطور که از عبارات مذکور مشخص است برخی کسب و کارها صرفاً با ثبت درخواست مربوطه، متقاضی می‌تواند فعالیت خود را در آن رسته‌ی مورد نظرش شروع نماید.

برخی دیگر که تأیید محور هستند نیاز است که متقاضی از برخی مراجع ذی‌صلاح تاییدیه‌هایی را اخذ نماید که در همین راستا و از جمله آن تاییدیه‌های امنیتی و گواهی‌های الزامی پلیس نظارت بر اماکن عمومی فراجا، اخذ گواهی نظارت بر سامانه تجهیزات نظارت تصویری اماکن است که متقاضی باید از درگاه سپتام به آدرس اینترنتی saptam.ir نسبت به اخذ آن اقدام نماید.

البته تاکید می‌شود که درخواست این گواهی باید پس از اینکه متقاضی محل کسب و کار خود را به سامانه نظارت تصویری اماکن مجهز نمود صورت پذیرد. اینکه متقاضی باید چه مدارک و اطلاعاتی را در سامانه سپتام درج نماید به عرض همه متقاضیان محترم و همراهان گرامی می‌رسانم که پس از تصمیم به راه‌اندازی فعالیت و کسب و کاری، عبارت کسب و کار مربوطه را که عیناً از درگاه ملی مجوزها دریافت کردند در صفحه مربوط، در قسمت فعالیت‌ها جستجو کرده تا نسبت به تشخیص سطح امنیتی رسته مورد نظر پی ببرند و در ادامه در قسمت محل من، اطلاعات کاملی از کسب وکار خود و نیز اطلاعات واقعی و موثقی از محل کسب وکار (آدرس ،کدپستی ، تلفن ثابت و همراه و غیره) و نیز اطلاعات سجلی اعم از نام و نام خانوادگی، کد ملی و همچنین درج صحیح و متراژ واقعی از مساحت محل کسب وکار خود اقدام نماید و در ادامه نسبت به بارگزاری تصاویر خواسته شده در سامانه(سند، اجارنامه و غیره) اقدام لازم را به‌عمل آورد.

۴. در خصوص روال اخذ تاییدیه از سپتام و انواع تاییدیه‌هایی که صادر می‌شود از زمان ثبت‌نام تا اخذ تاییدیه توضیحاتی ارائه فرمایید؟

همان‌طور که در پاسخ به سوالات قبل توضیح داده شد، متقاضی پس از ثبت محل خود در سامانه سپتام و درج اطلاعاتی صحیح از محل کسب وکار خود و البته تاکید می‌شود پس از اینکه محل خود را به سامانه نظارت تصویری و دوربین مدار بسته تجهیز نمود، منتظر تماس کارشناسان محترم شرکت سپتام می‌ماند که پس از برقراری ارتباط با کارشناس تعیین شده برای محل مورد نظر و تعیین و تایید وقت و زمان انجام امر کارشناسی با هماهنگی با یکدیگر اقدام می‌نمایند. کارشناس محترم سپتام نیز در وقت و زمان هماهنگ شده به محل متقاضی مراجعه و نسبت به انجام کارشناسی و جمع‌آوری اطلاعات مورد نیاز برطبق الزاماتی که پلیس نظارت بر اماکن عمومی فراجا مشخص نموده اقدام و نسبت به بارگزاری این اطلاعات در سامانه سپتام اقدام می‌کند. در اینجا لازم است به این مهم اشاره نمایم که متقاضیان محترم بدانند که کارشناسان محترم سپتام هیچ‌گونه دخالت و اظهارنظری در اعلام نتیجه بررسی و کارشناسی خود نداشته و نخواهند داشت و نتیجه کارشناسی محل متقاضی پس از دریافت مستندات و مدارک صرفاً و صرفاً پس از بررسی در آزمایشگاه‌های تخصصی سپتام صورت می‌گیرد و هر محل با توجه به سطح امنیتی و رعایت همه و یا بخشی از الزامات مربوطه، امکان دریافت یکی از گواهی‌های طلایی، نقره‌ای یا تعهدی را دارد و اگر هیچ یک از الزامات را رعایت نکرده باشد محل مورد نظر به طور سیستمی صرفا اعلام مردودی خواهد شد و هیچ یک از گواهی‌های مذکور را دریافت نخواهد کرد.

۵. در حال حاضر سپتام چند کارشناس در سراسر کشور دارد و روال جذب این کارشناسان و نحوه فعالیت آنها چگونه است؟

شرکت سامان پایش تصویر امن (سپتام) در حال حاضر بیش از ۶۵۰ کارشناس در اقصی نقاط کشور دارد که بر تعداد این کارشناسان هر روزه با برگزاری آزمون‌های برخط برای متقاضیان انجام کارشناسی طرح سپتام افزوده خواهد شد. لازم به ذکر است که همه عزیزانی که تمایل به فعالیت در حوزه کارشناسی سپتام را دارند می‌توانند با مراجعه به آدرس در سامانه سپتام، از قسمت کارشناس شوید جهت اشتغال در امر کارشناسی اقدام نمایند.

۶. مدت زمان میانگین جهت اخذ گواهینامه از سپتام چند روز است و تا این لحظه چند گواهینامه صادر شده است؟

سپتام ظرف چهار روز کاری پاسخ هر یک از متقاضیان را اعلام نماید اما با توجه به اینکه برخی از متقاضیان محترم در مراکزی جهت درج اطلاعات محل یا ثبت اطلاعات هویتی اقدام می‌نمایند, متأسفانه این مراکز دقت کافی و لازم را جهت ثبت دقیق اطلاعات بعمل نمی‌آورند که این موضوع عدم درج اطلاعات صحیح و موثق موجب اتلاف وقت متقاضیان محترم و کارشناسان آزمایشگاه‌ها شده و اعلام نتایج نهایی زمان بیشتری می‌برد. البته که شرکت سپتام درصدد است تا با راه‌اندازی دفاتر فنی سپتام‌نت در سراسر کشور نسبت به انجام امور ثبت نامی متقاضیان محترم و بررسی و درج اطلاعات صحیح از متقاضیان و محل مورد نظرشان از زمان انتظار جهت صدور گواهی سپتام برای کسب وکار هموطنان عزیز کشورمان بکاهد.

۷. برای اخذ تاییدیه از سپتام، متقاضی باید چه الزاماتی را در خصوص سامانه نظارت تصویری محل رعایت کند؟ متقاضی چگونه می‌تواند از این الزامات آگاه شود؟

بر طبق ضوابط پایش تصویری اصناف و اماکن عمومی، ابلاغی پلیس نظارت بر اماکن عمومی فراجا، اصناف و به چهار سطح امنیتی از SL1 تا SL4 تقسیم می‌شوند که مقررات و الزامات هر سطح با سطح دیگر متفاوت است. لذا متقاضیان محترم دریافت گواهی سپتام می‌توانند با درج فعالیت و عبارت کسب و کار خود در سامانه سپتام به آدرس www.saptam.ir نسبت به اطلاع و آگاهی از سطح امنیتی رستهٔ خود مطلع و نسبت به رعایت آن ضوابط و الزامات قبل از ثبت درخواست کارشناسی در سامانه اقدام نمایند.

۸. در خصوص لزوم نصب دوربین‌های ابری در برخی اماکن و قابلیت‌های سرویس‌هایی که توسط این دوربین‌های ارائه می‌شود توضیحاتی ارائه فرمایید.

برخی از مشاغل هستند که به دلیل حساسیت بالای شغلی در سطوح امنیتی بالا و یا اماکن پر ازدحام و شلوغ قرار دارند که پلیس نظارت بر اماکن عمومی برای این مشاغل، نصب حداقل یک دوربین ابری را در مرحله اول برای هر یک از ورودی‌های محل کسب آنها الزامی کرده است. به زبان عامیانه باید بگویم که دوربین ابری دوربینی است که اطلاعات و تصاویر ضبط شده توسط آن دوربین در فضایی خارج از آن محل در سرورهای مخابرات ذخیره می‌شود تا اطلاعات ضبط شده در حوادث و اتفاقات احتمالی از بین نرفته و قابل دسترسی و استناد باشد.

سپتام

سامانه پایش تصویری اماکن

توسعه خدمات سپتام

رشد تولیدات تجهیزات نظارت تصویری و رونق عرضه در بازار کشور مطابق با استانداردهای جهانی را به همراه دارد.

saptam.ir

+۹۸ ۲۱-۲۲۹۴۸۸۶۸

+۹۸ ۲۱-۲۲۹۶۷۷۶۹

www.electronicsecurity.ir

info@electronicsecurity.ir