

ترویجی

ارائه راهکار پیاده سازی اعتماد صفر در سیستم‌های نظارت تصویری

سید علی صموتی ^۱ | سجاد طرهانی ^۲ | حسام حسن‌پور ^۳

چکیده:

در عصر دیجیتال، امنیت سایبری به یکی از چالش‌های جدی برای سازمان‌ها و شرکت‌ها تبدیل شده است. با افزایش تعداد دستگاه‌های متصل به اینترنت و پیچیدگی حملات سایبری، مدل‌های سنتی امنیت دیگر پاسخگوی نیازهای امروزی نیستند. در این زمینه، معماری اعتماد صفر^۱ به عنوان یک رویکرد نوین و مؤثر در تأمین امنیت اطلاعات، جایگاه ویژه‌ای پیدا کرده است. این معماری بر این اصل استوار است که هیچ کاربری یا دستگاهی، چه در داخل شبکه و چه در خارج از آن، به طور پیش‌فرض قابل اعتماد نیست. در سیستم‌های نظارت تصویری که به طور مداوم اطلاعات حساسی را جمع‌آوری و ذخیره می‌کنند، پیاده‌سازی اعتماد صفر می‌تواند به طور قابل توجهی امنیت را افزایش دهد. ارکان اصلی این معماری شامل احراز هویت مداوم، اصل حداقل دسترسی، رمزنگاری داده‌ها و نظارت و تحلیل مداوم بر فعالیت‌ها هستند. احراز هویت مداوم به معنای بررسی هویت کاربران و دستگاه‌ها در هر بار درخواست دسترسی است و اصل حداقل دسترسی به این معناست که هر کاربر تنها به منابعی دسترسی دارد که برای انجام وظایف خود به آن‌ها نیاز دارد. همچنین، رمزنگاری داده‌ها در تمام مراحل انتقال و ذخیره‌سازی، از دسترسی غیرمجاز جلوگیری می‌کند. با استفاده از این رویکرد، سازمان‌ها می‌توانند به طور مؤثرتری به شناسایی و مدیریت تهدیدات سایبری پرداخته و تاب‌آوری خود را در برابر حملات افزایش دهند. در نهایت، پیاده‌سازی معماری اعتماد صفر در سیستم‌های نظارت تصویری نه تنها به افزایش امنیت کمک می‌کند، بلکه به سازمان‌ها این امکان را می‌دهد که کنترل بیشتری بر دسترسی‌ها و فعالیت‌های مرتبط با داده‌های حساس داشته باشند و به طور مؤثرتر به الزامات قانونی و استانداردهای امنیتی پاسخ دهند.

کلید واژه‌ها: امنیت سایبری، معماری اعتماد صفر، احراز هویت مداوم، اصل حداقل دسترسی، نظارت و تحلیل مداوم، سیستم‌های نظارت تصویری

^۱ گروه مهندسی کامپیوتر، واحد سبزوار، دانشگاه آزاد اسلامی، سبزوار ایران،

Ali.Samouti@iaui.ac.ir

^۲ گروه مهندسی مکترونیک، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران،

Sajad.tarhani@gmail.com

^۳ گروه مهندسی کامپیوتر و فناوری اطلاعات، واحد سبزوار، دانشگاه آزاد اسلامی، سبزوار ایران،

Hesamhasanpour@iaui.ac.ir

نویسنده مسئول

*سید علی صموتی، دانشجو دکترای گروه مهندسی کامپیوتر و فناوری اطلاعات، واحد سبزوار، دانشگاه آزاد اسلامی، سبزوار ایران،

Ali.samouti@iaui.ac.ir

تاریخ دریافت: ۱۴۰۴/۰۲/۱۴

تاریخ پذیرش: ۱۴۰۴/۰۳/۱۴

<https://doi.org/...>

۱- مقدمه

در عصر دیجیتال، امنیت سایبری به یکی از مهم ترین چالش های سازمان ها و شرکت ها تبدیل شده است. با افزایش تعداد دستگاه های متصل به اینترنت و پیچیدگی حملات سایبری، مدل های سنتی امنیت دیگر پاسخگوی نیازهای امروزی نیستند. در این میان، معماری اعتماد صفر^۲ به عنوان یک رویکرد نوین و مؤثر، جایگاه ویژه ای در تأمین امنیت اطلاعات پیدا کرده است. این معماری بر این اصل استوار است که هیچ کاربری یا دستگاهی، چه در داخل شبکه و چه در خارج از آن، به طور پیش فرض قابل اعتماد نیست. معماری اعتماد صفر به معنای حذف فرضیات مربوط به اعتماد پیش فرض در شبکه های سازمانی است. در این رویکرد، هر درخواست دسترسی به منابع باید به طور دقیق بررسی و مراحل احراز هویت/اصالت و مجوزدهی به درخواست کننده تکمیل گردد. برخلاف مدل های سنتی که بر اساس موقعیت جغرافیایی یا عضویت در شبکه داخلی اعتماد می کنند، اعتماد صفر بر پایه اصولی مانند احراز هویت چندعاملی^۳، رمزنگاری داده ها و نظارت پیوسته بر فعالیت ها عمل می کند. این معماری به ویژه برای مقابله با حملات داخلی و خارجی طراحی شده است. [۷، ۱]

۱-۱- بیان مسئله

سیستم های نظارت تصویری، از جمله دوربین های مدار بسته، به عنوان یکی از ابزارهای حیاتی در حفظ امنیت فیزیکی و سایبری شناخته می شوند. این سیستم ها اطلاعات حساسی را جمع آوری و ذخیره می کنند که می تواند هدف جذابی برای مهاجمان سایبری باشند. [۸، ۹] از نفوذ به دوربین ها برای دسترسی به تصاویر زنده گرفته تا سوء استفاده از اطلاعات ذخیره شده، تهدیدات مرتبط با این سیستم ها به طور مداوم در حال افزایش است. بنابراین، تأمین امنیت این سیستم ها از اهمیت بالایی برخوردار است. معماری اعتماد صفر می تواند به طور قابل توجهی امنیت سیستم های نظارت تصویری را بهبود بخشد. با استفاده از این رویکرد، هر دستگاه نظارتی مانند دوربین ها باید قبل از دسترسی به شبکه، احراز اصالت شود و ارتباطات آن ها رمزنگاری گردد. علاوه بر این، نظارت پیوسته بر فعالیت های این دستگاه ها و شناسایی رفتارهای غیرعادی می تواند از وقوع حملات جلوگیری کند. اعتماد صفر همچنین به سازمان ها امکان می دهد تا در برابر تهدیدات داخلی و خارجی، یک لایه امنیتی اضافی ایجاد کنند. در این مقاله مروری بر مفاهیم اعتماد صفر و کاربردهای آن خواهیم داشت. [۹، ۱۳، ۳، ۱]

در ادامه این مقاله به تشریح کلی مفاهیم اعتماد صفر خواهیم پرداخت. در بخش دوم به معرفی کاربردهای مدل اعتماد صفر پرداخته می شود. بخش سوم به بررسی مفهوم معماری اعتماد صفر و ارکان آن اختصاص دارد. در بخش چهارم، معماری اعتماد صفر و نحوه پیاده سازی این مدل مورد بررسی قرار می گیرد. در بخش پنجم، روش های پیاده سازی معماری اعتماد صفر تشریح می شود. بخش ششم به بررسی دلایل نیاز به اعتماد صفر در شبکه های نظارت تصویری می پردازد. در بخش هفتم، کاربرد معماری اعتماد صفر در دوربین های مدار بسته بررسی می شود و در بخش هشتم، مزایای استفاده از این معماری در سامانه های نظارتی تبیین می گردد. در بخش نهم، راهکارهایی برای پیاده سازی اعتماد صفر در سیستم های نظارت تصویری ارائه می شود. نهایتاً، در بخش پایانی مقاله، جمع بندی مطالب مطرح شده ارائه خواهد شد.

۱-۲- روش شناسی

در این پژوهش، رویکردی ساختارمند برای گردآوری منابع علمی اتخاذ شد. ابتدا، بیش از ۵۰ منبع معتبر از پایگاه های علمی نظیر ScienceDirect، Scopus و Google Scholar جمع آوری گردید. این منابع شامل مقالات، گزارش های فنی و مطالعات مرتبط با امنیت سایبری و معماری اعتماد صفر بودند. پس از خوانش اولیه، ۲۰ مقاله که بیشترین هم راستایی را با موضوع پیاده سازی اعتماد صفر در سیستم های نظارت تصویری داشتند، انتخاب شدند. این مقالات شامل تحقیقات کاربردی و مروری بودند که دیدگاه

² Zero Trust Architecture

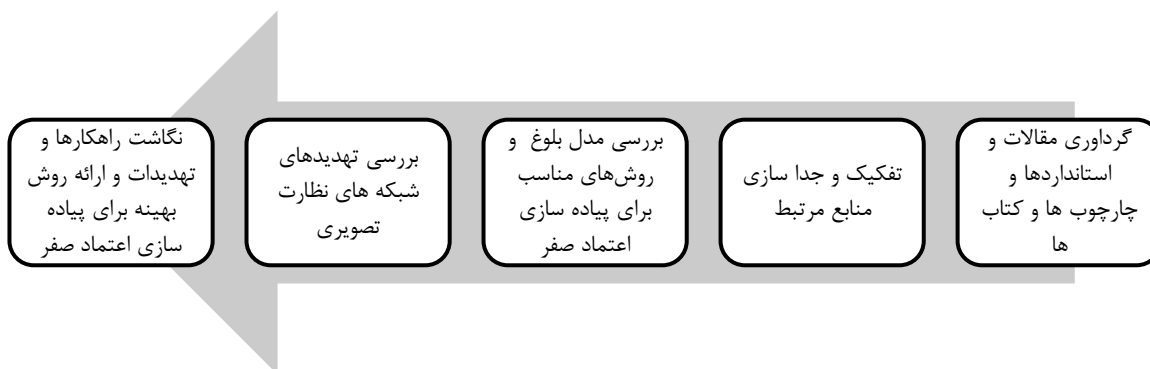
³ MFA Multi Factor Authentication

جامعی از چالش‌ها و راهکارهای موجود ارائه می‌دادند. همچنین، ۱۰ کتاب مرتبط بررسی و ۳ کتاب با تمرکز بر اعتماد صفر و امنیت سیستم‌های نظارتی به‌عنوان منابع اصلی انتخاب شدند.

در مرحله دوم، چارچوب‌های استاندارد جهانی مانند NIST SP 800207 و مدل بلوغ اعتماد صفر ارائه‌شده توسط وزارت دفاع ایالات متحده به طور عمیق تحلیل شدند. این چارچوب‌ها به دلیل ارائه اصول و راهنمایی‌های عملی برای پیاده‌سازی اعتماد صفر، نقش کلیدی داشتند. علاوه بر این، استانداردهای مرتبط از سایر کشورها بررسی و در تحلیل‌ها لحاظ شدند تا رویکردی جامع ایجاد شود.

مرحله نهایی، تهدیدات سایبری مرتبط با سیستم‌های نظارت تصویری، باتکیه بر پیشینه تحقیقاتی نویسندگان، بازنگری و طبقه‌بندی شدند. این تهدیدات شامل حملات در بخش‌های مختلف بودند. سپس، این تهدیدات با راهکارهای ارائه‌شده در مقالات و استانداردها تطبیق داده شدند تا نقاط ضعف و قوت شناسایی شود. با استفاده از چارچوب NIST و مدل بلوغ اعتماد صفر وزارت دفاع آمریکا، راهکارهای عملی برای چهار رکن کلیدی (کاربران، دستگاه‌های دوربین، شبکه، انتقال داده‌ها) طراحی شد. این راهکارها باهدف کاهش مخاطرات سایبری و تقویت امنیت در محیط‌های حساس تدوین شدند.

روش‌شناسی این پژوهش با ترکیب گردآوری منابع معتبر، تحلیل استانداردها و تطبیق تهدیدات، چارچوبی علمی و عملی برای پیاده‌سازی معماری اعتماد صفر ارائه می‌دهد.



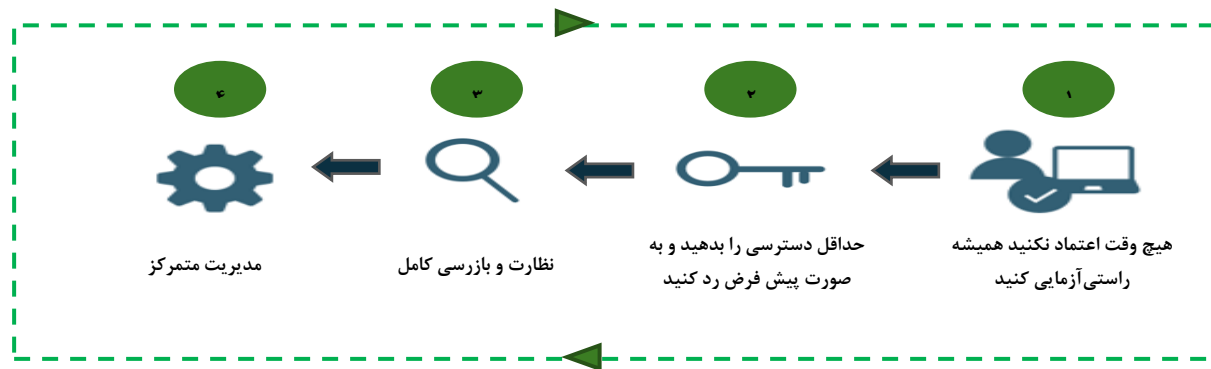
شکل ۱: روش شناسی پژوهش

۲- مروری بر کاربردهای اعتماد صفر و ادبیات پیشین

مطالعات متنوعی در زمینه اعتماد صفر صورت گرفته است که در ادامه به تشریح این مطالعات می‌پردازیم همچنین در جدول ۱ این مفاهیم به اختصار تشریح شده است.

سند NIST Special Publication 800207 به طور جامع به معرفی و تبیین مفهوم معماری اعتماد صفر می‌پردازد. [۴] بر اساس این سند و این رویکرد امنیتی به‌جای اتکا به مرزهای شبکه‌ای سنتی، بر روی احراز هویت و مجوزدهی متمرکز است و فرض می‌کند که هیچ کاربر یا دستگاهی به طور پیش‌فرض مورداعتماد نیست. سند به تشریح اجزای منطقی معماری اعتماد صفر، شامل احراز هویت چندعاملی، میکرو قطاع‌بندی (ریز بندی) و زیرساخت‌های نرم‌افزاری تعریف‌شده می‌پردازد. همچنین، مدل‌های مختلفی برای پیاده‌سازی معماری ارائه می‌دهد که می‌تواند به سازمان‌ها در مدیریت چالش‌های امنیتی مرتبط با کاربران از راه دور و دارایی‌های ابری کمک کند. در نهایت، این سند به‌عنوان یک راهنمای عملی برای معماران امنیت سایبری و مدیران فناوری اطلاعات طراحی شده است تا به آن‌ها در پیاده‌سازی مؤثر این رویکرد کمک کند.

استراتژی امنیتی صفر اعتماد وزارت دفاع ایالات متحده [۱۴] به منظور مقابله با تهدیدات سایبری طراحی شده و بر اساس اصول "هرگز اعتماد نکن، همیشه تأیید کن" است. این استراتژی شامل چهار هدف اصلی است: فرهنگ سازی برای پذیرش صفر اعتماد، تأمین و دفاع از سیستم های اطلاعاتی، شتاب دهی به فناوری و توانمند سازی صفر اعتماد. از ویژگی های کلیدی آن می توان به تأکید بر احراز هویت چند عاملی و میکرو قطع بندی اشاره کرد. هدف نهایی کاهش سطح حمله و افزایش امنیت اطلاعات و سیستم ها در برابر تهدیدات است. (شکل ۱)



شکل ۲: اصول اولیه اعتماد صفر بر مبنای دید امنیتی تطبیقی [۱۷]

هریشتکی در [۱۵] به بررسی تأثیر فناوری های نوظهور بر معماری اعتماد صفر و چالش های آن در زمینه امنیت سایبری می پردازد. باتوجه به تهدیدات پیچیده و در حال تغییر، ادغام فناوری های نوین مانند هوش مصنوعی، یادگیری ماشین، بلاک چین و محاسبات کوانتومی با اصول معماری اعتماد صفر، راهکارهای جدید و چالش های تازه ای را به همراه دارد. مقاله پیشنهاد می کند که سازمان ها باید استراتژی های معماری اعتماد صفر خود را به طور مداوم با پیشرفت های فناوری تطبیق دهند تا امنیت خود را در برابر تهدیدات سایبری تقویت کنند. همچنین مقاله [۱۳] به اهمیت ادغام فناوری بلاک چین و مدل امنیتی اعتماد صفر در حفاظت از سیستم های بانکی آنلاین اشاره دارد. بلاک چین با ایجاد یک دفترکل غیرمتمرکز و غیرقابل تغییر، شفافیت و یکپارچگی داده ها را افزایش می دهد، درحالی که مدل اعتماد صفر با تأیید هویت مداوم، سطح حمله را کاهش می دهد.

سند مدل بلوغ اعتماد صفر CISA [۱۶] که توسط آژانس امنیت سایبری و زیرساخت منتشر شده است، رویکردی ساختاریافته برای پیاده سازی معماری اعتماد صفر در سازمان ها ارائه می دهد. این مدل شامل پنج رکن اصلی است: شناسایی، دستگاه ها، شبکه ها، برنامه ها و بارهای کاری، و داده ها، و به سازمان ها کمک می کند تا مراحل لازم برای بهبود وضعیت امنیت سایبری خود را شناسایی و اجرا کنند. همچنین، چالش های موجود در پذیرش این مدل و اهمیت همکاری میان سطوح مختلف سازمانی را موردبررسی قرار می دهد. در نهایت، سند به سازمان ها توصیه می کند که با استفاده از این مدل، به تدریج و باتوجه به نیازهای خاص خود، به سمت پیاده سازی کامل معماری اعتماد صفر حرکت کنند.

پونام در [۱۲] ضمن بررسی معماری امنیتی اعتماد صفر و تشریح اصول اساسی آن چالش ها و فرصت های موجود در پیاده سازی این معماری را شناسایی کرده و مسیرهای تحقیقاتی آینده را شامل بهبود روش های احراز هویت، تحلیل تکنیک های کنترل دسترسی، اتوماسیون امنیتی و به کارگیری فناوری های نوین مانند بلاک چین و هوش مصنوعی پیشنهاد می کند.

نهار و همکاران در مقاله [۳] به بررسی معماری اعتماد صفر در شبکه‌های نسل ششم^۴ می‌پردازد که با افزایش تعداد دستگاه‌های متصل و پیچیدگی‌های امنیتی جدید، به‌عنوان یک راهکار ضروری شناخته می‌شود. نهار و همکاران، بر اساس فرض عدم اعتماد به هیچ کاربری یا دستگاهی، نیاز به احراز هویت مداوم و ارزیابی ریسک‌ها را برجسته می‌کند.

جان لوان در [۱۷] به بررسی معماری اعتماد صفر در بانکداری دیجیتال می‌پردازد و به چالش‌های امنیتی ناشی از تحول دیجیتال اشاره می‌کند. این معماری به عنوان یک الگوی امنیتی مؤثر، نیاز به تأیید مداوم هویت‌ها و کاهش سطح حملات را مطرح می‌کند. نتایج نشان می‌دهند که پیاده‌سازی معماری نه تنها امنیت را تقویت می‌کند، بلکه انطباق با الزامات نظارتی را نیز تسهیل می‌نماید.

اشفق و همکاران مقاله [۱۸] به تحلیل پارادایم امنیتی اعتماد صفر پرداخته و بر لزوم تغییر از مدل‌های سنتی به این رویکرد تأکید می‌کند. یافته‌ها نشان می‌دهند که این پارادایم با تأکید بر "هرگز اعتماد نکن، همیشه تأیید کن" می‌تواند امنیت را به طور قابل توجهی افزایش دهد. چالش‌های پیاده‌سازی شامل مقاومت سازمانی و نیاز به توازن بین امنیت و تجربه کاربری است. در نهایت پیشنهاداتی برای استراتژی‌های مؤثر در تطابق با این رویکرد ارائه می‌دهد. در [۱۹] به بررسی معماری اعتماد صفر و تأثیر آن بر امنیت اطلاعات می‌پردازد و با مرور ادبیات موجود، چالش‌ها و فرصت‌های پذیرش این مدل را شناسایی می‌کند. نتایج نشان می‌دهند که باوجود پتانسیل بالای این معماری، موانع مفهومی و عملیاتی قابل توجهی در مسیر پذیرش آن وجود دارد. همچنین، ایجاد درک صحیح از این مدل برای کاهش شک‌وترددید در پذیرش آن حیاتی است.

چاندری و همکاران در [۱۱] به بررسی مدل امنیتی مبتنی بر اعتماد صفر در بانکداری می‌پردازد و تأکید می‌کند که با افزایش حملات سایبری، نیاز به یک چارچوب امنیتی قوی ضروری است. این مدل با استفاده از الگوریتم‌های اجماع بلاک‌چین، اطمینان از یکپارچگی و غیرقابل تغییر بودن تراکنش‌ها را فراهم می‌کند. همچنین، اصول اعتماد صفر به تأیید مداوم هویت کاربران و دستگاه‌ها می‌پردازد تا امنیت را افزایش دهد. ادغام این دو رویکرد می‌تواند به بهبود حفاظت از دارایی‌های بانک‌ها و کاهش آسیب‌پذیری‌ها کمک کند.

سارکار و همکاران در [۲۰] به بررسی امنیت شبکه‌های صفر اعتماد در رایانش ابری می‌پردازد و تأکید دارد که هیچ نهادی به طور ضمنی قابل اعتماد نیست. هدف آن کمک به سازمان‌ها برای بهبود امنیت و دستیابی به بلوغ در پیاده‌سازی این معماری است.

در فصل ۱۲ کتاب [۲۱]، در یک مقاله به بررسی معماری اعتماد صفر در صنعت بانکداری و فین‌تک می‌پردازد و بر ضرورت همکاری در اکوسیستم‌های مبتنی بر API و چالش‌های امنیت اطلاعات تأکید دارد. این فصل عناصر کلیدی این معماری شامل احراز هویت کاربران، مدیریت دستگاه‌ها، و کنترل دسترسی به منابع را معرفی می‌کند. پیاده‌سازی مؤثر معماری اعتماد صفر مستلزم توجه مدیریت به طراحی مناسب و اجرای اصل حداقل دسترسی است. در این نوشتار، اعتماد صفر به‌عنوان یک راهکار راهبردی برای کاهش خطرات سایبری و حفاظت از داده‌ها در محیط‌های پیچیده مالی مطرح می‌شود.

گوپتا در [۲۲]، تحول در امنیت سایبری اشاره می‌کند، و به شرح اعتماد صفر به تأیید مداوم و احراز هویت در برابر تهدیدات پویا تأکید دارد و مدل‌های امنیتی قدیمی را به چالش می‌کشد. ارکان اصلی: شامل هویت، دستگاه، شبکه، بار کاری برنامه و داده است که هر یک به تأمین امنیت و کاهش سطح تهدید کمک می‌کند. در این مقاله نقش شبکه‌های خصوصی مجازی^۵ برای ایجاد ارتباطات امن و رمزگذاری شده در سازمان‌ها حیاتی هستند و امنیت داده‌ها را در حین انتقال تضمین می‌کنند.

^۴ 6G

^۵ VPN

سلمنت در [۱] به بررسی پیاده سازی مدل اعتماد صفر در مؤسسات مالی می پردازد و بر حفاظت از داده ها، مدیریت هویت و دسترسی^۶ و امنیت دستگاه و شبکه تأکید دارد. چارچوب پیشنهادی از طریق توسعه یک اپلیکیشن بانکی دمو ارزیابی شده و نقاط قوت و چالش های آن مورد بحث قرار می گیرد. مؤسسات مالی با اجرای این مدل می توانند تأیید مداوم کاربران و دستگاه ها را بهبود بخشند و امنیت اطلاعات حساس را تضمین کنند.

نورعلی و همکاران در [۲۳] به بررسی ادغام مدل اعتماد صفر و فناوری بلاک چین در سیستم های بانکی آنلاین می پردازد و تأکید دارد که این رویکرد می تواند امنیت سایبری را به طور چشمگیری تقویت کند. مدل اعتماد صفر با تأیید مداوم درخواست های دسترسی، خطر دسترسی غیرمجاز را کاهش می دهد، در حالی که بلاک چین با ایجاد یک دفتر کل غیرقابل تغییر، از تقلب و دست کاری داده ها جلوگیری می کند. این ادغام به مؤسسات مالی کمک می کند تا یک زیرساخت امنیتی قوی و مقاوم در برابر تهدیدات سایبری ایجاد کنند و به حفاظت از اطلاعات حساس مشتریان و بهبود مدیریت هویت منجر می شود.

نعیم و همکاران در مقاله [۶] به تحلیل مدل امنیتی اعتماد صفر و اهمیت احراز هویت و کنترل دسترسی در زیرساخت های حیاتی می پردازد. همچنین، چالش ها و نیاز به تحقیقات بیشتر برای پیاده سازی مؤثر این مدل در محیط های پیچیده مورد بررسی قرار می گیرد. همچنین سعید قاسمی و همکاران در [۲۴] به بررسی کاربردها و چالش های معماری اعتماد صفر می پردازد و نشان می دهد که این مدل با وجود پتانسیل بالا برای تقویت امنیت، با موانع فرهنگی و فنی قابل توجهی در پیاده سازی مواجه است. ادغام آن با فناوری های نوین مانند هوش مصنوعی می تواند به بهبود کارایی امنیتی کمک کند.

دیپا آجیش در [۲۵] با موضوع اهمیت هوش مصنوعی در فناوری های اعتماد صفر، به بررسی نقش کلیدی هوش مصنوعی در تقویت امنیت سایبری می پردازد. با افزایش استفاده از خدمات ابری، مدل های اعتماد صفر به عنوان راهکارهای جدید برای مقابله با تهدیدات سایبری ضروری شده اند. این مقاله تأکید می کند که هوش مصنوعی می تواند به شناسایی تهدیدات و بهبود فرایندهای امنیتی کمک کند. همچنین، جمع آوری داده های زمینه ای به هوش مصنوعی امکان می دهد تا واکنش های دقیق تری به رویدادهای امنیتی ارائه دهد.

یوانهانگ و همکاران در [۲۶] چالش ها و روندهای آینده به بررسی مدل امنیتی اعتماد صفر می پردازد که بر اساس تأیید هویت کاربران و دستگاه ها در همه شبکه ها طراحی شده است. این مقاله به چالش های موجود در پذیرش این مدل و اجزای کلیدی آن، از جمله احراز هویت، کنترل دسترسی و ارزیابی اعتماد، اشاره دارد و بر ضرورت تحقیقات بیشتر در این حوزه تأکید می کند.

مقاله [۲۷] به تحلیل چالش ها و مزایای مدل امنیت اعتماد صفر در سازمان ها می پردازد. باتوجه به نیاز به کار از راه دور ناشی از پاندمی COVID19، این رویکرد امنیتی به عنوان یک راهکار ضروری برای مقابله با آسیب پذیری های جدید مطرح شده است. نویسندگان، کرنیلیوس ایتودو و مورات اوزر، یک چارچوب مفهومی جامع برای هدایت فرایند پیاده سازی این مدل ارائه می دهند که شامل ارزیابی وضعیت کنونی و آینده، نقشه راه پیاده سازی و نظارت مستمر است.

جدول ۱- مقایسه کلی مطالعات انجام شده در باره اعتماد صفر

منبع	موضوع اصلی	مفاهیم کلیدی	اجزای اصلی	چالش ها	کاربردها و پیشنهادات
NIST SP 800207 [4]	معرفی و تبیین معماری اعتماد صفر	اصل "هرگز اعتماد نکن، همیشه تأیید کن"	احراز هویت چندعاملی (MFA) میکرو قطع بندی زیرساخت نرم افزار تعریف شده (SDI)	پیچیدگی پیاده سازی نیاز به تغییر فرهنگ سازمانی	راهنمای عملی برای معماران امنیت سایبری مناسب برای مدیریت کاربران از راه دور و دارایی های ابری

۷ ارائه راهکار پیاده سازی اعتماد صفر در سیستم‌های نظارت تصویری / سید علی صموتی ، سجاد طرهانی ، حسام حسن‌پور

منبع	موضوع اصلی	مفاهیم کلیدی	اجزای اصلی	چالش‌ها	کاربردها و پیشنهادات
استراتژی DoD [۱۴]	استراتژی اعتماد صفر وزارت دفاع آمریکا	چهار هدف: فرهنگ‌سازی، تأمین سیستم‌ها، شتاب‌دهی فناوری، توانمندسازی	احراز هویت چندعاملی میکرو قطاع‌بندی	مقاومت سازمانی نیاز به آموزش و فرهنگ‌سازی	کاهش سطح حمله افزایش امنیت در برابر تهدیدات سایبری
هریشکی [۱۵]	تأثیر فناوری‌های نوظهور بر اعتماد صفر	ادغام AI، ML، بلاک‌چین و محاسبات کوانتومی	احراز هویت مداوم ارزیابی ریسک	پیچیدگی‌های فناوری جدید نیاز به تطبیق مداوم	تطبیق استراتژی‌ها با پیشرفت‌های فناوری تقویت امنیت سایبری
مدل بلوغ CISA [۱۶]	مدل بلوغ اعتماد صفر	پنج رکن: شناسایی، دستگاه‌ها، شبکه‌ها، برنامه‌ها، داده‌ها	احراز هویت کنترل دسترسی ارزیابی مداوم	همکاری بین سطوح سازمانی موانع عملیاتی	پیاده‌سازی تدریجی بهبود وضعیت امنیت سایبری
پونام [۱۲]	اصول و چالش‌های اعتماد صفر	اصول اساسی: عدم اعتماد پیش‌فرض، تأیید مداوم	احراز هویت کنترل دسترسی اتوماسیون امنیتی	موانع فنی و فرهنگی پیچیدگی پیاده‌سازی	استفاده از AI و بلاک‌چین تحقیقات در احراز هویت و اتوماسیون
نهار و همکاران [۳]	اعتماد صفر در شبکه‌های G6	نیاز به احراز هویت مداوم در شبکه‌های پیچیده	ارزیابی ریسک کنترل دسترسی	افزایش پیچیدگی‌های امنیتی تعداد بالای دستگاه‌ها	امنیت شبکه‌های نسل ششم مدیریت دستگاه‌های متصل
جان لوان [۱۷]	اعتماد صفر در بانکداری دیجیتال	تأیید مداوم هویت‌ها کاهش سطح حمله	احراز هویت مدیریت دسترسی	چالش‌های تحول دیجیتال انطباق با مقررات	تقویت امنیت و انطباق نظارتی در بانکداری
اشفق و همکاران [۱۸]	تحلیل پارادایم اعتماد صفر	تغییر از مدل‌های سنتی به اعتماد صفر	احراز هویت کنترل دسترسی	مقاومت سازمانی توازن امنیت و تجربه کاربری	استراتژی‌های مؤثر برای پیاده‌سازی
چاندری و همکاران [۱۱]	اعتماد صفر و بلاک‌چین در بانکداری	افزایش ۱۳۱۸٪ حملات سایبری ادغام بلاک‌چین و اعتماد صفر	الگوریتم‌های اجماع بلاک‌چین تأیید هویت مداوم	پیچیدگی ادغام فناوری‌ها	حفاظت از دارایی‌های بانکی کاهش آسیب‌پذیری‌ها
سارکار و همکاران [۲۰]	اعتماد صفر در رایانش ابری	عدم اعتماد ضمنی به هیچ نهادی	احراز هویت کنترل دسترسی	پیچیدگی‌های ابری	بهبود امنیت در محیط‌های ابری

منبع	موضوع اصلی	مفاهیم کلیدی	اجزای اصلی	چالش‌ها	کاربردها و پیشنهادات
کتاب فصل ۱۲ [۲۱]	اعتماد صفر در بانکداری و فین تک	همکاری در اکوسیستم‌های API اصل حداقل دسترسی	احراز هویت مدیریت دستگاه و دسترسی	نیاز به بلوغ سازمانی	کاهش خطرات سایبری حفاظت از داده‌ها
گوپتا [۲۲]	تحول در امنیت سایبری با اعتماد صفر	تأیید مداوم در برابر تهدیدات پویا	هویت، دستگاه، شبکه، برنامه، داده VPN برای ارتباطات امن	تغییر مدل‌های قدیمی پیچیدگی پیاده‌سازی	تضمین امنیت داده‌ها در انتقال
سلمنت [۱]	اعتماد صفر در مؤسسات مالی	حفاظت از داده‌ها و مدیریت هویت	احراز هویت مداوم امنیت دستگاه و شبکه	چالش‌های پیاده‌سازی اپلیکیشن	بهبود امنیت اطلاعات حساس
نورعلی و همکاران [۲۳]	ادغام بلاک چین و اعتماد صفر در بانکداری	دفترکل غیرقابل تغییر بلاک چین تأیید مداوم دسترسی	احراز هویت مدیریت هویت	پیچیدگی ادغام فناوری‌ها	ایجاد زیرساخت امنیتی قوی حفاظت از داده‌های مشتریان
نعیم و همکاران [۶]	اعتماد صفر در زیرساخت‌های حیاتی	اهمیت احراز هویت و کنترل دسترسی	ارزیابی ریسک مدیریت دسترسی	پیچیدگی محیط‌های حیاتی	تحقیقات بیشتر برای پیاده‌سازی مؤثر
سعید قاسمی و همکاران [۲۴]	کاربردها و چالش‌های اعتماد صفر	پتانسیل بالا برای امنیت	احراز هویت اتوماسیون امنیتی	موانع فرهنگی و فنی	ادغام با AI برای بهبود کارایی
دیپا آجیش [۲۵]	نقش AI در اعتماد صفر	شناسایی تهدیدات با AI جمع‌آوری داده‌های زمینه‌ای	تحلیل امنیتی اتوماسیون	پیچیدگی ادغام AI	بهبود فرایندهای امنیتی واکنش دقیق به تهدیدات
یوانهانگ و همکاران [۲۶]	چالش‌ها و روندهای آینده اعتماد صفر	تأیید هویت و کنترل دسترسی در همه شبکه‌ها	احراز هویت ارزیابی اعتماد	موانع پذیرش	تحقیقات بیشتر برای بهبود مدل
ایتودو و اوزر [۲۷]	اعتماد صفر در دوران کار از راه دور	چارچوب مفهومی برای پیاده‌سازی	ارزیابی وضعیت نظارت مستمر	آسیب‌پذیری‌های کار از راه دور	نقشه‌راه پیاده‌سازی نظارت مداوم

در یک شرکت بزرگ، کارمندان مختلف به سیستم‌های داخلی دسترسی دارند، با پیاده‌سازی مدل اعتماد صفر، هر کارمند باید هویت خود را هر بار که به یک منبع حساس دسترسی پیدا می‌کند، تصدیق کند در معماری گذشته تهدیدها فقط از خارج شبکه محسوب می‌شد؛ اما با رویکرد اعتماد صفر در داخل نیز تهدیدها برشمارده می‌شوند. در سازمانی دیگر، اطلاعات مشتریان به شدت حساس هستند و برای حفاظت از آن‌ها، داده‌ها رمزنگاری می‌شوند. در این حالت، حتی اگر نفوذی به سیستم صورت گیرد، هکرها

نمی‌توانند به داده‌های رمزنگاری شده دسترسی پیدا کنند و تنها افرادی که مجوز دارند می‌توانند کلیدهای رمزگشایی را دریافت کنند. در بیمارستانی، پزشکان و پرستاران نیاز دارند که به اطلاعات بیماران دسترسی داشته باشند، اما تنها پزشکان مجاز به تغییر اطلاعات پزشکی هستند. با پیاده‌سازی مدل اعتماد صفر، سیستم به طور خودکار بررسی می‌کند که آیا کاربر مجاز به انجام این عمل هست یا خیر و در صورت عدم وجود مجوز، دسترسی را مسدود می‌کند. در یک شرکت نرم‌افزاری، برای شناسایی رفتارهای مشکوک از سیستم‌های نظارتی استفاده می‌شود. اگر یک کارمند به طور غیرمعمولی به اطلاعات حساس دسترسی پیدا کند، سیستم به طور خودکار هشدار می‌دهد و مدیران می‌توانند بررسی کنند که آیا این دسترسی مجاز بوده است یا خیر. [۲۶، ۲۵، ۲۳، ۱۵، ۱۲، ۵، ۳]

در نهایت، در یک سازمان امنیت سایبری، وقتی که یک حمله سایبری شناسایی می‌شود، تیم امنیتی بلافاصله اقدام می‌کند. با استفاده از مدل اعتماد صفر، آن‌ها می‌توانند دسترسی‌های مشکوک را مسدود کنند و به سرعت به تهدیدات پاسخ دهند، بدون اینکه نیاز به بررسی تمام سیستم‌ها داشته باشند. [۲۴، ۲۲، ۲۱]

مدل‌های سنتی امنیت شبکه که عمدتاً بر پایه فرض اعتماد به کاربران و دستگاه‌های داخلی و جداسازی محیط داخلی از تهدیدات خارجی طراحی شده‌اند، در برابر تهدیدات مدرن و پیچیده امروزی ناکارآمد هستند. این مدل‌ها باتکیه بر مرزهای شبکه‌ای و اعتماد پیش‌فرض به اجزای داخلی، قادر به پاسخگویی به نیازهای امنیتی سیستم‌های نظارت تصویری در محیط‌های پویا و پیچیده کنونی نیستند. این محدودیت‌ها، ضرورت بازنگری در رویکردهای امنیتی و حرکت به سوی راهکارهای نوین را اجتناب‌ناپذیر کرده است.

معماری اعتماد صفر به عنوان یک رویکرد نوآورانه در امنیت سایبری، با تأکید بر اصل «هیچ‌گاه اعتماد نکن، همیشه تأیید کن»، راهکاری مؤثر برای مقابله با این چالش‌ها ارائه می‌دهد. این معماری با استفاده از احراز هویت مداوم، اصل حداقل دسترسی، رمزنگاری داده‌ها و نظارت بلادرنگ، امکان مدیریت دقیق‌تر دسترسی‌ها و کاهش سطح حمله را فراهم می‌کند. در حوزه سیستم‌های نظارت تصویری، این رویکرد می‌تواند با اعمال سیاست‌های امنیتی پویا و مبتنی بر هویت، از نفوذ غیرمجاز و سوءاستفاده از داده‌های حساس جلوگیری کند.

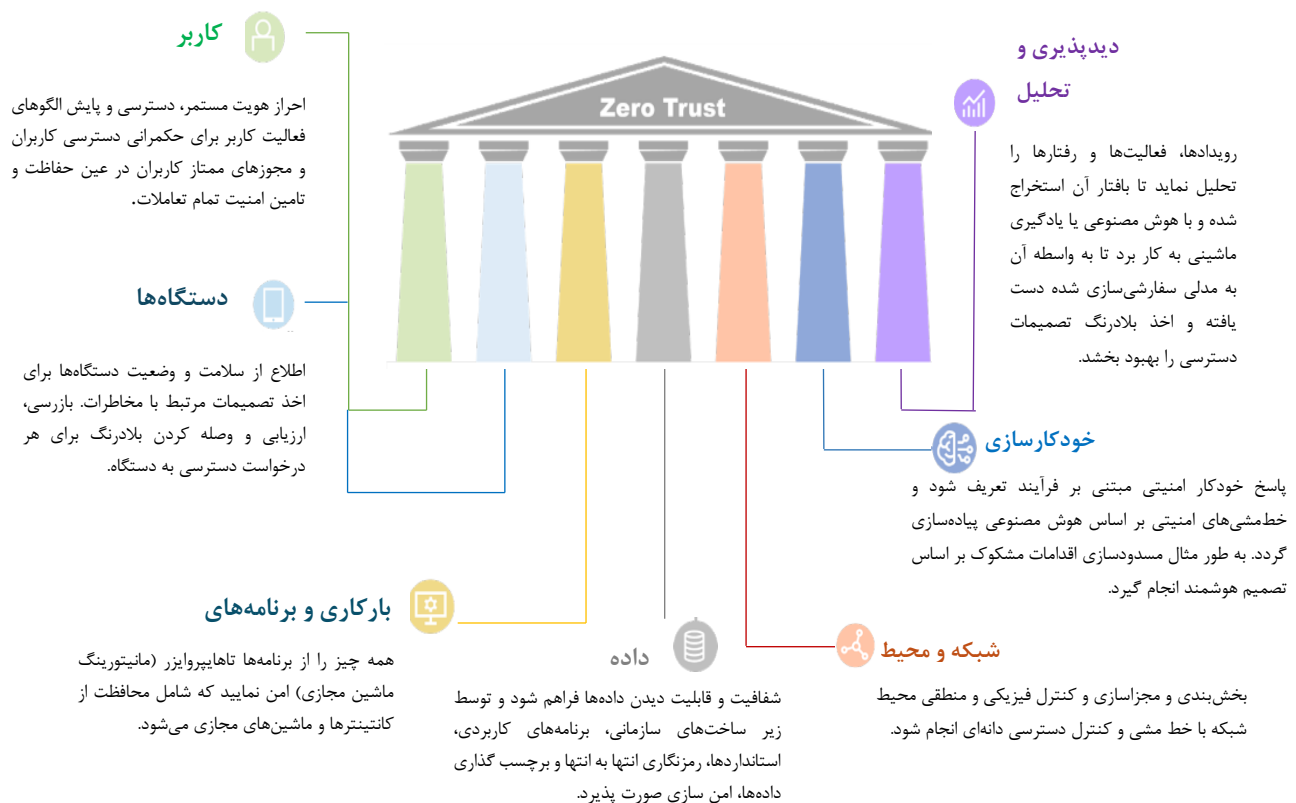
باوجود مزایای بالقوه، پیاده‌سازی معماری اعتماد صفر در سیستم‌های نظارت تصویری با چالش‌هایی نظیر نیاز به بازطراحی زیرساخت‌های امنیتی، هماهنگی میان دستگاه‌های متنوع، مدیریت هویت و دسترسی در مقیاس بزرگ، و حفظ عملکرد سیستم در حین اعمال سیاست‌های امنیتی همراه است. علاوه بر این، انطباق با الزامات قانونی و استانداردهای امنیتی مرتبط با داده‌های تصویری، پیچیدگی‌های بیشتری را به این فرایند اضافه می‌کند. این پژوهش باهدف بررسی جامع مفاهیم، چالش‌ها و فرصت‌های معماری اعتماد صفر، به دنبال ارائه یک چارچوب کاربردی برای ارتقای امنیت سیستم‌های نظارت تصویری است. این چارچوب با تمرکز بر کاهش آسیب‌پذیری‌ها و مقابله با تهدیدات سایبری، راهکارهایی علمی و عملی برای پیاده‌سازی این معماری در محیط‌های واقعی ارائه خواهد داد.

۳- مفهوم معماری اعتماد صفر و ارکان آن

معماری اعتماد صفر به عنوان یک مدل امنیتی، بر این باور است که باید به طور مداوم هویت و اعتبار هر کاربر و دستگاهی که به شبکه متصل می‌شود، تأیید شود. این مدل به‌ویژه در دنیای امروز که تهدیدات سایبری پیچیده‌تر و متنوع‌تر شده‌اند، اهمیت بیشتری پیدا کرده است. برخلاف مدل‌های سنتی که بر فرضیات اعتماد به کاربران داخلی شبکه تکیه دارند، اعتماد صفر هیچ‌گونه اعتماد پیش‌فرضی را نمی‌پذیرد و تمامی تعاملات و دسترسی‌ها را به‌دقت بررسی می‌کند. [۲۶، ۲۳، ۱۴، ۱۲، ۵، ۴، ۱۰]

ارکان اصلی معماری اعتماد صفر شامل احراز هویت مداوم، اصل حداقل دسترسی، رمزنگاری داده‌ها، نظارت و تحلیل مداوم، و یکپارچگی و اتوماسیون فرایندهای امنیتی است. این ارکان به‌عنوان ستون‌های اصلی، با یکدیگر در ارتباط هستند تا یک ساختار امنیتی جامع ایجاد کنند. به طور مثال، احراز هویت مداوم و اصل حداقل دسترسی با تحلیل مداوم فعالیت‌ها ترکیب می‌شوند تا دسترسی‌ها به‌صورت پویا مدیریت شوند. همچنین، رمزنگاری داده‌ها و نظارت مداوم از داده‌ها در برابر تهدیدات محافظت می‌کنند و اتوماسیون فرایندها تضمین می‌کند که پاسخ به تهدیدات به‌سرعت و بدون خطا انجام شود. (شکل ۲) [۱۹، ۶۴، ۲]

یکی از اصول اصلی معماری اعتماد صفر، احراز هویت مداوم^۷ است. در این اصل، هویت کاربران و دستگاه‌ها نه‌تنها در لحظه ورود به سیستم، بلکه در طول مدت فعالیت آن‌ها نیز به طور مداوم بررسی می‌شود. این فرایند شامل استفاده از احراز هویت چندعاملی، بررسی رفتارهای کاربری و تحلیل داده‌های مربوط به دسترسی است. این رویکرد اطمینان می‌دهد که حتی اگر یک کاربر معتبر به شبکه دسترسی پیدا کند، رفتار غیرعادی او شناسایی و مسدود می‌شود. [۱۹، ۶، ۴، ۲]



شکل ۳: ارکان اعتماد صفر [۱۴]

معماری اعتماد صفر بر اصل حداقل دسترسی تأکید دارد. این اصل به این معناست که هر کاربر یا دستگاه تنها به منابع و اطلاعاتی دسترسی دارد که برای انجام وظایف خود به آن نیاز دارد. این رویکرد نه‌تنها سطح دسترسی‌ها را محدود می‌کند، بلکه در صورت وقوع یک نفوذ، دامنه آسیب‌پذیری را به حداقل می‌رساند. پیاده‌سازی این اصل نیازمند تعریف دقیق نقش‌ها و مجوزها در شبکه است. [۲۷، ۱۷، ۱۳، ۶، ۵]

⁷ Continous Authentication

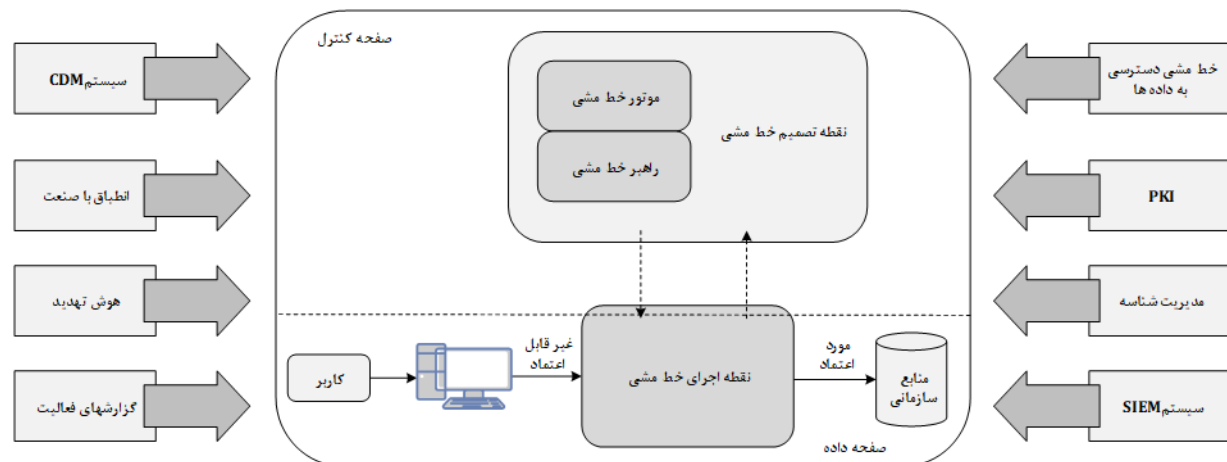
یکی دیگر از ارکان مهم اعتماد صفر، رمزنگاری تمامی داده‌ها در تمامی مراحل انتقال و ذخیره‌سازی است. این اصل تضمین می‌کند که حتی اگر داده‌ها توسط مهاجمان رهگیری شوند، قابل استفاده نباشند. علاوه بر این، استفاده از پروتکل‌های امن مانند TLS و VPN و همچنین مدیریت کلیدهای رمزنگاری به صورت متمرکز، از جمله اقداماتی است که در این راستا انجام می‌شود. [۲۶، ۲۳، ۲۰، ۱۸، ۱۵، ۳]

نظارت و تحلیل مداوم یکی دیگر از ارکان کلیدی معماری اعتماد صفر است. در این رویکرد، تمامی فعالیت‌ها و تعاملات در شبکه به طور پیوسته بررسی و تحلیل می‌شوند تا هرگونه رفتار غیرعادی یا تهدید بالقوه شناسایی شود. ابزارهایی مانند سیستم‌های تشخیص نفوذ^۸ و تحلیل رفتار کاربری^۹ در این فرایند نقش مهمی ایفا می‌کنند. [۵، ۴، ۲]

معماری اعتماد صفر نیازمند یکپارچگی و اتوماسیون در تمامی فرایندهای امنیتی است. این اصل به سازمان‌ها کمک می‌کند تا بتوانند به سرعت به تهدیدات پاسخ دهند و از وقوع حملات جلوگیری کنند. استفاده از فناوری‌هایی مانند هوش مصنوعی^{۱۰} و یادگیری ماشین^{۱۱} برای شناسایی الگوهای تهدید و ایجاد پاسخ‌های خودکار، از جمله روش‌هایی است که به تحقق این هدف کمک می‌کند. [۱۷، ۱۶، ۵، ۳]

۴- معماری اعتماد صفر

معماری اعتماد صفر به عنوان یکی از پیشرفته‌ترین رویکردهای امنیت سایبری، بر پایه اصل "هرگز اعتماد نکن و همیشه تأیید کن" طراحی شده است. این معماری برای مدیریت دسترسی به منابع سازمانی، از ابزارها و اجزای مختلفی استفاده می‌کند که موتور خط‌مشی^{۱۲} و راهبر خط‌مشی^{۱۳} از مهم‌ترین آن‌ها هستند. این دو بخش، نقش کلیدی در اجرای سیاست‌های امنیتی و مدیریت دسترسی ایفا می‌کنند. در ادامه، به بررسی جزئیات این دو مؤلفه در ادامه توضیح داده می‌شود. (شکل ۳) [۲۶، ۱۴، ۶۴، ۲]



شکل ۴: مولفه‌های منطقی هسته معماری اعتماد صفر [۴]

⁸ IDS : Intrusion Detection Systems

⁹ UBA : User Behavior Analytics

¹⁰ AI : Artificial Intelligence

¹¹ ML : Machine learning

¹² Policy Engine

¹³ Policy Administrator

۴-۱- موتور خطمشی

موتور خطمشی، قلب تصمیم‌گیری در معماری اعتماد صفر است. این مؤلفه مسئول ارزیابی درخواست‌های دسترسی و تصمیم‌گیری درباره اجازه یا عدم اجازه دسترسی به منابع است. موتور خطمشی بر اساس مجموعه‌ای از قوانین و سیاست‌های امنیتی که توسط سازمان تعریف شده‌اند، عمل می‌کند. این قوانین می‌توانند شامل معیارهایی مانند هویت کاربر، وضعیت دستگاه، مکان جغرافیایی، زمان درخواست و حتی نوع داده‌های مورد درخواست باشند. به‌طور کلی، موتور خطمشی وظیفه دارد که تمامی داده‌های مرتبط با درخواست دسترسی را تحلیل کرده و بر اساس سیاست‌های تعریف‌شده، تصمیم‌نهایی را اتخاذ کند. این تصمیم‌گیری‌ها به‌صورت پویا انجام می‌شوند و بر اساس تغییرات در محیط یا وضعیت کاربران، به‌روزرسانی می‌شوند. این ویژگی باعث می‌شود که موتور خطمشی بتواند به‌طور مؤثر به تهدیدات جدید پاسخ دهد. [۴، ۶]

۴-۲- منابع داده برای موتور خطمشی

برای اینکه موتور خطمشی بتواند تصمیمات دقیقی بگیرد، نیاز به دسترسی به منابع داده مختلف دارد. این منابع شامل اطلاعات مربوط به کاربران (مانند هویت و نقش آن‌ها)، وضعیت دستگاه‌ها (مانند به‌روزرسانی‌ها و سطح امنیتی)، رفتارهای کاربران (مانند الگوهای دسترسی معمول) و حتی داده‌های محیطی (مانند مکان جغرافیایی و زمان) می‌شوند. یکی از مهم‌ترین منابع داده‌ای برای موتور خطمشی، سیستم‌های مدیریت هویت و دسترسی^{۱۴} است که اطلاعات هویتی کاربران را فراهم می‌کند. همچنین، ابزارهای مدیریت دستگاه‌های موبایل^{۱۵} و سیستم‌های تشخیص تهدید^{۱۶} نیز اطلاعاتی درباره وضعیت دستگاه‌ها و تهدیدات احتمالی ارائه می‌دهند. موتور خطمشی با تجمیع این داده‌ها و تحلیل آن‌ها، می‌تواند تصمیمات امنیتی دقیقی بگیرد. [۴، ۶]

۴-۳- راهبر خطمشی:

راهبر خطمشی، به‌عنوان یک مؤلفه اجرایی در معماری اعتماد صفر، وظیفه دارد که تصمیمات گرفته‌شده توسط موتور خطمشی را اجرا کند. این مؤلفه مستقیماً با زیرساخت‌های فناوری اطلاعات سازمان در ارتباط است و دستورات لازم برای اعمال سیاست‌های امنیتی را به آن‌ها ارسال می‌کند. به‌عنوان مثال، اگر موتور خطمشی تصمیم بگیرد که دسترسی یک کاربر به یک منبع خاص مسدود شود، راهبر خطمشی این تصمیم را به سیستم‌هایی مانند فایروال‌ها، کنترل‌کننده‌های دسترسی یا پروکسی‌ها ارسال می‌کند. به همین ترتیب، اگر دسترسی مجاز باشد، راهبر خطمشی مجوز لازم را صادر می‌کند و مسیر ارتباطی را باز می‌کند. این مؤلفه به‌عنوان پل ارتباطی بین تصمیم‌گیری و اجرای سیاست‌ها عمل می‌کند. [۴، ۶]

۴-۴- تعامل موتور خطمشی و راهبر خطمشی:

تعامل بین موتور خطمشی و راهبر خطمشی یکی از مهم‌ترین جنبه‌های معماری اعتماد صفر است. موتور خطمشی تمامی اطلاعات لازم برای تصمیم‌گیری را از منابع داده جمع‌آوری می‌کند و پس از تحلیل آن‌ها، تصمیم‌نهایی را اتخاذ می‌کند. این تصمیم سپس به راهبر خطمشی ارسال می‌شود تا اجرا شود. این تعامل باید به‌صورت بلادرنگ و بدون تأخیر انجام شود تا کاربران بتوانند به‌سرعت به منابع موردنیاز خود دسترسی پیدا کنند. از سوی دیگر، این تعامل باید به‌گونه‌ای طراحی شود که از هرگونه ضعف یا آسیب‌پذیری جلوگیری کند. برای این منظور، از پروتکل‌های امن و مکانیزم‌های رمزنگاری برای ارتباط بین این دو مؤلفه استفاده می‌شود. [۴، ۵، ۱۹، ۲۶]

¹⁴ IAM : Identity and Access Management

¹⁵ MDM : Mobile Device Management

¹⁶ Threat Detection Systems

۴-۵- چالش‌های پیاده‌سازی موتور و راهبر خطمشی:

پیاده‌سازی مؤلفه‌های موتور خطمشی و راهبر خطمشی با چالش‌های متعددی همراه است. یکی از این چالش‌ها، نیاز به هماهنگی بین منابع داده مختلف است. برای اینکه موتور خطمشی بتواند تصمیمات دقیقی بگیرد، باید داده‌های متنوعی از منابع مختلف جمع‌آوری شود. این فرایند ممکن است به دلیل ناسازگاری بین سیستم‌ها یا کمبود داده‌های به‌روز، با مشکل مواجه شود. چالش دیگر مربوط به عملکرد راهبر خطمشی است. این مؤلفه باید به‌گونه‌ای طراحی شود که بتواند تصمیمات موتور خطمشی را به‌سرعت و بدون ایجاد تأخیر اجرا کند. در سازمان‌های بزرگ با حجم بالای درخواست‌های دسترسی، این موضوع می‌تواند به یک چالش جدی تبدیل شود. علاوه بر این، امنیت ارتباط بین موتور و راهبر خطمشی نیز باید به‌دقت مدیریت شود تا از هرگونه سوءاستفاده جلوگیری شود. [۴، ۵، ۱۹، ۲۶]

۴-۶- نقش موتور و راهبر خطمشی در بهبود امنیت سازمان:

موتور خطمشی و راهبر خطمشی، به‌عنوان دو مؤلفه کلیدی در معماری اعتماد صفر، نقش مهمی در بهبود امنیت سازمان ایفا می‌کنند. موتور خطمشی با تحلیل دقیق داده‌ها و اتخاذ تصمیمات مبتنی بر سیاست‌های امنیتی، از دسترسی غیرمجاز به منابع جلوگیری می‌کند. از سوی دیگر، راهبر خطمشی با اجرای سریع و دقیق این تصمیمات، از ایجاد شکاف‌های امنیتی جلوگیری می‌کند. این دو مؤلفه با همکاری یکدیگر، امکان مدیریت پویا و بلادرنگ دسترسی‌ها را فراهم می‌کنند. این ویژگی به سازمان‌ها این امکان را می‌دهد که به‌سرعت به تهدیدات جدید پاسخ دهند و امنیت اطلاعات خود را تضمین کنند. به‌طور کلی، موتور خطمشی و راهبر خطمشی با ایجاد یک‌لایه اضافی از کنترل و نظارت، امنیت کلی سازمان را به‌طور قابل‌توجهی افزایش می‌دهند و به تحقق اهداف معماری اعتماد صفر کمک می‌کنند. [۴، ۵، ۱۹، ۲۶]

۵- روش‌های پیاده‌سازی معماری اعتماد صفر

معماری اعتماد صفر به‌عنوان یک رویکرد نوین در امنیت سایبری، به‌ویژه در دنیای پیچیده و متغیر فناوری اطلاعات امروز، به‌طور فزاینده‌ای موردتوجه قرار گرفته است. این معماری بر اساس اصل «هرگز به هیچ‌کس اعتماد نکن» طراحی شده و شامل چندین مدل مختلف است که هر یک به‌منظور تأمین امنیت منابع و اطلاعات سازمان‌ها طراحی شده‌اند. در این راستا، چهار مدل اصلی برای پیاده‌سازی معماری اعتماد صفر شناسایی شده‌اند: مدل مبتنی بر شبکه^{۱۷}، مدل مبتنی بر کاربر^{۱۸}، مدل مبتنی بر دستگاه^{۱۹} و مدل ترکیبی^{۲۰}. [۱، ۵، ۱۱، ۲۰، ۲۳، ۲۶]

۵-۱- مدل مبتنی بر شبکه

مدل مبتنی بر شبکه، به‌عنوان یکی از اساسی‌ترین رویکردها در معماری اعتماد صفر، بر پایه قطاع‌بندی شبکه^{۲۱} و شبکه‌های تعریف شده مبتنی بر نرم‌افزار^{۲۲} استوار است. قطاع‌بندی شبکه به معنای ایجاد بخش‌های کوچک‌تر و ایزوله در شبکه است که هر بخش می‌تواند سیاست‌های امنیتی خاص خود را داشته باشد. این امر به سازمان‌ها این امکان را می‌دهد که ترافیک بین بخش‌ها را به‌دقت کنترل کنند و از انتقال تهدیدات از یک بخش به بخش دیگر جلوگیری نمایند.

¹⁷ Network-Centric

¹⁸ User-Centric

¹⁹ Device-Centric

²⁰ Hybrid Model

²¹ Micro-Segmentation

²² SDN : Software Define Network

از سوی دیگر، شبکه‌های تعریف‌شده با نرم‌افزار به سازمان‌ها این امکان را می‌دهند که شبکه‌ها را به‌صورت مرکزی مدیریت کنند و سیاست‌های امنیتی را به‌سرعت اعمال کنند. این فناوری به‌ویژه در محیط‌های پویا و پیچیده که نیاز به تغییرات سریع در ساختار شبکه وجود دارد، مفید است. به‌طور کلی، مدل مبتنی بر شبکه با کاهش سطح حمله و کنترل دقیق‌تر بر ترافیک، امنیت کلی سازمان را به طور قابل توجهی افزایش می‌دهد. [۱، ۵، ۱۱، ۲۰، ۲۳، ۲۶]

۲-۵- مدل مبتنی بر کاربر

مدل مبتنی بر کاربر، بر احراز هویت و کنترل دسترسی کاربران تأکید دارد و معمولاً از روش‌های احراز هویت چندعاملی و ورود یک‌باره^{۲۳} بهره می‌برد. احراز هویت چندعاملی به معنای استفاده از دو یا چند روش تأیید هویت است که می‌تواند شامل ترکیبی از رمز عبور، کد ارسال‌شده به تلفن همراه، یا احراز هویت بیومتریک باشد. این رویکرد به طور قابل توجهی امنیت دسترسی به سیستم‌ها را افزایش می‌دهد و ریسک دسترسی غیرمجاز را به حداقل می‌رساند. ورود یک‌باره نیز به کاربران این امکان را می‌دهد که با یک مجموعه اعتبارنامه به چندین سیستم و برنامه دسترسی داشته باشند. این روش نه تنها تجربه کاربری را بهبود می‌بخشد، بلکه احتمال افشای رمز عبور را نیز کاهش می‌دهد. با توجه به اینکه کاربران معمولاً از چندین سیستم و برنامه استفاده می‌کنند، این مدل به‌ویژه در سازمان‌های بزرگ و پیچیده اهمیت دارد و می‌تواند به طور مؤثری به تأمین امنیت اطلاعات کمک کند. [۱، ۵، ۱۱، ۲۰، ۲۳، ۲۶]

۳-۵- مدل مبتنی بر دستگاه

مدل مبتنی بر دستگاه، به‌عنوان یک رویکرد کلیدی در معماری اعتماد صفر، بر اساس وضعیت دستگاه و اعتبار آن عمل می‌کند. در این مدل، قبل از اینکه یک دستگاه به شبکه متصل شود، باید اعتبار آن مورد بررسی قرار گیرد. این بررسی شامل ارزیابی وضعیت امنیتی، به‌روزرسانی‌های نرم‌افزاری و وجود نرم‌افزارهای مخرب می‌شود. این فرایند به‌عنوان یک لایه اضافی از امنیت عمل می‌کند و به جلوگیری از دسترسی دستگاه‌های آلوده به شبکه کمک می‌کند. علاوه بر این، مدیریت دستگاه‌های موبایل (MDM) به سازمان‌ها این امکان را می‌دهد که دستگاه‌های موبایل را مدیریت و کنترل کنند. این ابزارها شامل نصب نرم‌افزارهای امنیتی و اعمال سیاست‌های امنیتی هستند و به سازمان‌ها کمک می‌کنند تا از بروز مشکلات امنیتی جلوگیری کنند. به‌طور کلی، مدل مبتنی بر دستگاه با تمرکز بر اعتبارسنجی و مدیریت دستگاه‌ها، امنیت شبکه را به طور قابل توجهی افزایش می‌دهد. [۱، ۵، ۱۱، ۲۰، ۲۳، ۲۶]

۴-۵- مدل ترکیبی

مدل ترکیبی، به‌عنوان یک رویکرد جامع و چندوجهی در معماری اعتماد صفر، ترکیبی از مدل‌های مبتنی بر شبکه، کاربر و دستگاه است. این مدل به سازمان‌ها این امکان را می‌دهد که از مزایای هر یک از مدل‌های قبلی بهره‌برداری کنند و راه‌حل‌های امنیتی جامع‌تری ارائه دهند. به‌ویژه در سازمان‌های بزرگ که نیاز به تأمین امنیت در سطوح مختلف دارند، این مدل به‌عنوان یک راهکار مؤثر شناخته می‌شود. ترکیب مدل‌ها به سازمان‌ها این امکان را می‌دهد که به‌سرعت به تغییرات محیطی و تهدیدات جدید پاسخ دهند و سیاست‌های امنیتی را به طور مؤثر تنظیم کنند. با توجه به اینکه سازمان‌ها معمولاً با تهدیدات پیچیده و متنوعی مواجه هستند، استفاده از یک مدل ترکیبی می‌تواند به بهبود امنیت و کاهش ریسک‌ها کمک کند. به‌طور کلی، مدل ترکیبی به‌عنوان یک راهکار مقیاس‌پذیر و بهینه، می‌تواند به سازمان‌ها در تأمین امنیت اطلاعات و منابع خود کمک نماید. [۱، ۵، ۱۱، ۲۰، ۲۳، ۲۶]

²³ Single Sign-On

۶- کاربرد معماری اعتماد صفر در دوربین‌های مدار بسته

با ظهور خدمات ابری و افزایش تعداد دستگاه‌های متصل، شبکه‌ها به شدت پیچیده شده‌اند. جداسازی شبکه‌ها با دیوارهای آتش به دلیل این تحولات، دیگر به تنهایی کارآمد نیست. به عنوان مثال، کارکنان ممکن است از دستگاه‌های شخصی خود برای دسترسی به منابع سازمانی استفاده کنند که این امر باعث افزایش خطرات امنیتی می‌شود. در نتیجه، سازمان‌ها باید به دنبال راه‌حل‌های جدیدی باشند که بتوانند این چالش‌ها را مدیریت کنند. مدل اعتماد صفر بر این اصل استوار است که هیچ موجودیتی به طور ذاتی قابل اعتماد نیست. این رویکرد به سازمان‌ها این امکان را می‌دهد که هر درخواست دسترسی را به دقت بررسی کنند و فقط به کاربرانی که هویت آن‌ها تأیید شده است، اجازه دسترسی به منابع حساس را بدهند. این فرایند شامل تأیید هویت، بررسی رفتار و ارزیابی ریسک است. یکی از ویژگی‌های کلیدی شبکه‌های اعتماد صفر، میکرو قطع‌بندی است. این تکنیک به سازمان‌ها این امکان را می‌دهد که شبکه را به بخش‌های کوچک‌تر تقسیم کنند و برای هر بخش سطوح امنیتی متفاوتی تعیین کنند. به این ترتیب، حتی اگر یک بخش از شبکه به خطر بیفتد، سایر بخش‌ها ایمن باقی می‌مانند. این رویکرد همچنین به شناسایی و محدود کردن تهدیدات کمک می‌کند. [۱، ۱۲، ۱۸]

. با افزایش تعداد دستگاه‌های متصل به شبکه، تأمین امنیت آن‌ها اهمیت بیشتری پیدا می‌کند. بسیاری از دستگاه‌ها ممکن است به روزرسانی‌های امنیتی را دریافت نکنند و در معرض حملات قرار گیرند؛ بنابراین، سازمان‌ها باید از راه‌حل‌های نوآورانه مانند بلاک‌چین برای تأیید اعتبار دستگاه‌ها و کاربران استفاده کنند. این اقدامات به کاهش خطرات امنیتی و افزایش اعتماد به دستگاه‌های متصل کمک می‌کند. تغییر به معماری اعتماد صفر نیازمند آماده‌سازی و برنامه‌ریزی دقیق است. سازمان‌ها باید به تجزیه و تحلیل دقیق ریسک‌ها و نیازهای خود پرداخته و استراتژی‌های مناسبی را برای پیاده‌سازی این مدل امنیتی طراحی کنند. این تغییر نه تنها به افزایش امنیت کمک می‌کند، بلکه می‌تواند به بهبود کارایی و بهره‌وری سازمان‌ها نیز منجر شود. جدول ۲ در باره کاربرد اعتماد صفر در سیستم‌های نظارت تصویری اشاره دارد. [۲۸]

جدول ۲- کاربرد اعتماد صفر در سیستم‌های نظارت تصویری

موضوع	توضیحات	اقدامات کلیدی	مزایا	منابع
چرایی نیاز به اعتماد صفر	با پیچیدگی شبکه‌ها، افزایش دستگاه‌های متصل و تهدیدات سایبری (هک، نفوذ، سرقت داده)، اعتماد صفر از داده‌های حساس دوربین‌ها و شبکه‌ها محافظت می‌کند.	- احراز هویت چندعاملی رمزنگاری داده‌ها - میکرو قطع‌بندی استفاده از بلاک‌چین	حفاظت از حریم خصوصی کاهش خطر نفوذ انطباق با استانداردها (مانند GDPR)	[۱، ۲، ۵، ۱۲، ۱۷، ۱۸، ۲۰، ۲۸]
احراز هویت چندعاملی	استفاده از چندین روش تأیید (رمز عبور، کد یک بار مصرف، بیومتریک) برای جلوگیری از دسترسی غیرمجاز به سیستم‌های نظارت تصویری.	- ترکیب رمز عبور، کدهای ارسالی و بیومتریک - تأیید مداوم هویت	کاهش احتمال نفوذ افزایش امنیت در محیط‌های حساس	[۲، ۵، ۱۷، ۲۰]
قطع‌بندی شبکه	جداسازی شبکه دوربین‌ها از سایر بخش‌های سازمان برای کاهش خطر نفوذ و بهبود مدیریت ترافیک شبکه.	- ایجاد شبکه مستقل برای دوربین‌ها استفاده از دیوارهای آتش و IDS/IPS - میکرو قطع‌بندی	محدود کردن گسترش تهدیدات بهبود عملکرد و کنترل شبکه	[۱، ۴، ۵، ۷، ۱۲، ۱۴، ۱۸، ۱۹]

موضوع	توضیحات	اقدامات کلیدی	مزایا	منابع
کنترل دسترسی مبتنی بر نقش	محدود کردن دسترسی کاربران به داده های مورد نیاز بر اساس نقش های سازمانی برای جلوگیری از سوء استفاده.	- تخصیص دسترسی بر اساس نقش بازبینی و محدود سازی دسترسی ها	جلوگیری از دسترسی غیرمجاز افزایش امنیت داده های حساس	[۴، ۵، ۷، ۱۴، ۲۶]
نظارت و ثبت فعالیت ها	ثبت و بررسی فعالیت های کاربران و دسترسی ها برای شناسایی تهدیدات و استفاده به عنوان شواهد در صورت بروز حادثه.	- ثبت زمان و نوع دسترسی ها تحلیل رفتارهای مشکوک	شناسایی سریع تهدیدات بهبود عملکرد سازمانی	[۱، ۴، ۱۴، ۲۱، ۲۴]
به روز رسانی و وصله گذاری منظم	به روز رسانی نرم افزارها و میان افزارهای دوربین ها برای رفع آسیب پذیری ها و افزایش مقاومت در برابر تهدیدات جدید.	- بررسی و اعمال پچ های امنیتی به روز رسانی منظم سیستم ها	کاهش خطرات امنیتی بهبود عملکرد سیستم ها	[۲۲، ۲۴، ۲۶]

با اتخاذ این رویکرد، سازمان ها می توانند تاب آوری خود را در برابر حملات سایبری افزایش دهند و از منابع خود به بهترین نحو محافظت کنند. در ادامه توضیح بیشتری برای هر یک از اجزا ارائه می دهیم.

۱-۶- روش پیشنهادی

در روش پیشنهادی با توجه به مطالعات انجام شده برای شناسایی مخاطرات و تهدیدهای سیستم های نظارت تصویری در مقالات [۸-۱۰] که توسط نویسندگان تهیه شده است. رویکردی ارائه شده که با توجه به روش های اعتماد صفرو مدل بلوغ و پیاده سازی تدریجی آن بتوان این راهکار را این سیستم ها پیاده کرد. برای این منظور مراحل و گام های زیر طی شده است.



شکل ۵ - روش پیشنهادی و گام‌های طی شده

۶-۲- چرایی نیاز به اعتماد صفر در شبکه‌های نظارت تصویری

در دنیای امروز، دوربین‌ها به بخشی جدایی‌ناپذیر از زندگی شخصی و حرفه‌ای ما تبدیل شده‌اند. از دوربین‌های نظارتی در محیط‌های کاری تا دوربین‌های لپ‌تاپ‌ها و موبایل‌ها، این دستگاه‌ها دائماً در حال ضبط و انتقال داده‌های حساس هستند. با افزایش تهدیدات سایبری مانند هک، نفوذ به سیستم‌ها و سرقت داده‌ها، نیاز به امنیت اعتماد صفر بیش‌ازپیش احساس می‌شود. امنیت اعتماد صفر به این معناست که هیچ دستگاه یا کاربری به طور پیش‌فرض قابل اعتماد نیست و هر دسترسی باید به‌دقت بررسی و تأیید شود. این رویکرد از نفوذ هکرها به دوربین‌ها و سوءاستفاده از داده‌های ضبط‌شده جلوگیری می‌کند.

دوربین‌ها اغلب در موقعیت‌هایی استفاده می‌شوند که حریم خصوصی افراد در خطر است، مانند جلسات کاری، کلاس‌های آنلاین یا حتی محیط‌های شخصی. اگر امنیت این دوربین‌ها به‌درستی تأمین نشود، ممکن است داده‌های حساس در معرض خطر قرار بگیرند. امنیت اعتماد صفر با استفاده از روش‌هایی مانند احراز هویت چندمرحله‌ای، رمزنگاری داده‌ها و محدودکردن دسترسی‌ها، از نقض حریم خصوصی و سوءاستفاده از اطلاعات جلوگیری می‌کند. این رویکرد اطمینان می‌دهد که تنها افراد مجاز می‌توانند به دوربین‌ها و داده‌های آن دسترسی داشته باشند.

امنیت اعتماد صفر با ایجاد لایه‌های امنیتی متعدد و بررسی مداوم دسترسی‌ها، از نفوذ هکرها جلوگیری می‌کند. این رویکرد نه تنها از دوربین‌ها محافظت می‌کند، بلکه کل شبکه را در برابر حملات سایبری ایمن می‌سازد. با اجرای امنیت اعتماد صفر، سازمان‌ها می‌توانند اطمینان حاصل کنند که حتی اگر یکی از لایه‌های امنیتی شکسته شود، لایه‌های دیگر همچنان از داده‌ها محافظت می‌کنند.

امروزه بسیاری از صنایع و سازمان‌ها موظف به رعایت قوانین و استانداردهای امنیتی مانند مقررات عمومی حفاظت از داده‌ها اتحادیه اروپا^{۲۴} هستند. این قوانین بر حفظ حریم خصوصی و امنیت داده‌ها تأکید می‌کنند و نقض آنها می‌تواند منجر به جریمه‌های سنگین و آسیب به اعتبار سازمان شود. امنیت اعتماد صفر با ایجاد یک چارچوب امنیتی قوی، به سازمان‌ها کمک می‌کند تا با این قوانین و استانداردها سازگار شوند. این رویکرد نه تنها از داده‌های حساس محافظت می‌کند، بلکه اعتماد مشتریان و کاربران را نیز جلب می‌کند. با توجه به اهمیت روزافزون امنیت سایبری، امنیت اعتماد صفر برای دوربین‌ها و سایر دستگاه‌های متصل به شبکه یک ضرورت است.

۶-۳- احراز هویت و تأیید هویت

احراز هویت چندعاملی یکی از مؤثرترین روش‌ها برای تأمین امنیت دوربین‌های مداربسته است. این روش به کاربران این امکان را می‌دهد که برای دسترسی به سیستم‌های نظارت تصویری، علاوه بر رمز عبور، از یک یا چند روش دیگر مانند کدهای ارسال شده به تلفن همراه یا ایمیل استفاده کنند. با این کار، حتی در صورت افشای رمز عبور، دسترسی غیرمجاز به دوربین‌ها دشوارتر می‌شود. احراز هویت چندعاملی به‌ویژه در محیط‌های حساس که اطلاعات مهمی در دسترس است، اهمیت بیشتری پیدا می‌کند. این روش باعث می‌شود که هر کاربر برای تأیید هویت خود، مراحل بیشتری را طی کند و در نتیجه احتمال نفوذ به سیستم به حداقل برسد. [۲۰، ۱۷، ۵، ۲]

۶-۴- قطاع بندی شبکه

تقسیم بندی یا قطاع بندی شبکه به معنای جداسازی بخش های مختلف شبکه است که دوربین ها و سیستم های نظارت تصویری در یک شبکه مستقل قرار می گیرند. این کار به کاهش خطر نفوذ به سایر بخش های سازمان کمک می کند. به عنوان مثال، اگر یک هکر به شبکه عمومی سازمان دسترسی پیدا کند، نمی تواند به راحتی به دوربین ها و داده های حساس دسترسی یابد. این روش همچنین به بهبود عملکرد شبکه کمک می کند، زیرا ترافیک مربوط به دوربین ها و سایر دستگاه ها به طور مستقل مدیریت می شود. با جداسازی شبکه، سازمان ها می توانند کنترل بیشتری بر دسترسی ها داشته باشند و در صورت بروز یک حمله، به سرعت اقدام کنند. این کار به ویژه در محیط های بزرگ و پیچیده که تعداد زیادی دوربین و دستگاه وجود دارد، حیاتی است. [۱۹، ۱۴، ۷، ۵، ۴]

۶-۵- کنترل دسترسی مبتنی بر نقش

کنترل دسترسی مبتنی بر نقش^{۲۵} روشی است که به سازمان ها این امکان را می دهد تا دسترسی به دوربین ها و داده های ضبط شده را بر اساس نیازهای واقعی کاربران محدود کنند. با استفاده از کنترل دسترسی مبتنی بر نقش، هر کاربر تنها به اطلاعاتی دسترسی دارد که برای انجام وظایف خود به آن نیاز دارد. این کار از دسترسی غیرمجاز به اطلاعات حساس جلوگیری می کند و امنیت کلی سیستم را افزایش می دهد. به عنوان مثال، یک کارمند امنیتی ممکن است به تمامی دوربین ها دسترسی داشته باشد، در حالی که یک کارمند اداری تنها به دوربین های مربوط به بخش خود دسترسی خواهد داشت. این نوع کنترل دسترسی به سازمان ها کمک می کند تا از سوءاستفاده های احتمالی جلوگیری کنند و اطمینان حاصل کنند که تنها افراد مجاز به اطلاعات حساس دسترسی دارند. [۲۶، ۱۴، ۷، ۵، ۴]

۶-۶- نظارت و ثبت فعالیت ها

پیاده سازی سیستم های نظارتی برای ثبت و بررسی فعالیت های کاربران و دسترسی ها به دوربین ها از اهمیت بالایی برخوردار است. این سیستم ها می توانند اطلاعات دقیقی درباره زمان، نوع دسترسی و فعالیت های انجام شده توسط کاربران را ثبت کنند. این اطلاعات به شناسایی و پاسخ به تهدیدات کمک می کند و در صورت وقوع یک حادثه، می توانند به عنوان شواهد مورد استفاده قرار گیرند. همچنین، نظارت بر فعالیت ها به مدیران این امکان را می دهد که رفتارهای مشکوک را شناسایی کنند و اقدامات لازم را انجام دهند. در نتیجه، این سیستم ها نه تنها به افزایش امنیت کمک می کنند، بلکه به بهبود عملکرد کلی سازمان نیز می انجامند. [۲۱، ۱۴، ۷، ۴، ۱]

۶-۷- به روز رسانی و وصله گذاری منظم

اطمینان از به روز رسانی منظم نرم افزار دوربین ها و سیستم های وابسته به منظور جلوگیری از آسیب پذیری ها و تهدیدات جدید بسیار حائز اهمیت است. با گذشت زمان، ممکن است باگ ها و آسیب پذیری های نرم افزارها توسط مهاجمان یا محققان کشف شوند که می تواند به نفوذگران اجازه دسترسی به سیستم را بدهد؛ بنابراین، سازمان ها باید به طور مداوم نرم افزارهای خود را بررسی و به روز رسانی کنند تا از جدیدترین پچ ها و بهبودها بهره مند شوند. این کار به کاهش خطرات امنیتی کمک می کند و اطمینان حاصل می کند که سیستم ها در برابر تهدیدات جدید مقاوم هستند. به علاوه، به روز رسانی های منظم می توانند به بهبود عملکرد دوربین ها و سیستم های نظارت تصویری نیز کمک کنند. [۲۶، ۲۴، ۲۲]

²⁵ RBAC: Role Base Access Control

۷- مزایای استفاده از معماری اعتماد صفر در دوربین‌های مدار بسته

باتوجه به مطالعات مقالات مروری و مخاطرات و تهدیدهای سایبری مزایای اعتماد صفر برای سیستم‌های نظارت تصویری به‌صورت زیر پیش‌بینی می‌شود (جدول ۳):

جدول ۳ - مزایای کاربری اعتماد صفر در سیستم‌های نظارت تصویری

مزیت	توضیحات	ویژگی‌های کلیدی	منابع
افزایش امنیت	نقاط ضعف سیستم‌های نظارت تصویری به حداقل می‌رسد و کنترل بیشتری بر دسترسی‌ها فراهم می‌شود. تنها کاربران با هویت تأیید شده (از طریق احراز هویت چندعاملی و بررسی رفتار) به داده‌های دوربین دسترسی دارند.	- احراز هویت چندعاملی (MFA) - بررسی رفتار کاربران	[۳، ۹، ۱۴، ۱۵، ۲۲]
کاهش خطر نفوذ	با تأکید بر احراز هویت مداوم و نظارت مستمر بر فعالیت‌ها، خطر نفوذ به سیستم‌های دوربین کاهش می‌یابد. رفتارهای مشکوک به سرعت شناسایی و مدیریت می‌شوند.	- تأیید هویت مداوم - نظارت مستمر بر فعالیت‌ها	[۳، ۹، ۱۴، ۲۲، ۲۷]
پاسخ سریع به تهدیدات	ثبت و نظارت بر فعالیت‌ها امکان شناسایی الگوهای غیرعادی و واکنش سریع به تهدیدات را فراهم می‌کند. دسترسی سریع به داده‌ها، تصمیم‌گیری و اقدامات پیشگیرانه را تسهیل می‌کند.	- شناسایی الگوهای غیرعادی - کاهش زمان واکنش	[۳، ۵، ۶، ۹، ۱۴، ۲۲]
بهبود مدیریت داده‌ها	سیاست‌های دقیق دسترسی امکان مدیریت مؤثر داده‌های ویدئویی و تصویری را فراهم می‌کند. این امر به حفظ حریم خصوصی و جلوگیری از نشت داده‌های حساس کمک می‌کند.	- سیاست‌های دقیق دسترسی - حفاظت از داده‌های حساس	[۹، ۱۴، ۲۲، ۶۳]
افزایش انطباق با استانداردها	پیاده‌سازی سیاست‌های دسترسی و نظارت، انطباق با الزامات قانونی و استانداردهای امنیتی را بهبود می‌بخشد. فعالیت‌ها مستند شده و قابل پیگیری هستند.	- مستندسازی فعالیت‌ها - انطباق با مقررات	[۲، ۴، ۹، ۱۴، ۱۷، ۲۲، ۲۷]
کاهش هزینه‌های امنیتی	کاهش نفوذها و تهدیدات منجر به صرفه‌جویی در هزینه‌های واکنش به حوادث، تعمیرات و جبران خسارات می‌شود. بهبود کارایی و مدیریت منابع نیز هزینه‌ها را کاهش می‌دهد.	- کاهش حوادث امنیتی - بهینه‌سازی منابع	[۱، ۴، ۵، ۱۵، ۲۰، ۲۲]

۸- ارائه راهکار برای پیاده سازی اعتماد صفر در سیستم های نظارت تصویری

معماری اعتماد صفر به عنوان یکی از رویکردهای پیشرفته در امنیت سایبری، راهکاری جامع برای مقابله با تهدیدات پیچیده و روزافزون ارائه می دهد. این معماری، با اصل بنیادین "هرگز اعتماد نکن، همیشه تأیید کن"، امکان مدیریت دقیق دسترسی به منابع حساس را فراهم می کند. در زمینه سیستم های نظارت تصویری، به ویژه دوربین های مدار بسته، پیاده سازی اعتماد صفر می تواند امنیت این سامانه ها را به طور چشمگیری بهبود بخشد. این مقاله به بررسی راهکارهای علمی و عملی برای اعمال معماری اعتماد صفر در چهار بخش کلیدی سیستم های نظارت تصویری شامل کاربران، دستگاه های دوربین، شبکه و انتقال داده ها می پردازد. [۲۲، ۲۰، ۱۶، ۱۵، ۵، ۱۴]

کاربران، شناسایی و تأیید هویت کاربران به طور مداوم از اصول اساسی این معماری است. این فرایند نه تنها در زمان ورود به سیستم، بلکه در طول تعاملات کاربر با سیستم نیز باید انجام شود تا از دسترسی غیرمجاز جلوگیری گردد. دستگاه های دوربین، اطمینان از اینکه تنها دستگاه های مجاز به شبکه متصل می شوند، یکی دیگر از ارکان این رویکرد است. این امر به همراه استفاده از روش های رمزنگاری امن برای انتقال اطلاعات، به حفاظت از داده های حساس کمک می کند و امکان نفوذ به سیستم را کاهش می دهد. شبکه، ایجاد شبکه های مجزا و امن، به کاهش سطح آسیب پذیری کمک می کند. با تفکیک شبکه ها، حتی در صورت نفوذ به یکی از آن ها، امکان دسترسی به سایر بخش ها محدود می شود. انتقال داده ها، استفاده از پروتکل های امن مانند TLS برای حفاظت از داده ها در حین انتقال، از دیگر جنبه های حیاتی این معماری است. این پروتکل ها تضمین می کنند که اطلاعات در برابر حملات سایبری محافظت شده و از امنیت لازم برخوردارند. در مجموع، اجرای معماری اعتماد صفر در سیستم های نظارت تصویری می تواند به طور قابل توجهی امنیت این سیستم ها را افزایش دهد و از تهدیدات سایبری محافظت کند، به ویژه در دنیای امروز که حملات سایبری به طور فزاینده ای رایج شده اند. [۱۴، ۱۰، ۷، ۴]

۸-۱- شناسایی و تشخیص دارایی ها: پایه گذاری امنیت ساختاریافته

اولین گام در پیاده سازی معماری اعتماد صفر، شناسایی دقیق دوربین ها، کاربران مجاز و جریان های داده ای مرتبط است. این فرایند شامل ایجاد یک نقشه جامع از تمامی دستگاه ها، مسیرهای انتقال داده و نقاط دسترسی می شود. شناسایی مدل دوربین ها، نسخه های میان افزار^{۲۶}، موقعیت فیزیکی و نحوه ارتباط آن ها با شبکه، امکان تحلیل آسیب پذیری ها و شناسایی نقاط ضعف را فراهم می کند. همچنین، نقشه برداری از جریان داده ها (مانند انتقال تصاویر به سرور مرکزی یا فضای ابری) برای تعیین مکان های بالقوه نفوذ ضروری است. این مرحله به سازمان ها کمک می کند تا پایه ای ساختاریافته برای اعمال سیاست های امنیتی فراهم کنند و کنترل دقیقی بر دارایی های خود اعمال نمایند. [۲۲، ۲۰، ۱۵، ۵، ۴، ۱]

۸-۲- احراز هویت چندمرحله ای: تقویت امنیت دسترسی کاربران

یکی از اصول کلیدی معماری اعتماد صفر، تضمین صحت هویت کاربران پیش از دسترسی به سیستم است. در این راستا، استفاده از احراز هویت ضروری است. این روش با ترکیب عوامل مختلف، از جمله رمز عبور، کدهای یک بار مصرف^{۲۷}، و احراز هویت بیومتریک (مانند اثر انگشت یا تشخیص چهره)، سطح امنیتی سیستم را افزایش می دهد. علاوه بر این، اصل حداقل دسترسی باید اعمال شود، به گونه ای که هر کاربر تنها به داده ها و بخش هایی که برای انجام وظایف خود نیاز دارد، دسترسی داشته باشد. بازبینی دوره ای دسترسی ها و حذف دسترسی های غیرضروری نیز از دیگر اقدامات ضروری در این بخش است. این کنترل ها از سوءاستفاده احتمالی کاربران داخلی یا نفوذگران خارجی جلوگیری می کند. [۲۲، ۲۰، ۱۵، ۵، ۴، ۱]

²⁶ Firmware version

²⁷ OTP : One Time Password

۸-۳- ایمن‌سازی دستگاه‌های دوربین: حفاظت از نقاط انتهایی شبکه

دوربین‌های مدار بسته به‌عنوان نقاط انتهایی^{۲۸} شبکه، یکی از اهداف اصلی حملات سایبری هستند. برای ایمن‌سازی این دستگاه‌ها، باید اقدامات متعددی انجام شود. به‌روزرسانی میان‌افزار دوربین‌ها برای رفع آسیب‌پذیری‌های شناخته‌شده، یکی از مهم‌ترین گام‌ها است. علاوه بر این، رمزهای عبور پیش‌فرض دوربین‌ها باید با رمزهای قوی و منحصر به فرد جایگزین شوند. غیرفعال کردن قابلیت‌های غیرضروری مانند دسترسی از راه دور بدون رمزنگاری و پروتکل‌های ناامن (مانند Telnet یا FTP) نیز از اهمیت بالایی برخوردار است. همچنین، داده‌های تولیدشده توسط دوربین‌ها (مانند ویدئو و صدا) باید در حین انتقال و ذخیره‌سازی به طور کامل رمزنگاری شوند. این اقدامات، نه تنها از نفوذ به دستگاه‌ها جلوگیری می‌کند، بلکه امنیت داده‌های حساس را نیز تضمین می‌نماید. [۱، ۴، ۵، ۲۰، ۲۲]

۸-۴- ایمن‌سازی شبکه: ایجاد زیرساختی مقاوم در برابر تهدیدات

شبکه‌ای که دوربین‌های مدار بسته در آن استقرار یافته‌اند، باید به‌عنوان یک محیط ایزوله و کاملاً ایمن طراحی شود. تفکیک شبکه (قطاع‌بندی) یکی از اصول اساسی در این زمینه است. با جداسازی شبکه دوربین‌ها از سایر بخش‌های شبکه سازمان، می‌توان از گسترش تهدیدات به سایر سیستم‌ها جلوگیری کرد. علاوه بر این، استفاده از شبکه خصوصی مجازی برای دسترسی از راه دور به دوربین‌ها، امنیت ارتباطات را افزایش می‌دهد. پیاده‌سازی دیوارهای آتش و سیستم‌های تشخیص و پیشگیری از نفوذ^{۲۹} نیز امکان شناسایی و مسدودسازی ترافیک مشکوک را فراهم می‌کند. نظارت مداوم بر ترافیک شبکه و تحلیل فعالیت‌های غیرعادی، به‌عنوان یک لایه اضافی امنیتی، از اهمیت ویژه‌ای برخوردار است [۱، ۱۳، ۱۵].

۸-۵- ایمن‌سازی انتقال و ذخیره‌سازی داده‌ها: حفاظت از داده‌های حساس

داده‌های تولیدشده توسط دوربین‌های مدار بسته، شامل تصاویر و ویدئوهای حساس، باید در تمامی مراحل انتقال و ذخیره‌سازی ایمن شوند. استفاده از الگوریتم‌های رمزنگاری قوی مانند AES256 برای رمزنگاری داده‌ها در حالت انتقال و ذخیره‌سازی، یکی از الزامات کلیدی است. همچنین، انتقال داده‌ها باید از طریق پروتکل‌های امن مانند HTTPS یا SFTP انجام شود تا از شنود و دستکاری جلوگیری شود. پشتیبان‌گیری منظم از داده‌ها و ذخیره‌سازی آن‌ها در مکان‌های امن و رمزنگاری شده، از دیگر اقدامات ضروری است. علاوه بر این، دسترسی به داده‌های ذخیره‌شده باید به افراد مجاز محدود شود و هرگونه دسترسی غیرمجاز به طور مداوم نظارت و بررسی گردد. این اقدامات از سرقت، دست‌کاری یا از دست رفتن داده‌های حساس جلوگیری می‌کند. [۱، ۲، ۴، ۹، ۱۴، ۱۵، ۱۷]

۹- بررسی مفاهیم بلوغ در پیاده‌سازی اعتماد صفر در سیستم‌های نظارت تصویری

بر اساس سند [۱۶] که یک روش مناسب برای پیاده‌سازی مرحله‌ای و سطح تکامل بلوغ برای اعتماد صفر پیشنهاد شده است، می‌توان مراحل پیاده‌سازی را برای سیستم‌های نظارت تصویری به صورت زیر پیشنهاد داد. (جدول ۴)

جدول ۴ مفاهیم بلوغ در پیاده‌سازی اعتماد صفر در شبکه‌های نظارت تصویری

رکن	سنتی	ابتدایی	پیشرفته	بهینه
هویت	احراز هویت با رمز عبور یا احراز هویت چندگانه ساده، ذخیره‌سازی داخلی،	احراز هویت چندگانه با عوامل ترکیبی، ذخیره‌سازی داخلی و	احراز هویت چندگانه مقاوم در برابر فیشینگ، ذخیره‌سازی	احراز هویت مداوم، ذخیره‌سازی کاملاً یکپارچه، دسترسی پویا و

²⁸ Endpoints

²⁹ IDS/IPS: Intrusion Detection Systems / Intrusion Prevention Systems

رکن	سنتی	ابتدایی	پیشرفته	بهینه
	دسترسی ایستا، ارزیابی دستی مخاطرات	ابری با یکپارچگی محدود، دسترسی موقت، ارزیابی دستی	یکپارچه، دسترسی جلسه محور، تحلیل خودکار مخاطرات	خودکار، تحلیل بلادرنگ مخاطرات
دستگاه‌ها	فهرست‌بندی دستی، بدون نظارت جامع، حفاظت دستی تهدیدات، دسترسی بدون پایش	خوداظهاری ویژگی‌های دستگاه، پایش اولیه، حفاظت خودکار محدود، دسترسی مبتنی بر ویژگی‌ها	فهرست‌بندی خودکار، حفاظت متمرکز، دسترسی مبتنی بر وضعیت دستگاه، مدیریت خودکار آسیب‌پذیری‌ها	پایش بلادرنگ انطباق، حفاظت یکپارچه، تحلیل بلادرنگ مخاطرات، خودکارسازی کامل چرخه عمر دستگاه
شبکه	تقسیم‌بندی کلان، رمزگذاری محدود، مدیریت دستی ترافیک، تاب‌آوری محدود	رمزگذاری داخلی، پایش مبتنی بر شاخص‌های شناخته‌شده، تهدید، جداسازی اولیه، تنظیمات پویا محدود	میکرو قطاع بندی، رمزگذاری جامع، مدیریت پویای ترافیک، تاب‌آوری گسترده	میکرو قطاع بندی کامل، رمزگذاری چابک، مدیریت خودکار زیرساخت به‌عنوان کد، تاب‌آوری پویا
برنامه‌ها	دسترسی ثابت، حفاظت عمومی، دسترسی محدود به شبکه‌های داخلی، توسعه موردی	دسترسی بافتاری، حفاظت در برنامه‌های حیاتی، دسترسی عمومی محدود، CI/CD اولیه ^{۳۰}	دسترسی خودکار با حداقل امتیاز، حفاظت یکپارچه، دسترسی گسترده‌تر، آزمون پویا	تحلیل بلادرنگ مخاطرات، حفاظت پیشرفته، دسترسی کامل عمومی، خودکارسازی کامل CI/CD
داده‌ها	فهرست‌بندی دستی، رمزگذاری محدود، دسترسی ایستا، دید محدود	فهرست‌بندی خودکار محدود، رمزگذاری داخلی، کنترل دسترسی خودکار، دید اولیه	فهرست‌بندی و رمزگذاری جامع، کنترل دسترسی بافتاری، تحلیل پیش‌بینی‌کننده	فهرست‌بندی مداوم، رمزگذاری چابک، کنترل دسترسی پویا، تحلیل بلادرنگ و پیش‌بینی‌کننده

۹-۱- رکن هویت

پیاده‌سازی مرحله‌ای مدیریت رکن هویت در چارچوب اعتماد صفر برای سیستم‌های نظارت تصویری از احراز هویت مبتنی بر رمز عبور به احراز هویت چندعاملی مقاوم در برابر فیشینگ و ارزیابی مداوم هویت تکامل می‌یابد. مدیریت دسترسی از حالت ایستا به دسترسی‌های جلسه محور و خودکار محدود به عملیات ضروری تغییر می‌یابد. محل‌های ذخیره‌سازی هویت از مدیریت داخلی به یکپارچگی ایمن داخلی و ابری توسعه می‌یابد. ارزیابی مخاطرات و هماهنگی هویت‌ها از روش‌های دستی به تحلیل بلادرنگ و خودکار با اجرای پویای خط‌مشی‌های هویتی ارتقا می‌یابد.

۹-۲- رکن دستگاه

پیاده‌سازی مرحله‌ای مدیریت رکن دستگاه‌ها در چارچوب اعتماد صفر برای سیستم‌های نظارت تصویری از فرایندهای دستی به خودکارسازی یکپارچه و پویا تکامل می‌یابد. در سطح سنتی، فقدان نظارت جامع بر دستگاه‌ها و مدیریت دستی آسیب‌پذیری‌ها، امنیت را شکننده می‌سازد. در سطح ابتدایی، خوداظهاری ویژگی‌های دستگاه و پایش خودکار اولیه معرفی می‌شود. در سطح پیشرفته، مدیریت خودکار نرم‌افزار، آسیب‌پذیری‌ها و دسترسی به منابع با تحلیل داده‌های تأییدشده دستگاه تقویت می‌گردد. در سطح بهینه، پایش بلادرنگ انطباق، مدیریت خودکار مخاطرات زنجیره تأمین و راهکارهای متمرکز حفاظتی، دید جامع و هماهنگی کامل چرخه عمر دستگاه‌ها و دارایی‌های مجازی را تضمین می‌کند. این تکامل، امنیت و تاب‌آوری سیستم‌های نظارت تصویری را در برابر تهدیدات پیچیده به طور قابل توجهی ارتقا می‌دهد.

³⁰ CI/CD = Continuous Integration / Continuous Delivery or Continuous Deployment

۹-۳- رکن شبکه

پیاده‌سازی رکن شبکه در چارچوب اعتماد صفر برای سیستم‌های نظارت تصویری از معماری‌های سنتی با قطاع‌بندی ساده و رمزگذاری محدود به‌سوی خودکارسازی پیشرفته و میکرو قطاع بندی پویا تکامل می‌یابد. در سطح ابتدایی، رمزگذاری ترافیک داخلی و پایش مبتنی بر شاخص‌های شناخته‌شده تهدید^{۳۱} آغاز می‌گردد. در سطح پیشرفته، میکرو قطاع بندی (قطاع‌بندی) گسترده، رمزگذاری جامع و مدیریت پویای ترافیک با خودکارسازی تقویت می‌شود. در سطح بهینه، معماری شبکه با میکرو قطاع بندی کامل، رمزگذاری مداوم، تاب‌آوری پویا و مدیریت خودکار زیرساخت به‌عنوان کد، امنیت و دید بلادرنگ را تضمین می‌کند. این پیشرفت، حفاظت از ارتباطات و منابع سیستم‌های نظارت تصویری را در برابر تهدیدات پیچیده به طور مؤثری بهینه‌سازی می‌نماید.

۹-۴- رکن برنامه

پیاده‌سازی رکن برنامه‌ها و بارهای کاری در چارچوب اعتماد صفر برای سیستم‌های نظارت تصویری از مدیریت دستی و دسترسی محلی به خودکارسازی پیشرفته و پویا تکامل می‌یابد. در سطح سنتی، دسترسی به برنامه‌ها مبتنی بر مجوزهای ثابت و حفاظت‌های عمومی با پایش محدود است. در سطح ابتدایی، خودکارسازی اولیه دسترسی بافتاری^{۳۲}، آزمون امنیتی و پایش پروفایل برنامه آغاز می‌شود. در سطح پیشرفته، تصمیم‌گیری دسترسی خودکار، حفاظت یکپارچه تهدیدات و آزمون پویا تقویت می‌گردد. در سطح بهینه، تحلیل بلادرنگ مخاطرات، حفاظت پیشرفته در برابر تهدیدات، پایش مستمر و خودکارسازی کامل چرخه عمر توسعه و استقرار، امنیت و کارایی برنامه‌های نظارت تصویری را به طور جامع تضمین می‌کند.

۹-۵- رکن داده

پیاده‌سازی رکن داده‌ها در چارچوب اعتماد صفر برای سیستم‌های نظارت تصویری از مدیریت دستی و محدود به خودکارسازی جامع و پویا تکامل می‌یابد. در سطح سنتی، فهرست‌بندی و رمزگذاری داده‌ها به‌صورت دستی و با دید محدود انجام می‌شود. در سطح ابتدایی، خودکارسازی اولیه فهرست‌بندی، رمزگذاری و کنترل دسترسی با رعایت اصول کمترین امتیاز آغاز می‌گردد. در سطح پیشرفته، فرایندهای خودکار فهرست‌بندی، طبقه‌بندی و رمزگذاری جامع‌تر شده و تحلیل پیش‌بینی‌کننده معرفی می‌شود. در سطح بهینه، مدیریت پویا و مداوم چرخه عمر داده‌ها، رمزگذاری چابک، و تحلیل بلادرنگ، امنیت و دسترسی به داده‌های ویدیویی و مرتبط را به طور کامل تضمین می‌کند.

۱۰- نتیجه‌گیری

در دنیای دیجیتال امروز، تهدیدات سایبری به طور فزاینده‌ای پیچیده و متنوع شده‌اند و امنیت سیستم‌های نظارت تصویری، از جمله دوربین‌های مداربسته، به یکی از اولویت‌های اصلی سازمان‌ها تبدیل شده است. معماری اعتماد صفر به‌عنوان یک رویکرد نوین در تأمین امنیت اطلاعات، به سازمان‌ها این امکان را می‌دهد که با حذف فرضیات مربوط به اعتماد پیش‌فرض، کنترل بیشتری بر دسترسی‌ها و فعالیت‌ها داشته باشند. این رویکرد با تأکید بر احراز هویت مداوم، رمزنگاری داده‌ها و نظارت پیوسته، می‌تواند به طور قابل توجهی امنیت سیستم‌های نظارتی را افزایش دهد و دسترسی هکرها را به اطلاعات حساس جلوگیری کند.

با پیاده‌سازی معماری اعتماد صفر، سازمان‌ها می‌توانند خطر نفوذ به سیستم‌های دوربین‌های مداربسته را به‌شدت کاهش دهند. این مدل امنیتی با بررسی مداوم فعالیت‌ها و دسترسی‌ها، امکان شناسایی رفتارهای مشکوک را فراهم می‌کند و به سازمان‌ها این

³¹ Indicator of Compromise

³² Context

امکان را می دهد که به سرعت به تهدیدات پاسخ دهند. همچنین، با بهبود مدیریت داده ها و افزایش انطباق با استانداردهای امنیتی، سازمان ها می توانند از نشت داده ها جلوگیری کرده و اعتماد مشتریان و کاربران را جلب کنند.

در نهایت، اگرچه پیاده سازی معماری اعتماد سفر ممکن است در ابتدا هزینه بر به نظر برسد، اما در بلندمدت می تواند به کاهش هزینه های امنیتی و افزایش کارایی سازمان ها منجر شود. با توجه به افزایش روزافزون تهدیدات سایبری و اهمیت حفاظت از داده های حساس، استفاده از این رویکرد در سیستم های دوربین های مدار بسته یک ضرورت اجتناب ناپذیر است. سازمان ها باید به طور مستمر به بررسی و به روزرسانی استراتژی های امنیتی خود بپردازند تا از منابع خود به بهترین نحو محافظت کنند و تاب آوری خود را در برابر حملات سایبری افزایش دهند.

مراجع

- [1] C. Daah, A. Qureshi, and I. Awan, "Zero Trust Model Implementation Considerations in Financial Institutions: A Proposed Framework," in *2023 10th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2023: IEEE, pp. 71–77, doi: 10.1109/FiCloud58648.2023.00019. [Online]. Available: <https://ieeexplore.ieee.org/document/10410790/>
- [2] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 6476274, 2022, doi: 10.1155/2022/6476274.
- [3] N. Nahar, K. Andersson, O. Schelén, and S. Saguna, "A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3425350.
- [4] *SP 800207, Zero Trust Architecture* NIST, 2020.
- [5] V. Stafford, "Zero Trust Architecture," *NIST special publication*, vol. 800, no. 207, pp. 800–207, 2020.
- [6] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (zta): A comprehensive survey," *IEEE access*, vol. 10, pp. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.
- [7] A. Kudrati and B. A. Pillai, *Zero Trust Journey Across the Digital Estate*. CRC Press, 2022.
- [8] A. Samouti, M. Fathy, and A. Khalili, "Overview of Preventive Measures and Maintenance in the Performance of Video Surveillance Systems," (in Per), *International Conference on Security, Advancement, and Sustainable Development of Border Regions, Territories, and Metropolises: Strategies and Challenges Focusing on Passive Defense and Crisis Management*, 2018. [Online]. Available: <https://civilica.com/doc/884324>.
- [9] A. Samouti, H. Hesam, and K. Ali, "Overview of Cyber Threats in Networked Video Surveillance Systems and Solutions for Enhancing Security," (in Per), *4th National Conference on Computer, Information Technology, and Applications of Artificial Intelligence*, 2019. [Online]. Available: <https://civilica.com/doc/1238737>.
- [10] A. Samouti and Y. Elmi sola, "Overview of ways to enhance the security of video surveillance networks using blockchain," (in Per), *Biannual Journal Monadi for Cyberspace Security (AFTA)*, Review Article vol. 9, no. 2, pp. 81–97, 2021. [Online]. Available: <http://monadi.isc.org.ir/article1190fa.html>.

- [11] U. B. Chaudhry and A. K. Hydros, "Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm," *IET blockchain*, vol. 3, no. 2, pp. 98–115, 2023, doi: 10.1049/blc2.12028.
- [12] P. Dhiman *et al.*, "A review and comparative analysis of relevant approaches of zero trust network model," *Sensors*, vol. 24, no. 4, p. 1328, 2024, doi: 10.3390/s24041328.
- [13] A. Z. Jackson Mason, "Protecting Online Banking Systems with Blockchain and Zero Trust Security: Strategies for Data Security and Cyber Defense," 2023.
- [14] *DoD Zero Trust Strategy*, DOD, 2022.
- [15] H. Joshi, "Emerging Technologies Driving Zero Trust Maturity Across Industries," *IEEE Open Journal of the Computer Society*, vol. 6, pp. 25–36, 2025, doi: 10.1109/OJCS.2024.3505056.
- [16] C. a. I. S. A. C. Division, "Zero Trust Maturity Model " vol. 2, 2022.
- [17] J. P. Ioannidis, "Zero Trust Architecture in Financial Services: A Model for Secure Digital Banking," July 2023.
- [18] S. Ashfaq, S. A. Patil, S. Borde, P. Chandre, P. M. Shafi, and A. Jadhav, "Zero Trust Security Paradigm: A Comprehensive Survey and Research Analysis," *Journal of Electrical Systems*, vol. 19, no. 2, 2023, doi: 10.1109/ACCESS.2022.3174679.
- [19] O. C. Edo, T. Tenebe, E.E. Etu, A. Ayuwu, J. Emakhu, and S. Adebisi, "Zero Trust Architecture: Trend and Impact on Information Security," *International Journal of Emerging Technology and Advanced Engineering*, vol. 12, no. 7, p. 140, 2022, doi: 10.46338/ijetae0722_15.
- [20] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of zero trust networks in cloud computing: A comparative review," *Sustainability*, vol. 14, no. 18, p. 11213, 2022, doi: 10.3390/su141811213.
- [21] T. Endress, "Zero Trust in Banking and FinTech," in *Digital Project Practice for Banking and FinTech*: Auerbach Publications, 2024, pp. 135–146.
- [22] A. Gupta, P. Gupta, U. P. Pandey, P. Kushwaha, B. P. Lohani, and K. Bhati, "ZTSA: Zero Trust Security Architecture a Comprehensive Survey," in *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)*, 2024: IEEE, pp. 378–383, doi: 10.1109/IC3SE62002.2024.10593067. [Online]. Available: <https://ieeexplore.ieee.org/document/10593067/>
- [23] N. Ali and N. Rehman, "Zero Trust Security and Blockchain Technology: Reimagining Cyber Defense in Online Banking Systems and Financial Institutions," 2024, doi: 10.13140/RG.2.2.11051.66088.
- [24] S. Ghasemshirazi, G. Shirvani, and M. A. Alipour, "Zero trust: Applications, challenges, and opportunities," *arXiv preprint arXiv:2309.03582*, 2023, doi: 10.48550/arXiv.2309.03582.
- [25] D. Ajish, "The significance of artificial intelligence in zero trust technologies: a comprehensive review," *Journal of Electrical Systems and Information Technology*, vol. 11, no. 1, p. 30, 2024, doi: 10.1186/s4306702400155z.
- [26] X. Yan and H. Wang, "Survey on zerotrust network security," in *International Conference on Artificial Intelligence and Security*, 2020: Springer, pp. 50–60, doi: 10.1007/9789811580833_5. [Online]. Available: https://link.springer.com/chapter/10.1007/9789811580833_5
- [27] C. Itodo and M. Ozer, "Multivocal literature review on zerotrust security implementation," *Computers & Security*, p. 103827, 2024, doi: 10.1016/j.cose.2024.103827.
- [28] W. Dorris. "Zero trust networks, and the implications for video surveillance " (accessed.

A Solution for Implementing Zero Trust Architecture in Video Surveillance System

Seyed Ali Samouti, PhD student ¹  | Sajad Tarhani, Reasercher ²  | Hessam Hassanpour ³ 

¹Department of Computer Engineering and Information Technology, Sab.C., Islamic Azad University, Sabzevar, Iran, Ali.samouti@iau.ac.ir

²Department of Mechatronics Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran, Sajad.tarhani@gmail.com

³Department of Computer Engineering and Information Technology, Sab.C., Islamic Azad University, Sabzevar, Iran, Hesamhasanpour@iau.ac.ir

Correspondence

^{*}PhD student, Department of Computer Engineering and Information Technology, Sab.C., Islamic Azad University, Sabzevar, Iran, Ali.samouti@iau.ac.ir

Received: 4 May 2025

Accepted: 4 June 2025

<https://doi.org/...>

Abstract

In an era defined by the relentless evolution of digital connectivity and the escalating complexity of cyber threats, the imperative for robust cybersecurity frameworks has never been more pronounced. Traditional security paradigms, anchored in perimeter-centric defenses and presumptive trust, have proven inadequate against the sophisticated and dynamic nature of contemporary cyberattacks. In response, the Zero Trust architecture has emerged as a paradigmatic shift, predicated on the axiom of "never trust, always verify." This scholarly review elucidates the foundational principles, constituent elements, and implementation methodologies of Zero Trust, with a particular emphasis on its transformative application in securing video surveillance systems, which serve as critical repositories of sensitive data and are increasingly vulnerable to cyber exploitation. The Zero Trust model fundamentally redefines security by eschewing implicit trust, mandating rigorous and continuous validation of all entities—users, devices, or applications—irrespective of their position relative to the network perimeter. This approach is particularly salient for video surveillance systems, which perpetually capture and store sensitive visual data, rendering them prime targets for malicious actors seeking unauthorized access or data manipulation. By embedding Zero Trust principles, organizations can fortify these systems against both internal and external threats, ensuring the integrity and confidentiality of critical information assets. Central to the Zero Trust framework are several interlocking components: continuous authentication, the principle of least privilege, comprehensive data encryption, and real-time behavioral monitoring.

Continuous authentication employs multi-factor authentication (MFA) mechanisms—encompassing passwords, biometric identifiers, or ephemeral codes—to verify identities at every access juncture. The principle of least privilege restricts access rights to the minimal resources requisite for a user's function, thereby constricting the potential attack surface. Data encryption, implemented across both transit and storage phases, ensures that intercepted information remains indecipherable to unauthorized entities. Concurrently, real-time monitoring and advanced analytics facilitate the prompt detection of anomalous activities, enabling rapid response to emergent threats. In the context of video surveillance systems, the operationalization of Zero Trust necessitates a structured approach. The initial step involves meticulous

asset identification, mapping all cameras, users, and data flows to establish a comprehensive security baseline. Regular firmware updates and the replacement of default credentials with robust, unique identifiers are critical to mitigating device vulnerabilities. Network segmentation, or micro-segmentation, isolates surveillance infrastructure from broader organizational networks, curtailing lateral threat propagation. Secure communication protocols, such as Transport Layer Security (TLS), safeguard data in transit, while role-based access control (RBAC) ensures that permissions align strictly with operational roles. Continuous monitoring systems, underpinned by advanced analytics, log and scrutinize activities to preemptively address potential security breaches. The adoption of Zero Trust in video surveillance systems yields profound advantages, including heightened security, diminished risk of data breaches, and enhanced compliance with stringent regulatory frameworks, such as the General Data Protection Regulation (GDPR). Nevertheless, challenges such as infrastructure overhaul, device interoperability, and balancing security with user experience demand careful consideration. Drawing upon an extensive corpus of over 50 peer-reviewed sources, including NIST SP 800-207 and the U.S. Department of Defense's Zero Trust Strategy, this study articulates a rigorous and actionable framework for integrating Zero Trust into video surveillance systems. Through this scholarly synthesis, it underscores the architecture's capacity to bolster cybersecurity resilience in an increasingly perilous digital landscape.

Keywords: Cybersecurity, Zero Trust Architecture, Continuous Authentication, Least Privilege, Video Surveillance Systems, Data Encryption