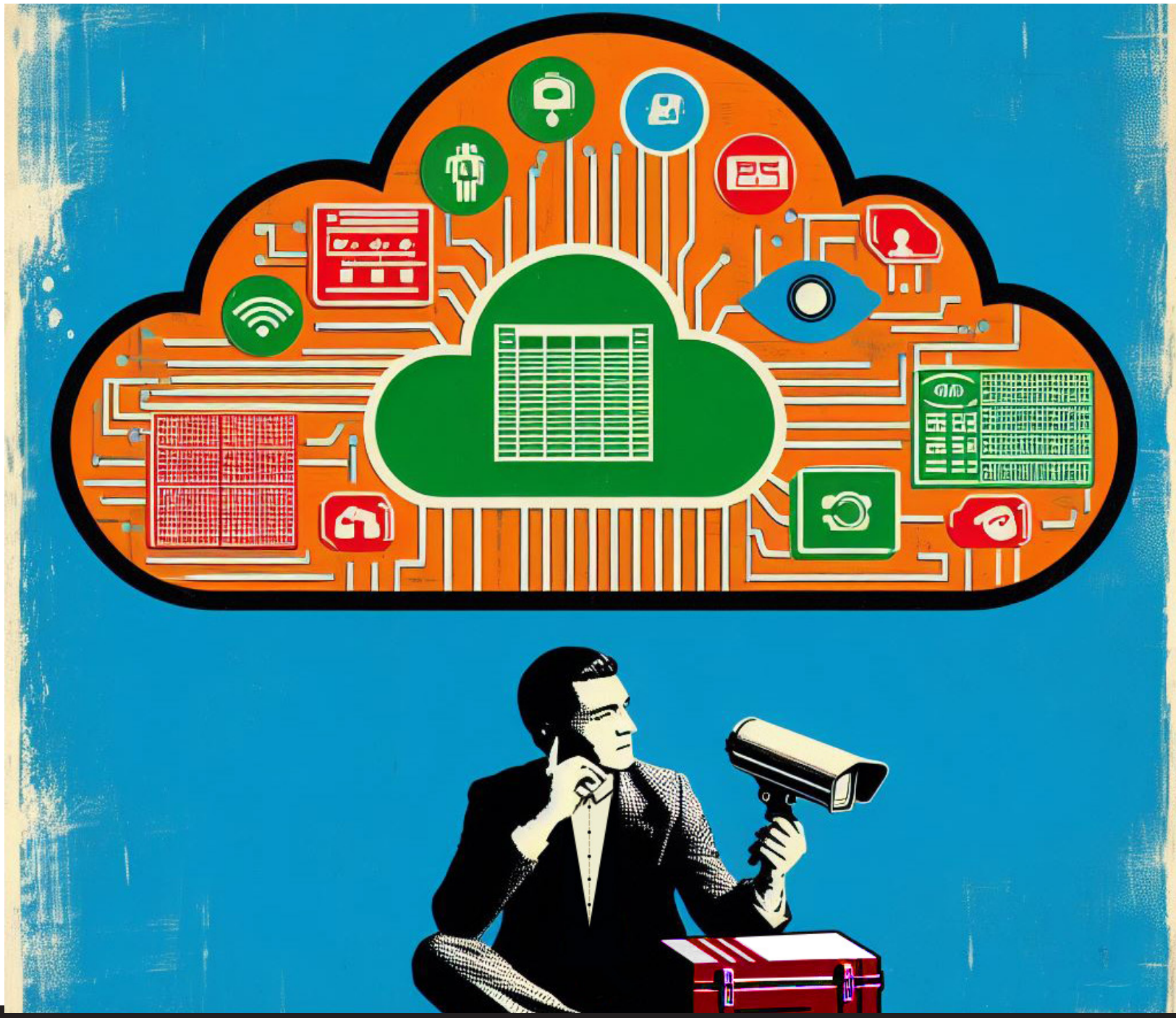
امنیت الکترونیک

فصل‌نامهٔ اختصاصی صنعت تجهیزات ایمنی و حفاظت

سال ششم | شمارهٔ سوم | تابستان ۱۴۰۳ | ۲۵۰هزار تومان



در این شماره می‌خوانیم:


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

امنیت الکترونیک

صاحب امتیاز و مدیرمسئول: محمد قلمچی
سردبیر: معصومه عباسیان

هیئت تحریریه (به‌ترتیب حروف الفبا): محمود سعیدی
سید علی صموتی
معصومه عباسیان
یاسر علمی سولا
محمد قلمچی

ویراستار: معصومه عباسیان
صفحه‌آرایی و طراحی: زهرا سنجابی
معصومه عباسیان

مشخصات نشر: تهران، مجتمع چاپ ایران‌کهن

نشانی دبیرخانه: تهران- اقدسیه- بلوار ارتش- اراج- شانزده‌متری ولیعصر- نبش خیابان پروین- پلاک ۲- واحد ٤
تلفن: ۰۲۱-۲۲۹٦۷۷٦۳
نمابر: ۰۲۱-۲۲۹٦۷۷٦۹
نشانی اینترنتی: www.electronicsecurity.ir
پست الکترونیک: info@electronicsecurity.ir

فهرست

سرمقاله

نویسنده:
محمد قلم‌چی

سامانه‌های نظارت تصویری به‌عنوان پرکاربردترین تجهیزات امنیت الکترونیک، در تأمین امنیت کشورمان نقشی اساسی ایفا می‌کنند. سال ۱۴۰۳ اتفاقات ساختاری و مبارکی در حوزهٔ قوانین و مقررات نظارت تصویری در کشور رخ داده است و تحولاتی دیگر در ادامهٔ این زنجیره موجب ارتقای اساسی سامانه‌های نظارت تصویری خواهد شد. «سند الزامات و ملاحظات پدافند غیرعامل سامانه‌های نظارت تصویری» که ویرایش اول آن در مهرماه ۱۴۰۲ توسط سازمان پدافند غیرعامل کشور تهیه شده بود، در مردادماه سال ۱۴۰۳ به دستگاه‌ها ابلاغ شد.

سامانه‌های نظارت تصویری صنوف نیز با طرح سپتام به‌صورت کامل در سازوکاری کارآمد، علمی و تخصصی بر طبق سندی بومی برگرفته از استانداردهای ملی و بین‌المللی ساماندهی شد. طبق مادهٔ ۱۷ قانون نظام صنفی مصوب ۱۳۹۲ و همچنین نظر به تبصرهٔ ۱ مادهٔ ۵ ضوابط انتظامی پلیس نظارت بر اماکن عمومی فراجا مصوب یک‌صدوبیست‌وهفتمین جلسهٔ هیئت عالی نظارت بر سازمان‌های صنفی کشور به ریاست وزیر محترم صمت به تاریخ ۱۴۰۱/۰۸/۰۴ و ابلاغ آن به تاریخ ۱۴۰۲/۰۱/۲۹، سند «ضوابط پایش تصویری اماکن عمومی و صنوف» با هدف بهبود کارایی و امنیت نظارت تصویری در سطح صنوف و اماکن عمومی توسط ریاست محترم پلیس نظارت بر اماکن عمومی فراجا ابلاغ گردید و توسط پرتال سپتام به نشانی اینترنتی https://saptam.ir اجرایی گردید.

به‌نظر می‌رسد این بهبودها درحال توسعه است و به‌زودی شاهد تصویب «استاندارد ملی امنیت سامانه‌های نظارت تصویری» که در راستای دو سند فوق نیز هست، خواهیم بود. انتظار می‌رود چنین اقداماتی موجب ارتقای سامانه‌های نظارت تصویری، توسعهٔ بازار برای متخصصان، تولیدکنندگان تجهیزات باکیفیت، فعالان صنفی خدماتی قانون‌مدار و حذف سودجویان و تجهیزات بی‌کیفیت شود. این نشریهٔ تخصصی بر خود لازم می‌داند تا از تمامی متولیان این امور ارزشمند در کشور ازجمله سازمان پدافند غیرعامل، سازمان ملی استاندارد، سازمان فناوری اطلاعات و پلیس نظارت بر اماکن عمومی فراجا تقدیر و تشکر نماید.

اخبار فناوری در حوزه‌ی امنیت در ۲۰۲۴

مترجم:
معصومه عباسیان

در این بخش ابتدا حوزه‌ی کاری جدیدی برای متخصصان امنیت معرفی می‌شود؛ در این حوزه متخصصان امنیت به کمک متخصصان بازاریابی می‌آیند. در ادامه فناوری جدیدی در حوزه‌ی امنیت خانگی معرفی می‌شود.

۱- «دعوی قضایی مربوط به پیکسل»[1]: چگونه متخصصان امنیت می‌توانند به کاهش ریسک پیکسل کمک کنند

چرا پیکسل‌ها مهم هستند؟

موضوع جدیدی که به وبسایت‌ها مربوط می‌شود، دعوی قضایی مربوط به پیکسل است که سازمان‌ها را غافلگیر می‌کند. این موضوع در سال گذشته مشکلات قابل‌توجهی در جهان ایجاد کرده است. فهرست اشخاصی که در سراسر جهان از آنها بابت این مسئله شکایت شده است به‌طور تصاعدی درحال افزایش است. اتهامات مربوط به این نوع پرونده‌ها متفاوت است، اما در وهلهٔ نخست ادعا می‌شود که سازمان‌ها اطلاعات شخصی مشتریانی را که در وبسایت می‌چرخند بدون کسب رضایت آنها جمع‌آوری و افشا می‌کنند. وقتی کسی شروع به گشت‌وگذار در وبسایتی می‌کند، فناوری ردگیری و تجزیه‌وتحلیل وبسایت می‌تواند او را ردگیری کند، ازجمله اینکه دقیقاً کدام صفحات را مشاهده کرده است، چه مدتی روی صفحه‌ای مانده است و اگر از کوکی‌ها یا پیکسل‌ها استفاده کند می‌تواند در وبسایت‌های دیگر نیز ردگیری شود. ممکن است این داده‌ها با سایر سازمان‌ها به‌اشتراک گذاشته شوند و از این طریق سازمان‌ها آدرس IP کاربر را با پلتفرم‌های خود پیوند می‌دهند.

غالباً، وقتی از فناوری جدیدی برای فروش و بازاریابی استفاده می‌شود، تیم‌های فروش و بازاریابی با متخصصان فناوری اطلاعات مشورت نمی‌کنند.

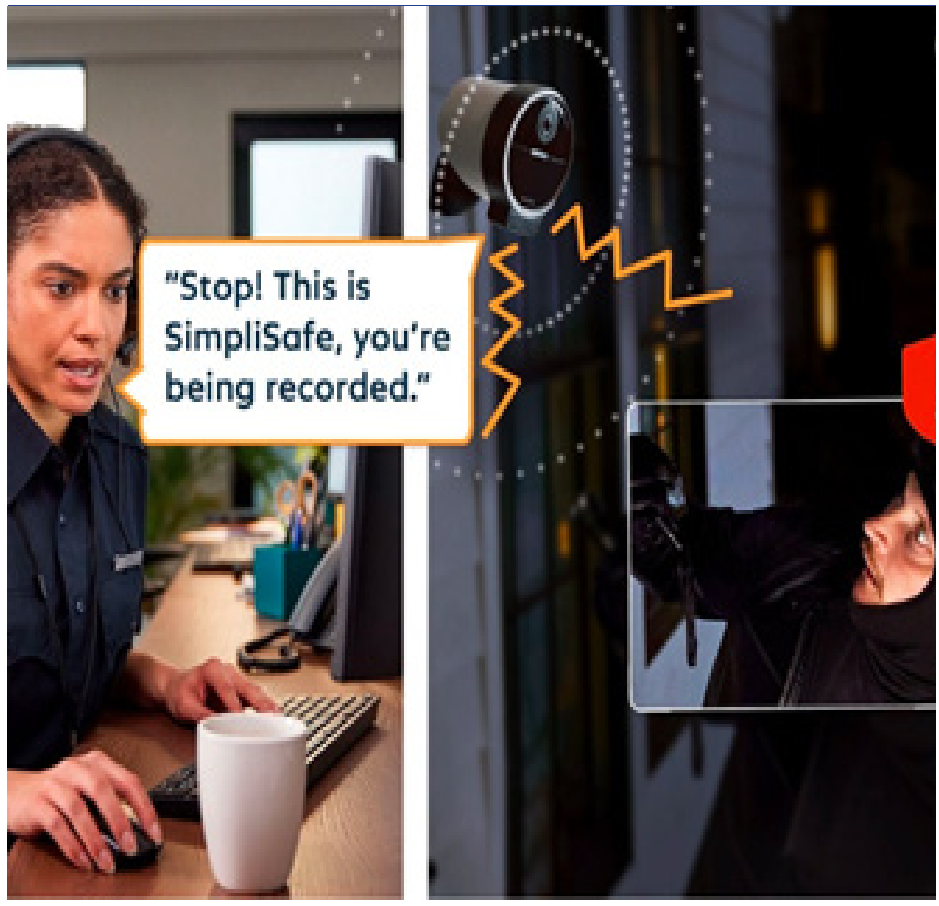
دو پیکسل پرکاربردْ متا (فیس‌بوک) و گوگل هستند. اگر این پیکسل‌ها و سایر فناوری‌های ردگیری که اصطلاحاً «فناوری تبلیغات» نامیده می‌شوند توسط سازمانی فعال شوند، کد رایانه‌ای را به فعالیت کاربر الصاق می‌کنند و آن را با متا و گوگل به‌اشتراک می‌گذارند. سپس از آن فعالیت برای تبلیغات هدفمند ازطریق آدرس IP کاربر استفاده می‌شود.

فناوری ردگیری ازطریق بهبود محتوای وبسایت، یافتن بخش موردعلاقهٔ سازمان ازسوی مصرف‌کنندگان و توسعهٔ محصولات و خدمات جدید براساس علاقه‌ای که کاربر هنگام مشاهدهٔ وبسایت نشان می‌دهد، برای فعالیت‌های فروش و بازاریابی سازمان‌ها سودمند هستند.

اما به‌اشتراک‌گذاری این تجزیه‌وتحلیل‌ها با متا، گوگل و سایر شرکت‌ها در دعاوی قضایی با عنوان افشای داده‌های مشتری بدون رضایت او و نقض قوانین حفظ حریم خصوصی موردحمله قرار می‌گیرد. دفاع از این اتهامات شامل، اما نه محدود به، این می‌شود که: کاربران هنگام بازدید از یک وبسایت کاملاً می‌دانند که ردگیری می‌شوند یا جست‌وجو در وبسایت معادل جمع‌آوری یا افشای «اطلاعات شخصی» نیست و مجموعهٔ کلیک‌های مشتری در وبسایت نه معادل «ضبط» است و نه معادل «شنود» که در قوانین استراق سمع هر دو ممنوع شده‌اند.

در مواجهه با شکایات، برخی از سازمان‌ها حتی نمی‌دانند که آیا از فناوری ردگیری در وبسایت خود استفاده کرده‌اند یا آیا آن فناوری منع قانونی داشته است؟ فناوری تبلیغات سال‌هاست که همه‌جا استفاده می‌شود و افزودن فناوری ردگیری برای تجزیه‌وتحلیل در یک وبسایت، غالباً افزونه‌ای است که توسط میزبان در وبسایت

1. pixel litigation



ارائه می‌شود و متخصصان فروش و بازاریابی در سازمان با این کار موافق‌اند. متخصصان فروش و بازاریابی که از ریسک‌های قانونی مرتبط با فناوری تبلیغات بی‌اطلاع هستند، افزوده‌شدن آن را به‌عنوان ارزش سازمان در نظر می‌گیرند و راجع به ریسک‌های آن با متخصصان امنیت و فناوری اطلاعات مشورت نمی‌کنند.

معمولاً تازه پس از طرح دعویِ مبنی بر وجود مشکلی در فناوری، با متخصصان فناوری اطلاعات مشورت می‌شود تا مشخص شود که این ادعاها تا چه حد دردسرساز هستند. در این مرحله، متخصصان فروش، بازاریابی و فناوری اطلاعات باید با همکاری یکدیگر این اتهامات را بررسی کنند.

در برخی موارد، نه متخصصان فروش و بازاریابی و نه متخصصان فناوری اطلاعات از استفاده از فناوری یا عملکرد آن آگاه نبوده‌اند. در این مورد، سازمان ابتدا باید تعیین کند که از چه نوع فناوری ردگیری و برای چه مدت استفاده شده است، چه اطلاعاتی از این طریق ذخیره شده است و اینکه آیا پیکسل‌ها یا سایر فناوری‌های تبلیغاتی داده‌ها را برای متا، گوگل یا سایر شرکت‌ها فاش کرده‌اند یا خیر. اینجاست که متخصصان امنیت برای کمک به جمع‌آوری شواهد طرف مشورت قرار می‌گیرند.

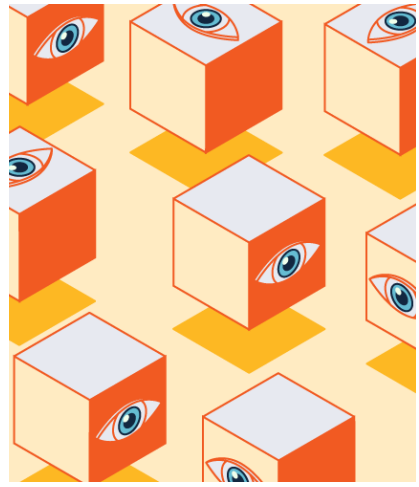
امنیت داده کاری گروهی است؛ همکاری کلید کاهش ریسک سازمان است

لین فریدمن رئیس تیم حریم خصوصی داده و تیم‌های امنیت سایبری و هوش مصنوعی در رابینسون و کول[۲] است. فعالیت‌های فریدمن بر انطباق با تمام قوانین و مقررات ایالتی و فدرال امنیت و حریم خصوصی داده و همچنین پاسخ‌های اضطراری به نقض داده و دعوی قضایی متمرکز است.

گام‌های بعدی برای حرفه‌ای‌های امنیت

در حال حاضر، برای پیشی‌گرفتن از موج دعواهای قضایی در حوزهٔ امنیت، متخصصان در زمینه‌های حقوقی، مدیریت ریسک و امنیت می‌توانند برای ارزیابی ریسک حفظ حریم خصوصی افراد اقداماتی از نظیر آنچه در ادامه می‌آید، انجام دهند:

2. Robinson & Cole



- با کمک متخصصان فروش و بازاریابی مشخص کنند که آیا «فناوری ردگیری»[3]، ازجمله «پیکسل‌های متا و گوگل»[4] در وبسایتشان استفاده می‌شود یا خیر.
- تعیین کنند که از فناوری تبلیغات به چه نحوی در وبسایت استفاده می‌شود؛ مثلاً، این فناوری چه اطلاعاتی را جمع‌آوری می‌کند و چه اطلاعاتی را در اختیار اشخاص ثالث قرار می‌دهد.
- ارزیابی کنند که آیا پیکسل‌ها یا سایر فناوری‌های ردگیری، ارزش ریسک‌کردن دارند یا خیر. اگر چنین است، تعیین کنند که چه اقداماتی برای کاهش ریسک باید اجرا شود. اگر نه، نحوهٔ غیرفعال‌کردن فناوری ردگیری را تعیین کنند.
- اگر از ردگیری تبلیغات، پیکسل‌ها و کوکی‌ها استفاده می‌شود، خط‌مشی رازداری وبسایت را بررسی کنند تا مشخص شود که آیا باید روشن‌تر به فناوری ردگیری در آن اشاره شود، این فناوری چه چیزی را ضبط می‌کند و داده‌ها برای چه کسانی افشا می‌شود.
- مکانیسم‌هایی را برای کاربران فراهم کنند تا هنگام بازدید از وبسایت، بتوانند از آن طریق از استفاده از فناوری ردگیری انصراف دهند. مثلاً پنجره‌ای در نظر وبسایت در نظر گرفته شود که به‌محض ورود به مشتریان گزینه‌هایی برای انصراف از این فناوری ارائه دهد.
- به‌کمک متخصصان بازاریابی فرایندی برای استفاده از فناوری‌های در حال تکامل در سازمان خود ایجاد کنند، طوری که کاربر از نیاز به ارزیابی فناوری جدید قبل از استقرار آن آگاهی داشته باشد.
- رویه‌های درون‌سازمانی ایجاد کنند تا متخصصان امنیت بتوانند به ارزیابی ریسک فناوری جدید کمک کنند.

آگاه نگه‌داشتن متخصصان امنیتی از استفاده از هر فناوری جدید یا «افزونه‌های» پیشنهادی می‌تواند برای کاهش خطرات امنیت داده برای سازمان حیاتی باشد.

متأسفانه، هرچه فروشندگان ابزارهای هوش مصنوعی بیشتری در محصولاتشان تعبیه می‌کنند، ریسک فناوری جدید فزونی می‌یابد. تیم‌های تجاری، همچنان که از فناوری‌های ردگیری تبلیغات مطلع نیستند، راجع به نحوهٔ استفاده از ابزارهای هوش مصنوعی توسط فناوری ارائه‌شده توسط فروشندگان و ریسک ناشی از استفاده از هوش مصنوعی، ازجمله سوگیری، حریم خصوصی و امنیت داده‌ها، نشت داده‌ها و جمع‌آوری و مالکیت معنوی توسط ابزارهای هوش مصنوعی اطلاعی ندارند. ایجاد خطوط مستحکم ارتباطات و فرایندها در داخل سازمان در ارتباط با استفاده از فناوری جدید و ارزیابی آن، شامل ابزارهای هوش مصنوعی، ریسک‌های احتمالی را چنان کاهش می‌دهد که چیزی از بین نرود.

۲- خدمات نگهبان زنده در فضای باز با دسترسی زودهنگام

شرکت امنیت خانگیِ SimpliSafe اعلام کرده است که به مشتریان منتخب خودْ خدمات نگهبان زنده در فضای باز با دسترسی زودهنگام می‌دهد.

SimpliSafe می‌گوید خدمت جدیدش در پایش، رویکردی دولایه برای امنیت خانگی معرفی می‌کند که با مجهزکردن تیمی از متخصصان در حوزهٔ پایش

3. tracking technology

۴. که به آن پیکسل هدف‌گیری مجدد فیس‌بوک نیز می‌گویند، قطعه‌کدی است که می‌توانید آن را در بک‌اند وبسایت خود وارد کنید. این کد مثل سایر تگ‌ها به هدایت و کدگشایی معیارهای عملکرد کلیدیِ تولیدشده توسط یک پلتفرم خاص کمک می‌کند.

به فناوری هوش مصنوعی از وقوع جرم قبل از وقوع آن جلوگیری می‌کنند.

کریستین سردا، مدیرعامل SimpliSafe می‌گوید:

«دهه‌هاست که صنعت امنیت خانگی تنها زمانی وارد عمل شده که تهاجمی درحال انجام بوده است. SimpliSafe تصمیم گرفته است تا این استاندارد را به‌چالش بکشد و به مشتریان خود راهکارهای جدید و فعال‌تری ارائه دهد تا بیشتر احساس امنیت کنند. پایش زنده در فضای باز جدیدترین دستاورد ماست. این فناوری تغییری واقعی در حوزهٔ ایمنی مشتری ایجاد می‌کند.»

Simplisafe می‌گوید سالانه نزدیک به ۲ میلیون نفر در ایالات متحده قربانی سرقت و تجاوز جنسی می‌شوند و در نتیجه اغلب با آسیب‌های روحی و مالی قابل‌توجهی مواجه می‌شوند. طبق گفتهٔ این شرکت، سرقت از منازل معمولاً تنها ۱۰ دقیقه طول می‌کشد، بنابراین برای واکنش سریع هر ثانیه اهمیت دارد. وقتی متجاوز توانست وارد خانه شود، دیگر برای جلوگیری از آسیب ناشی از او خیلی دیر شده است.

هومن شهیدی، معاون ارشد محصولات SimpliSafe می‌گوید:

«این خدمت جدید نیاز به «مسلح کردن» دوربین‌ها را برطرف می‌کند. پایش در فضای باز، کار را برای کاربران بسیار ساده می‌کند – مهم‌ترین چیز مسلح کردن سیستم است. وقتی سیستم کاربر مسلح باشد، هوش مصنوعی پیشرفتهٔ دوربین‌های ما می‌تواند هر حرکت انسانی را در اطراف خانهٔ کاربر تشخیص دهد. اگر حرکت انسان تشخیص داده شود، این خدمت از تطبیق خودکار چهره استفاده می‌کند تا به مأموران ما در تعیین اینکه آیا چهرهٔ این فرد با پروفایل‌های ذخیره‌شده به‌عنوان اعضای خانوادهٔ کاربر یا بازدیدکنندگان مورداعتماد او مطابقت دارد یا خیر. تنظیم این پروفایل‌ها آسان است و مهم‌تر از همه، پروفایل‌ها کاملاً توسط کاربر تنظیم می‌شوند.

به‌عنوان بخشی از دسترسی زودهنگام، کاربران ازطریق اپلیکیشن SimpliSafe، هشداری را روی تلفن همراه خود مبنی بر شناسایی حرکتی دریافت می‌کنند و همزمان یکی از مأموران پایشِ Simplisafe درحال مشاهدهٔ زندهٔ دوربین آنهاست. کاربران همچنین در مواردی هشدار دریافت می‌کنند که:

- مأموری ارتباط صوتی دوطرفه‌ای با فرد یا افراد موجود در ملک کاربر آغاز می‌کند؛
- ارتباط دوطرفه همراه با نتیجهٔ آن ارتباط پایان می‌یابد (تهدید در مقابل عدم‌تهدید)؛
- خدمات اضطراری برای رسیدگی به موقعیت فراخوانده می‌شوند.

دوربین‌های ما از هوش مصنوعی پیشرفته برای متمایزکردن افراد از سایر اجسام متحرک مانند ماشین‌ها و حیوانات استفاده می‌کنند. وقتی حرکت انسان شناسایی شود، سیستمْ تطبیق خودکار چهره را آغاز می‌کند. هستهٔ اصلی محصول ما ترکیبی از همکاری فناوری و افراد انسانی است، بنابراین وقتی خدمت تشخیص می‌دهد که فرد مذکور با هیچ‌یک از پروفایل‌های معرفی‌شده به سیستم مطابقت ندارد، مأموران متخصص ما با هدف جلوگیری از هر جنایت احتمالی وارد عمل می‌شوند.»

SimpliSafe این خدمت را اواخر سال ۲۰۲۴ در دسترس همهٔ مشتریان خود قرار خواهد داد.

منابع

- https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2024/april/pixel-litigation/
- https://simplisafe.com/

مقایسه‌ی خدمت ابری نظارت تصویری هوبان[1] با راهکارهای سنتی- با نگاه ویژه به کسب‌وکارهای سازمانی

نویسنده:
محمد قلم‌چی

۱. نگهبان خوبی‌ها: اولین خدمت نظارت تصویری ابری در ایران، http://ivsaas.ir.

VSaaS یا نظارت تصویری به‌عنوان خدمت، به نظارت تصویری مبتنی‌بر اَبر اشاره دارد. این خدمت معمولاً شامل ضبط ویدئو، ذخیره‌سازی، مشاهده از دور، هشدارهای مدیریتی، امنیت سایبری و سایر موارد است. در حال حاضر ۹۳٪ از کسب‌وکارها در امریکا و اروپا از راهکارهای ابری بهره می‌برند. پیشرفت‌های فناوری ابری و دسترس‌پذیریِ پهنای باند بیشتر باعث می‌شود VSaaS جذاب‌تر شود.

این متن با نگاهی به مقالهٔ «یازده دلیل برای انتقال نظارت تصویری به فضای ابری» نوشتهٔ آقای دین دارک، مدیرعامل شرکت ایگل‌آی نتورک، با در نظر گرفتن شرایط ایران تألیف شده است. آقای دین دارک مدعی است مقاله‌اش با استفاده از دستورالعمل‌های تعیین‌شده توسط مؤسسهٔ ملی استاندارد و فناوری ایالات متحده (NIST)[1] اصول یک سیستم ابری واقعی را مشخص می‌کند.

در این مقاله یازده مزیتِ سیستم مدیریت ویدئوی مبتنی‌بر اَبر در مقابل NVR، DVR یا VMS سنتیِ متصل به اینترنت برشمرده می‌شوند.

چرا فناوری‌های ابری موردتوجه قرار گرفته‌اند؟

- **صرفه‌جویی اقتصادی دلیل اصلی پذیرش فناوری ابری:** در جهان از هر ۱۰ کسب‌وکار ۹ تای آن، ازجمله ایمیل، تلفن، پشتیبان‌گیری، خدمت‌های تحت وب و نظارت تصویری، از فناوری ابری استفاده می‌کنند. نظرسنجی از ۹۳۰ بهره‌بردارِ زیرساخت ابری نشان می‌دهد که استفاده از فناوری ابری به‌جای فناوری‌های سنتی فاوا توانسته ۸۸٪ در هزینهٔ سخت‌افزار و ۶۰٪ در هزینه‌های پشتیبانی فناوری اطلاعات صرفه‌جویی کند. همچنین اغلب کارکنان فناوری اطلاعات می‌توانند در پروژه‌های دیگر مستقر شوند و تقریباً نیمی از آنها (۴۹٪) توانسته‌اند کسب‌وکار خود را از این طریق توسعه دهند.
- **کاهش سرمایه‌گذاری اولیه:** یک مزیت اصلی فناورهای مبتنی‌بر ابر، کاهش میزان سرمایهٔ اولیهٔ موردنیاز است که به مشتری فرصت می‌دهد تا سرمایهٔ گران‌بهای خود را در سایر حوزه‌های تجاری سرمایه‌گذاری کند.
- **نهایت بهره‌وری سخت‌افزاری:** ازآنجاکه چندین شرکت، زیرساخت سرور را به‌طور اشتراکی استفاده می‌کنند، سخت‌افزار به‌طور کامل استفاده می‌شود و هزینهٔ پشتیبانی در واحد حجم کار کاهش می‌یابد.
- **کاهش هزینه‌های انرژی:** استفادهٔ کارآمدتر از سخت‌افزار به‌معنای نبود سرورهای بیکار است. وقتی مرکزداده راه‌اندازی می‌شود، به‌ندرت به‌طور کامل از سرورهای آن استفاده می‌شود. سرورهای بیکار انرژی هدر می‌دهند، بنابراین استفادهٔ بهتر از سخت‌افزارِ زیرساخت مشترک به‌معنای استفادهٔ کارآمدتر از انرژی و کاهش هزینه‌های مربوط به آن است.
- **کاهش هزینهٔ کارکنان فناوری اطلاعات:** هزینه‌های مرتبط با کارکنان IT باتجربه ازجمله حقوق، مزایا و سایر هزینه‌های استخدام معمولاً بیشتر از هزینهٔ سخت‌افزار و نرم‌افزار است. کارکنان فناوری اطلاعاتِ ارائه‌دهندهٔ ابر از زیرساخت مشترکی پشتیبانی می‌کنند، بنابراین هزینهٔ کل کارکنانِ فناوری اطلاعات کمتر از شیوه‌های سنتی است. در نتیجه هزینه‌های IT کاهش می‌یابد، همچنین کارمندان این حوزه

1. National Institute of Standards and Technology

می‌توانند به پست‌هایی منتقل شوند که درآمدزایی بیشتری ایجاد کنند.

- **قابلیت اطمینان و افزونگی:** برای دستیابی به یک سیستم پایدار و قابل‌اتکا، باید سخت‌افزارهای اضافی برای محافظت در برابر خرابی خریداری شود. وجود سخت‌افزار یدکی در حالت بیکار، راهی گران برای بیشینه‌کردنِ زمان کار است. راهکارهای ابری معمولاً سطوح افزونگی متعدد و چندین مرکزداده دارند. در مقابل، در روش‌های سنتی، ایجاد چنین سطحی از افزونگی برای پررونق‌ترین کسب‌وکارها و متمول‌ترین افراد نیز ممکن یا اقتصادی نیست.

عناصر اساسی یک سیستم نظارت تصویری ابری

فناوری ابری آن‌قدر در حوزهٔ نظارت تصویری بدیع است که برای بسیاری از افراد هنوز کاملاً شناخته‌شده نیست و همین مسئله سردرگمی‌هایی را در این حوزه به‌وجود آورده است. یک سیستم VSaaS، بسیار با راهکارهای سنتی NVR، DVR یا VMS متصل به اینترنت برای دسترسی از دور یا ذخیره‌سازی از دور متفاوت است. NIST ۵ ویژگی برای سیستم ابری به‌شرح ادامه برمی‌شمرد:

۱. خدمتی متناسب و منعطف با نوع درخواست: کاربر می‌تواند به‌طور خودکار قابلیت‌ها را بدون نیاز به تعامل حضوری با ارائه‌دهندهٔ خدماتْ تنظیم و دریافت کند.

۲. دسترسی به شبکه‌ای گسترده: قابلیت‌های فناوری ابری ازطریق شبکه و همچنین مکانیسم‌های استانداردی که استفاده از کلاینت‌های ضعیف یا قوی (مانند تلفن‌های همراه، تبلت‌ها، لپ‌تاپ‌ها و ایستگاه‌های کاری) را ترویج می‌کنند در دسترس هستند.

۳. تجمیع منابع: منابع ارائه‌شده در فناوری ابری به مصرف‌کنندگان متعدد با منابع فیزیکی و مجازی مختلف بر طبق محاسباتی اصولی و به‌صورت پویا و براساس تقاضای مصرف‌کننده تخصیص داده می‌شوند. منابع در رایانش ابری شامل ذخیره‌سازی، پردازش، حافظه و پهنای باند شبکه هستند.

٤. انعطاف‌پذیری سریع: قابلیت‌ها را می‌توان به‌صورت انعطاف‌پذیر تهیه و آزاد کرد، در برخی موارد حتی می‌توان فناوری ابری را طوری تنظیم کرد که به‌صورت خودکار منابع را به‌میزان نیاز تقسیم کند.

۵. خدمات اندازه‌گیری‌شده: سیستم‌های ابری با استفاده از قابلیت اندازه‌گیری متناسب با نوع خدمت، به‌طور خودکار استفاده از منابع را کنترل و بهینه می‌کنند. استفاده از منابع را می‌توان نظارت، کنترل و گزارش کرد. شفافیت از ویژگی‌های اساسی خدمت‌های ابری است. مدیران در خدمت ابری دقیقاً می‌دانند بابت چه چیزی چقدر هزینه می‌کنند و هزینهٔ پنهانی وجود ندارد.

این پنج ویژگی ضروری «ابر واقعی» در یک زیرساخت ابری مشترک ارائه می‌شوند. این زیرساخت می‌تواند عمومی یا خصوصی باشد. به بیان دیگر، خدمت ابری نه به معنی از دست دادن مالکیت اطلاعات است و نه به معنی نشت اطلاعات و دسترسی غیرمجاز به اطلاعات، در واقع این امکان وجود دارد که بهره‌بردار از ابر اختصاصی خودش استفاده کند.

یازده مزیت اصلی VSaaS نسبت به راهکار سنتی نظارت تصویری که در در جدول ادامه به‌طور کامل تشریح شده‌اند

بهره‌وری و هزینهٔ کل مالکیت	• نصب و راه‌اندازی • نگهداری و پشتیبانی • ساختار پرداخت • هزینهٔ کل مالکیت
انعطاف‌پذیری، مقیاس‌پذیری و تکامل فناوری	• انعطاف‌پذیری ذخیره‌سازی • افزودن و مدیریت دوربین‌ها • مدیریت پهنای باند • طول عمر فناوری، سرویس‌های ارزش افزوده و APIها
امنیت سایبری، دسترسی از دور و افزونگی	• امنیت سایبری • افزونگی و قابلیت اطمینان • دسترسی از دور

معیار مقایسه		DVR/NVR/VMS سنتی متصل به اینترنت
بهره‌وری و هزینهٔ کل مدیریت	نصب و راه‌اندازی	استقرار سیستم سنتیْ فرایندی طولانی و پیچیده است. پس از نصب فیزیکیِ تجهیزات، نصاب باید دوربین‌ها و DVR/NVR/VMS را تنظیم کند و نرم‌افزار را برای کلاینت‌ها روی سیستم عامل نصب کند، روترها برای انتقال تصویر باید پیکربندی شوند، سرورهای ذخیره‌سازی راه‌اندازی گردند و در آخر تنظیمات نهایی دوربین‌ها بهینه‌سازی شده و نرم‌افزار کاربری به کاربران آموزش داده شود. این روند در پروژه‌های کوچک، دست‌کم ۱۰ روز و در پروژه‌های بزرگ تا چندین ماه طول می‌کشد.
	نگهداری و پشتیبانی	در راهکارهای سنتی، یک فرایند فشردهٔ دستی برای پشتیبانی و نگهداری سخت‌افزاری و نرم‌افزاری به‌صورت دوره‌ای باید انجام شود. طبق تعرفهٔ نظام صنفی رایانه‌ای کشور، هزینهٔ نگهداری سالیانه حدود ۲۵٪ تا ۳۵٪ ارزش تجهیزات است. جدای از آن هیچ اطمینانی وجود ندارد که خدمات نگهداری و پشتیبانی از بروز مشکلات در سیستم ازجمله قطعی تصویر، سوختن دیسک سخت و مواردی از این دست پیشگیری کند. سیستم‌های نظارت تصویری برای ثبت وقایع مهم تهیه می‌شوند، اما در سیستم‌های سنتی ممکن است در لحظهٔ بروز اتفاق، سیستم از کار افتاده باشد، درحالی‌که کنترل یا پایش خودکاری بر عملکرد آن وجود ندارد.
	ساختار پرداخت	هزینه‌های سرمایهٔ اولیه این سیستم‌ها شامل سخت‌افزار و نرم‌افزار زیاد است. از سوی دیگر راهکارهای سنتی معمولاً مقیاس‌پذیر نیستند. مثلاً وقتی بخواهید ۲ دوربین به یک NVR که تمامی کانال‌های آن قبلاً استفاده شده، اضافه کنید، باید دستگاه جدیدی خریداری کنید. به بیان دیگر، یا باید منابع زیادی را برای توسعهٔ بعدی خریداری کرده و بدون استفاده رها کنید یا وقتی نیازمند توسعه‌ای هستید، سخت‌افزارهای قبلی‌تان قابل‌استفاده نبوده و از نو نیازمند تأمین سخت‌افزار هستید.
	هزینهٔ کل مالکیت (TCO)	در راهکارهای سنتی، هزینهٔ اولیه شامل هزینهٔ سخت‌افزار/ نرم‌افزار همچنین نصب و راه‌اندازی زیاد است. اقدامات جاری ازجمله هزینهٔ نگهداری سالانه، پیکربندی روتر، پیکربندی سیستم و پشتیبان‌گیری، وصله‌های امنیتی، دسترسی از دور به شبکه (حجم بالای پهنای باند مصرفی انتقال تصویر و هزینهٔ قابل‌توجهِ آن)، دستمزد کارکنان فناوری اطلاعات، فضا، برق، تعمیرات، آموزش کارکنان برای پایش و بازیابی، به‌روزرسانی نرم‌افزار، مدیریت مرکزی، افزونگی، برنامه‌های موبایل، پشتیبان‌گیری ویدئو، تأمین امنیت سایبری و ادغام چند سایت (یکپارچه‌سازی)، هزینه‌های سربار قابل‌توجهی برای مشتری در بر خواهد داشت.
انعطاف‌پذیری، مقیاس‌پذیری و تکامل فناوری	انعطاف‌پذیری در ذخیره‌سازی	یک VMS، NVR، DVR سنتی، ویدئو را در محل ذخیره می‌کند. ذخیره‌سازیْ مهم، هزینه‌بر و پیچیده است، زیرا کارکرد اصلی سامانهٔ نظارت تصویری، ضبط تصاویر است. هزینهٔ دیسک‌های سخت بالاست، بسیاری از دستگاه‌های DVR/NVR/VMS از دیسک‌های سخت با ظرفیت بالا پشتیبانی نمی‌کنند. مشتری به ظرفیت سخت‌افزاری که هنگام خرید و نصب سیستم خود انتخاب کرده، محدود می‌شود. اگر مشتری بخواهد رزولوشن، کیفیت یا مدت‌زمان نگهداری تصاویر دوربین‌های خود را افزایش دهد، باید سخت‌افزار اضافی یا جایگزین بخرد و آن را مجدداً پیکربندی کند.
	افزودن و مدیریت دوربین‌ها	این سیستم‌ها معمولاً از طیف وسیعی از دوربین‌های آنالوگ و IP پشتیبانی می‌کنند. وقتی سیم‌کشی اولیهٔ دوربین کامل شد، کاربران باید به‌صورت دستی دوربین‌های جدید را متصل و پیکربندی کنند.
	مدیریت پهنای باند	ذخیره‌سازی تصاویر دوربین‌ها در محلْ نیازی به پهنای باند ندارد، اما اگر تصاویر دوربین‌ها به محل دیگری برای ضبط منتقل نشود، با سرقت یا از بین رفتن DVR/NVR/VMS تمامی هزینه‌ای که مشتری برای سامانهٔ نظارت تصویری صرف کرده، هدر می‌رود. بنابراین برای مشاهده از دور پهنای باند موردنیاز است.
	طول عمر فناوری، خدمت‌های ارزش افزوده و APIها	سیستم‌های سنتی به‌سرعت منسوخ می‌شوند. ممکن است در آغاز ویژگی‌های بسیار خوبی داشته باشند، اما ویژگی‌های اصلی سخت‌افزاری‌شان ثابت باقی می‌ماند. می‌شود به‌روزرسانی‌های فریم‌افزار را بارگیری کرد، اما توانایی به‌روزرسانی فناوری محدود است. در ایران APIهای سیستم‌های سنتی یا در دسترس نیستند (به‌دلیل تحریم) یا اساساً کاربریِ قابل‌قبولی ندارند. به بیان دیگر، با خرید سیستم‌های سنتی نظارت تصویری، باید با بیشتر مزیت‌ها و قابلیت‌های خدمت‌های ارزش افزوده خداحافظی کرد.
امنیت سایبری، دسترسی از دور و افزونگی	امنیت سایبری	الزامات کاربر نهایی برای دسترسی از دور به ویدئوهای خود باعث شده است DVRها، NVRها و VMSهای سنتی معمولاً توسط یکپارچه‌ساز یا نصاب برای دسترسی ویدئوییِ از دور به اینترنت متصل شوند. در نتیجه برای تأمین امنیت سایبری، نیاز به نصب و پیکربندی فایروالِ اختصاصی نظارت تصویری وجود دارد که بسیار گران‌قیمت و کمیاب است. حتی فایروال اختصاصی نظارت تصویری نیز مشکل را به‌طور کامل حل نمی‌کند. سیستم‌های سنتی نظارت تصویری آسیب‌پذیرترین تجهیزات تحت شبکه از نظر امنیت سایبری هستند. به بیان دیگر، وقتی DVR یا NVR خود را به اینترنت متصل می‌کنید، همیشه نگران امنیت آن خواهید بود و مهاجمان به‌آسانی می‌توانند به آن به‌صورت غیرمجاز دسترسی داشته باشند.
	دسترسی از دور	معمولاً در سیستم‌های سنتی، دسترسیِ ویدئویی از دور در سیستم اصلی طراحی نشده و به‌دلیل نیاز مشتری اضافه می‌شود. کیفیت دسترسی به ویدئو می‌تواند غیر قابل پیش‌بینی باشد. معمولاً در بسترهای بومی کشور، با قطعی متناوب و کیفیت پایین تصویر انتقالی سیستم‌های سنتی مواجه هستیم. علاوه بر این، رمزنگاری در سیستم‌های سنتی نادر است و مشتریان آگاه، نگرانی جدی راجع به حفظ حریم خصوصی‌شان دارند. از سوی دیگر بیشتر سیستم‌های سنتی با مرورگرهای متعارف نظیر کروم و موزیلا مشکلات جدی دارند.
	افزونگی و قابلیت اطمینان	دستگاه‌های NVR، DVR و VMS سنتی ناپایدارند و برای افزایش سطح پایداری نیازمند سطوح افزونگی بسیار زیاد و متغیر هستند. علاوه بر این، روزانه لازم است متخصصان اقدامات بسیاری برای تأمین پایداری انجام دهند. سرورهای پشتیبان غالباً بیکار هستند و به هزینه‌های سربار اضافه می‌کنند.

VSaaS مبتنی‌بر ابر
یک سیستم مبتنی‌بر ابر براساس تقاضای مشتری مستقر می‌شود. مشتری با ثبت تقاضای خود ازطریق وبسایت ارائه‌دهندهٔ خدمات ابری نظارت تصویری، دستور نصب و راه‌اندازی دوربین به تعداد موردنظر خود را صادر می‌کند. نصب و راه‌اندازی فیزیکی هر دوربین حداکثر ۴ ساعت زمان نیاز دارد. با توجه به ویژگی‌های خدمت ابری، نیازی به انجام تنظیمات در سمت مشتری نیست و چند دقیقه پس از اتمام نصب فیزیکی، راهکار آمادهٔ بهره‌برداری است.
ازآنجایی که در فضای ابری، ارائهٔ خدمت بر عهدهٔ سخت‌افزار و نرم‌افزار بسیار قدرتمندی است، تنها با یک مودمِ (پل ارتباطی) در محل برای اتصال دوربین‌ها به VMS مبتنی‌بر ابر، پشتیبانی مداوم در خارج از وبسایتْ توسط ارائه‌دهندهٔ خدمت نظارت تصویری ابری انجام می‌شود. در سیستم‌های ابری عملکرد کامل خدمت- دوربین‌های مداربستهٔ نصب‌شده در محل مشتری، لینک ارتباطی، ذخیره‌ساز و پردازشگر ابری- مداوماً پایش می‌شود و در صورت بروز هرگونه مشکل، به‌صورت برخط مشکل شناسایی و برطرف خواهد شد.
نه‌تنها، هزینهٔ سرمایهٔ اولیه در راهکار VSaaS بسیار کم است، بلکه هزینهٔ عملیاتی ماهانهٔ آن قابل‌پیش‌بینی است. قیمت‌گذاری VSaaS براساس استفادهٔ مشتری انجام می‌شود، بنابراین، هزینهٔ اشتراک دوره‌ای براساس تعداد دوربین‌ها، دوره و ظرفیت نگهداری و خدمت‌های ارزش افزودهٔ دریافتی تعیین می‌شود. این سیستم با کسب‌وکار مشتری رشد می‌کند و هزینهٔ اضافی ندارد.
در راهکار ابری، درصورتی‌که همهٔ هزینه‌های آشکار و پنهان راهکار سنتی در نظر گرفته شوند، هزینهٔ اولیه کاهش می‌یابد. هزینه‌های اشتراک ماهانهٔ جاری به‌دلیل صرفه‌جویی در مقیاس ناشی از زیرساخت‌های ابری و پشتیبانی مشترک کمتر می‌شود.
سیستم‌های ابری پیشرفته ترکیبی انعطاف‌پذیر از فضای ذخیره‌سازی ارائه می‌کنند. مشتری بدون توجه به جایی که ویدئو در آنجا مشاهده یا ذخیره می‌شود، همواره دسترسی مستقیم به تصاویر زنده و ضبط‌شده دارد. وضوح یا دورهٔ نگهداری بلادرنگ قابل‌افزایش است، بی‌اینکه نیاز باشد سخت‌افزار موجود تغییر کند. ازآنجاکه سیستم‌های ابری از یک زیرساخت ابری مشترک بزرگ برای ذخیره‌سازی ویدئو استفاده می‌کنند، صرفه‌جویی‌ای در مقیاس و انعطاف‌پذیریِ فوق‌العاده و مقرون‌به‌صرفه‌ای ارائه می‌کنند.
سیستم‌های ابری پیشرفته از طیف وسیعی از دوربین‌های آنالوگ و IP پشتیبانی می‌کنند. وقتی سیم‌کشی اولیهٔ دوربین کامل شد، دوربین‌ها به‌طور خودکار پیکربندی می‌شوند. داشبوردها وضعیت اتصال دوربین را، با امکان اطلاع‌رسانی هشدارهای فوری در صورت بروز مشکلات دوربین یا اینترنت پایش می‌کنند.
پهنای باند موردنیاز برای مشاهده از دور در خدمت ابری هوبان جزء هزینهٔ خدمت نظارت تصویری مخابرات ایران بوده که در مقایسه با خرید مستقیم پهنای باند بسیار مقرون‌به‌صرفه‌تر است. خدمت نظارت تصویری مخابرات ایران مدیریت پهنای باند پیشرفته‌ای دارد که مصرف آن را مدیریت کرده و مشاهده از دور را هموارتر، با کیفیت بالاتر و بدون قطعی به مشتریان ارائه می‌دهد.
تکامل سریع فناوری ارائه‌دهنده، به‌روزرسانی‌های فناوری خودکار را ازطریق اینترنت به دستگاهِ در محل مشتری ارسال می‌کند. سیستم مشتری مداوماً به نوآوری‌های جدید مجهز می‌شود، بنابراین در این سیستم عمر فناوری طولانی است. رابط‌های برنامهٔ کاربردی با هدف تجزیه‌وتحلیل، یکپارچه‌سازی و ارائهٔ خدمت‌های ارزش افزوده به‌صورت عمومی منتشر می‌شوند.
سیستم‌های پیشرفتهٔ مدیریت ویدئوییِ مبتنی‌بر ابر، آسیب‌پذیری‌های امنیت سایبری سیستم‌های سنتی را ندارند. هیچ پورت باز، هیچ فایروال و هیچ نرم‌افزاری در محل مشتری برای تأمین امنیت سایبریِ سیستم‌های ابری لازم نیست.
سیستم‌های مبتنی‌بر ابر برای دسترسی از دور طراحی شده‌اند، به همین دلیل برای مدیریت مطمئن دسترسی و پخش ویدئو قابلیت‌های پیشرفتهٔ روان و پایدار دارند. راهکار ابری نظارت تصویری هوبان رمزنگاری اختصاصی و پیشرفته‌ای دارد. در این راهکار، استفاده از مرورگرهای جهانی، نرم‌افزارهای موبایل و کامپیوتر به‌آسانی در بالاترین سطح امنیت، مقدور است.
مراکز دادهٔ ابریْ فناوری افزونگی دوگانه و سه‌گانه دارند. زیرساخت مشترکْ منجر به استفادهٔ کامل از سرور و صرفه‌جویی در مقیاس می‌شود. مشتری اطلاعات ارزشمند نظارت تصویری خود را به خدمت ابری سپرده و مسئولیت نگهداری این اطلاعات ارزشمند و ارائه به مشتری در زمان نیاز بر عهدهٔ فضای ابری است.

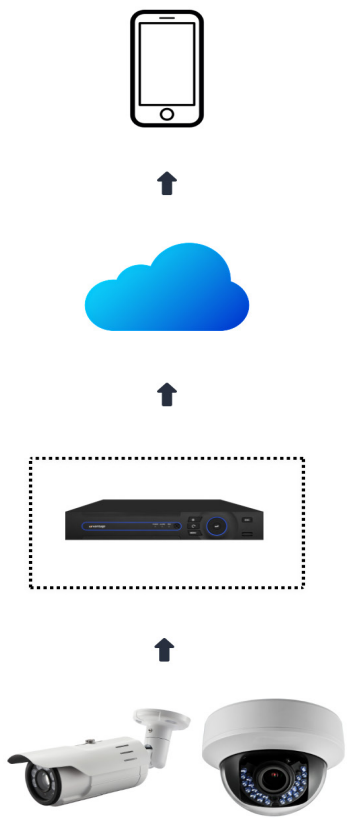
تعاریف

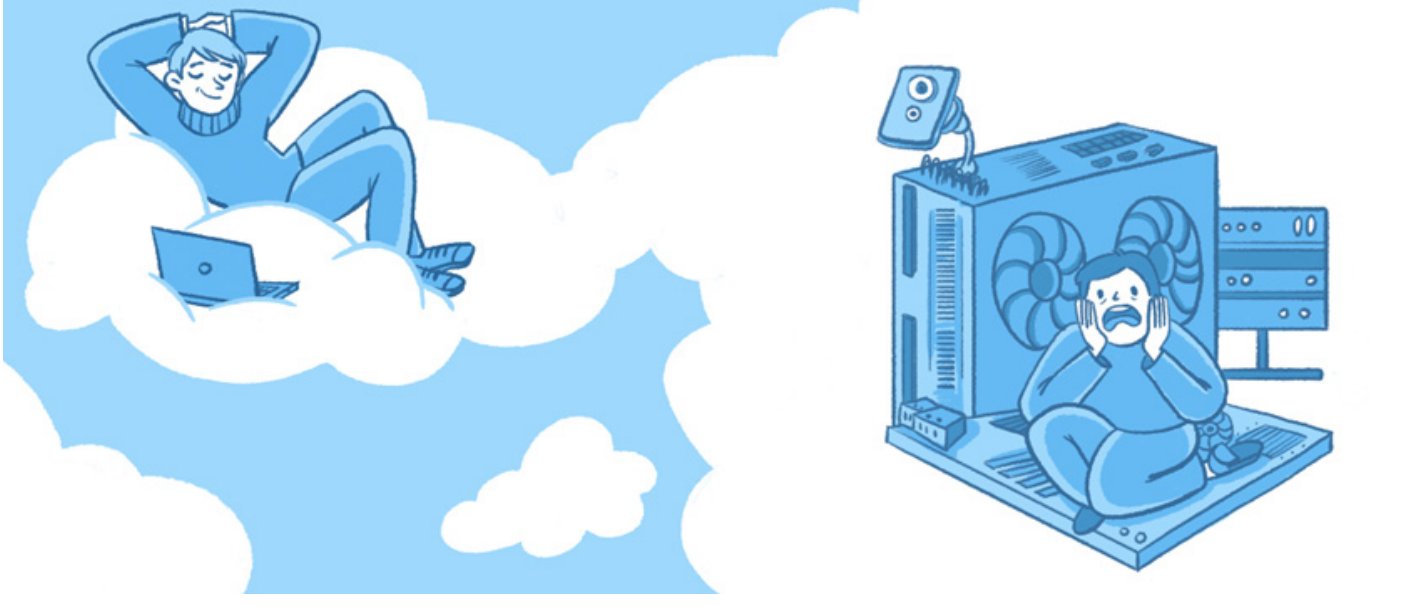
هزینهٔ کل مالکیت (Total Cost of Ownership): یک برآورد و تخمین مالی است که به خریداران خدمت و مالکان کمک می‌کند تا هزینه‌های مستقیم و غیرمستقیم یک محصول یا خدمت را تعیین کنند. به بیان دیگر، هزینهٔ کل مالکیت، هزینه‌ای است که در تمام عمر یک خدمت به مشتری تحمیل می‌شود.

مدیریت پهنای باند: سیستم‌های نظارت تصویری، به‌خاطر ماهیت ویدئویی‌شان، بیشترین مصرف پهنای باند را دارند. اپراتورهای متعددی پهنای باند ارائه می‌کنند و تقریباً در تمامی کشور امکان اتصال به اینترنت وجود دارد، ولی اینترنت باکیفیت و اختصاصی بسیار گران است. یک دوربین مداربستهٔ FULLHD که با سرعت ۳۰ فریم بر ثانیه و با کیفیت خوب تصویر ارسال می‌کند، به‌طور متوسط نیازمند پهنای باند اختصاصیِ ۲Mbps است. هر Mbps پهنای باند در کشور در زمان تألیف این مقاله (خرداد ۱۴۰۲) حدود ماهیانه یک میلیون تومان هزینه دارد.

امنیت سایبری: امنیت سایبری برای همهٔ مشتریان مهم است. نفوذ سایبری به سیستم‌های نظارت تصویری تهدید مضاعفی برای امنیت اجتماع است. سیستم‌های نظارت تصویری به دلایل متعدد برای مهاجمان و سارقان اینترنتی جذاب هستند. بیشترین حمله‌های سایبری در حال حاضر مربوط به سیستم‌های نظارت تصویری است.

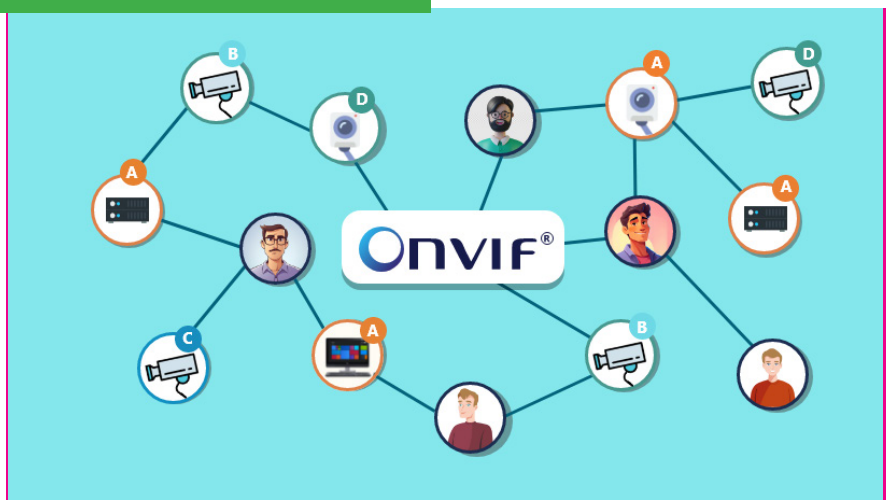
دسترسی از دور: بیشتر مشتریان به مشاهدهٔ برخط تصاویر دوربین‌های مداربسته یا همان انتقال تصاویر نیاز دارند. طبق بررسی‌های به‌عمل‌آمده، ۸۹٪ از بهره‌برداران سیستم‌های نظارت تصویری، برای مشاهده از دور ازطریق موبایل یا کامپیوتر اقدام می‌کنند.





یکپارچگی در سامانهٔ نظارت تصویری مبتنی بر استاندارد ONVIF

نویسنده:
محمود سعیدی



استاندارد سندی است که در آن الزامات فنی، مشخصات و دستورالعمل‌هایی به‌منظور اطمینان از تناسب دستگاه‌ها، تجهیزات و نرم‌افزارهای حاکم بر شبکه ارائه می‌شود.

پروتکل مجموعه‌ای از قوانین برای قالب‌بندی و پردازش داده‌هاست. با توجه به اینکه کامپیوترهای درون یک شبکه ممکن است از نرم‌افزارها و سخت‌افزارهای متفاوتی استفاده کنند، لازم است که زبان مشترکی میان آنها برای برقراری ارتباط با یکدیگر تعریف شود که به آن پروتکل می‌گویند.

استانداردها قابلیت همکاری بین دستگاه‌های مختلف را ارتقا می‌دهند و نیز هزینهٔ یکپارچه‌سازی تجهیزات شبکه‌ای را کاهش می‌دهند. فقدان استاندارد، علاوه بر محدودکردن مشتری در انتخاب، هزینه‌های یکپارچه‌سازی را نیز افزایش می‌دهد و باعث کاهش نوآوری در پیاده‌سازی سامانه می‌شود. همچنین درصورتی‌که استاندارد مناسبی وجود نداشته باشد، به جای اینکه پژوهشگران و توسعه‌دهندگان بر عملکردها و قابلیت‌های جدید متمرکز شوند، بیشتر وقت خود را با فعالیت‌های مربوط به یکپارچه‌سازی هدر می‌دهند.

گرچه صنعت نظارت تصویری در ایجاد استانداردها کُند عمل کرده است، با این حال مدتی است که پاسخگوی این نیاز بوده و استانداردسازی تجهیزات مرتبط را آغاز نموده است. در این راستا دو استاندارد ONVIF[1] و PSIA[2] در حوزهٔ یکپارچگی تجهیزات مربوط به سامانهٔ نظارت تصویری ارائه شده‌اند.

PSIA یک کنسرسیوم جهانی است که در سال ۲۰۰۸ با هدف ایجاد واسطهای استاندارد برای پلتفرم‌های سخت‌افزاری و نرم‌افزاری امنیت فیزیکی به‌وجود آمد. کنسرسیوم یادشده متشکل از ۶۵ سازندهٔ محصولات امنیت فیزیکی و یکپارچه‌ساز سامانه مانند Assa Abloy, Cisco Systems, HID, Ingersoll-Rand, Inovonics, IQinVision, Last Lock, Lenel, Kastle Systems, NICE Systems, Object Video, OnSSL Proximex, SCCG, Sentry Enterprises UTC, Vernit, Security, Honywell, Tyco Vidsys, Z۹ International, United Technologies, Milestone Systems و غیره است. تمرکز این کنسرسیوم بر ارتقای تعامل بین محصولات مبتنی‌بر IP در سامانه‌های امنیت فیزیکی و نیز سامانه‌های اتوماسیون ساختمانی و تجاری است. در واقع، PSIA مشخصات مرتبط با فناوری امنیت شبکه را در تمام بخش‌های صنعت ازجمله ویدئو، ذخیره‌سازی، تجزیه‌وتحلیل، نفوذ و کنترل دسترسی، ارتقا و توسعه می‌دهد. در این کنسرسیوم پنج کارگروه با عناوین ویدئوی IP، تجزیه‌وتحلیل ویدئو، ضبط و مدیریت محتوا، کنترل نواحی و سامانه‌ها وجود دارد.

استاندارد ONVIF در سال ۲۰۰۸ توسط Bosch و Axis و Sony معرفی و پایه‌گذاری شد و بیشتر سازندگان تجهیزات صنعت امنیت فیزیکی آن را پذیرفتند. این استاندارد در حال حاضر بیش از ۵۰۰ عضو دارد و بیش از ۵۰۰۰ محصول نظارت تصویری و کنترل دسترسی با آن سازگار است. لازم به ذکر است که بیشتر سامانه‌های مدرن امنیت فیزیکیِ مبتنی‌بر IP با استاندارد ONVIF سازگار هستند.

1. Open Network Video Interface Forum
2. Physical Security Interoperability Alliance

با توجه به هدف و مأموریت یکسان دو استاندارد PSIA و ONVIF، ممکن است تولیدکنندگان و یکپارچه‌سازان سامانهٔ نظارت تصویری در انتخاب بین این دو تردید داشته باشند و همچنین بسیاری از کاربران تفاوت بین این دو استاندارد را ندانند. تفاوت این دو استاندارد از این قرار است که در PSIA مشخصات تعریف‌شده بسیار کلی و عمومی‌تر است و برای گسترهٔ بزرگی از بازار امنیت فیزیکی شامل کنترل دسترسی، ذخیره‌سازی و غیره در نظر گرفته شده است، درحالی‌که تمرکز ONVIF بر جریان ویدئوی مبتنی‌بر IP به‌خصوص دوربین‌های مداربستهٔ تحت شبکه و تحلیل ویدئوست و مشخصات لازم را با هدف حل مشکل رابط فرستنده و گیرندهٔ جریان ویدئو ارائه می‌دهد. در واقع، معیارهایی که در ONVIF برای تعیین مشخصات در نظر گرفته می‌شود شامل کشف خدمت‌دهنده، پیکربندی خدمت‌دهنده، رویدادها، کنترل PTZ[3]، جریان ویدئو، تحلیل ویدئو و غیره است.

اهمیت استاندارد ONVIF در سامانهٔ نظارت تصویری

ONVIF مجموعه‌ای از استانداردهای برنامه‌نویسی توافق‌شده است که توسط توسعه‌دهندگان نرم‌افزار به‌کار گرفته می‌شود تا از ارتباط و تبادل اطلاعات محصول تولیدشده توسط آنها با سایر محصولات سازگار با استاندارد یادشده اطمینان حاصل شود. به عبارت دیگر، در استاندارد ONVIF یک زبان نرم‌افزاری مشترک به‌منظور برقراری ارتباط، اشتراک‌گذاری اطلاعات و تبادل داده، بین تجهیزات مبتنی‌بر IP در سامانهٔ نظارت تصویری ارائه می‌شود. قبل از ظهور استاندارد ONVIF، هریک از تولیدکنندگان محصول، پروتکل‌های خاص خود را تعریف می‌کردند و شرکت‌های تولیدکنندهٔ «نرم‌افزار مدیریت ویدئو» (VMS)[4] را مجبور می‌کردند تا سامانهٔ نظارت تصویری خود را سازگار با این پروتکل‌ها طراحی و پیاده‌سازی کنند. این موضوع مشکلات و چالش‌های زیر را برای شرکت‌های VMS به‌همراه داشت:

- احتمال داشت که شرکت‌ها نتوانند از محصولات سایر تولیدکنندگان در سامانهٔ خود بهره ببرند و در نتیجه طراحی و یکپارچه‌سازی سامانه با پیچیدگی و محدودیت زیادی همراه می‌شد.
- روند ارتقای سامانه به‌سختی، به‌کندی و حتی با هزینهٔ بالا همراه بود.
- هر زمان که تولیدکنندهٔ محصول، تغییراتی در پروتکل ایجاد می‌کرد یا یک ویژگی جدید به آن اضافه می‌نمود، سامانهٔ پیاده‌سازی‌شده باید از نو به‌روزرسانی می‌شد که این مستلزم صرف زمان و هزینهٔ زیاد برای عملکرد صحیح سامانه بود.

با ظهور استاندارد ONVIF، استفاده از محصولات مبتنی‌بر این استاندارد باعث آزادی بیشتر در انتخاب دوربین‌های مختلف مبتنی‌بر IP و تجهیزات کنترل دسترسی شد. مثلاً، دوربین‌های ONVIF می‌توانند با سایر تجهیزات نظارتی و امنیتی مانند VMS، سامانه‌های کنترل دسترسی و «سامانه‌های مدیریت هشدار» (AMS)[5] که با استاندارد ONVIF سازگار هستند، مستقل از اینکه توسط چه سازنده‌ای تولید شده‌اند، به‌صورت یکپارچه ارتباط برقرار کنند و تبادل داده انجام دهند. در واقع، دوربین‌ها و تجهیزات سازگار با ONVIF مکانیسم کشف آسانی دارند که شناسایی و مدیریت خودکار آنها را توسط سامانه‌های مدیریت ویدئو و سایر نرم‌افزارهای سازگار با ONVIF ممکن می‌سازد. با داشتن چنین قابلیتی، می‌توان با ترکیب و تطبیق محصولات از برندهای مختلف، یک سامانهٔ نظارت تصویری خاص و منحصربه‌فرد طراحی و پیاده‌سازی کرد. علاوه‌براین، یکپارچه‌سازی تجهیزات نظارتی و امنیتی با پیچیدگی کمتری همراه خواهد بود و ارتقای سامانه‌ها ساده، سریع و با هزینهٔ کم انجام می‌شود.

به‌منظور یکپارچه‌سازی در سامانهٔ نظارت تصویری، نمایه‌های S, M, G, D, C, A, T در ONVIF تعریف شده‌اند که مرتبط با کنترل دسترسی، ضبط ویدئو، جریان ویدئو و تحلیل ویدئو در سامانهٔ مذکور هستند. لازم به ذکر است که نمایهٔ Q از ابتدای آوریل ۲۰۲۲ منسوخ شده است و دیگر توسط ONVIF پشتیبانی نمی‌شود. دلیل عدم‌پشتیبانی از این نمایه این است که برخی از ویژگی‌های نمایهٔ Q با راهکارهای فعلی امنیت سایبری سازگاری ندارند. نمایهٔ Q این قابلیت را برای کلاینت ایجاد می‌کرد که بتواند با پیمایش دوربین‌ها و سایر تجهیزات امنیتیِ موجود در شبکه، دوربین یا تجهیز امنیتی موردنظر در شبکه را کشف کند. در واقع این نمایه باعث می‌شد که فرایند نصب در محیطی با برندهای مختلف، سریع‌تر و آسان‌تر انجام شود.

کنترل دسترسی در استاندارد ONVIF

نمایه‌های مرتبط با کنترل دسترسی در استاندارد ONVIF شامل A, C, D است.

نمایهٔ A

نمایهٔ A در سامانهٔ کنترل دسترسی، به‌منظور پشتیبانی از یکپارچگی سامانه به‌منظور ایجاد و اعمال قوانین خاص است. نمایهٔ A می‌تواند اطلاعات، وضعیت و رویدادها را در تجهیزات بازیابی کند و مواردی مانند قوانین دسترسی، اعتبار و برنامهٔ زمان‌بندی را پیکربندی کند. به عبارت دیگر، سامانهٔ کنترل دسترسی می‌تواند از نمایهٔ A برای پشتیبانی از ایجاد قوانین خاص برای اعطا یا لغو دسترسی به مناطق کنترل‌شونده توسط کارت‌خوان‌ها و سایر تجهیزات سازگار با نمایهٔ A بهره‌برداری کند. می‌توان گفت که ویژگی‌هایی که نمایهٔ A در پروتکل ONVIF، برای پیکربندی کنترل دسترسی از آنها پشتیبانی می‌کند، شامل موارد زیر هستند:

- «اعطا/ ابطال اعتبار»[6]؛
- ایجاد برنامهٔ زمان‌بندی؛
- تعیین قوانین دسترسی.

نمایهٔ C

نمایهٔ C برای تجهیزات مرتبط با «سامانهٔ کنترل دسترسی فیزیکی» (PACS)[7] استفاده می‌شود. کنترل دسترسی فیزیکی به این معناست که چه کسی، «دارندگان اعتبار»[8]، در چه زمانی، که توسط برنامهٔ زمان‌بندی تعریف شده است، به کجا، منطقه یا ناحیه، و چگونه، در چه «سطح امنیت»[9]، می‌تواند دسترسی داشته باشد. این نمایه از کنترل دسترسی، مدیریت رویداد و مدیریت هشدار پشتیبانی می‌کند. همچنین این نمایه برای کنترل دسترسی به نواحی خاص بسیار مفید است.

نمایهٔ D

نمایهٔ D مرتبط با تجهیزات جانبی کنترل دسترسی است و موارد زیر را در بر می‌گیرد:

3. Pan, Tilt, and Zoom
4. Video Management Software
5. Alarm Management Systems
6. Granting/ revoking credentials
7. Physical Access Control System
8. Credential holders
9. Security Levels

- انتقال شناسه‌های اعتبار ورودی و درخواست‌ها برای دسترسی؛
- انجام اقداماتی مانند قفل‌کردن و بازکردن قفل.

این نمایهٔ واسطهایی را برای دستگاه‌های ورودی و خروجی جانبی تعیین می‌کند. خروجی جانبی تعیین می‌کند. دستگاه‌های خروجی می‌توانند شامل قفل‌ها، نمایشگرها و LEDها باشند.

نمونه‌هایی از دستگاه‌های ورودی شامل موارد زیر هستند:

- دستگاه‌های ورودی نشانه‌خوان (برای کارت‌ها، کلیدها، تلفن‌های همراه یا بارکدها)؛
- بیومتریک‌خوان‌ها (برای تشخیص اثر انگشت)؛
- دوربین‌ها (برای تشخیص عنبیه، چهره یا پلاک خودرو)؛
- حسگرها (برای وضعیت قفل، وضعیت در، دما یا حرکت).

در واقع، نمایهٔ D مکمل نمایه‌های A و C در ایجاد ارتباطات استاندارد در سامانهٔ کنترل دسترسی مبتنی‌بر IP است. دستگاه جانبی سازگار با نمایهٔ D، شناسه‌های اعتبار ورودی را می‌گیرد و آنها را به کلاینت سازگار با نمایهٔ D مانند واحد کنترل دسترسی یا نرم‌افزار مدیریت ارسال می‌کند. سپس کلاینت با توجه به اینکه قوانین دسترسی، زمان‌بندی‌ها و اعتبارنامه‌ها را در خود ذخیره دارد، در خصوص دسترسی یا عدم‌دسترسی تصمیم‌گیری می‌کند و فرمانی را برای اعطا یا رد دسترسی، نمایش پیام یا درخواست ورودیِ اضافی مانند کد پین به دستگاه جانبی ارسال می‌کند.

ضبط ویدئو در استاندارد ONVIF

نمایهٔ G مرتبط با کنترل ذخیره‌سازی داده‌های ویدئویی است. این نمایه از ویژگی‌های مرتبط با ضبط، جست‌وجو و بازپخش پشتیبانی می‌کند. همچنین این نمایه شامل پشتیبانی برای دریافت جریان صوت و فراداده[10] است.

نمایهٔ G موجود در تجهیزات، مثلاً در دوربین IP یا انکودر ویدئو، این قابلیت را در آنها ایجاد می‌کند که بتوانند داده‌های ویدئویی را روی شبکهٔ IP یا روی سخت‌افزار خود ضبط و ذخیره کنند. همچنین نمایهٔ G موجود روی یک کلاینت مانند VMS، این قابلیت را در آن ایجاد می‌کند که بتوان پیکربندی، درخواست و کنترل ضبط داده‌های ویدئویی را ازطریق شبکهٔ IP روی تجهیزاتِ دارای نمایهٔ G انجام داد. به عبارت دیگر، نمایهٔ G به VMS امکان می‌دهد که داده‌های ویدئویی را از «ضبط‌کننده‌های ویدئوی شبکه» (NVR)[11] یا حتی از کارت‌های SD نصب‌شده روی دوربین مبتنی‌بر IP بازیابی کند.

10. Metadata

جریان ویدئوی پایه در استاندارد ONVIF

نمایهٔ S یک نمایهٔ پایه‌ای برای دوربین‌ها و NVRهای مبتنی‌بر IP است که جریان ویدئو را از دوربین به تجهیزاتِ پایش و ضبط پشتیبانی می‌کند. خدمت‌دهندهٔ ONVIF که با نمایهٔ S مطابقت دارد، خدمت‌دهنده‌ای است که داده‌های ویدئویی را ازطریق IP به خدمت‌گیرنده ارسال می‌کند. همچنین این نمایه شامل پشتیبانی از دوربین‌های PTZ، فراداده و صوت است. خدمت‌گیرندهٔ ONVIF که با نمایهٔ S مطابقت دارد، خدمت‌گیرنده‌ای است که ازطریق IP، جریان داده‌های ویدئویی از خدمت‌دهنده را پیکربندی، درخواست و کنترل می‌کند.

جریان ویدئوی پیشرفته در استاندارد ONVIF

نمایهٔ T به‌منظور ایجاد قابلیت‌های پیشرفته مانند آشکارسازی حرکت، تحلیل ویدئو و پشتیبانی از کدک H.۲۶۵ ایجاد شده است. نمایهٔ T از فناوری‌های جدیدِ استفاده‌شده در دوربین‌های امنیتی پشتیبانی می‌کند، به همین دلیل اهمیت بالایی در کاربردهای نظارت تصویری دارد. این اهمیت از آنجا ناشی می‌شود که فناوری‌های جدید مانند آشکارسازی حرکت و تحلیل ویدئو در بهبود بهره‌وری سامانهٔ نظارت تصویری بسیار مؤثر واقع شده‌اند.

نمایهٔ T با جریان ویدئوی پیشرفته مرتبط است و موارد زیر را در بر می‌گیرد:

- فشرده‌سازی ویدئو با استاندارد H.۲۶۵ /H.۲۶۴؛
- تنظیمات تصویربرداری؛
- هشدار حرکت و دست‌کاری در ویدئو؛
- جریان فراداده؛
- صدای دوطرفه.

لازم به ذکر است که نمایهٔ T جایگزین نمایهٔ S نیست و هردو نمایه کاربردهای مخصوص به خود را دارند و می‌توانند با یکدیگر ترکیب شوند.

کاربردهای تحلیلی در استاندارد ONVIF

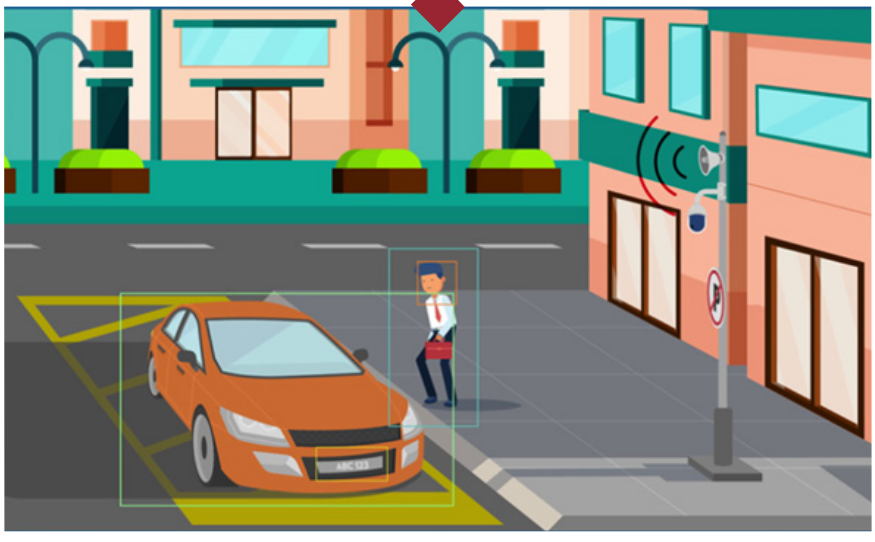
نمایهٔ M در ONVIF از پیکربندی تحلیل ویدئو، پرس‌وجوی اطلاعات برای فراداده، فیلترینگ و جریان فراداده پشتیبانی می‌کند. این نمایه واسطهایی برای طبقه‌بندی اشیا و فرادادهٔ مشخصی برای موقعیت جغرافیایی، وسیلهٔ نقلیه، پلاک، چهره و بدن انسان دارد. اگر محصولات به‌کارگرفته‌شده در سامانهٔ نظارت تصویری، از ویژگی‌هایی نظیر جریان ویدئو، مدیریت رویدادها یا پیکربندی قوانین پشتیبانی کنند، آنگاه باید از واسطهای نمایهٔ M نیز برای آن ویژگی‌ها پشتیبانی نمایند. همچنین اگر محصولات از تحلیل ویدئو در شمارش اشیا نظیر افراد، خودرو و غیره، «بازشناسی چهره»[12] یا «بازشناسی پلاک»[13] پشتیبانی کنند، آنگاه باید مدیریت رویداد نمایهٔ M نیز برای این توابع پشتیبانی شوند.

11. Network Video Recorders

12. Face Recognition

13. License plate recognition

نمایهٔ M شامل فراداده‌ها و رویدادها برای تحلیل ویدئو



یک محصول منطبق بر نمایهٔ M می‌تواند یک «دستگاه لبه»[14] مانند دوربین مبتنی‌بر IP یا یک خدمت برنامهٔ کاربردی مبتنی‌بر سرور یا ابر با قابلیت تحلیل باشد که می‌تواند از واسطهای نمایهٔ M برای ارسال فراداده به کلاینت ازطریق IP استفاده کند. همچنین یک کلاینت منطبق‌بر نمایهٔ M می‌تواند یک VMS، یک NVR شبکه یا یک خدمت مبتنی‌بر سرور یا ابر باشد که از واسطهای نمایهٔ M برای پیکربندی، درخواست و کنترل جریان فراداده دستگاه لبه یا خدمت استفاده کند.

به‌طورکلی، نمایهٔ M مرتبط با فراداده‌های تحلیل ویدئوست و موارد زیر را در بر می‌گیرد:

- پیکربندی تحلیل و پرس‌وجوی اطلاعات برای فراداده؛
- پیکربندی و جریان فراداده؛
- پشتیبانی از طبقه‌بندی اشیا؛
- تعریف فراداده برای موقعیت جغرافیایی، وسیلهٔ نقلیه، پلاک، چهره و بدن انسان؛
- واسطهای رویداد برای تحلیل‌های مرتبط با بازشناسی چهره، پلاک و شمارندهٔ اشیا؛
- ارسال رویدادها ازطریق جریان فراداده، خدمت رویداد ONVIF یا MQTT[15]؛
- پیکربندی قوانین برای رویدادها.

نتیجه‌گیری

استاندارد ONVIF یک استاندارد جهانی برای ایجاد سازگاری بین تجهیزات نظارتی و امنیتی مختلف و نیز یکپارچه‌سازی آنها در سامانهٔ نظارت تصویری است. این استاندارد با تمرکز بر جریان ویدئوی مبتنی‌بر IP به‌خصوص دوربین‌های شبکه و تحلیل ویدئو ارائه شده است تا تولید سامانه‌های نظارت تصویری با انعطاف‌پذیری، نوآوری و سرعت بیشتری همراه باشد. استاندارد ONVIF شامل نمایه‌های S, M, G, D, C, A, T است تا بتوان براساس ویژگی‌های آنها از یکپارچگی تجهیزات مرتبط با کنترل دسترسی، ضبط ویدئو، جریان ویدئو و تحلیل ویدئو در سامانهٔ نظارت تصویری اطمینان حاصل کرد. در استاندارد یادشده، نمایه‌های A, C, D مرتبط با کنترل دسترسی، نمایهٔ G مرتبط با کنترل ذخیره‌سازی داده‌های ویدئویی، نمایهٔ S مرتبط با جریان ویدئوی پایه از دوربین به تجهیزات پایش و ضبط، نمایهٔ T مرتبط با جریان ویدئوی پیشرفته و ایجاد قابلیت‌های پیشرفته مانند آشکارسازی حرکت، تحلیل ویدئو و پشتیبانی از کدک H.۲۶۵ و نمایهٔ M مرتبط با تعریف فراداده‌هایی برای طبقه‌بندی و شمارش اشیا، شناسایی موقعیت جغرافیایی، شناسایی وسایل نقلیه، شناسایی پلاک، شناسایی چهره و تشخیص وجود انسان در تحلیل ویدئوست.

14. Edge device

15. Message Queuing Telemetry Transport

دوربین‌های نظارت تصویری سیم‌کارتی

نویسنده:
محمود سعیدی

به‌طور کلی فناوری‌های مرتبط با شبکه‌های بی‌سیم برای بسیاری از کاربران اینترنت محبوب است و به همین دلیل استفاده از محصولات و پروتکل‌های مرتبط با این نوع از شبکه‌ها گسترش یافته است. همچنین عواملی مانند هزینهٔ ناچیز نصب و استقرار، عدم‌نیاز به سیم، انعطاف‌پذیری و قابلیت‌های ویژهٔ شبکه‌های بی‌سیم باعث شده است که شبکه‌های یادشده هم برای تأمین‌کنندگان زیرساخت و هم کاربران جذاب باشد.

بستر انتقال داده‌های ویدئویی در دوربین‌های سیم‌کارتی، شبکهٔ تلفن همراه است. با توجه به ماهیت بی‌سیم شبکهٔ تلفن همراه و نیز امکان نظارت تصویری در هر نقطه، مشروط به آنکه شبکه در آن نقطه امکان آنتن‌دهی داشته باشد و در هر زمان، مشروط به نبود اختلال در شبکه، جذابیت این دوربین‌ها برای کاربران دوچندان می‌شود.

گرچه داشتن دوربین قابل‌کنترل ازطریق تلفن همراه جذاب به‌نظر می‌رسد، اما پیش از خرید و به‌کارگیری آن باید بررسی شود که چنین دوربین‌هایی چه نقاط قوت و ضعفی دارند و ما را با چه چالش‌هایی مواجه می‌کنند. در این مقاله، قابلیت‌ها و نیز معایب دوربین‌های سیم‌کارتی از نظر عملکرد دوربین، «زیرساخت انتقال داده»[1] و «آسیب‌پذیری‌های امنیتی»[2] بررسی می‌شود.

عملکرد «دوربین‌های نظارت تصویری سیم‌کارتی»[3]

عملکرد و موارد استفادهٔ دوربین‌های سیم‌کارتی و دوربین‌های کابلی یکسان نیست. دوربین‌های سیم‌کارتی از نظر عملکرد، بیشتر شبیه به تلفن همراه هستند و به‌جای اتصال به اینترنت از اتصال «شبکهٔ سلولی»[4] 5G/4G/3G استفاده می‌کنند و بدین صورت پیام‌ها و اعلان‌ها را ازطریق شبکهٔ تلفن همراه به ایستگاه‌های نظارتی ارسال می‌کنند. همچنین دوربین‌های نظارتیِ سیم‌کارتی از سیم‌کارت برای اتصال به اینترنت استفاده می‌کنند تا بتوانند تصاویر و ویدئوهای ضبط‌شده را به ایستگاه نظارتی یا یک دستگاه بی‌سیم دیگر ارسال کنند.

این دوربین‌ها به‌دلیل قابلیت اتصال به اینترنت و امکان ارسال تصاویر و ویدئوها به‌صورت بی‌سیم، برای نظارت بر اماکن مختلف به‌خصوص در محیط‌های دورافتاده کاربرد دارند. منبع تغذیهٔ این دوربین‌ها ممکن است باتری یا «صفحهٔ خورشیدی»[5] باشد.

مقایسهٔ عملکرد دوربین‌های نظارت تصویری سیم‌کارتی و کابلی

تنها بستر انتقال داده‌های ویدئویی در دوربین‌های نظارت تصویری سیم‌کارتی، شبکهٔ تلفن همراه است. بنابراین، اختلال در شبکهٔ تلفن همراه، انتقال داده‌ها را غیرممکن می‌کند. افزون‌براین، انتقال داده‌ها ازطریق شبکهٔ تلفن همراه، به‌دلیل حجم زیاد داده‌های ویدئویی هزینه‌های زیادی به کاربران تحمیل می‌کند.

مزیت اصلی دوربین‌های نظارتی کابلی نسبت به دوربین‌های نظارتی سیم‌کارتی این است که با استفاده از کابل مستقیماً به دستگاه ضبط تصاویر متصل می‌شوند و نیاز ندارند به اینترنت متصل شوند. به عبارت دیگر، دوربین مداربستهٔ کابلی مستقیماً تصاویر را به دستگاه ضبط می‌فرستد. این مزیت، به‌خصوص در مواقعی که ارتباط اینترنتی کافی در محل نصب دوربین موجود نیست، اهمیت دارد. همچنین دوربین‌های نظارتی کابلی نیاز به تغییر باتری ندارند، درحالی‌که دوربین‌های سیم‌کارتی نیاز به باتری و تعویض یا شارژ دوره‌ای دارند.

سایر مزایای عملکردی دوربین نظارت تصویری کابلی نسبت به دوربین نظارت تصویری سیم‌کارتی از قرار ادامه‌اند:

- امکان ضبط مداوم و طولانی‌مدت به‌دلیل حجم حافظهٔ بیشتر؛
- امکان استفاده در پروژه‌های بزرگ؛
- دسترس‌پذیری و امکانات کاربری بیشتر؛
- کارکرد و عمر بیشتر دستگاه.

1. Data transmission infrastructure
2. Security vulnerabilities
3. Cellular cameras
4. Cellular network
5. Solar panel

در مقابل، دوربین‌های سیم‌کارتی مزایایی دارند مانند قابلیت اتصال به اینترنت و ارسال تصاویر و داده‌ها بدون نیاز به کابل، قابلیت حمل‌ونقل، نصب و استفادهٔ آسان‌تر. همچنین دوربین‌های نظارتی کابلی در یک جا به‌طور ثابت باقی می‌مانند چراکه جابه‌جایی آن هزینه‌بر است ولی دوربین‌های سیم‌کارتی را می‌توان بدون هزینه یا با هزینهٔ خیلی کم جابه‌جا کرد.

کاربردهای دوربین‌های نظارت تصویری سیم‌کارتی

دوربین‌های نظارت تصویری سیم‌کارتی کمتر برای نظارت تصویری اماکن استفاده می‌شوند. معمولاً در مکان‌هایی که بستر اینترنت وجود دارد، استفاده از دوربین‌های نظارتی کابلی در اولویت قرار دارد. دلیل آن هزینهٔ بهره‌برداری بالا و آسیب‌پذیری بیشتر دوربین‌های سیم‌کارتی نسبت به دوربین‌های کابلی است.

دوربین‌های نظارت تصویری سیم‌کارتی بیشتر در مناطق دورافتاده و نیز مکان‌هایی مورداستفاده قرار می‌گیرند که فاقد بستر اینترنت هستند یا امکان نصب سامانه‌های مبتنی‌بر سیم‌کشی در آن اماکن وجود نداشته باشد. ازجمله کاربردهای دوربین‌های نظارتی سیم‌کارتی، ثبت تصاویر حیات وحش[۱] است که برای این کار در کوه‌ها، جنگل‌ها و اطراف رودخانه‌ها نصب می‌شوند. همچنین این دوربین‌ها به‌منظور امنیت یا نظارت در کمپ‌ها، آروی‌ها (RV)، قایق‌ها و اسکله‌ها، کارگاه‌های ساخت‌وساز، انبارها و مزارع کشاورزی به‌کار می‌روند که در آنها امکان نصب دوربین‌های کابلی وجود ندارد.

معایب دوربین‌های سیم‌کارتی

به دلایلی که در ادامه می‌آید دوربین‌های سیم‌کارتی را نمی‌توان به‌عنوان بهترین انتخاب برای امنیت و نظارت تصویری اماکن برگزید.

- **امکان ایجاد اختلال در عملکرد دوربین‌های سیم‌کارتی یا سلولی در نتیجهٔ عملکرد دستگاه‌های بی‌سیم پیرامون آن:** امواج دستگاه‌های رادیویی و بی‌سیم پیرامون دوربین‌های سیم‌کارتی ممکن است باعث ایجاد اختلال در عملکرد دوربین‌های سیم‌کارتی شود.
- **عدم امکان استقرار سامانهٔ نظارت تصویری در صورت بروز اختلال در شبکهٔ تلفن همراه:** با توجه به اینکه تنها بستر دوربین‌های سیم‌کارتی، شبکهٔ تلفن همراه است، ازاین‌رو اختلال در این شبکه امکان نظارت تصویری برخط را از بین می‌برد.
- **هزینه‌بربودن دوربین‌های نظارتی سیم‌کارتی و استفاده از آنها:** استفاده از این نوع دوربین‌های نظارتی به‌دلیل دادهٔ سلولی و فناوری راه دور گران درمی‌آید. همچنین قیمت این دوربین‌ها بسته به دوام دوربین‌ها و قابلیت‌هایی مانند اتصال به صفحه‌های خورشیدی تا چند برابرِ دوربین‌های نظارتی کابلی است.
- **محدودیت انرژی و عمر کوتاه باتری دوربین‌های نظارتی سیم‌کارتی:** با توجه به اینکه دوربین‌های سیم‌کارتی، داده‌های ویدئویی را ازطریق شبکهٔ تلفن همراه ارسال می‌کنند، مصرف باتری بالایی دارند و در نتیجه عمر باتری بسیار کوتاه می‌شود. درصورتی‌که از صفحهٔ خورشیدی برای تغذیهٔ دوربین استفاده نشود باید باتری این دوربین‌ها پس از دوره‌ای بسیار کوتاه تعویض یا شارژ شود. درصورتی‌که دوربین مجهز به صفحهٔ خورشیدی باشد، قیمت آن افزایش خواهد داشت. افزون‌براین، صفحهٔ خورشیدی زمانی برای تولید انرژی مؤثر خواهد بود که دوربین در فضای بیرونی نصب شده باشد.
- **امکان دریافت ویدئوی فاقد کیفیت لازم از دوربین‌های نظارتی سیم‌کارتی:** با توجه به وابستگی دوربین‌های سیم‌کارتی به شبکهٔ تلفن همراه، کیفیت ویدئوی ارسالی توسط این دوربین‌ها وابسته به وضعیت شبکهٔ تلفن همراه در شرایط مختلف آب‌وهوایی و سایر عوامل محیطی خواهد بود. همچنین عدم تعویض یا شارژ به‌موقعِ باتری باعث افت کیفیت داده‌های ویدئوییِ دوربین‌های نظارتی سیم‌کارتی می‌شود.
- **امکان استفاده از دوربین‌های نظارتی سیم‌کارتی در مکان‌های فاقد آنتن شبکهٔ تلفن همراه یا دارای آنتن ضعیف وجود ندارد:** یکی از الزامات استفاده از دوربین‌های نظارتی سیم‌کارتی، پوشش آنتن‌دهی مکان دوربین توسط شبکهٔ تلفن همراه است. عدم آنتن‌دهی شبکهٔ تلفن همراه یا آنتن‌دهی ضعیف شبکهٔ تلفن همراه باعث عدم دسترسی به داده‌های ویدئویی توسط کاربران مجاز و افت کیفیت ارائهٔ خدمات به کاربران می‌شود. به‌خصوص اینکه در این مکان‌ها نظارت تصویری برخط امکان‌پذیر نخواهد بود. حتی در مکان‌هایی که پوشش آنتن‌دهی شبکهٔ تلفن همراه وجود دارد، دو عاملِ شرایط آب‌وهوایی و تراکم زیاد ساختمان‌ها قدرت سیگنال دوربین‌های سیم‌کارتی و همچنین آنتن‌دهی شبکهٔ تلفن همراه را کاهش می‌دهند.
- **محدودیت فضای ذخیره‌سازی داده‌های ویدئویی در دوربین‌های نظارتی سیم‌کارتی:** ذخیره‌سازی داده‌های ویدئویی در دوربین‌های نظارتی سیم‌کارتی معمولاً روی کارت‌های حافظهٔ SD[۶] انجام می‌شود که در مقایسه با ضبط‌کننده‌های ویدئو در دوربین‌های کابلی فضای ذخیره‌سازی بسیار کمتری دارند. این محدودیت باعث می‌شود که نتوان بخش بزرگی از اطلاعات ویدئو را در کارت‌های SD ذخیره کرد، همچنین باید به‌صورت مداوم تصاویر ویدئویی ضبط‌شده را حذف کرد تا فضای ذخیره‌سازی دوربین آزاد شود.

حملات در شبکه‌های بی‌سیم

معمولاً شبکه‌های بی‌سیم امنیت کمتری نسبت به شبکه‌های کابلی دارند چراکه سیگنال‌ها ازطریق هوا منتقل می‌شوند و در این میان ممکن است توسط هکرها رهگیری و دست‌کاری شوند[۲]. ماهیت حمله به لایه‌های فیزیکی و MAC در شبکهٔ بی‌سیم با شبکه‌های کابلی متفاوت است. در واقع شبکه‌های بی‌سیم در دو لایهٔ یادشده نسبت به شبکه‌های کابلی آسیب‌پذیرترند.

حملات در لایهٔ فیزیکی شبکه‌های بی‌سیم

در واقع ماهیت پخش و انتشار داده‌ها در شبکه‌های بی‌سیم باعث می‌شود که ارتباطات بی‌سیم نسبت به ارتباطات کابلی در برابر حمله‌های مخرب در لایهٔ فیزیکی آسیب‌پذیرتر باشد که ازجملهٔ آنها می‌توان به حملات شنود داده‌ها یا استراق سمع[۳]، پارازیت[۴] و دست‌کاری[۵] اشاره کرد.

- **استراق سمع[۷]:** در حملهٔ استراق سمع، کاربر غیرمجاز تلاش می‌کند تا انتقال داده بین کاربران مجاز را رهگیری کند و به آنها دسترسی یابد.
- **پارازیت[۸]:** حملهٔ پارازیت از نوع حملات «بندآوری خدمات» (DoS)[۹]

6. Secure Digital
7. Eavesdropping
8. Jamming
9. Denial of Service

در لایهٔ فیزیکی است. در این حمله، وجود یک «گرهٔ مخرب»[10] در شبکه‌های بی‌سیم می‌تواند به‌آسانی تداخل عمدی در ارتباطات داده‌ای بین کاربران مجاز ایجاد کند. هدف از حملهٔ پارازیت، جلوگیری از دسترسی کاربران مجاز به منابع شبکه بی‌سیم و در نتیجه مختل‌شدن دسترس‌پذیری[11] شبکه است.

- **دست‌کاری[12]:** حملهٔ دست‌کاری یکی دیگر از انواع حملات DoS در لایهٔ فیزیکی است. در این حمله، مهاجم با دسترسی فیزیکی می‌تواند اطلاعات حساس مانند کلیدهای رمزنگاری یا سایر داده‌های موجود در دوربین سیم‌کارتی را استخراج کند یا آنها را تغییر دهد که این باعث خدشه‌دارشدن هر سه عنصر مثلث امنیت CIA[13] یعنی محرمانگی، پایداری و دسترس‌پذیری در سامانهٔ نظارت تصویری می‌شود.

حملات در لایهٔ MAC[14] شبکه‌های بی‌سیم

شبکه‌های بی‌سیم دربرابر حملاتی که در لایهٔ MAC نیز رخ می‌دهد نسبت به شبکه‌های کابلی آسیب‌پذیرترند. ازجمله حملاتی که در لایهٔ مذکور اتفاق می‌افتد به‌شرح زیر است:

- **MAC spoofing:** در این حمله، مهاجم آدرس MAC خود را با هدفی مخرب تغییر می‌دهد و یک آدرس MAC جعلی به خود اختصاص می‌دهد[6].
- **Identity theft:** جعل آدرس MAC به مهاجم امکان می‌دهد که هویت واقعی خود را پنهان و هویت دیگری را جعل کند و بدین صورت سرقت هویت رخ می‌دهد. مهاجمی که اقدام به سرقت هویت می‌کند، وانمود می‌کند که گره‌ای مجاز در شبکه است و بدین ترتیب به اطلاعات محرمانهٔ گرهٔ قربانی دسترسی پیدا می‌کند[6].
- **MITM[15]:** در این حمله مهاجم ابتدا شبکه را «شنود می‌کند»[16] تا آدرس‌های MAC یک جفت گرهٔ «ارتباطی قانونی»[17] را رهگیری کند، سپس دو قربانی را «جعل می‌کند»[18] و در نهایت با آنها ارتباط برقرار می‌کند[7].
- **Network Injection:** در این حمله در عملکرد صحیح تجهیزات شبکه مانند روتر، سوئیچ و غیره اختلال ایجاد می‌شود. این کار با تزریق دستورات جعلی به‌منظور پیکربندی مجدد تجهیزات موجود در شبکه انجام می‌شود[8].

اهمیت و پیچیدگی امنیت در دوربین‌های سیم‌کارتی

ازآنجایی‌که دوربین‌های نظارت تصویری وظایفی حیاتی و مرتبط با امنیت اماکن بر عهده دارند، امنیت بستر انتقال داده در این دوربین‌ها بسیار مهم است. درصورتی‌که بستر انتقال دادهٔ دوربین‌های نظارتی به‌صورت بی‌سیم باشد، مسائل امنیتی سامانهٔ نظارت تصویری آن نسبت به شبکه‌های کامپیوتری کابلی چالش‌برانگیزتر خواهد بود. در واقع، نگرانی‌های امنیتی شبکه‌های بی‌سیم به‌دلیل کانال ارتباطی غیرقابل‌اعتماد آنْ مانعی جدی برای پذیرش گستردهٔ این شبکه‌ها در سامانهٔ نظارت تصویری است.

دوربین‌های نظارت تصویری به‌طور فعال محیط اطراف خود را نظارت می‌کنند و اغلب اطلاعاتی غیر از داده‌های نظارتی دارند. از طرف دیگر، به‌دلیل محدودیت منابع دوربین‌های سیم‌کارتی، تأمین امنیت داده‌های آن بسیار دشوارتر و پرهزینه‌تر از دوربین‌های IP کابلی است. ازاین‌رو، احتمال نشت اطلاعات ناخواسته که غالباً منجر به نقض حریم خصوصی افراد در محیط می‌شود، در دوربین‌های سیم‌کارتی بیشتر از دوربین‌های IP کابلی است. همچنین با توجه به ماهیت انتشار در شبکه‌های بی‌سیم، حملهٔ مهاجمان به لایه‌های فیزیکی و MAC آسان‌تر می‌شود. ترکیب این عوامل باعث می‌شود که تضمین امنیت در طراحی و راه‌اندازی سامانه‌های نظارت تصویریِ مبتنی‌بر دوربین‌های سیم‌کارتی برای اطمینان از ایمنی عملیات، پایداری، محرمانگی، دسترس‌پذیری و حریم خصوصی افراد بسیار مهم باشد[9].

به‌طور کلی ایجاد امنیت در سامانهٔ نظارت تصویریِ مبتنی‌بر دوربین‌های سیم‌کارتی به‌دلیل قابلیت‌های محدود سخت‌افزاری و مسائل مربوط به توسعهٔ آنها دشوار است. جزئیات پیچیدگیِ این دسته از دوربین‌ها از قرار ادامه است[9]، [10]، [11]:

- دوربین‌های سیم‌کارتی در لایه‌های فیزیکی و MAC در برابر تهدیدهای امنیتی بسیار آسیب‌پذیرند؛
- کمینه‌کردنِ مصرف منابع و بیشینه‌کردنِ سطح امنیت در دوربین‌های سیم‌کارتی، دو فرایند مغایر و ناسازگار با یکدیگرند و باید مصالحه‌ای میان این دو فرایند ایجاد کرد؛
- استفاده از روش‌های پیشرفتهٔ ضدپارازیت به‌دلیل پیچیدگی بیشترِ دوربین‌های سیم‌کارتی نسبت به دوربین‌های کابلی، در طراحی و مصرف انرژی، امکان‌پذیر نیست؛
- استفاده از الگوریتم‌های رمزنگاری نامتقارن به‌دلیل پیچیدگی بیشترِ دوربین‌های سیم‌کارتی نسبت به دوربین‌های کابلی، در طراحی و مصرف انرژی، امکان‌پذیر نیست.

چالش‌های استفاده از دوربین‌های سیم‌کارتی

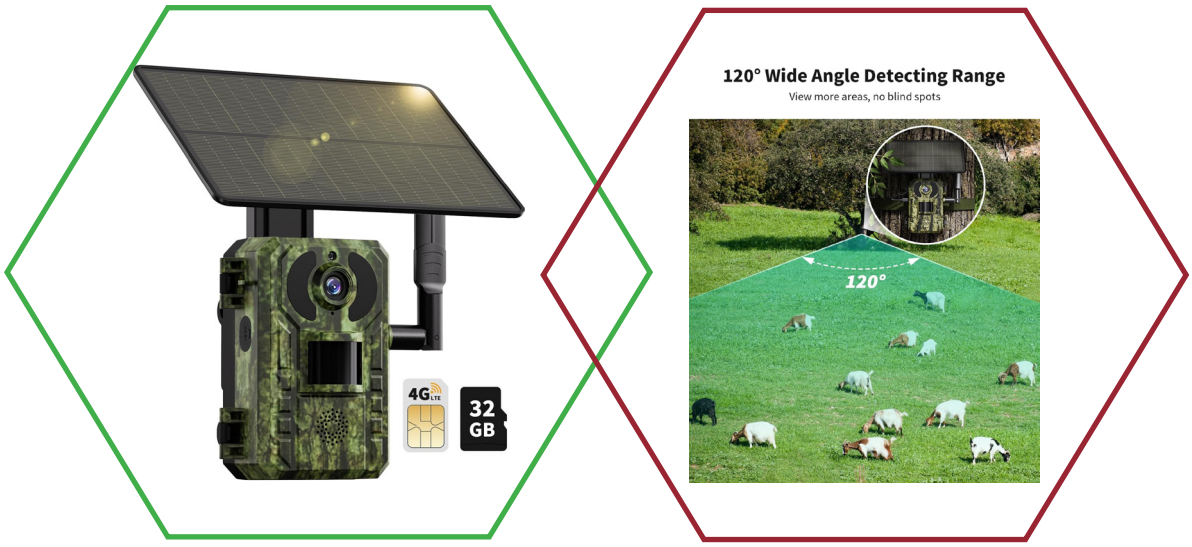
ازجمله چالش‌های استفاده از دوربین‌های سیم‌کارتی در سامانه‌های نظارت تصویری غیر قابل اعتماد بودن رسانهٔ بی‌سیم، مدیریت توان، امنیت، پیچیدگی سامانه، مسیریابی[19]، «واسطه‌سازی ازطریق شبکه‌های کابلی»[20] و نگرانی‌های مربوط به سلامت است[12]، [13].

همچنین عملکرد دوربین‌های سیم‌کارتی پرهزینه بوده و تضمین امنیت آنها دشوار است. ازجمله عواملی که باعث تحمیل هزینه‌های بالا برای استقرار دوربین‌های سیم‌کارتی می‌شوند می‌توان به موارد زیر اشاره کرد: قیمت بالای خرید دوربین، تعویض مداوم باتری با توجه به کوتاهی عمر آن و هزینهٔ بالای استفاده از بستر شبکهٔ تلفن همراه است[14].

از دیگر چالش‌های استفاده از دوربین‌های سیم‌کارتی در سامانهٔ نظارت تصویری، محدودیت ذاتی در منابع آن است که باعث پیچیده‌ترشدن فرایند امن‌سازی سامانه می‌شود[15]. در واقع محدودیت‌های مرتبط با منابع در دوربین‌های سیم‌کارتی از موانع اصلی پیاده‌سازی روش‌های معمول ایجاد امنیت در آنهاست. محدودیت منابع در سامانهٔ نظارت تصویری مبتنی‌بر دوربین‌های سیم‌کارتی شامل محدودیت پهنای باند، محدودیت حافظه، محدودیت ظرفیت محاسباتی و محدودیت انرژی است.

- **محدودیت پهنای باند:** با توجه به محدودیت پهنای باند در شبکهٔ بی‌سیم، انتقال داده‌های

10. Malicious node
11. Availability
12. Tampering
13. Confidentiality, Integration, Availability
14. Mandatory Access Control
15. Man-In-The-Middle
16. Sniffs
17. Legitimate communicating
18. Impersonates
19. Routing
20. Interfacing with wired networks



4G Cellular Trail Camera with
300M SIM Card and 32GB SD Card
Extra plus free 30 days of cloud storage

حجیم ویدئویی باعث می‌شود که پهنای باند زیادی توسط این دوربین‌ها در شبکهٔ بی‌سیم اشغال شود و کیفیت ارائهٔ خدمات به سایر کاربران کاهش یابد.

- **محدودیت حافظه:** محدودیت در حجم حافظهٔ دوربین‌های سیم‌کارتی باعث می‌شود که مدت‌زمان ضبط داده‌های ویدئویی در حافظه محدود باشد.
- **محدودیت ظرفیت محاسباتی:** باتری دوربین‌های سیم‌کارتی عمر محدودی دارد و این موضوع باعث غیرعملی‌شدنِ استفاده از روش‌های کلید نامتقارن در رمزنگاری می‌شود، چراکه این الگوریتم‌ها محاسبات ریاضیاتی پیچیده‌ای دارند و در اجرا انرژی زیادی مصرف می‌کنند. ازاین‌رو، فقط روش‌های کلید متقارن در این دوربین‌ها قابل‌استفاده است که مبتنی‌بر روش‌های محاسباتی کمتری است. بنابراین، محدودیت عمر باتری غیرمستقیماً باعث کاهش سطح تضمین محرمانگی داده‌های تصویری در دوربین‌های سیم‌کارتی می‌شود.
- **محدودیت انرژی:** همچنین هرچه محدودهٔ انتقال داده‌های تصویری بیشتر باشد و لازم باشد این داده‌ها تا فواصل بیشتری انتقال یابند، مصرف انرژی باتری بیشتر می‌شود. به عبارت دیگر، افزایش برد ممکن است منجر به تخلیهٔ انرژی باتری شود. درصورتی‌که باتری دوربین به‌موقع تعویض نشود ممکن است باعث عملکرد نادرست دوربین و افت کیفیت داده‌های ویدئویی شود. یکی دیگر از دلایل تخلیهٔ زودهنگام باتری دوربین‌های سیم‌کارتی، ارسال مرتب داده‌های حجیم ویدئویی است. به عبارت دیگر، هرچه کیفیت و تفکیک‌پذیری تصاویر ارسالی بیشتر باشد، مصرف انرژی موردنیاز دوربین برای ارسال داده‌های ویدئویی بیشتر می‌شود.

جمع‌بندی و نتیجه‌گیری

در جدول ۱، به‌صورت اجمالی، دوربین‌های سیم‌کارتی با دوربین‌های کابلی مقایسه می‌شوند. برای کارکردهای حائز اهمیت، تنها بستر قابل‌قبول، بستر کابلی است و استفاده از دوربین‌های سیم‌کارتی صرفاً برای کارکردهای موقت و فاقد اهمیت و برای مدتی محدود پیشنهاد می‌شود.

منابع و مراجع

1. D. A. Keiter, T. R. Stoddart, D. H. Jackson (2022), “Use of cellular-linked cameras to monitor live-trapping of wildlife”, Wildlife Management.
2. Y. Zou, J. Zhu, X. Wang, L. Hanzo (2016), “A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends”, Proceedings of the IEEE.
3. A. Perrig, J. Stankovie, D. Wanger (2004), “Security in wireless sensor networks”, Communication of the ACM, vol. 47, no. 6, pp. 53-57.
4. A. Mpitziopoulos (2009), “A survey on jamming attacks and countermeasures in WSNs”, IEEE Communications Surveys & Tutorials, vol. 11, no. 4, pp. 42-56.
5. S. Alam, D. De (2014), “ANALYSIS OF SECURITY THREATS IN WIRELESS SENSOR NETWORK”, International Journal of Wireless & Mobile Networks (IJWMN), Vol.6, No. 2.
6. V. Nagarajan, D. Huang (2010), “Using power hopping to counter MAC spoof attacks in WLAN”, Proceedings of the 2010 IEEE Consumer Communications and Networking Conference.
7. W. Zhou, A. Marshall, Q. Gu (2010), “A novel classification scheme for 802.11 WLAN active attacking traffic patterns”,

Proceedings of the 2006 IEEE Wireless Communications and Networking Conference.

8. J. Park, S. Kasra (2007), “Securing Ad Hoc wireless networks against data injection attacks using firewalls”, Proceedings of The 2007 IEEE Wireless Communications and Networking Conference.
9. E. Shi, A. Perrig (2004), “Designing Secure Sensor Networks”, Wireless Commun. Mag., vol. 11, no. 11, no. 6, pp. 38-43.
10. H. K. D. Sarma, A. Kar (2006), “Security Threats in Wireless Sensor Networks”, IEEE.
11. Y. Zhou, Y. Fang, Y. Zhang (2008), “Securing Wireless Sensor Networks: A Survey”, IEEE Communications Surveys & Tutorials, Vol. 10, Issue 3, pp. 6-28, Third Quarter.
12. M. Ilyas, I. Mahghoub (2005), “Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems”, CRC Press LLC.
13. R. M. Crovella (2000), “Sensor Networks and Communication”, CRC Press LLC.
14. Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, M. Galloway (2007), “A survey of Key management schemes in wireless sensor networks”, Elsevier, Computer Communications, doi: 10.1016/j.comcom.2007.04.009.
15. T. Kavitha, D. Sridharan (2010), “Security Vulnerabilities in Wireless Sensor Networks: A Survey”, Journal of Information Assurance and Security, pp. 31-44.
16. T. Zia, A. Zomaya (2006), “Security Issues in Wireless Sensor Networks”, IEEE, Proceedings of the International Conference on Systems and Networks Communications (ICSNC).
17. Y. Wang, G. Attebury, A. B. Ramamurthy (2006), “A Survey of security issues in wireless sensor networks”, IEEE Communications Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter.
18. S. Cho, DS. Lee, YD Lee, HJ Lee (2010), “A secure data framework for wireless sensor networks using authenticated encryption”, Journal of Information and Communication Convergence Engineering.

جدول ۱	مقایسهٔ
آسیب‌پذیری در برابر حملات	به‌دلیل ماهیت پخش و انتشار داده‌ها در شبکهٔ تلفن همراه و محدودیت‌های منابع موجود در دوربین‌ه برابر حملات مخرب آسیب‌پذیرترند[۳، ۴، ۵، ۶، ۷، ۸، ۱۴، ۱۵، ۱۶، ۱۷].
امنیت	به‌دلیل ماهیت پخش و انتشار داده‌ها در شبکهٔ تلفن همراه، دفاع امنیتی دوربین‌های سیم‌کارتی نسبت به دوربین‌های کابلی دربر
محرمانگی	به‌دلیل محدودیت انرژی و محدودیت در ظرفیت‌های محاسباتی در اجرای الگوریتم‌های رمزنگاری نامتقارن، سطح تضمین محر
پایداری	حمله‌های مرتبط با از بین بردن پایداری سامانهٔ نظارت تصویری شامل جعل داده‌های مسیریابی به‌منظ دیجیتال و الگوریتم‌های کلید نامتقارن استفاده می‌شود که این پردازش‌ها باعث ایجاد سربار اضافی
دسترس‌پذیری	شبکه‌های بی‌سیم نسبت به شبکه‌های کابلی دربرابر حملات DoS و DDoS آسیب‌پذیرترند. وقتی دوربی می‌شوند، به‌طوری که در نهایت این منابع به‌اتمام رسیده و دوربین دیگر قادر نخواهد بود که به
حریم خصوصی	به‌دلیل محدودیت انرژی و محدودیت در ظرفیت‌های محاسباتی در اجرای الگوریتم‌های مرتبط با حریم خصوصی افراد، سطح تض
پهنای باند	با توجه به آسیب‌پذیری شبکه‌های بی‌سیم نسبت به شبکه‌های کابلی دربرابر حمله‌های DoS و DDoS مبتنی‌بر دوربین‌های سیم‌کارتی در برابر حملات، احتمال کاهش و اتلاف پهنای باند در این سامانه‌ها بی به‌سمت ایستگاه پایه در شبکهٔ تلفن همراه ارسال می‌شود و بدین ترتیب باعث کاهش و اتلاف پهنای
کیفیت عمومی تصویر	عدم تعویض یا شارژ به‌موقع باتری باعث افت کیفیت داده‌های ویدئویی دوربین‌های نظارتیِ سیم‌کا آب‌وهوایی یا در مکان‌هایی با تراکم زیاد کاهش می‌یابد. علاوه بر موارد یادشده، با توجه به اینک تصاویر در شبکه‌های تلفن همراه کمتر از کیفیت عمومی تصاویر در بستر کابلی است[۵، ۱۸].
منبع تغذیه	ازجمله محدودیت‌های منابع در دوربین‌های سیم‌کارتی، محدودیت انرژی در دوربین‌های مذکور است[۱۶، ۱ مدیریت انرژی اهمیت بسزایی دارد. عواملی مانند برد زیاد انتقال داده، ارسال داده‌های ویدئویی حجیم، ا با حریم خصوصی و به‌طور کلی اجرای الگوریتم‌های دربرگیرندهٔ محاسبات پیچیدهٔ ریاضی باعث مصر الگوریتم‌های حاوی محاسبات پیچیدهٔ ریاضی خودداری کرد و آنها را با الگوریتم‌هایی با پیچیدگی کم مح
هزینهٔ بهره‌برداری	گرانیِ دوربین‌های نظارتی سیم‌کارتی، هزینه‌بربودن استفاده از آنها، به‌دلیل هزینهٔ چندبرابریِ بستر شبک تصویریِ مبتنی‌بر دوربین‌های سیم‌کارتی نسبت به دوربین‌های کابلی می‌شود.
حجم حافظه	ذخیره‌سازی داده‌های ویدئویی در دوربین‌های نظارتیِ سیم‌کارتی روی کارت‌های SD انجام می‌شود که د زیادی از فایل ویدئو را در کارت‌های SD ذخیره کرد.

ۀ دوربین سیم‌کارتی و دوربین کابلی

ای سیم‌کارتی، سامانه‌های نظارت تصویریِ مبتنی‌بر دوربین‌های سیم‌کارتی نسبت به سامانه‌های نظارت تصویریِ مبتنی‌بر دوربین‌های کابلی در

ابر حملات مخرب لایۀ فیزیکی[۳، ۴، ۵] و لایۀ MAC[۶، ۷، ۸] ضعیف‌تر است.

مانگی در دوربین‌های نظارتیِ سیم‌کارتی نسبت به دوربین‌های نظارتی کابلی کمتر است[۵، ۱۵].

ور ایجاد اختلال در سامانه و همچنین جعل داده‌های موجود در دوربین نظارتی است. به‌منظور دفاع در برابر حملات مرتبط با پایداری، از امضای در دوربین‌های سیم‌کارتی و مصرف انرژی زیادی می‌شود[۵].

ین‌های سیم‌کارتی در برابر سیلی از درخواست‌های مکرر قرار می‌گیرند، منابع زیادی مانند پردازشگر و حافظهْ صرف پاسخ به درخواست‌ها درخواست‌های مجاز پاسخ دهد. در این حالت دوربین سیم‌کارتی از دسترس خارج می‌شود[۵].

ضمین محافظت از حریم خصوصی در دوربین‌های نظارتیِ سیم‌کارتی نسبت به دوربین‌های نظارتی کابلی کمتر است[۱۵].

D، پهنای باند این شبکه‌ها نیز در نتیجۀ حمله‌های یادشده کاهش می‌یابد. به عبارت دیگر، به‌دلیل آسیب‌پذیریِ سامانه‌های نظارت تصویریِ شتر است[۱۵]. در واقع در حملات DDoS، با درخواست‌های جعلی از دوربین‌های سیم‌کارتی، داده‌های ویدئویی حجیم دائماً از سمت این دوربین‌ها باند شبکۀ تلفن همراه می‌شود.

رتی می‌شود. همچنین با توجه به وابستگی دوربین‌های سیم‌کارتی به شبکۀ تلفن همراه، ویدئوی ارسالی توسط این دوربین‌ها در شرایط بد ه تفاوت زمانیِ دریافت بسته‌ها در مقصد و از دست دادن بسته‌ها در شبکه‌های بی‌سیم نسبت به شبکه‌های کابلی بیشتر است، کیفیت عمومی

۱۷]. در دوربین‌های کابلی که محدودیت انرژی وجود ندارد، نیازی هم به مدیریت مصرف انرژی نیست، درحالی‌که در دوربین‌های سیم‌کارتی اجرای الگوریتم‌های فشرده‌سازی، اجرای الگوریتم‌های رمزنگاری، اجرای الگوریتم‌های مرتبط با تحلیل تصاویر ویدئویی، اجرای الگوریتم‌های مرتبط رف زیاد انرژی و تخلیۀ باتری در زمان کوتاهی می‌شود[۱۴، ۱۵]. به‌منظور مدیریت انرژی در دوربین‌های سیم‌کارتی باید تا حد امکان از استفاده از حاسباتی که در عین حال مؤثر و کارآمد نیز باشند، جایگزین کرد.

کۀ تلفن همراه نسبت به شبکه‌های ثابت و زمینی و هزینه‌بربودن تضمین امنیت[۵] در آنها موجب هزینه‌بربودن بهره‌برداری از سامانه‌های نظارت

رمقایسه با ضبط‌کننده‌های ویدئو در دوربین‌های کابلی فضای ذخیره‌سازی بسیار کمتری دارند. این محدودیت باعث می‌شود که نتوان زمان

مفاهیم کنترل دسترسی از طریق بلاک چین

نویسنده:
سید علی صموتی
یاسر علمی سولا

با توجه به توسعهٔ سریع شبکه‌ها و ارتباطات در دنیای مدرن و نیاز به کنترل دسترسی به منابع و اطلاعات در محیط‌های حساس مانند سیستم‌های مدیریت ترافیک، مسئلهٔ اصلی در مقالهٔ حاضر، معرفی یک روش کنترل دسترسی امن و اثربخش در این حوزه است. این مقاله بر روش‌های مدیریت کنترل دسترسی متمرکز است که در سیستم توزیع‌شده استقرار یافته‌اند. با توجه به گسترش چشمگیر فناوری‌های ارتباطی و انبوهی از اطلاعات حساس که در این سیستم‌ها پردازش می‌شوند، مسئلهٔ حفظ حریم خصوصی و محرمانگی اهمیت چشمگیری پیدا می‌کند. همچنین مسئلهٔ شفافیت نیز در سیستم‌های بلاک‌چین اهمیت بسزایی دارد. در این زمینه، نیاز به روش‌های امنیتی پیشرفته و کارآمد برای حفظ حریم خصوصی کاربران و اطلاعات محرمانهٔ اساسی، مهم و ضروری است. در سیستم‌های نوین با استفاده از ترکیب سیستم‌های بلاک‌چین و سیستم‌های کنترل دسترسیِ توزیع‌شده، پیشرفت‌های خوبی صورت پذیرفته است.

در سال‌های اخیر، با افزایش شدید دستگاه‌های هوشمند، اینترنت اشیا (IoT) توسعهٔ سریع‌تری داشته است. در این راهکار دنیای فیزیکی ازطریق زیرساخت شبکهٔ موجود به‌طور مؤثر با اینترنت ادغام می‌شود تا اشتراک‌گذاری داده‌ها میان دستگاه‌های هوشمند تسهیل شود. بااین‌حال، ساختار پیچیده و مقیاس بزرگ داده‌ها در شبکه، خطرات و چالش‌های امنیتی جدیدی برای سیستم‌های اینترنت اشیا به‌وجود می‌آورد. برای اطمینان از امنیت داده‌ها در سیستم‌های اینترنت اشیا فناوری‌های کنترل دسترسی سنتی مناسب نیستند.

در دنیای مدرن، فناوری بلاک‌چین در حوزه‌های مختلف ازجمله کنترل دسترسی، امنیت داده، حریم خصوصی و تمرکززداییِ شبکه‌های بی‌سیم با اقبال زیادی از سوی پژوهشگران و دانشمندان مواجه بوده است. اگرچه بلاک‌چین مزیت‌هایی نظیر فناوری نظیربه‌نظیر، ناشناس‌بودگی، افزایش ظرفیت و امنیت بهتر دارد. دلیل اصلی برتری آن‌ْ ساختار تغییرناپذیرش است. ازآنجاکه بلاک‌چین ماهیتی توزیع‌شده دارد، برای ازبین‌بردن نقش شخص ثالث قابل‌اعتماد در شبکه‌های به‌هم‌پیوسته می‌تواند به‌عنوان یک فناوری اصلی استفاده شود. هایپرلجر، آی‌بی‌ام بلاک‌چین، اتریوم، ریپل و مالتی برجسته‌ترین پلتفرم‌های بلاک‌چین در دسترس هستند.

در این مقاله، یک طرح کنترل دسترسی مبتنی‌بر سیستم‌های توزیع‌شده برای سیستم‌های اینترنت اشیا پیشنهاد می‌شود که مدیریت دسترسی را تا حد زیادی ساده‌تر می‌کند. سیستم‌های کنترل دسترسی توزیع‌شده توسط بلاک‌چین به افزایش امنیت و اعتماد در کنترل دسترسی مبتنی‌بر ویژگی و حفظ حریم خصوصی و جلوگیری از تقلب کمک می‌کنند. همچنین اهداف ادامه ازطریق پیاده‌سازی این سیستم‌ها حاصل می‌شود:

- برآوردن یک سیستم کنترل دسترسی به‌روز و امن در سیستم‌های مدیریت کنترل دسترسی مانند کنترل تردد، با توجه به تغییرات سریع در فناوری و افزایش حجم داده‌ها؛
- توجیه استفاده از سیستم‌های کنترل دسترسی مبتنی‌بر ویژگی به‌عنوان رویکردی نوآورانه برای تسهیل کنترل دسترسی در محیط‌های پیچیده و پویا.

تمرکز این مقاله بر سیستم‌های کنترل تردد و روش‌های متداول در این زمینه در حوزهٔ اینترنت اشیا و شبکه‌های ابری است.

چرایی کنترل دسترسی توسط بلاک‌چین

شکی نیست که اینترنت اشیا یکی از امیدبخش‌ترین فناوری‌هاست. در میان تمام فناوری‌های موجود برای امنیت داده و حفظ حریم خصوصی، بلاک‌چین کارآمدترین فناوری است؛ به‌دلیل ویژگی‌هایی مانند تغییرناپذیری و برگشت‌ناپذیری. بلاک‌چین اجازه نمی‌دهد، داده‌ها اصلاح شوند، تغییر کنند یا حذف شوند. هر زمان که با استفاده از تراکنش‌ها تغییری در دفترکل ایجاد شود، تغییرات در همهٔ گره‌ها توزیع می‌شود تا رونوشت خاص آنها از دفتر تأیید و به‌روز شود. وقتی تمام گره‌های شبکه تراکنش را تأیید کردند، امکان تغییر تراکنش بدون تغییر بلوک‌های بعدی و قبلی وجود ندارد؛ بنابراین، تراکنش‌های بلاک‌چین برگشت‌ناپذیر و تغییرناپذیر هستند و داده‌های آنها دائماً اضافه می‌شوند. هر بلوک به پیوندی که به آن زنجیره نیز می‌گویند متصل است. بلوک بعدی شامل هشِ بلوک قبلی برای بازدید از زنجیره به‌ترتیب زمانیِ معکوس است. بلاک‌چین از ساختار غیرمتمرکز و توزیع‌شده همراه با رمزنگاری استفاده می‌کند. در نتیجه کارکردی منحصربه‌فرد ارائه می‌کند. فناوری بلاک‌چین در جایی برتری دارد که امنیت و محرمانگی اطلاعات، اولویت اول شبکه باشد. کنترل دسترسی در اینترنت اشیا با پیاده‌سازی بلاک‌چین کارآمدتر می‌شود.

براساس پیش‌بینی گارتنر، در سال ۲۰۱۷، بیش از ۸,۴ میلیارد شیء متصل در سراسر جهان به این شبکه پیوسته است که نسبت به سال ۲۰۱۶ رشد ۳۱ درصدی داشته است که در سال ۲۰۲۰ به عدد ۲۰,۴ میلیارد رسیده است.

آخرین گزارش تحلیل وضعیت اینترنت اشیا در بهار ۲۰۲۳ نشان می‌دهد که تعداد اتصالات IoT جهانی در سال ۲۰۲۲ با رشد ۱۸ درصدی به ۱۴,۳ میلیارد نقطهٔ پایانیِ فعال رسیده است. تحلیلگران انتظار دارند که در سال ۲۰۲۳، دستگاه‌های IoT متصل در جهان ۱۶ درصد دیگر رشد کنند و به عدد ۱۶,۷ میلیارد نقطهٔ پایانی فعال برسند.

بااین‌حال، افزایش تعداد دستگاه‌های متصل، خطرات و چالش‌های امنیتی جدیدی برای سیستم‌های IoT به‌همراه دارد. ازآنجایی‌که دستگاه‌های اینترنت اشیا به‌طور گسترده توزیع می‌شوند، اِعمال کنترل امنیتی سختگیرانه به‌قدری دشوار است که آنها را در برابر حملات مختلف توسط مهاجمان آسیب‌پذیر می‌کند. همان‌طور که می‌دانیم کنترل دسترسی یکی از مهم‌ترین فناوری‌ها برای تضمین امنیت داده‌هاست. ترکیب اینترنت اشیا با فناوری بلاک‌چین امیدبخش است و انتظار می‌رود ضمن تضمین اطمینان، هزینه‌های کلی سیستم‌های اینترنت اشیا را کاهش دهد. این فناوری به اینترنت اشیا کمک می‌کند تا پایگاه‌دادهٔ غیرمتمرکز، معتبر و قابل‌تأیید عمومی ایجاد کند تا میلیاردها شیء متصل بتوانند ازطریق آن به‌صورت مطمئن توزیع شوند.

روش‌های کنترل دسترسی اینترنت اشیا مبتنی‌بر بلاک‌چین

اتصال دستگاه‌های هوشمند مختلف ازطریق اینترنت مزایای بسیاری دارد نظیر اشتراک‌گذاری داده، سهولت دسترسی و نظارت از دور. یکی از مسائل مهمی که اینترنت اشیا با آن مواجه است، ساختار متمرکز آن است، یعنی مدل مشتری–سرور. نبود اعتماد بین دستگاه‌های مختلف ممکن است باعث خرابی کل شبکه شود، بنابراین برای جلوگیری از این مشکل، راه‌حل معتبری لازم است. در

سال‌های اخیر، چندین رویکرد مبتنی‌بر بلاک‌چین پیشنهاد شده است که در ادامه به آنها می‌پردازیم.

کنترل دسترسی مبتنی‌بر ویژگی (ABAC)[1]

طراحی کنترل دسترسی مبتنی‌بر ویژگی برای ساده‌ترکردن مدیریت دسترسی در IoT پیشنهاد شده است. در این شیوه، فناوری بلاک‌چین برای اضافه‌کردن و حفظ توزیع ویژگی‌هایی شامل ویژگی‌های کاربر، ویژگی‌های منبع و ویژگی‌های شیء براساس نیاز کاربر، پیاده‌سازی می‌شود. ABAC ویژگی‌هایی را از مرجع صفات استخراج می‌کند و از آنها برای تشخیص منحصربه‌فرد بودن یا بازنمایی‌ها استفاده می‌کند که این ویژگی‌ها توسط مرجع ویژگی منتشر می‌شوند. هر مجموعه‌ای از ویژگی‌ها با فرمول‌های بولی که خط‌مشی‌های دسترسی متفاوتی را تعریف می‌کنند، نشان داده می‌شود. این سیاست‌های دسترسی برای دسترسی معتبر و مجاز استفاده می‌شوند. تمرکز بر تخصیص نقش‌ها یا ایجاد فهرست کنترل دسترسی برای تمام دستگاه‌ها تنش سیستم را کاهش می‌دهد. تجزیه‌وتحلیل عملکرد این روش نشان می‌دهد که ABAC در حفظ محرمانگی، انعطاف‌پذیری و مقیاس‌پذیری قدرتمند است.

در برخی از مقاله‌ها روشی برای کنترل دسترسی مبتنی‌بر ویژگی‌ها پیشنهاد شده است که از شش مؤلفهٔ اصلیِ شبکهٔ بلاک‌چین نظیر کنسرسیوم، گره‌های مرجع (AN)، دستگاه‌های IoT، Chaincode و دفترکل عمومی و درخت دسترسی تشکیل شده است. گره‌های مجوزدهی بخشی از شبکهٔ بلاک‌چین کنسرسیوم هستند و مسئولیت رسیدگی به تمام تعاملات دستگاه‌های اینترنت اشیا با شبکهٔ بلاک‌چین را بر عهده دارند. وقتی درخواستی برای دسترسی به هدف ارسال می‌شود، توسط آن هدف به گرهٔ مرجع ارسال می‌شود. کد زنجیره‌ای توسط AN جست‌وجو می‌شود و اعتبارنامه‌های دسترسیِ ثبت‌شده برای بررسی مشروعیت منحصربه‌فردی درخواست‌کنندگان و قانون دسترسیِ هدفْ بازیابی می‌شوند. پس از آن درخت دسترسی توسط AN برای ایجاد مجوز ساخته می‌شود. بلاک‌چین برای ثبت اطلاعات دسترسی نهایی به‌همراه نتیجهٔ مجوز استفاده می‌شود که به‌دنبال آن نتایج توسط AN برای درخواست‌کننده ارسال می‌شود.

1. Attribute-Based Access Control

دسترسی منصفانه

به‌منظور ساده‌سازی کنترل دسترسی کاربران به داده‌های خود، تکنیکی کاملاً مستعار و بدون حاکمیت مرکزی معرفی شده است. برای استفاده از نام مستعار، از آدرس‌های مشابهِ بیت‌کوین برای شناساییِ تمام موجودیت‌های تعاملی استفاده می‌شود و خط‌مشی کنترل دسترسی در قراردادهای هوشمند تعریف می‌شود.

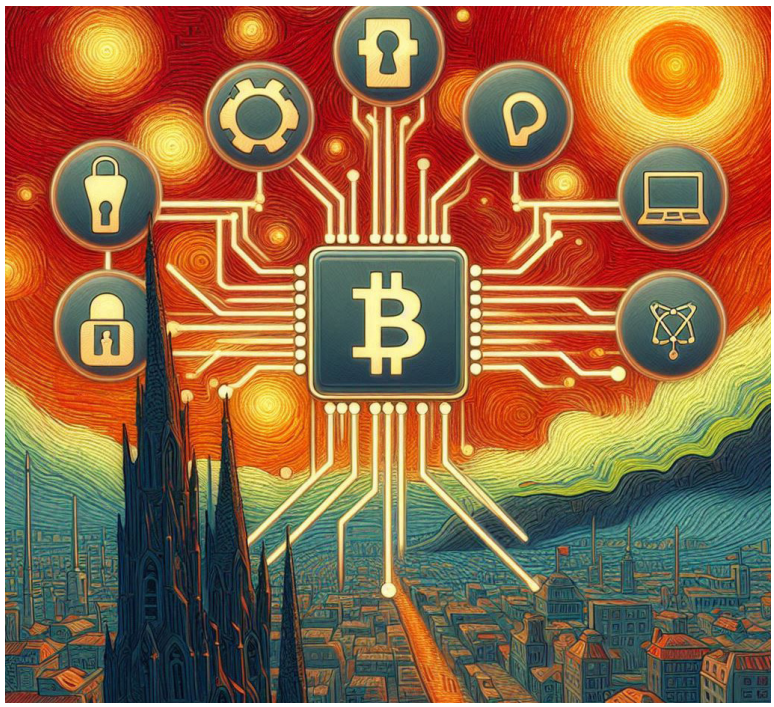
قرارداد هوشمند، نوعی برنامهٔ کامپیوتری است که روی بلاک‌چین اجرا می‌شود و برخی از وظایف اجتماعی و تجاری را به‌صورت خودکار انجام می‌دهد. این قراردادها با استفاده از یک زبان برنامه‌نویسی خاص، معمولاً Solidity برای بلاک‌چین، تعریف و اجرا می‌شوند. یکی از ویژگی‌های اساسی قراردادهای هوشمند، اجرای کارها بدون نیاز به اعتماد میان طرفین است.

قراردادهای هوشمند در حوزه‌های گوناگونی ازجمله انتقال ارزهای دیجیتال، امور مالی معاملات املاک و مستغلات و حتی اجرای NFT استفاده می‌شوند. این قراردادها به‌طور خودکار شرایط تعیین‌شده را اجرا کرده و معاملات را سریع‌تر، شفاف‌تر و بدون واسطه انجام می‌دهند. این ویژگی‌ها باعث افزایش اعتماد، کاهش احتمال خطا و افزایش کارایی در فرایندهای تجاری می‌شوند و همچنین هزینه‌های مرتبط با واسطه‌ها را کاهش می‌دهند. اطلاعات ذخیره‌شده در بلاک‌چین همچنین توکن‌های تأییدی را به‌گردش درمی‌آورد که به‌عنوان شناسه‌های منحصربه‌فرد به‌کار می‌روند و مجوز ورود به یک منبع خاص را نشان می‌دهند. این توکن‌ها تأییدی برای ارتباط و اتصال به دستگاه‌ها یا منابع موردنیاز فراهم می‌کنند. برای پیشگیری از جعل و استفادهٔ مجدد از توکن‌ها، یکپارچگی تراکنش و سازوکار تشخیصِ هزینهٔ مضاعف اِعمال می‌شود. این چهارچوب پیشنهادی، مشکلات مدیریت حجم عظیم داده‌های کنترل‌پذیر را در دستگاه‌های IoT بهبود می‌بخشد و آنها را از محدودیت‌هایی که با این موضوع مرتبط هستند، رهایی می‌بخشد.

کنترل دسترسیِ توزیع‌شده

اسکار نوو رویکرد نوینی ارائه کرده است که برای کنترل دسترسی در شبکه‌های حسگر توزیع‌شده در نقاط مختلف جغرافیایی استفاده می‌شود. در این روش، شبکه‌های حسگر بی‌سیم، گره‌های مدیر، عامل‌ها، قراردادهای هوشمند، شبکهٔ بلاک‌چین و هاب‌های مدیریتی به‌طور هماهنگ با یکدیگر عمل می‌کنند. این ایده بر ایجاد یک بستر کنترل دسترسی پویا، امن و مقیاس‌پذیر برای سیستم‌های حسگر متمرکز است که در نقاط مختلف جغرافیایی پخش شده‌اند، در نتیجه هزینه‌ها در محیط‌های پراکنده کاهش و بهره‌وری افزایش می‌یابد.

- شبکه‌های حسگر بی‌سیم گروهی هستند متشکل از تجهیزات مختلف اینترنت اشیا و



می‌توان آنها را ازطریق هاب مدیریت به سیستم بلاک‌چین متصل کرد؛

- مدیران گره‌های مدیریت، به‌عنوان گره‌های سبک شناخته می‌شوند. به این معنا که پیچیدگی کمتری درمقایسه‌با سیستم‌های سنتی دارند. این افراد مسئولیت اجرای مقررات کنترل دسترسی را بر عهده دارند و عملکرد آنها به‌دلیل سبکی بهینه‌تر و کارآمدتر است؛
- گرۀ عامل، گرۀ خاصی متعهد به تنظیم قرارداد هوشمند در شبکۀ بلاک‌چین است که در طول عمر سیستم کنترل دسترسی، مالک قرارداد هوشمند است؛
- قرارداد هوشمند قطعه‌کدی است که در شبکۀ بلاک‌چین مستقر شده و تمام عملیات مربوط به مدیریت دسترسی را تعیین می‌کند؛
- شبکۀ بلاک‌چین خصوصی به‌منظور ذخیره و مدیریت سیاست‌های مقررات پذیرش استفاده می‌شود، به این معنی که این شبکۀ مجازی امن و خودکار برای ثبت و اجرای قوانین و مقررات مربوط به پذیرش و تأیید اطلاعات استفاده می‌شود. این نوع شبکۀ بلاک‌چین معمولاً برای سازمان‌ها و شرکت‌ها مناسب است که نیاز دارند کنترل دقیقی بر قوانین و سیاست‌ها داشته باشند و درعین‌حال از امنیت بالایی برخوردار هستند که از آن برای حفظ صحت و قابلیت اعتماد داده‌ها استفاده می‌کنند.
- هاب‌های مدیریتی پیوندهایی هستند که پیام‌های پروتکل برنامۀ محدود (CoAP) را که توسط تجهیزات مبتنی‌بر اینترنت اشیا تولید شده به پیام‌های پروتکلِ فراخوانی از دورِ علامت‌گذاریِ شیءِ جاوا اسکریپت (JSONRPC) تغییر می‌دهند. این پیام‌ها توسط گره‌های بلاک‌چین تشخیص داده می‌شوند. دستگاه‌های اینترنت اشیا می‌توانند با استفاده از هاب مدیریت، درخواست دسترسی به داده‌ها را در زنجیره مسدود کنند.

برای توصیف تمام تراکنش‌های تأییدشده در سیستم پایش که موردپذیرش همگان قرار گرفته یک قرارداد هوشمند منحصربه‌فرد استفاده می‌شود. این نوع قراردادهای هوشمند توسط مدیران به‌منظور شفافیت قوانین و سیاست‌های پذیرش استفاده می‌شوند. یکی از مزایای کلیدی این رویکرد افزایش قابلیت اعتماد آن است، زیرا با استفاده از گره‌های ویژه به‌نام هاب‌های مدیریت، می‌توان چند سیستم را هم‌زمان به بلاک‌چین متصل کرد. این رویکرد به سازمان‌ها و شرکت‌ها امکان می‌دهد که قوانین و سیاست‌های خود را به‌طور مؤثر و امن در سیستم‌های مختلف اجرا کنند، همچنین قابلیت اعتماد و شفافیت را در فرایندهای پذیرش و تأیید داده‌ها بهبود می‌دهد.

هوانگ دی و همکارانش روش جدیدی برای مبادلۀ اطلاعات بین دستگاه‌های اینترنت اشیا در مناطق جغرافیایی دور از یکدیگر پیشنهاد داده‌اند. در این روش، به جای ارسالِ مستقیم درخواست دسترسی به اطلاعات به یک دستگاه خاص، درخواست دسترسی به مرکز مدیریت ارسال می‌شود. سپس مرکز مدیریت مجوز دسترسی را که در بلاک‌چین ثبت شده، بررسی و تأیید می‌کند. پس از تأیید، اطلاعات موردنظر از دستگاه مربوط به دستگاه درخواست‌کننده ارسال می‌شود.

این روش به‌ویژه برای دستگاه‌های دور از یکدیگر که نمی‌توانند مستقیماً با هم در ارتباط باشند، مناسب است. همچنین، برای دستگاه‌هایی که خط‌مشی‌های کنترل دسترسی آنها ثبت نشده است، پیشنهاد می‌شود که از سیاست‌های پویا استفاده شود. ازجمله مزایای این رویکرد، بهبود قابلیت مقیاس‌پذیری در مبادلۀ اطلاعات بین دستگاه‌هاست.

نتیجه‌گیری

در این مقاله، طرح‌های نوآورانۀ کنترل دسترسی مبتنی‌بر ویژگی با بهره‌گیری از فناوری بلاک‌چین به‌منظور بهبود مدیریت دسترسی برای میلیاردها دستگاه در اینترنت اشیا بررسی شد. این سیستم نه‌تنها میزان اعتماد و امنیت را بهبود بخشیده، بلکه با ارائۀ یک ساختار کنترل دسترسیِ غیرمتمرکز و مقیاس‌پذیر، به کاهش اعتمادناپذیری و بهبود اثربخشیِ سیستم‌های مدیریتی کمک کرده است.

در این روش، دستگاه‌های اینترنت اشیا مستقل از فرایند اجماع شبکۀ بلاک‌چین عمل می‌کنند. بدین ترتیب عملکرد بهبود می‌یابد و هزینه‌های مرتبط با محاسبات و ارتباطات کاهش پیدا می‌کند. طراحی این سیستم شامل استفاده از الگوریتم‌های پیشرفتۀ اجماع، پروتکل‌های امنیتیِ مبتنی‌بر احراز هویت، مانند AKA و ابزارهای ماژولار برای افزایش انعطاف‌پذیریِ سیستم در مواجهه با نیازهای متغیر است.

اتوماسیون و وابستگی به داده‌ها با سرعت بیشتری درحال افزایش است. با اینکه فناوری‌های متداول در این فرایند استفاده می‌شوند، مشکلاتی ازقبیل خرابی نقطه‌ای و دست‌کاری داده‌ها هنوز معضلاتی حل‌نشده برای صنعت هستند. بنابراین، فناوری بلاک‌چین به‌همراه اینترنت اشیا، محاسبات ابری، کلان‌داده و یادگیری ماشین می‌توانند به‌عنوان راهکارهایی مؤثر در حل این چالش‌ها مطرح شوند.

مراجع

- J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang (2020), "A Survey on Access Control in the Age of Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4682-4696, doi: 10.1109/JIOT.2020.2969326.
- J. Abou Jaoude and R. George Saade (2019), "Blockchain Applications – Usage in Different Domains," *IEEE Access*, vol. 7, pp. 45360-45381, doi: 10.1109/ACCESS.2019.2902501.
- H. Guo, W. Li, E. Meamari, C.-C. Shen, and M. Nejad (2020), "Attribute-based Multi-Signature and Encryption for EHR Management: A Blockchain-based Solution".
- P. Patil, M. Sangeetha, and V. Bhaskar (2021), "Blockchain for IoT Access Control, Security and Privacy: A Review," *Wireless Personal Communications*, vol. 117, no. 3, pp. 1815-1834, doi: 10.1007/s11277-020-07947-2.
- Blockchain for Access Control Systems, N. i. o. s. a. technology, 2022.
  [Online]. Available: https://csrc.nist.gov/pubs/ir/8403/final

رمزنگاری در مقابل قطعه‌بندی

نویسنده:
معصومه عباسیان

امروزه، در عصر دیجیتال، امنیت داده اهمیت بسزایی دارد. با شیوع روزافزون تهدیدهای سایبری و الزامات نظارتی سختگیرانه، سازمان‌ها باید از راهبردهای مستحکم‌تری برای محافظت از اطلاعات حساس استفاده کنند. در میان زرادخانه‌ی شیوه‌های حفاظت از داده، رمزنگاری و قطعه‌بندی دو تکنیک کلیدی برجسته هستند.

درک تفاوت بین رمزنگاری[1] و قطعه‌بندی[2] برای پیاده‌سازی کارآمد اقدامات امنیتیِ دادهٔ حیاتی است. در این مقاله، در مفاهیم رمزنگاری و قطعه‌بندی کندوکاو می‌کنیم و کارکردها و مزیت‌هایشان را بررسی می‌کنیم. با درک تفاوت‌های اساسی بین این روش‌ها، کسب‌وکارها می‌توانند برای تقویت شیوه‌های دفاعی خود از داده‌هایشانْ تصمیم‌های آگاهانه‌ای بگیرند و الزامات انطباق را با اطمینان دنبال کنند.

رمزنگاری چیست؟

رمزنگاری روشی برای ایمن‌سازی داده‌ها ازطریق تبدیل آنها به شکلی کدگذاری‌شده[3] است که فقط توسط اشخاص مجاز قابل‌گشودن باشد. اساساً، رمزنگاری شامل به‌هم ریختن داده‌های واضح و قابل‌خواندن[4] (معروف به «متن اصلی»[5]) به قالبی غیرقابل‌خواندن (معروف به متن‌رمز[6]) با استفاده از یک الگوریتم و یک کلید رمزنگاری است. این رویه تضمین می‌کند که حتی اگر شخصی به‌شکل غیرقانونی به داده‌های رمزنگاری‌شده دسترسی پیدا کند، نتواند بدون کلید رمزگشاییِ لازمْ این کار را انجام دهد.

فرایند رمزنگاری معمولاً شامل اِعمال یک الگوریتم ریاضی به متن اصلی به‌همراه کلید رمزنگاری است. الگوریتمْ متن اصلی را براساس دستورالعمل‌های کلید دست‌کاری می‌کند و آن را به متن‌رمز تبدیل می‌کند. متن‌رمزِ حاصل‌شده به‌صورت توالیِ ظاهراً تصادفی از کاراکترها ظاهر می‌شود و برای هر کسی که کلید رمزگشایی را در اختیار ندارد، قابل‌درک نیست.

رمزنگاری نقشی حیاتی در امنیت داده ایفا می‌کند و ارمغان آن محرمانگی و حفظ حریم خصوصی اطلاعات حساسْ درحین انتقال و ذخیره‌سازی است. این شیوه در بخش‌های مختلف، ازجمله امور مالی، مراقبت‌های بهداشتی، دولتی و مخابرات برای محافظت از داده‌ها از دسترسی غیرمجاز، رهگیری و دست‌کاری استفاده می‌شود.

انواع رمزنگاری

دو نوع اصلی رمزنگاری وجود دارد:

۱. رمزنگاری متقارن: در رمزنگاری متقارن، داده‌ها با همان کلیدی که رمزنگاری شده‌اند، رمزگشایی می‌شوند. دو طرف ارتباط با خیال راحت این کلید را مبادله می‌کنند. استاندارد رمزنگاری پیشرفته (AES)[7]، استاندارد رمزنگاری داده (DES)[8] و DES سه‌گانه (3DES) نمونه‌هایی از روش‌های رمزنگاری متقارن هستند

۲. رمزنگاری نامتقارن: بدیلی است برای رمزنگاری با استفاده از کلید عمومی[9] که از دو کلید برای رمزنگاری استفاده می‌کند: یک «کلید خصوصی»[10] برای رمزگشایی و یک کلید عمومی برای رمزنگاری. کلید خصوصی پنهان می‌ماند، درحالی‌که، کلید عمومی بدون محدودیت به‌اشتراک گذاشته می‌شود. RSA (Rivest–Shamir–Adleman) و رمزنگاری مبتنی‌بر خم بیضوی (ECC)[11] دو نمونه از تکنیک‌های رمزنگاری نامتقارن هستند.

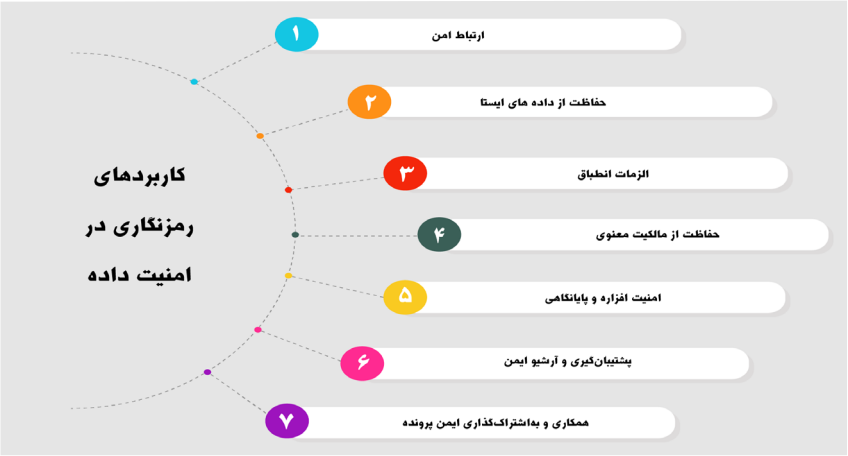
1. Encryption
2. Tokenization
3. Encoded
4. Readable
5. Plaintext
6. Ciphertext
7. Advanced Encryption Standard
8. Data Encryption Standard
9. public-key
10. private key
11. Elliptic Curve Cryptography

فرایند رمزگشایی

گیرندهٔ کلید رمزگشایی و الگوریتم رمزگشایی را روی متن‌رمز اعمال می‌کند و فرایند رمزنگاری را معکوس می‌کند. این الگوریتمْ تبدیل‌های اعمال‌شده در طول رمزنگاری را معکوس می‌کند و متن‌رمز به متن اصلی تبدیل می‌شود.

خروجی

متن اصلیِ رمزگشایی‌شده به‌دست می‌آید و داده‌های اصلی و قابل‌خواندن آشکار می‌شوند. حالا گیرنده می‌تواند متن اصلی را پردازش کند، نمایش بدهد یا از آن استفاده کند.



کاربردهای رمزنگاری در امنیت داده

۱. ارتباط امن

رمزنگاریْ محرمانگیِ اطلاعاتِ حساسِ منتقل‌شده ازطریق شبکه‌هایی نظیر ایمیل، «پیام فوری»[۱۲] و تراکنش آنلاین را تضمین می‌کند. پروتکل‌های ایمن مانند SSL/TLS از رمزنگاری برای ایجاد ارتباطات امن بین کلاینت‌ها و سرورها استفاده می‌کنند و از استراق سمع و رهگیری داده‌ها جلوگیری می‌کنند. «شبکه‌های خصوصی مجازی» (VPN)[۱۳] از رمزنگاری برای ایجاد تونل‌های امن روی شبکه‌های عمومی استفاده می‌کنند که دسترسی و ارتباط از دورِ ایمن را ممکن می‌سازد.

۲. حفاظت از «داده‌های ایستا»[۱۴]

رمزنگاریْ از داده‌های ذخیره‌شده در افزاره‌ها، پایگاه‌های داده و فضای ذخیره‌سازی ابری در برابر دسترسی غیرمجاز، سرقت یا نقض داده محافظت می‌کند. «رمزنگاری فول دیسک»[۱۵]، کل دستگاه‌های ذخیره‌سازی، مانند دیسک سخت یا «دیسک حالت جامد» (SSD)[۱۶] را رمزنگاری می‌کند و تضمین می‌کند که تمام داده‌های روی دستگاه محافظت می‌شوند. «رمزنگاری در سطح پرونده»[۱۷] به‌طور انتخابی پرونده‌ها یا دایرکتوری‌ها را رمزنگاری می‌کند و امکان کنترل دقیق بر حفاظت از داده‌ها را فراهم می‌کند.

۳. الزامات انطباق

رمزنگاری توسط استانداردها و مقررات انطباق مختلف، مانند «قانون انتقال‌پذیری و حساب‌دهی بیمهٔ سلامت» (HIPAA)[۱۸]، «استاندارد امنیت دادهٔ صنعت کارت پرداخت» (PCI DSS)[۱۹] و «مقررات حفاظت از داده‌های عمومی» (GDPR)[۲۰] الزامی است. پیروی از این مقررات غالباً به اجرای اقدامات رمزنگاری برای محافظت از اطلاعات حساس، ازجمله «اطلاعات سلامت شخصی» (PHI)[۲۱]، داده‌های مالی و «اطلاعات هویتی قابل‌ردیابی» (PII)[۲۲] نیاز دارد.

٤. حفاظت از مالکیت معنوی

رمزنگاری از مالکیت معنوی و اسرار تجاریِ ذخیره‌شده در قالب‌های دیجیتال در برابر دسترسیِ غیرمجاز، افشا یا سرقت محافظت می‌کند. فناوری‌ها، صنایع دارویی و رسانه برای محافظت از اطلاعاتِ تحت مالکیت خود، داده‌های پژوهشی و دارایی‌های ارزشمند، به رمزنگاری متکی هستند.

۵. امنیت افزاره و پایانگاهی[۲۳]

رمزنگاری داده‌های ذخیره‌شده روی افزاره‌ها و پایانگاه‌ها نظیر تلفن همراه و لپ‌تاپ را ایمن می‌کند و از دسترسی غیرمجاز به آنها در صورت گم‌شدن یا سرقت جلوگیری می‌کند. راهکارهای «مدیریت تلفن همراه» (MDM)[۲۴] غالباً شامل ویژگی‌های رمزنگاری برای محافظت از داده‌های شرکت در دستگاه‌های متعلق به کارمندان است.

٦. پشتیبان‌گیری و آرشیو ایمن

رمزنگاریْ محرمانگی و یکپارچگیِ پشتیبان‌گیری و بایگانی داده‌هایی را که به‌صورت محلی یا در فضای ابری ذخیره می‌شوند، تضمین می‌کند. راهکارهای پشتیبان‌گیری غالباً شامل رمزنگاری برای محافظت از داده‌های حساس در حین انتقال و ذخیره‌سازی است و خطر نقض داده‌ها یا دسترسی غیرمجاز را کاهش می‌دهد.

۷. همکاری و به‌اشتراک‌گذاری ایمن پرونده

رمزنگاریْ همکاری و به‌اشتراک‌گذاری ایمنِ پرونده را میان افراد یا سازمان‌ها امکان‌پذیر می‌کند و تضمین می‌کند که داده‌های مشترک از دسترسی غیرمجاز محافظت شوند. خدمات اشتراک‌گذاری پروندهٔ رمزنگاری‌شده و بسترکارهای[۲۵] همکاری، داده‌ها را هم در حین انتقال و هم در حالت ایستا رمزنگاری می‌کنند تا از محرمانگی و حریم خصوصیِ آنها محافظت کنند.

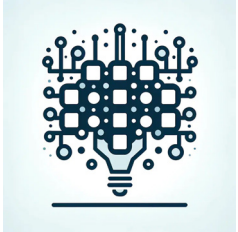
قطعه‌بندی چیست؟

قطعه‌بندی یک تکنیک امنیت داده است که داده‌های

۱۲. Instant message؛ پیامی که به‌سرعت بین دو یا چند نفرِ متصل به یک شبکه ازطریق حروف‌نگاری ردوبدل شود.
13. Virtual Private Networks
14. Data-at-Rest
15. Full-disk encryption
16. Solid-state drive
17. File-level encryption

۱۸. Health Insurance Portability and Accountability Act؛ ۵ عنوان دارد که با هدف بهبود نظام بیمه در حوزه‌هایی ازجمله دسترس‌پذیری، حریم خصوصی، امور مالیاتی، بیمه‌های گروهی و غیره تدوین شده است.
19. Payment Card Industry Data Security Standard
20. General Data Protection Regulation
21. Personal Health Information
22. Personally Identifiable Informationn
23. Endpoint

24. Mobile Device Management
25. Platforms



حساس را با «مقادیر مکان‌نمای غیرحساس»[۲۶] که توکن نامیده می‌شوند، جایگزین می‌کند. برخلاف رمزنگاری که داده‌ها را به قالبی غیرقابل‌خواندن تبدیل می‌کند، قطعه‌بندی داده‌های اصلی را با توکن جایگزین می‌کند که معمولاً رشته‌ای از کاراکترهاست که تصادفاً تولید شده‌اند. توکن هیچ معنا یا ارزش ذاتی ندارد و نمی‌توان آن را از نظر ریاضی معکوس کرد تا داده‌های اصلی را آشکار کند. قطعه‌بندی به‌طور گسترده در پردازش پرداخت، مراقبت‌های بهداشتی و سایر صنایع برای محافظت از اطلاعات حساس در عین حفظ قابلیت استفاده می‌شود.

انواع قطعه‌بندی

چهار نوع قطعه‌بندی به‌شرح ادامه وجود دارد:

- **«قطعه‌بندی کارت اعتباری»[۲۷]:** در قطعه‌بندی کارت اعتباری، شماره‌های حساس کارت اعتباری با توکن جایگزین می‌شوند و به بازرگانان و پردازشگرهای پرداخت اجازه می‌دهند تا تراکنش‌ها را به‌طور ایمن ذخیره و پردازش کنند، بدون اینکه داده‌های صاحب کارت افشا شود. توکن‌ها توسط یک خدمت یا بسترکار تولید و مدیریت می‌شوند که به‌طور ایمن توکن‌ها را به شمارهٔ کارت اعتباری مربوطه در انباری از توکن‌ها نگاشت می‌کند. داده‌های کارت اعتباری قطعه‌بندی‌شده را می‌توان برای پرداخت‌های مکرر، کشف کلاهبرداری و سایر تراکنش‌ها بدون نیاز به دسترسی به شمارهٔ کارت اعتباریِ اصلی استفاده کرد.
- **قطعه‌بندی داده‌ها:** قطعه‌بندی داده‌ها از کاربری در حوزهٔ شمارهٔ کارت اعتباری فراتر رفته است و از انواع دیگر داده‌های حساس مانند شمارهٔ ملی، شماره‌حساب بانکی و PII، محافظت می‌کند. مانند استفاده‌ای که از توکن در کارت‌های اعتباری می‌شود، در اینجا هم توکن‌ها جایگزینِ داده‌های حساس می‌شوند با این تضمین که داده‌های اصلی از دسترسیِ غیرمجاز یا افشا محافظت شوند. در قطعه‌بندی این امکان وجود دارد که توکن‌های مربوط به داده‌های خاصی براساس الزامات و استانداردهای انطباق خاص یک سازمان سفارشی‌سازی شوند.
- **قطعه‌بندی ایمیل:** در این نوع قطعه‌بندی، آدرس‌های ایمیل با توکن‌های یکتا جایگزین می‌شوند. بدین ترتیب سازمان‌ها می‌توانند با مشتریان و کاربران، بدون افشای آدرس ایمیل آنها، ارتباط برقرار کنند. قطعه‌بندی ایمیل به محافظت از حریم خصوصی کاربر و کاهش ریسک هرزنامه‌های مرتبط با ایمیل، فیشینگ، و نقض داده‌ها کمک می‌کند.
- **قطعه‌بندی برای احراز هویت:** در اینجا توکن‌ها به‌عنوان اعتبار موقت یا توکن‌های دسترسی عمل می‌کنند. توکن‌های دسترسی برای احراز هویت کاربران و اعطای دسترسی به منابع یا خدمات ایمن مانند APIها، برنامه‌های کاربردی وب و خدمت‌های ابری استفاده می‌شوند. این دسته از توکن‌ها معمولاً به‌خاطر کاهش ریسک خطر دسترسی غیرمجاز یا سوءاستفاده، محدودیت زمانی دارند و دامنهٔ کاربرد آنها محدود است.

قطعه‌بندی چگونه کار می‌کند؟

گام اول: جمع‌آوری داده

ابتدا داده‌های حساس نظیر شمارهٔ کارت اعتباری، شمارهٔ ملی و سایر PIIها از کاربران یا سامانه‌ها جمع‌آوری می‌شود.

گام دوم: فرایند قطعه‌بندی

داده‌های حساس تحت فرایند قطعه‌بندی با توکن‌هایی که تصادفاً تولید شده‌اند جایگزین می‌شوند. قطعه‌بندی می‌تواند ازطریق نرم‌افزار یا خدمتی انجام شود که نگاشت داده‌های اصلی به توکن‌ها را به‌صورت ایمن مدیریت کند.

گام سوم: تولید توکن

توکن‌ها معمولاً رشته‌هایی شامل حرف و عدد هستند که با استفاده از روش‌های رمزنگاری تولید می‌شوند. این توکن‌ها هیچ معنا یا ارزش ذاتی ندارند و تصادفاً برای هر دادهٔ حساس تولید می‌شوند.

گام چهارم: نگاشت توکن

توکن‌ها و داده‌های اصلیِ اولیهٔ مربوطه به شکلی ایمن در انبار یا پایگاه‌دادهٔ توکن ذخیره می‌شوند. این نگاشت به کاربران مجاز اجازه می‌دهد تا در صورت نیاز داده‌های اصلی مرتبط با یک توکن را بازیابی کنند.

گام پنجم: استفاده از داده‌های جایگزین‌شده با توکن

توکن‌ها را می‌توان به‌جای داده‌های حساس اصلی برای اهداف مختلفی مانند پردازش پرداخت، تأیید هویت یا ذخیره‌سازی، بدون افشای اطلاعات حساسْ منتقل و ذخیره کرد. بدین ترتیب ریسک افشا یا سرقت داده‌ها کمینه می‌شود.

گام ششم: بازیابی توکن

کاربران مجاز می‌توانند داده‌های اصلی مرتبط با یک توکن را در صورت نیاز برای اهداف قانونی، مانند پردازش تراکنش یا تأیید مشتری از انبار توکن بازیابی کنند. دسترسی به انبار توکن به‌شدت کنترل می‌شود تا اطمینان حاصل شود که فقط کارکنان مجاز می‌توانند به داده‌های حساس دسترسی داشته باشند.

کاربردهای قطعه‌بندی در امنیت داده

قطعه‌بندی با ایمن‌کردن داده‌های حساس ازطریق جایگزین‌کردن توکن‌های غیرحساس، کاربرد گسترده‌ای در امور مالی، مراقبت‌های سلامت و تجارت الکترونیک دارد و تضمین می‌کند که حریم خصوصی داده‌ها حفظ شود و استانداردهای نظارتی استقرار یابد.

- **پردازش پرداخت:** قطعه‌بندی به‌طور گسترده در امور مربوط به پرداخت وجه به‌منظور ایمن‌کردن تراکنش‌های کارت اعتباری استفاده می‌شود. شماره‌های کارت اعتباری برای جلوگیری از افشای داده‌های دارندهٔ کارت در حین پرداخت، برای کاهش ریسک کلاهبرداری و نقض داده‌ها قطعه‌بندی‌می‌شوند.
- **حفاظت از داده‌های مراقبت‌های بهداشتی:** در بخش مراقبت‌های بهداشتی، قطعه‌بندی در حفاظت از «پرونده‌های الکترونیکی سلامت» (EHR)[۲۸] و سایر اطلاعات حساس بیمار استفاده می‌شود. شناسه‌های بیمار مانند شمارهٔ ملی و شمارهٔ پروندهٔ پزشکی، برای مطابقت با مقررات مراقبت‌های سلامت (مانند HIPAA) و حفظ حریم خصوصی بیمار با توکن جایگزین می‌شوند.
- **ذخیره‌سازی داده و خدمات ابری:** قطعه‌بندی به امنیت داده‌های ذخیره‌شده در پایگاه داده، ذخیره‌سازی ابری و سایر شیوه‌های ذخیره‌سازی کمک می‌کند. می‌توان داده‌های حساسی نظیر PII و سوابق مالی را برای کاهش

26. Non-sensitive placeholder values
27. Credit Card Tokenization
28. Electronic Health Records

ریسکِ دسترسیِ غیرمجاز یا نقض داده با توکن جایگزین کرد.

- **مدیریت هویت و دسترسی:** قطعه‌بندی در سیستم‌های «مدیریت هویت و دسترسی» (IAM)[29] برای احراز هویت کاربران و مدیریت دسترسی به منابع ایمن استفاده می‌شود. توکن‌های دسترسی برای اعطای دسترسی موقت به برنامه‌ها، APIها و خدمات برخط و به‌منظور کاهش وابستگی به گذرواژه‌های سنتی و افزایش امنیت تولید می‌شوند.
- **تجارت الکترونیک:** قطعه‌بندی در تجارت الکترونیک برای ایمن‌کردن اطلاعات پرداخت مشتری و ساده‌سازی فرایندهای پرداخت استفاده می‌شود. داده‌های پرداختی که با توکن جایگزین شده‌اند برای بازرگانان این امکان را فراهم می‌کنند تا تراکنش‌ها را بدون ذخیرهٔ اطلاعات حساس کارت اعتباری، به‌طور ایمن پردازش کنند. این کار علاوه بر جلب اعتماد مشتری با استاندارد PCI DSS مطابقت دارد.

تمایزهای اصلی میان رمزنگاری و قطعه‌بندی

قبل از پرداختن به مقایسه‌های دقیق، درک تفاوت‌های اساسی میان رمزنگاری و قطعه‌بندی ضروری است. درحالی‌که هدف هر دو تکنیک حفاظت از داده‌های حساس است، اما از نظر برگشت‌پذیری[30]، عملکرد، مقیاس‌پذیری[31] و ملاحظات انطباق با مقررات متفاوت هستند. مقایسهٔ این دو تکنیک در جدول ۱ آمده است.

نتیجه‌گیری

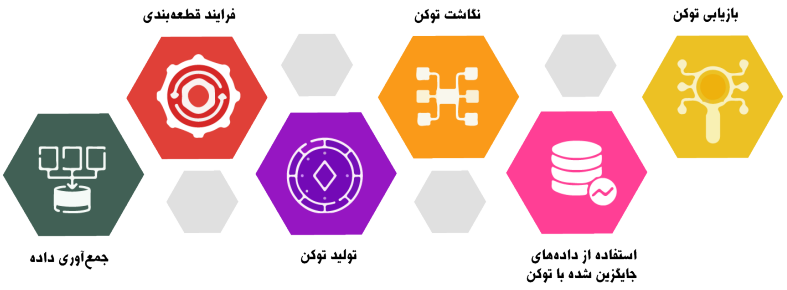
درک تفاوت‌های ظریف بین رمزنگاری و قطعه‌بندی برای سازمان‌هایی که به‌دنبال تقویت اقدامات امنیت داده‌ای خود هستند، ضروری است. درحالی‌که هر دو تکنیک راهکارهای قوی برای حفاظت از اطلاعات حساس هستند، اما از نظر هدف، برگشت‌پذیری، عملکرد و پیامدهای نظارتی متمایزند. قطعه‌بندی با جایگزینی داده‌های حساس با توکن‌های غیرحساس، رویکردی عمل‌گرایانه ارائه می‌کند و امنیت داده‌ها را بدون به خطر انداختن قابلیت استفاده تضمین می‌کند. از سوی دیگر، رمزنگاری روشی برگشت‌پذیر برای تبدیل داده‌ها به قالبی غیرقابل‌خواندن ارائه می‌دهد و ضمن حفظ ساختار داده‌های اصلی، از محرمانگی آنها محافظت می‌کند. با شناخت نقاط قوت و محدودیت‌های هر رویکرد، سازمان‌ها می‌توانند متناسب با الزامات امنیتیِ خاص، تعهدات انطباقی و نیازهایِ عملیاتی خود آگاهانه تصمیم بگیرند که از چه روشی استفاده کنند.

29. Identity and Access Management
30. Reversibility
31. Scalability

منابع

- https://shorturl.at/cevLN
- https://www.tokenex.com/blog/tokenization-vs-encryption/
- https://shorturl.at/atJU۴

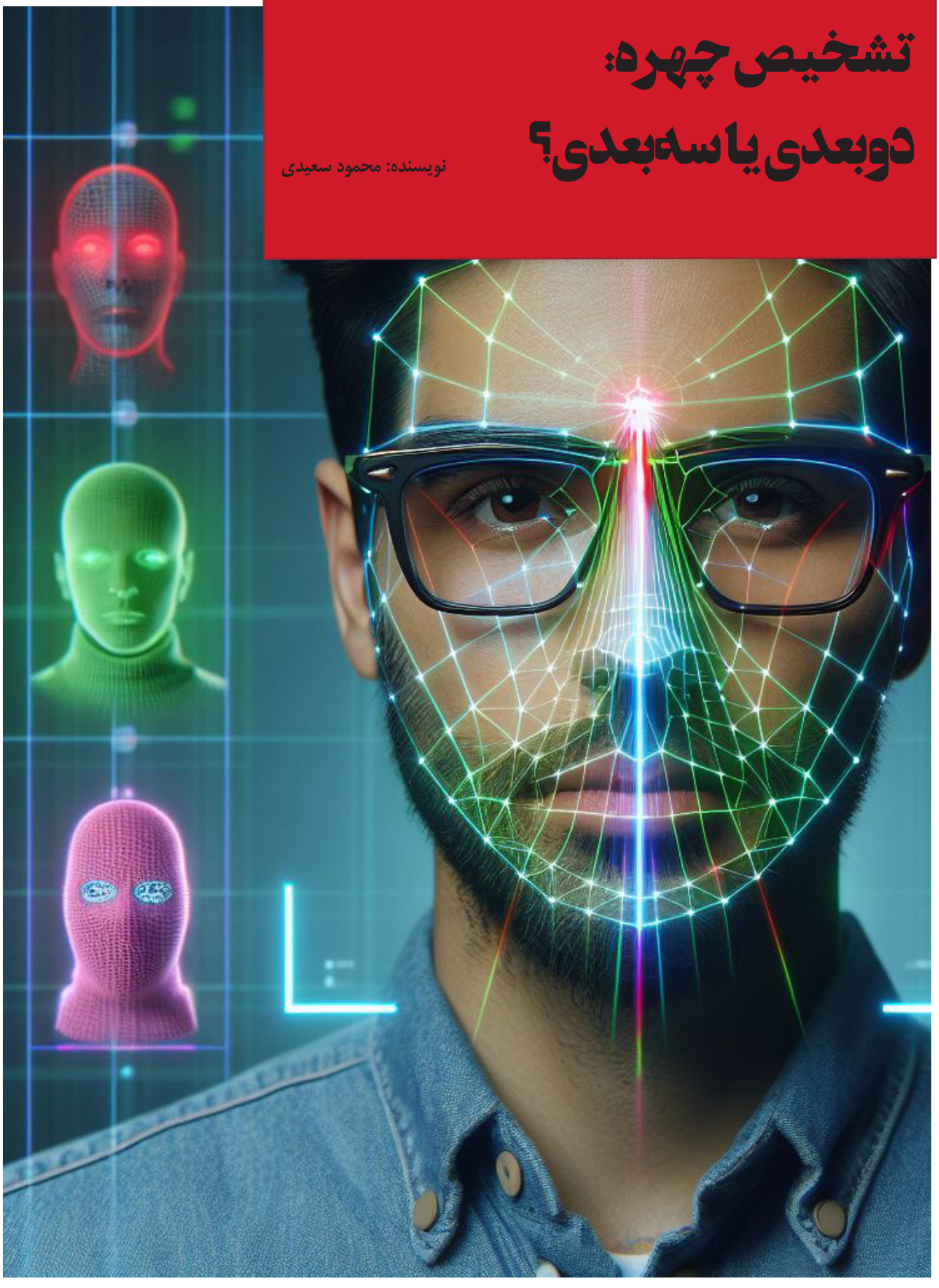
جدول ۱	رمزنگاری	قطعه‌بندی
هدف و کارکرد	– رمزنگاری داده‌ها را به قالبی غیرقابل‌خواندن بدل می‌کند اما ساختار اصلی داده را حفظ می‌کند. رمزنگاری از محرمانگیِ داده‌ها محافظت می‌کند. – در رمزنگاریْ داده‌ها دگرگون می‌شوند.	– قطعه‌بندی داده‌های حساس را با توکن‌های غیرحساس جایگزین می‌کند و ضمن حفظ قابلیت استفاده، امنیت داده‌ها را تضمین می‌کند. – در قطعه‌بندی داده‌ها با توکن جایگزین می‌شوند.
برگشت‌پذیری	رمزنگاری برگشت‌پذیر است. به عبارت دیگر می‌توان داده‌های رمزنگاری‌شده را با استفاده از کلید رمزگشایی به شکل اصلی خود بازگرداند. ماهیت برگشت‌پذیریِ رمزنگاریْ انتقال و ذخیرهٔ ایمن داده‌ها را تسهیل می‌کند و در عین حال تضمین می‌کند که اشخاص مجاز می‌توانند به اطلاعات دسترسی پیدا کرده و آنها را تفسیر کنند.	قطعه‌بندی برگشت‌ناپذیر است، به این معنی که نمی‌توان توکن‌ها را از نظر ریاضی برای به‌دست‌آوردن داده‌های اصلی معکوس کرد. حتی با دانستن الگوریتم قطعه‌بندی و مقادیر توکن، معکوس کردن فرایند و بازیابی داده‌های اصلی عملاً غیرممکن است.
عملکرد و مقیاس‌پذیری	فرایندهای رمزنگاری ممکن است بار محاسباتی زیادی داشته باشند، به‌خصوص وقتی حجم داده زیاد باشد، ممکن است عملکرد سیستم تحت تأثیر قرار بگیرد.	قطعه‌بندی معمولاً عملکرد سریع‌تری دارد، زیرا شامل جایگزینی سادهٔ داده‌ها با توکن‌هاست که بار محاسباتی کمتری دارد. علاوه بر این، قطعه‌بندی ذاتاً مقیاس‌پذیرتر از رمزنگاری است و آن را برای محیط‌هایی با حجم دادهٔ بالا مناسب می‌سازد. سیستم‌های تولیدکنندهٔ توکن به‌راحتی می‌توانند تعداد زیادی توکن را بدون کاهش قابل‌توجهِ عملکردْ تولید، ذخیره‌سازی و بازیابی کنند.
ملاحظات انطباق با مقررات	بسته به محیط نظارتی و مقررات خاص هر صنعت، سازمان‌ها ممکن است برای انجام تعهدات انطباقی و محافظت مؤثر از اطلاعات حساس، قطعه‌بندی، رمزنگاری یا ترکیبی از هر دو را پیاده‌سازی کنند.	

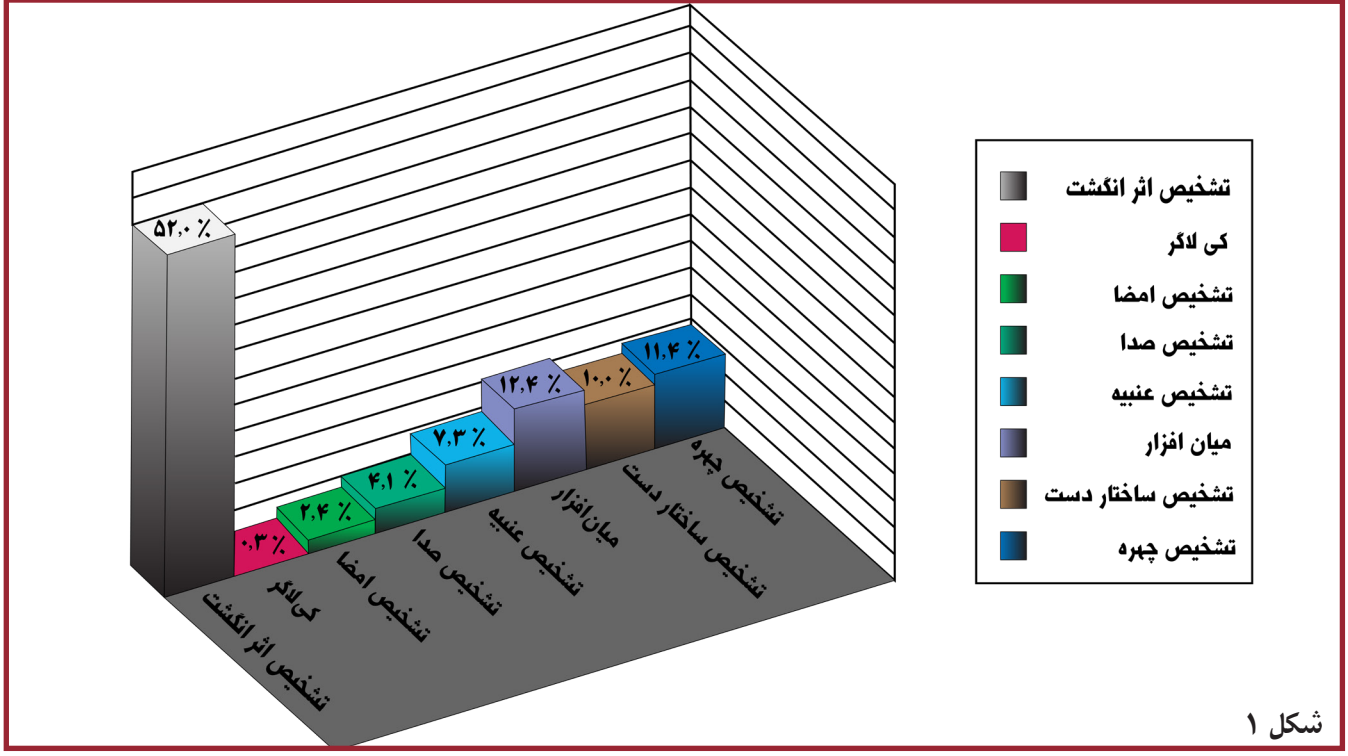


در شکل بالا مراحل قطعه‌بندی نشان داده شده است (از چپ به راست).

تشخیص چهره: دوبعدی یا سه‌بعدی؟

نویسنده: محمود سعیدی





شکل ۱

مفهوم تشخیص چهره

تشخیص چهره روشی برای تعیین یا تصدیق هویت افراد با استفاده از چهرهٔ آنهاست. سامانه‌های تشخیص چهره را می‌توان برای شناسایی افراد در تصاویر، ویدئوها یا درلحظه به‌منظور برقراری امنیت و اجرای قانون به‌کار برد. تشخیص چهره در کنار تشخیص صدا، تشخیص اثر انگشت و تشخیص عنبیهٔ چشم در دستهٔ امنیت بیومتریک قرار می‌گیرند. از میان شیوه‌های یادشده، تشخیص چهره طبیعی‌ترین آنهاست؛ چراکه انسان خود و دیگران را با نگریستن به چهرهٔ خود یا دیگران می‌شناسد نه با دیدن اثر انگشت و عنبیهٔ آنها. در حال حاضر، بیش از نیمی از جمعیت جهان مرتباً در معرض فناوری تشخیص چهره قرار می‌گیرند.

تشخیص چهره: محبوب‌ترین معیار احراز هویت

بسیاری از رویدادهای ناگوار مانند حمله‌های تروریستیْ سازمان‌های دولتی و خصوصی را بر آن داشته است که انگیزهٔ بیشتری برای رفع نقاط ضعف و بهبود سامانه‌های نظارتی و امنیتی خود داشته باشند. بهبود این سامانه‌ها براساس ویژگی‌های بدنی یا رفتاری که اغلب بیومتریک نامیده می‌شوند انجام شده است. این فناوریِ بسیار جذاب می‌تواند با برنامه‌های امنیتی و کنترل دسترسی ادغام شود.

شاید شناسایی اثر انگشت و عنبیه از رایج‌ترین روش‌های بیومتریک باشند، اما بسیاری از ویژگی‌های دیگرِ انسانی مانند هندسهٔ اثر انگشت یا کف دست، صدا، امضا و چهره نیز موردتوجه فناورهای بیومتریک قرار گرفته‌اند. شکل ۱ میزان به‌کارگیری محبوب‌ترین بیومتریک‌ها را در سال‌های گذشته از دیدگاه تجاری نشان می‌دهد. با این حال هریک از روش‌های مبتنی‌بر بیومتریک اشکالاتی دارند. مثلاً، تشخیص عنبیه بسیار دقیق است ولی علاوه بر اینکه پیاده‌سازی آن پرهزینه است، چندان از سوی مردم موردپذیرش واقع نشده است. فناوری اثر انگشت قابل‌اعتماد بوده و مزاحمتی برای افراد ایجاد نمی‌کند، ولی برای ارباب رجوع در یک سازمان یا شرکت مناسب نیست.

درمقابل به‌نظر می‌رسد که تشخیص چهره، سازگاریِ مناسبی میان قابلیت اطمینان[1] و پذیرش اجتماعی[2] ایجاد کرده است. همچنین این روش در توازن امنیت و حریم خصوصی عملکرد قابل‌قبولی دارد. گرچه سامانه‌های مبتنی‌بر تشخیص چهره، گاهی حقوق مدنی افراد را، مثلاً در موارد مثبت کاذب تهدید می‌کنند، ولی بسیاری از برنامه‌های تجاری و امنیتی نیاز دارند از فناوری‌های تشخیص چهره استفاده کنند.

سامانه‌های تشخیص چهره به دو دسته تقسیم می‌شوند: تصدیق[3] و شناسایی[4]. در واقع، تصدیق چهره نوعی تطبیق چهره است که در آن تصویر چهره با الگوهای تصاویر چهره مقایسه می‌شود. در عملیات شناسایی، تصویر چهرهٔ موردنظر با تمام الگوهای تصویر در پایگاه دادهٔ چهره‌ها مقایسه می‌شود تا هویت چهرهٔ موردنظر تعیین شود. در دههٔ گذشته، تشخیص چهره پیشرفت زیادی کرده است، طوری که بسیاری از سامانه‌ها به نرخ‌های تشخیص بیش از ۹۰٪ دست یافته‌اند.

گام‌های تشخیص چهره

۱. **آشکارسازی[5]:** منظور شناسایی چهره یا چهره‌ها در تصویر صرف‌نظر از هویت افراد است. در واقع، آنچه در گام اول انجام می‌شود این است که چهرهٔ فرد یا افراد در یک جمعیت، آشکار و مکان‌یابی می‌شود.

۲. **تحلیل:** در این گام چهرهٔ آشکارسازی‌شدهٔ فرد، هدف تحلیل قرار می‌گیرد. در بیشتر فناوری‌های مرتبط با تشخیص چهره، به‌جای استفاده از تصاویر سه‌بعدی، از تصاویر دوبعدی برای تشخیص چهره استفاده می‌شود؛ چراکه با استفاده از تصاویر دوبعدی به‌سادگی می‌توان یک تصویر دوبعدی را با تصاویر عمومی یا تصاویر موجود در پایگاه‌داده

1. Reliability
2. Social acceptance
3. Verification
4. Identification
5. Detection



شکل ۲: نمایش داده‌ها در مدل‌سازی سه‌بعدی چهره از راست به چپ: تصویر سه‌بعدی مطابق با ساختار آناتومیک داخلی، ۲٫۵بعدی و دوبعدی از چهره.

تطبیق داد. معیارهای اصلی برای تطبیق تصاویر شامل فاصلهٔ بین چشم‌ها، عمق حدقه‌های چشم، فاصلهٔ پیشانی تا چانه، شکل استخوان‌های گونه و شکل لب‌ها، گوش‌ها و چانه است.

۳. **تبدیل تصویر به داده:** فرایند ضبط چهره، اطلاعات آنالوگ چهره را به مجموعه‌ای از اطلاعات دیجیتال براساس ویژگی‌های چهرهٔ فرد تبدیل می‌کند. بدین ترتیب تجزیه‌وتحلیل چهره اساساً به روابط یا فرمول‌های ریاضی تبدیل می‌شود. در واقع همان‌طور که اثر انگشت منحصربه‌فرد است، «اثر چهرهٔ»[6] هر فرد نیز مخصوص به خودش است.

۴. **تطبیق[7] اثر چهره:** در مرحلهٔ تطبیق، اثر چهره با چهره‌های موجود در پایگاه داده مقایسه می‌شود. در صورتی که، اثر چهره با یکی از تصاویر موجود در پایگاه داده تطابق داشته باشد، آنگاه تصمیم‌گیری‌های بعدی انجام می‌شود.

عوامل مؤثر بر کارایی سامانه‌های تشخیص چهرهٔ دوبعدی

- با توجه به خاصیت بازتاب نور توسط پوست، تغییرات شدت روشنایی روش‌های تشخیص دوبعدی چهره را به‌چالش می‌کشد و روی دقت تشخیص چهره تأثیر می‌گذارد؛
- تغییر حالت چهره نیز از عواملی است که بر احراز هویت شخص تأثیر می‌گذارد. تغییراتی مثل اینکه فرد داخل تصویر بخندد یا اخم کند یا طوری جلوی دوربین قرار بگیرد که بخشی از چهره‌اش در تصویر دیده نشود.

نتایج ارزیابی الگوریتم‌های تشخیص چهرهٔ مبتنی‌بر پردازش تصاویر دوبعدی نشان می‌دهد که در شرایط کنترل‌شده دقت تشخیص بیش از ۹۰٪ است. در غیر این صورت کارایی الگوریتم‌های دوبعدی تشخیص چهره کاهش می‌یابد.

مزایای تشخیص چهرهٔ سه‌بعدی نسبت به تشخیص چهرهٔ دوبعدی

در الگوریتم‌های تشخیص چهرهٔ سه‌بعدی، از مدل‌های هندسی سه‌بعدی چهرهٔ انسان به‌منظور تشخیص چهره استفاده می‌شود. در این الگوریتم‌ها شکل چهره و شکل سر به‌صورت مش‌های چندظلعی نشان داده می‌شوند. پژوهش‌ها نشان می‌دهند که دقت تشخیص چهره در الگوریتم‌های سه‌بعدی به‌مراتب از دقت آن در الگوریتم‌های دوبعدی بیشتر است. یکی از مهم‌ترین دلایل برتری دقت روش تشخیص چهرهٔ سه‌بعدی به روش دوبعدی، قابلیت تشخیص الگو در روش سه‌بعدی است. همچنین، همان‌طور که پیش از این اشاره شد، الگوریتم‌های تشخیص چهرهٔ دوبعدی در برابر عواملی مانند تغییر در شدت روشنایی زمینه، آرایش چهره و جهت چهرهٔ فرد درمقابل دوربین با چالش مواجه می‌شوند، درحالی‌که الگوریتم‌های تشخیص چهرهٔ سه‌بعدی در برابر تغییرات شدت روشنایی، چرخش و مقیاس‌بندی مقاوم هستند. از دیگر قابلیت‌های الگوریتم‌های تشخیص چهرهٔ سه‌بعدی، قابلیت استخراج ویژگی‌های مرتبط با عمق چهره و تحلیل آن است.

مزیت اصلی الگوریتم‌های تشخیص چهرهٔ سه‌بعدی این است که تمام اطلاعات مربوط به هندسهٔ چهره در آن حفظ می‌شود. در واقع، در مدل سه‌بعدی چهره، ویژگی‌های چهره با انحناهای محلی و سراسری نشان داده می‌شوند که می‌تواند به‌عنوان امضای واقعی افراد در نظر گرفته شود.

نمایش داده‌ها در مدل‌سازی سه‌بعدی چهره

دو روش اصلی برای نمایش داده‌ها در مدل‌سازی ۳بعدی چهره، استفاده از تصاویر به‌اصطلاح ۲٫۵بعدی و ۳بعدی است. یک تصویر ۲٫۵بعدی از نمایش ۲بعدی مجموعه‌نقاط ۳بعدی تشکیل شده است که در آن هر پیکسل نشان‌دهندهٔ مقدار عمق z هم هست. مثلاً در تصویر ۲٫۵بعدی در مقیاس خاکستری پیکسل سیاه نشان‌دهندهٔ بیشترین فاصله از دوربین (زمینه) و پیکسل سفید نشان‌دهندهٔ نزدیک‌ترین نقطه به دوربین است. در تصاویر ۳بعدی، نمایشی سراسری از کل سر و سطح چهره مطابق با ساختار آناتومیک داخلی حاصل می‌شود. در شکل ۲ نمونه‌ای از نمایش چهره مطابق با ساختار آناتومیک داخلی، ۲٫۵بعدی و ۲بعدی نشان داده شده است. نمایش ۳بعدی چهره در ساده‌ترین شکل آن، یک شبکه یا مش چندضلعیِ ۳بعدی است که شامل رأس‌هایی است که توسط چندضلعی‌هایی به‌هم متصل شده‌اند. دو نمونهٔ متفاوت از نمایش ۳بعدی چهره با استفاده از شبکه یا مش چندضلعیِ ۳بعدی در شکل ۳ نشان داده شده است. روش‌های زیادی برای ساخت مش ۳بعدی وجود دارد؛ ازجمله ترکیب چندین تصویر ۲٫۵بعدی، تنظیم صحیح یک «مدل شکل‌پذیر سه‌بعدی»[8] یا به‌کارگیری یک سامانهٔ یادگیری سه‌بعدی با استفاده از اسکنر سه‌بعدی.

6. Faceprint
7. Matching
8. 3D morphable model

رویکردهای تولید مدل سه‌بعدی از چهره

تکنیک مبتنی‌بر تشخیص چهرهٔ سه‌بعدی ویژگی‌هایی دارد نظیر مقاومت در برابر تغییرات نور، تغییرات موقعیت، چرخش و مقیاس‌بندی در مدل اصلی. متأسفانه تکنیک ۳DFR به تمام این اهداف به‌طور کامل دست نمی‌یابد. با این حال، استفاده از داده‌های سه‌بعدی می‌تواند بهبودهایی را در رابطه با تصاویر دوبعدی ایجاد کند و مقاومت در برابر تغییر زاویهٔ دوربین نسبت به چهره و تغییرات روشنایی را افزایش دهد که نتیجهٔ آن توصیف مناسب ویژگی‌ها و افزایش دقت الگوریتم‌های سه‌بعدی چهره خواهد بود.

برای تولید مدل سه‌بعدی از یک چهره دو رویکرد وجود دارد که رویکرد اول مبتنی‌بر جمع‌آوری داده‌های سه‌بعدی چهره با استفاده از اسکنر سه‌بعدی است و رویکرد دوم مبتنی‌بر تطبیق یک مدل کلی چهره با تصویر داده‌شده از چهره با تنظیم درست پارامترهاست.

تولید مدل سه‌بعدی از چهره

رویکرد اول

در رویکرد اول با استفاده از اسکن سه‌بعدی چهره، مجموعه‌ای از نقاط به‌دست می‌آیند که سطح چهره را تخمین می‌زنند و عمق آن را نیز نشان می‌دهند. مراحلی که برای به‌دست‌آوردن آن نقاط باید طی کرد از این قرارند:

مرحلهٔ ۱: داده‌های سه‌بعدی براساس موقعیت دوربین تراز می‌شوند، طوری که محور z در امتداد محور نوری قرار بگیرد.

مرحلهٔ ۲: داده‌های سه‌بعدی که از نماهای مختلف به‌دست می‌آیند تحت فرایند هم‌جوشی[9] قرار می‌گیرند.

مرحلهٔ ۳: داده‌های سه‌بعدی براساس معیارهای مشخصی بهینه می‌شوند و در نهایت با استفاده از الگوریتم تولید مش یک چندضلعی سه‌بعدی از نقاط سه‌بعدی ایجاد می‌شود.

برای جمع‌آوری داده‌های سه‌بعدی چهره می‌توان به سه راهکار اصلی اشاره کرد. در راهکار اول، سامانهٔ «دوربین استریوسکوپی»[10] با گرفتن عکس‌های فوری از جسم، شکل سه‌بعدی اصلی را با استفاده از فرایند مثلث‌سازی بازسازی می‌کند و نقاط متناظر هر دو تصویر را تطبیق می‌دهد. در راهکار دوم، از پرتو نوریِ ساختاریافته برای اسکن اشیا استفاده می‌شود. در این راهکار، اعوجاج الگوهای مختلف نور مانند الگوهای شبکه‌ای، راه‌راه یا بیضوی برای ایجاد شکلی سه‌بعدی استفاده می‌شوند. در راهکار سوم، از سامانهٔ تعیین برد لیزری استفاده می‌شود که در آن نور لیزر روی سطح چهره تابیده می‌شود و هم‌زمان دوربین دیجیتال، موقعیت نقاط در امتداد نور لیزر را در فضای سه‌بعدی محاسبه می‌کند.

رویکرد دوم

در رویکرد دوم برای تولید مدل سه‌بعدی از چهره، می‌توان از یک مدل شکل‌پذیر استفاده کرد. در این روشْ با انتخاب مجموعهٔ بزرگی از پارامترها، هر چهرهٔ دلخواه را با تنظیم درست پارامترها ایجاد می‌کنند و مدل شکل‌پذیر را با تصویر چهرهٔ داده‌شده مطابقت می‌دهند. این رویکرد از نظر مقاومت در برابر تغییر موقعیت، چرخش و مقیاس‌بندی قوی‌تر از رویکرد قبلی عمل می‌کند، چون مدل سه‌بعدی شکل‌پذیر را می‌توان با توجه به سیستم مرجع آن با تصویر ورودی تراز کرد. با این حال، رویکرد یادشده دو مشکل دارد:

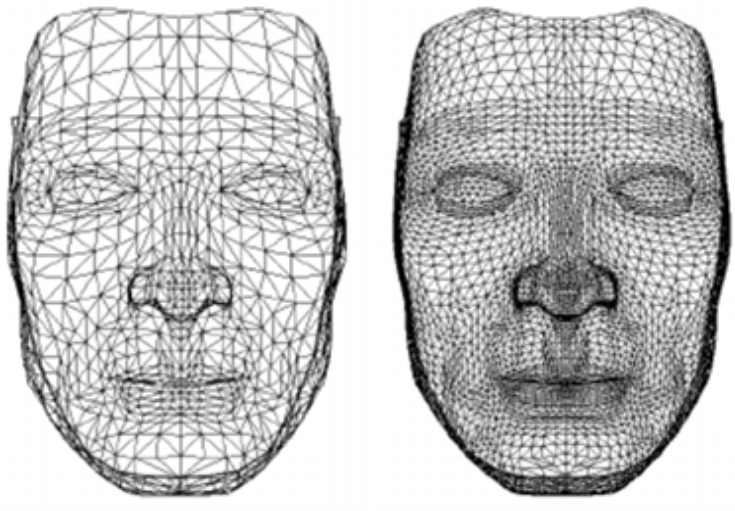
- هزینهٔ محاسباتی بالا؛
- وابستگی دقت مدل به تعداد و کیفیت پارامترهای انتخاب‌شده.

دسته‌بندی الگوریتم‌های تشخیص چهرهٔ سه‌بعدی

در این بخش شرح مختصری از جدیدترین الگوریتم‌های تشخیص چهرهٔ سه‌بعدی ارائه می‌شود. این الگوریتم‌ها در سه دستهٔ اصلی قرار می‌گیرند: مبتنی‌بر تصویر دوبعدی، مبتنی‌بر تصویر سه‌بعدی و مبتنی‌بر تصویر چندوجهی. بسته به طبقهٔ الگوریتم‌ها، مراحل تحلیل، تبدیل تصویر به داده و تطبیق آنها متفاوت از یکدیگر خواهد بود. طبقهٔ اول الگوریتم‌ها مبتنی‌بر تصاویر دوبعدی است که با یک فرایند سه‌بعدی پشتیبانی می‌شود تا مقاومت الگوریتم افزایش یابد. در طبقهٔ دوم الگوریتم‌هاْ روش‌ها براساس نمایش سه‌بعدیِ چهره مانند تصاویر محدوده یا مش‌ها دسته‌بندی می‌شوند. دستهٔ سومِ الگوریتم‌ها مبتنی‌بر ترکیب اطلاعات چندوجهی، یعنی اطلاعات مربوط به تصاویر دوبعدی و سه‌بعدی است.

تشخیص چهرهٔ سه‌بعدی مبتنی‌بر تصاویر دوبعدی

الگوریتم‌های تشخیص چهرهٔ سه‌بعدی مبتنی‌بر تصاویر دوبعدی، توسط داده‌های سه‌بعدی پشتیبانی می‌شوند و با عنوان الگوریتم‌های دوبعدی تشخیص چهره شناخته می‌شوند. در این



شکل ۳: دو نمونهٔ متفاوت از نمایش سه‌بعدی چهره با استفاده از شبکه یا مش چندضلعیِ سه‌بعدی

9. fusion
10. Stereoscopic camera

الگوریتم‌ها، از یک مدل پارامتریک سه‌بعدی برای بهبود عملکرد الگوریتم در برابر تغییرات ظاهری مانند وضعیت سر، روشنایی و حالت چهره استفاده می‌شود. در واقع، مدل پارامتریک چهره بر بازنمایی فضای برداری از چهره بنا شده است. مثلاً می‌توان از یک مدل شکل‌پذیر برای ایجاد تغییرات ظاهری در چهرهٔ هر فرد استفاده کرد و بدین صورت تعداد داده‌های آموزش را که همگی شامل تصاویر دوبعدی از چهره هستند، افزایش داد و تقویت کرد. افزایش تعداد داده‌های آموزش و تقویت آن با استفاده از مدل شکل‌پذیر برای چهره باعث می‌شود که الگوریتم بتواند تغییرات ظاهری چهره را نیز آموزش ببیند و بدین ترتیب دقت الگوریتم تشخیص چهره در برابر تغییرات ظاهری چهره نیز افزایش یابد. ایجاد چهره‌های مصنوعی دوبعدی متنوع می‌تواند برای الگوریتم‌های تشخیص چهره مفید باشد ولی باید به این نکته توجه داشت که چهرهٔ مصنوعی ایجادشده تا چه حد می‌تواند واقعی و دقیق باشد که در این خصوص، فناوری‌های گرافیکی کامپیوتری سه‌بعدی امروزی قادر به بازتولید تصاویر مصنوعی به‌صورت واقعی و دقیق هستند.

تشخیص چهرهٔ سه‌بعدی مبتنی‌بر تصاویر سه‌بعدی

یکی از چالش‌های مرتبط با الگوریتم‌های تشخیص چهرهٔ مبتنی‌بر تصاویر سه‌بعدی، تنظیم یک تراز صحیح بین سطوح دو تصویر است. در برخی از الگوریتم‌ها با شروع از نمای جلو و یک نمای دیگر از چهره، از مختصات سه‌بعدی مجموعه‌ای از نقاط ویژگی چهره برای تغییر شکل یک مدل شکل‌پذیر متناسب با سطح واقعی چهره استفاده می‌شود. در این الگوریتم‌ها، مراحل تغییر شکل مدل به شرح زیر است:

- تغییر شکل کلی به‌منظور مقیاس‌بندی و تراز کردن مدل به نقاط ویژگی استخراج‌شده از دو تصویر؛
- تغییر شکل محلی به‌منظور نزدیک کردن رئوس به نقاط ویژگی.

پس از تغییر شکل مدل، فرایند تشخیص چهره با محاسبهٔ فاصلهٔ اقلیدسی بین نقاط ویژگی در سطح چهرهٔ سه‌بعدی واقع روی دهان، بینی و چشم اجرا می‌شود.

تشخیص چهرهٔ سه‌بعدی مبتنی‌بر اطلاعات چندوجهی

الگوریتم‌های تشخیص چهرهٔ مبتنی بر اطلاعات چندوجهی از اطلاعات تصاویر دوبعدی و مدل سه‌بعدی چهره برای تشخیص چهره استفاده می‌کنند. درصورتی که هریک از الگوریتم‌های دوبعدی و سه‌بعدی به‌طور جداگانه روی تصویر چهره اعمال شوند نتایج مشابهی خواهند داشت. همچنین ترکیب وزنی نتایج الگوریتم‌های دوبعدی و سه‌بعدی نتایج بهتری نسبت به هریک از الگوریتم‌های دوبعدی و سه‌بعدی در پی خواهد داشت.

نتیجه‌گیری

در میان فناوری‌های متنوع امنیت بیومتریک، تشخیص چهره از طبیعی‌ترین و محبوب‌ترین آنهاست. فرایند تشخیص چهره همراه با چالش‌هایی مانند تغییرات شدت روشنایی، تغییرات حالت چهرهٔ افراد و انسداد است که دقت الگوریتم‌های تشخیص چهره را تحت تأثیر قرار می‌دهند.

ازجمله نقاط قوت الگوریتم‌های تشخیص چهرهٔ سه‌بعدی این است که از اطلاعات مربوط به هندسهٔ چهرهٔ افراد برای تشخیص چهره استفاده می‌کند. همچنین در این الگوریتم‌ها مدلی سه‌بعدی از چهره ایجاد می‌شود که دربرگیرندهٔ ویژگی‌های چهره با انحناهای محلی و سراسری است و به‌عنوان اثر چهرهٔ افراد در نظر گرفته می‌شود. قابلیت نمایش دقیق‌تر ویژگی‌های چهره در الگوریتم‌های سه‌بعدی باعث می‌شود که این نوع از الگوریتم‌ها قدرت تمایز بالاتری نسبت به الگوریتم‌های دوبعدی داشته باشند. برای تولید مدل سه‌بعدی از چهره دو رویکرد وجود دارد که در رویکرد اول از یک اسکنر سه‌بعدی برای جمع‌آوری داده‌های سه‌بعدی چهره استفاده می‌شود و در رویکرد دوم از یک مدل عمومی چهره استفاده می‌شود و با تنظیم درست پارامترهای آن، مدل یادشده با تصویر داده‌شده از چهره تطبیق داده می‌شود.

منابع

- Y. Jing, X. Lu, S. Gao, “3D face recognition: A comprehensive survey in 2022”, *Computational Visual Media*, Vol. 9, No. 4, PP. 657-685.
- AF. Abate, M. Nappi, D. Riccio, G. Sabatino, “2D and 3D Face Recognition: A Survey”, *ELSEVIER, Pattern Recognition Letters*, pages: 1885-1906.
- L.K. Huang (2023), “Multi-camera face detection and recognition in an unconstrained environment”.
- X. Chen, P.J. Flynn, K.W. Bowyer, “IR and Visible Light Face Recognition”.
- https://usa.kaspersky.com/resource-center/definitions/what-is-facial-recognition

مصاحبه کننده:
معصومه عباسیان

نشست با دکتر قادر قدیمی

سرپرست فنی قرارگاه الکترونیک پدافند غیرعامل کشوری

مهمان نشستِ این فصل از مجله‌ی امنیت الکترونیک، جناب آقای قادر قدیمی، دکترای مخابرات و متخصص در حوزه‌ی هوش مصنوعی و جنگ الکترونیک هستند که درحال‌حاضر به‌عنوان سرپرست فنی قرارگاه پدافند الکترونیک، در سازمان پدافند غیرعامل کشوری، مشغول به خدمت هستند.

۱. نقش هوش مصنوعی در آیندهٔ امنیت الکترونیکی، به‌ویژه خدمات نظارت تصویری را چگونه ارزیابی می‌کنید؟

هوش مصنوعی در آیندهٔ امنیت الکترونیکی نقش کلیدی ایفا خواهد کرد. AI می‌تواند با استفاده از تکنیک‌های پیشرفته‌مانندیادگیری‌عمیق‌ویادگیری ماشین، کارایی و دقت سیستم‌های نظارت تصویری را به‌طور چشمگیری افزایش دهد. ویژگی‌هایی مانند تشخیص خودکار چهره، شناسایی اشیا، تشخیص حرکت و تحلیل رفتار می‌توانند به بهبود امنیت و کاهش نرخ جرایم کمک کنند. همچنین، سیستم‌های مبتنی‌بر AI قادر به تحلیل حجم بالایی از داده‌های تصویری در زمان واقعی هستند که این امر می‌تواند زمان واکنش به حوادث را کاهش دهد.

۲. آیا می‌توانید نمونهٔ خاصی معرفی کنید که در آن فناوری‌های هوش مصنوعی به‌طور قابل‌توجهی کارایی یا دقت سیستم‌های نظارت تصویری را افزایش داده باشند؟

یک نمونهٔ بارز استفاده از هوش مصنوعی در نظارت تصویری، سیستم‌های تشخیص چهره است که در فرودگاه‌ها و مراکز امنیتی بزرگ به‌کار گرفته شده است. این سیستم‌ها می‌توانند افراد مشکوک را از میان جمعیت شناسایی و ردیابی کنند. همچنین، شرکت‌هایی مانند Hikvision و Dahua از الگوریتم‌های پیشرفتهٔ AI برای شناسایی رفتارهای غیرمعمول و تشخیص حرکت استفاده‌می‌کنند.

از سایر نمونه‌های برجستهٔ استفاده از AI در سیستم‌های نظارت تصویری، پروژهٔ «شیائومی» در چین است. این پروژه از الگوریتم‌های پیشرفتهٔ AI برای تشخیص چهره در فرودگاه‌ها و ایستگاه‌های قطار استفاده‌می‌کند. سیستم‌های هوشمند می‌توانند بادقت‌بالا چهره‌های افراد مشکوک را شناسایی کرده و در صورت لزوم به مقامات امنیتی هشدار دهند. این فناوری‌ها همچنین در جلوگیری از جرایم و دستگیری مجرمان فراری بسیار مؤثر بوده‌اند.

۳. برخی از چالش‌های اساسی مربوط به ادغام هوش مصنوعی در خدمات نظارت تصویری کدام‌اند و چه روش‌هایی برای غلبه بر آنها پیشنهاد می‌کنید؟

چالش‌های اصلی عبارتند از:

- **نقص در داده‌های آموزشی:** برای آموزش مدل‌های AI به داده‌های متنوع و باکیفیت نیاز است. استفاده از داده‌های ناقص یا نادرست می‌تواند منجر به کاهش دقت سیستم شود. برای غلبه بر این مشکل، باید از داده‌های متنوع و باکیفیت برای آموزش مدل‌ها استفاده کرد و فرایند پاک‌سازی داده‌ها را به کار گرفت.
- **مشکلات حریم خصوصی:** استفادهٔ گسترده از دوربین‌های نظارتی می‌تواند به نگرانی‌های حریم خصوصی منجر شود. برای حل این مشکل، باید از روش‌های رمزگذاری داده‌ها، کنترل‌های دسترسی سختگیرانه و ناشناس‌سازی داده‌ها استفاده کرد.
- **نیاز به قدرت پردازشی بالا:** تحلیل و پردازش داده‌های تصویری به قدرت پردازشیِ بالایی نیاز دارد. برای غلبه بر این چالش، می‌توان از زیرساخت‌های ابری و فناوری‌های پیشرفته‌تر

برای پردازش داده‌ها بهره برد.

- **هزینه‌های بالا:** پیاده‌سازی سیستم‌های AI ممکن است هزینه‌بر باشد. استفاده از راه‌حل‌های مقیاس‌پذیر و بهینه‌سازی فرایندهای موجود می‌تواند به کاهش هزینه‌ها کمک کند.

٤. به نظر شما، کدام الگوریتم‌ها یا فناوری‌های هوش مصنوعی بیشترین نوید را برای بهبود اثربخشی نظارت تصویری در برنامه‌های امنیتی الکترونیکی دارند؟

- **شبکه‌های عصبی کانولوشن (CNN):** این الگوریتم‌ها در تشخیص و طبقه‌بندی تصاویر بسیار مؤثر هستند و می‌توانند به شناسایی چهره‌ها و اشیا کمک کنند.
- **یادگیری عمیق[1]:** با استفاده از چندین لایهٔ پردازشی، این الگوریتم‌ها می‌توانند الگوهای پیچیده را شناسایی کنند و در تحلیل رفتار و تشخیص حرکت بسیار مؤثر باشند.
- **یادگیری تقویتی[2]:** این الگوریتم‌ها می‌توانند با تعامل با محیط و دریافت بازخورد، عملکرد خود را بهبود بخشند و در فرایندهای خودکارسازی نظارت تصویری استفاده شوند.
- **پردازش زبان طبیعی (NLP):** این فناوری می‌تواند در تحلیل و تفسیر اطلاعات متنی همراه با داده‌های تصویری، مانند گزارش‌های امنیتی، مفید باشد.

٥. چگونه می‌توان اطمینان حاصل کرد که استفاده از هوش مصنوعی در خدمات نظارت تصویری با قوانین و مقررات مربوط به حریم خصوصی، به‌ویژه از نظر حفاظت از داده‌ها و حریم خصوصی کاربر، مطابقت دارد؟

برای اطمینان از مطابقت استفاده از هوش مصنوعی در خدمات نظارت تصویری با قوانین و مقررات مربوط به حریم خصوصی، می‌توان اقدامات زیر را انجام داد:

- **رمزگذاری داده‌ها:** استفاده از روش‌های رمزگذاری قوی برای محافظت از داده‌های تصویری در برابر دسترسی غیرمجاز.
- **کنترل دسترسی:** اعمال کنترل‌های دسترسی سختگیرانه برای اطمینان از اینکه فقط افراد مجاز به داده‌ها دسترسی دارند.
- **ناشناس‌سازی داده‌ها:** حذف یا ناشناس‌سازی اطلاعات حساس به‌طوری که نتوان افراد را شناسایی کرد.
- **تبعیت از مقررات:** تطبیق کامل با قوانین حریم خصوصی مانند GDPR در اروپا و قانون حفاظت از حریم خصوصی در کشورهای مختلف.
- **آگاهی‌بخشی به کاربران:** اطلاع‌رسانی به کاربران دربارهٔ نحوهٔ جمع‌آوری، استفاده و نگهداری داده‌ها و دریافت رضایت از آن‌ها.
- **ممیزی‌های منظم:** انجام ممیزی‌های منظم برای بررسی تطابق سیستم‌ها با مقررات حریم خصوصی و شناسایی و رفع نواقص.

٦. آیا می‌توانید نمونه‌هایی معرفی کنید که چگونه تجزیه‌وتحلیل‌های مبتنی‌بر هوش مصنوعی فرایندهای نظارت تصویری و زمان پاسخگویی به حوادث امنیتی در سیستم‌های نظارت الکترونیکی را بهینه کرده‌اند؟

یکی از نمونه‌های موفق، استفاده از AI در سیستم‌های نظارت تصویری در شهرهای هوشمند است. در شهرهایی مانند سنگاپور و دبی، سیستم‌های نظارت تصویری مجهز به الگوریتم‌های AI می‌توانند به‌طور خودکار رفتارهای مشکوک را شناسایی کنند و بلافاصله به مراکز نظارتی هشدار دهند. این سیستم‌ها توانسته‌اند زمان پاسخگویی به حوادث را به‌طور چشمگیری کاهش دهند و امنیت عمومی را بهبود بخشند.

همچنین، در برخی از فرودگاه‌های بزرگ، سیستم‌های AI برای تجزیه‌وتحلیل تصاویر دوربین‌های نظارتی به‌کار گرفته شده‌اند. این سیستم‌ها می‌توانند صف‌های طولانی، رفتارهای غیرعادی و تهدیدهای بالقوه را شناسایی کرده و اقدامات پیشگیرانه را به‌سرعت اعمال کنند.

٧. چگونه با آخرین پیشرفت‌ها و روندهای فناوری هوش مصنوعی در ارتباط با امنیت الکترونیکی و خدمات نظارت تصویری هماهنگ می‌شوید؟

برای هماهنگی با آخرین پیشرفت‌ها و روندهای فناوری‌های هوش مصنوعی در حوزهٔ امنیت الکترونیکی و خدمات نظارت تصویری، می‌توان از روش‌های زیر استفاده کرد:

- **مطالعهٔ مقاله‌ها و نشریه‌های علمی:** دنبال کردن مقاله‌ها و نشریه‌های علمی معتبر برای آگاهی از جدیدترین پژوهش‌ها و دستاوردها.
- **شرکت در کنفرانس‌ها و سمینارها:** حضور در کنفرانس‌ها، سمینارها و وبینارهای تخصصی برای تبادل نظر با کارشناسان و متخصصان این حوزه.
- **عضویت در انجمن‌های حرفه‌ای:** عضویت در انجمن‌های حرفه‌ای و گروه‌های تخصصی برای دریافت اطلاعات به‌روز و شرکت در بحث‌های تخصصی.
- **پروژه‌های تحقیق و توسعه:** مشارکت در پروژه‌های تحقیق و توسعه برای آزمایش و ارزیابی فناوری‌های جدید.
- **شبکه‌سازی با متخصصان:** برقراری ارتباط و شبکه‌سازی با متخصصان و پژوهشگران حوزهٔ هوش مصنوعی و امنیت الکترونیکی.

٨. به نظر شما چه معیارهایی برای ارزیابی عملکرد و اثربخشی راهکارهای نظارت تصویری مبتنی‌بر هوش مصنوعی در حوزهٔ امنیت الکترونیکی مهم هستند؟

- **میزان خطاهای مثبت و منفی:** تعداد هشدارهای نادرست (خطای مثبت) و مواردی که سیستم از شناسایی آن‌ها غافل شده است (خطای منفی).
- **مقیاس‌پذیری:** توانایی سیستم در مدیریت و پردازش حجم زیادی از داده‌ها و افزایش تعداد دوربین‌ها بدون کاهش کارایی.
- **قابلیت تطبیق و یادگیری:** توانایی سیستم در یادگیری از داده‌های جدید و بهبود عملکرد خود با گذر زمان.

1. Deep Learning
2. Reinforcement Learning

- **پایداری و قابلیت اطمینان:** ثبات عملکرد سیستم در شرایط مختلف و عدم وقوع خرابی‌های مکرر.
- **سهولت استفاده:** کاربرپسند بودن سیستم و سهولت در نصب، راه‌اندازی و مدیریت آن.
- **هزینه‌های عملیاتی:** ارزیابی هزینه‌های نگهداری و عملیاتی سیستم در بلندمدت.
- **میزان بهره‌وری:** تأثیر سیستم بر بهبود فرایندهای امنیتی و کاهش زمان و هزینه‌های مرتبط با نظارت.

۹. هنگام اجرای راهکارهای نظارت تصویری برای پروژه‌های امنیت الکترونیکی چگونه ارائه‌کنندگان خدمات هوش مصنوعی را ارزیابی و انتخاب می‌کنید؟

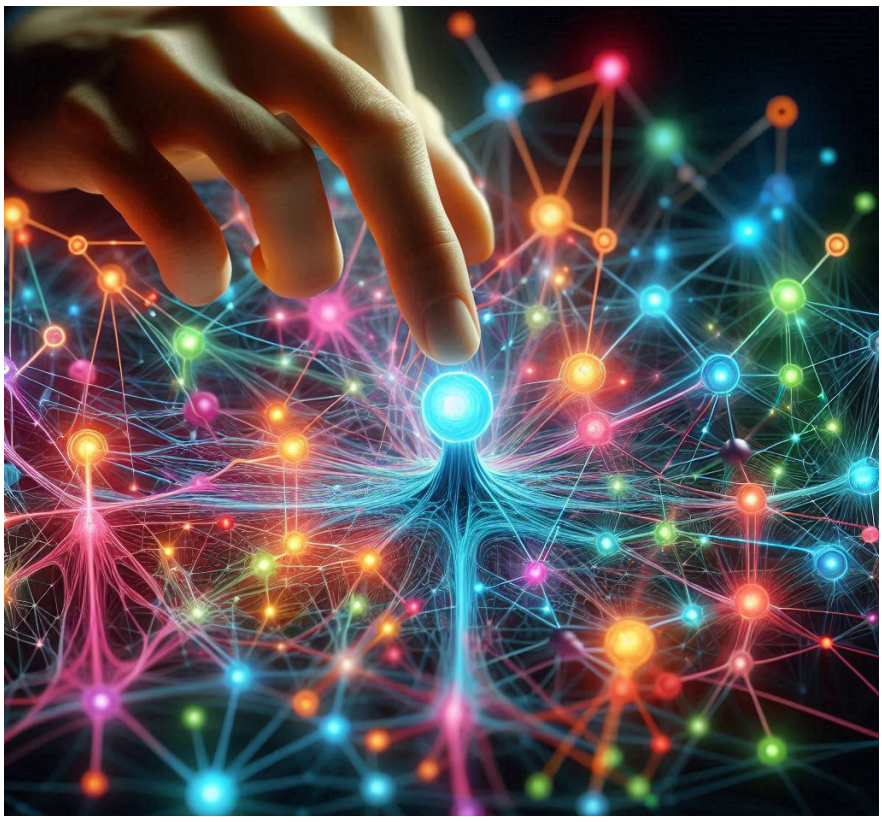
برای ارزیابی و انتخاب ارائه‌کنندگان خدمات هوش مصنوعی می‌توان از معیارهای زیر استفاده کرد:

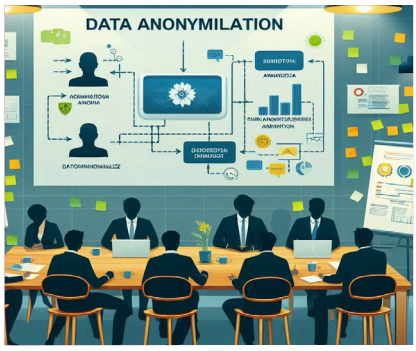
- **تجربه و پیشینه:** بررسی سابقه و تجربیات شرکت در ارائهٔ راهکارهای مشابه و موفقیت‌های گذشتهٔ آنها؛
- **کیفیت فناوری:** ارزیابی فناوری‌های استفاده‌شده از نظر دقت، کارایی و نوآوری؛
- **پشتیبانی فنی:** کیفیت خدمات پشتیبانی و توانایی شرکت در حل مشکلات فنی به‌صورت سریع و کارآمد؛
- **هزینه و بودجه:** بررسی هزینه‌های پیاده‌سازی و نگهداری سیستم و مقایسهٔ آنها با بودجهٔ موجود؛
- **نظرات و بازخوردها:** ارزیابی نظرات و بازخوردهای مشتریان قبلی و میزان رضایتمندی آنها؛
- **هم‌خوانی با نیازها:** تطابق خدمات ارائه‌شده با نیازها و الزامات خاص پروژه؛
- **تطابق با مقررات:** اطمینان از اینکه راهکارهای ارائه‌شده با قوانین و مقررات حریم خصوصی و امنیت داده‌ها مطابقت دارند؛
- **قابلیت سفارشی‌سازی:** توانایی ارائه‌دهنده در سفارشی‌سازی راهکارها براساس نیازهای خاص پروژه.

۱۰. چگونه ذی‌نفعان خدمات هوش مصنوعی در خدمات نظارت تصویری را از مزایا و خطرات بالقوهٔ استفاده از این فناوری آگاه می‌کنید؟

برای آگاهی‌بخشی به ذی‌نفعان راجع به مزایا و خطرات بالقوهٔ استفاده از هوش مصنوعی در خدمات نظارت تصویری می‌توان از روش‌های زیر استفاده کرد:

- **ارائهٔ گزارش‌ها و مستندهای جامع:** تهیهٔ گزارش‌های دقیق و مستندهایی که مزایا، کاربردها و خطرات بالقوه را به‌طور شفاف توضیح دهند؛
- **برگزاری جلسه‌های آموزشی:** ترتیب برگزاری جلسه‌های آموزشی و کارگاه‌های عملی برای توضیح فناوری و کاربردهای آن به ذی‌نفعان؛
- **مطالعات موردی:** ارائهٔ نمونه‌های موفق از کاربرد هوش مصنوعی در نظارت تصویری و تحلیل نتایج و مزایای کسب‌شده؛
- **مشاورهٔ تخصصی:** استفاده از مشاوران و متخصصان برای ارائهٔ راهنمایی‌های فنی و حقوقی به ذی‌نفعان؛
- **ارائهٔ دموی زنده:** نمایش دموی زنده از عملکرد سیستم‌های مبتنی بر هوش مصنوعی و قابلیت‌های آنها؛
- **تحلیل ریسک:** تهیهٔ تحلیل‌های ریسک و ارائهٔ راهکارهای پیشنهادی برای کاهش خطرات احتمالی؛
- **انتشار مقاله و مطالب آموزشی:** انتشار مقاله و مطالب آموزشی در وب‌سایت‌ها، مجله‌ها و شبکه‌های اجتماعی مرتبط با حوزهٔ امنیت الکترونیکی؛
- **پاسخ به سؤالات و رفع ابهامات:** فراهم کردن بستری برای پرسش و پاسخ و رفع ابهامات و نگرانی‌های ذی‌نفعان.





سپتام

سامانه پایش تصویری اماکن

سپتام خدماتی

به وسعت ایران

سپتام تضمینی برای ارتقای امنیت و آرامش خاطر محیط کسب و کار و منزل شما

سپتام با بهره‌گیری از ظرفیت آزمایشگاه های تخصصی دانش بنیان بومی, نسبت به ارزیابی صحت و دقت تجهیزات پایش تصاویر در اماکن عمومی اقدام می نماید.

saptam.ir

+۹۸ ۲۱-۲۲۹۴۸۸۶۸
+۹۸ ۲۱-۲۲۹۶۷۷۶۹
www.electronicsecurity.ir
info@electronicsecurity.ir