**Journal of New Technologies in Distributed Systems and Algorithmic Computing**
Islamic Azad University of Sabzevar
**E-ISSN: 3115-705X**
https://sanad.iau.ir/journal/ntds

*Research Article

# Zero Trust Implementation Framework for Video Surveillance Systems

Seyed Ali Samouti *[1] | Sajad Tarhani [2] | Hessam Hassanpour [3]

[1] Department of Computer Engineering and Information Technology, Islamic Azad University, Sabzevar Branch, Sabzevar, Iran, **Iran,ali.samouti@iau.ac.ir**

[2]Department of Mechatronics Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran, **sajad.Tarhani@gmail.com**

[3]Department of Computer Engineering and Information Technology, Islamic Azad University, Sabzevar Branch, Sabzevar, Iran, **hesamhasanpour@iau.ac.ir**

**Correspondence**
*Ali Samouti , PhD Student Department of Computer Engineering and Information Technology, Islamic Azad University, Sabzevar Branch, Sabzevar, Iran, **Ali.Samouti@iau.ac.ir**

**Main Subjects**: Zero Trust Implementation
**Received**: 04 May 2025
**Revised**: 16 May 2025
**Accepted**: 4 June 2025

https://doi.org/10.82195/ntds.2025.1205720

## Abstract

In an era of rapid digital interconnectivity and escalating cyber threats, traditional perimeter-based cybersecurity models, reliant on implicit trust, are insufficient against sophisticated cyberattacks. The Zero Trust architecture, based on the "never trust, always verify" principle, provides a transformative framework to secure critical systems, particularly video surveillance systems that store sensitive data and are vulnerable to exploitation. This review synthesizes Zero Trust's core principles, components, and implementation strategies, emphasizing its role in protecting video surveillance against internal and external threats. Zero Trust mandates continuous validation of all entities—users, devices, and applications—irrespective of network position, crucial for surveillance systems that capture sensitive visual data, making them targets for unauthorized access or manipulation. Key components include continuous multi-factor authentication (MFA) using passwords, biometrics, or ephemeral codes for every access point; the principle of least privilege to limit access to essential resources, reducing the attack surface; comprehensive encryption for data in transit and at rest to protect against interception; and real-time behavioral monitoring with advanced analytics for prompt anomaly detection and response. Implementing Zero Trust in video surveillance involves asset identification to map cameras, users, and data flows for a security baseline; regular firmware updates and strong credentials to mitigate device vulnerabilities; network micro-segmentation to isolate infrastructure and prevent lateral threat movement; secure protocols like Transport Layer Security (TLS) to safeguard data transmission; and role-based access control (RBAC) to align permissions with operational roles. Continuous monitoring with analytics ensures proactive threat detection. Adopting Zero Trust enhances security, minimizes breach risks, and supports compliance with regulations like GDPR, though challenges such as infrastructure upgrades and device interoperability require careful management. Drawing on sources like NIST SP 800-207, this analysis outlines a rigorous framework for Zero Trust integration in video surveillance, enabling organizations to strengthen cybersecurity resilience and protect critical assets in a volatile digital landscape.

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

**فناوری های نوین در سیستم های توزیع شده و محاسبات الگوریتمی**

دانشگاه آزاد اسلامی واحد سبزوار

**E-ISSN: 3115-705X**

**https://sanad.iau.ir/journal/ntds**

**پژوهشی**

# ارائه راهکار پیاده‌سازی اعتماد صفر در سیستم‌های نظارت تصویری

**سید علی صموتی*[1] | سجاد طرهانی[2] | حسام حسن‌پور[3]**

[1] گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه آزاد اسلامی واحد سبزوار، سبزوار، ایران،
**Ali.Samouti@iau.ac.ir**

[2] گروه مهندسی مکاتروتیک، واحد علوم تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران،
Sajad.Tarhani@gmail.com

[3] گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه آزاد اسلامی واحد سبزوار، سبزوار، ایران،
**Hesamhasanpour@iau.ac.ir**

**نویسنده مسئول**

***سید علی صموتی**، دانشجو دکترای مهندسی فناوری اطلاعات، گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه آزاد اسلامی واحد سبزوار، سبزوار، ایران،
**Ali.Samouti@iau.ac.ir**

**موضوع اصلی:** پیاده سازی اعتماد صفر
**تاریخ دریافت:** ۱۴۰۴/۰۲/۱۴
**تاریخ بازنگری:** ۱۴۰۴/۰۲/۲۶
**تاریخ پذیرش:** ۱۴۰۴/۰۳/۱۴

https://doi.org/10.82195/ntds.2025.120572

## 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[1] به‌عنوان 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 قابل‌اعتماد نیست. در سیستم‌های نظارت تصویری که به طور مداوم اطلاعات حساسی را جمع‌آوری و ذخیره می‌کنند، پیاده‌سازی اعتماد صفر می‌تواند به طور قابل‌توجهی 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 نه‌تنها 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.

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

[1] Zero Trust - ZT

## ۱- مقدمه

در عصر دیجیتال، امنیت سایبری به یکی از مهم‌ترین چالش‌های 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 میان، معماری اعتماد صفر [1] به‌عنوان یک رویکرد نوین و مؤثر، جایگاه ویژه‌ای 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 پیش‌فرض قابل‌اعتماد نیست. معماری اعتماد صفر به معنای حذف فرضیات مربوط به اعتماد پیش‌فرض در شبکه‌های سازمانی است. در این رویکرد، هر درخواست دسترسی به منابع باید به طور دقیق بررسی و مراحل احراز هویت/اصالت و مجوزدهی به درخواست‌کننده تکمیل گردد. برخلاف مدل‌های سنتی که بر اساس موقعیت جغرافیایی یا عضویت در شبکه داخلی اعتماد می‌کنند، اعتماد صفر بر پایه اصولی مانند احراز هویت چندعاملی[2]، رمزنگاری داده‌ها و نظارت پیوسته بر فعالیت‌ها عمل می‌کند. این معماری به‌ویژه برای مقابله با حملات داخلی و خارجی طراحی شده است. [۷، ۱]

### ۱-۱- بیان مسئله

سیستم‌های نظارت تصویری، از جمله دوربین‌های مداربسته، به‌عنوان یکی از ابزارهای حیاتی در حفظ امنیت فیزیکی و سایبری شناخته می‌شوند. این سیستم‌ها اطلاعات حساسی را جمع‌آوری و ذخیره می‌کنند که می‌تواند هدف جذابی برای مهاجمان سایبری باشند. [۸, ۹] از نفوذ به دوربین‌ها برای دسترسی به تصاویر زنده گرفته تا سوءاستفاده از اطلاعات ذخیره‌شده، تهدیدات مرتبط با این سیستم‌ها به طور مداوم در حال افزایش است. بنابراین، تأمین امنیت این سیستم‌ها از اهمیت بالایی برخوردار است. معماری اعتماد صفر می‌تواند به طور قابل‌توجهی امنیت سیستم‌های نظارت تصویری را بهبود بخشد. با استفاده از این رویکرد، هر دستگاه نظارتی مانند دوربین‌ها باید قبل از دسترسی به شبکه، احراز اصالت شود و ارتباطات آن‌ها رمزنگاری گردد. علاوه بر این، نظارت پیوسته بر فعالیت‌های این دستگاه‌ها و شناسایی رفتارهای غیرعادی می‌تواند از وقوع حملات جلوگیری کند. اعتماد صفر همچنین به سازمان‌ها امکان می‌دهد 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 . [۱۳، ۹، ۳، ۱]

در ادامه این مقاله به تشریح کلی مفاهیم اعتماد صفر خواهیم پرداخت. در بخش دوم به معرفی کاربردهای مدل اعتماد صفر پرداخته می‌شود. بخش سوم به بررسی مفهوم معماری اعتماد صفر و ارکان آن اختصاص دارد. در بخش چهارم، معماری اعتماد صفر و نحوه پیاده‌سازی این مدل موردبررسی قرار می‌گیرد. در بخش پنجم، روش‌های پیاده‌سازی معماری اعتماد صفر تشریح می‌شود. بخش ششم به بررسی دلایل نیاز به اعتماد صفر در شبکه‌های نظارت تصویری می‌پردازد. در بخش هفتم، کاربرد معماری اعتماد صفر در دوربین‌های مداربسته بررسی می‌شود و در بخش هشتم، مزایای استفاده از این معماری در سامانه‌های نظارتی تبیین می‌گردد. در بخش نهم، راهکارهایی برای پیاده‌سازی اعتماد صفر در سیستم‌های نظارت تصویری ارائه می‌شود. نهایتاً، در بخش پایانی مقاله، جمع‌بندی مطالب مطرح‌شده ارائه خواهد شد.

### ۱-۲- روش‌شناسی

در این پژوهش، رویکردی ساختارمند برای گردآوری منابع علمی اتخاذ شد. ابتدا، بیش از ۵۰ منبع معتبر از پایگاه‌های علمی نظیرScopus ، ScienceDirectو Google Scholar جمع‌آوری گردید. این منابع شامل مقالات، گزارش‌های فنی و مطالعات مرتبط با امنیت سایبری و معماری اعتماد صفر بودند. پس از خوانش اولیه، ۲۰ مقاله که بیشترین هم‌راستایی را با موضوع پیاده‌سازی اعتماد صفر در سیستم‌های نظارت تصویری داشتند، انتخاب شدند. این مقالات شامل تحقیقات کاربردی و مروری بودند که دیدگاه

[1] Zero Trust Architecture - ZTA

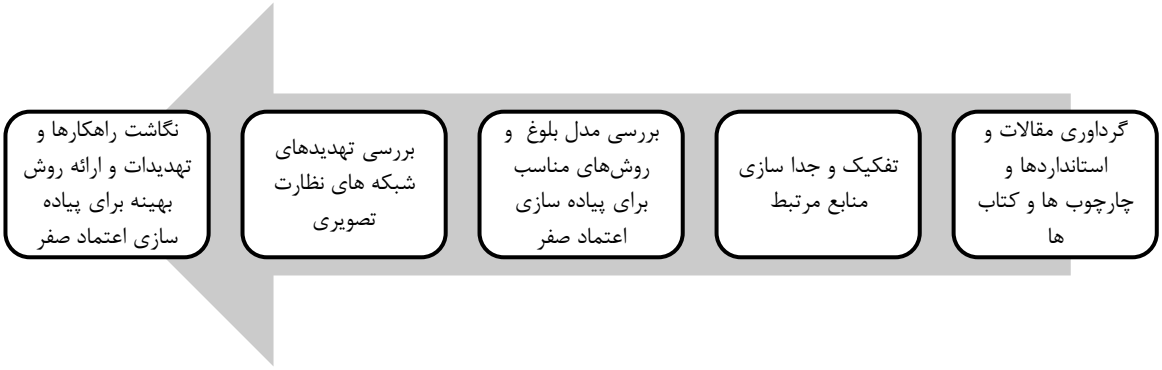
[2] Multi Factor Authentication - MFA

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، باتکیه‌بر 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.



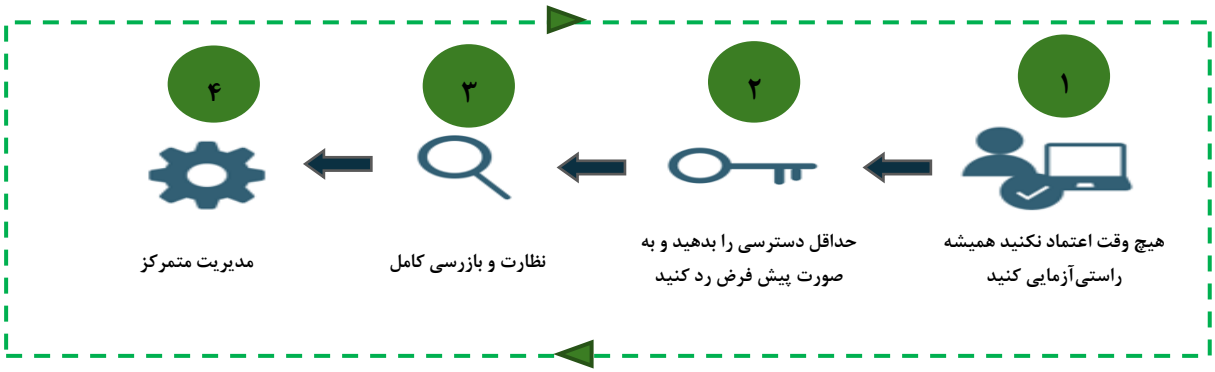

شکل ۱ : روش شناسی پژوهش
Figure 1: Research methodology

## ۱-۳- مروری بر کاربردهای اعتماد صفر و ادبیات پیشین

مطالعات متنوعی در زمینه اعتماد صفر صورت‌گرفته 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] به‌منظور مقابله با تهدیدات سایبری طراحی شده و بر اساس اصول "هرگز اعتماد نکن، همیشه تأیید کن" است. این استراتژی شامل چهار هدف اصلی است: فرهنگ‌سازی برای پذیرش صفر اعتماد، تأمین و دفاع از سیستم‌های اطلاعاتی، شتاب‌دهی به فناوری و توانمندسازی صفر اعتماد. از ویژگی‌های کلیدی آن می‌توان به تأکید بر احراز هویت چندعاملی و میکرو قطاع‌بندی اشاره کرد. هدف نهایی کاهش سطح حمله و افزایش امنیت اطلاعات و سیستم‌ها در برابر تهدیدات است. (شکل ۱)




شکل ۲: اصول اولیه اعتماد صفر بر مبنای دید امنیتی تطبیقی
Figure 1: Foundational Zero Trust principles operationalize an adaptive security approach

هریشکی در [۱۵] به بررسی تأثیر فناوری‌های نوظهور بر معماری اعتماد صفر و چالش‌های آن در زمینه امنیت سایبری می‌پردازد. باتوجه‌به تهدیدات پیچیده و در حال تغییر، ادغام فناوری‌های نوین مانند هوش مصنوعی، یادگیری ماشین، بلاک‌چین و محاسبات کوانتومی با اصول معماری اعتماد صفر، راهکارهای جدید و چالش‌های تازه‌ای را به همراه دارد. مقاله پیشنهاد می‌کند که سازمان‌ها باید استراتژی‌های معماری اعتماد صفر خود را به طور مداوم با پیشرفت‌های فناوری تطبیق دهند تا امنیت خود را در برابر تهدیدات سایبری تقویت کنند. همچنین مقاله [۱۳] به اهمیت ادغام فناوری بلاک‌چین و مدل امنیتی اعتماد صفر در حفاظت از سیستم‌های بانکی آنلاین اشاره دارد. بلاک‌چین با ایجاد یک دفترکل غیرمتمرکز و غیرقابل‌تغییر، شفافیت و یکپارچگی داده‌ها را افزایش می‌دهد، درحالی‌که مدل اعتماد صفر با تأیید هویت مداوم، سطح حمله را کاهش می‌دهد.

سند مدل بلوغ اعتماد صفر CISA [۱۶] که توسط آژانس امنیت سایبری و زیرساخت منتشر شده است، رویکردی ساختاریافته برای پیاده‌سازی معماری اعتماد صفر در سازمان‌ها ارائه می‌دهد. این مدل شامل پنج رکن اصلی است: شناسایی، دستگاه‌ها، شبکه‌ها، برنامه‌ها و بارهای کاری، و داده‌ها، و به سازمان‌ها کمک می‌کند تا مراحل لازم برای بهبود وضعیت امنیت سایبری خود را شناسایی و اجرا کنند. همچنین، چالش‌های موجود در پذیرش این مدل و اهمیت همکاری میان سطوح مختلف سازمانی را موردبررسی قرار می‌دهد. در نهایت، سند به سازمان‌ها توصیه می‌کند که با استفاده از این مدل، به‌تدریج و باتوجه‌به نیازهای خاص خود، به سمت پیاده‌سازی کامل معماری اعتماد صفر حرکت کنند.

پونام در [۱۲] ضمن بررسی معماری امنیتی اعتماد صفر و تشریح اصول اساسی آن چالش‌ها و فرصت‌های موجود در پیاده‌سازی این معماری را شناسایی کرده و مسیرهای تحقیقاتی آینده را شامل بهبود روش‌های احراز هویت، تحلیل تکنیک‌های کنترل دسترسی، اتوماسیون امنیتی و به‌کارگیری فناوری‌های نوین مانند بلاک‌چین و هوش مصنوعی پیشنهاد می‌کند.

نهار و همکاران در مقاله [۳] به بررسی معماری اعتماد صفر در شبکه‌های نسل ششم[1] 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 قابل‌توجهی 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 قابل‌توجهی در مسیر پذیرش آن وجود دارد. همچنین، ایجاد درک صحیح از این مدل برای کاهش شک‌وتردید 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 ۱۳۱۸٪ حملات سایبری، نیاز به یک چارچوب امنیتی قوی ضروری است. این مدل با استفاده از الگوریتم‌های اجماع بلاک‌چین، اطمینان از یکپارچگی و غیرقابل‌تغییربودن 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 قابل‌اعتماد 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[2] برای ایجاد ارتباطات امن و رمزگذاری‌شده در سازمان‌ها حیاتی هستند و امنیت داده‌ها را در حین انتقال تضمین می‌کنند.

[1] Sixth Generation Mobile Network - 6G
[2] Virtual Private Network - VPN

سلمنت در [۱] به بررسی پیاده‌سازی مدل اعتماد صفر در مؤسسات مالی می‌پردازد و بر حفاظت از داده‌ها، مدیریت هویت و دسترسی[1] و امنیت دستگاه و شبکه تأکید دارد. چارچوب پیشنهادی از طریق توسعه یک اپلیکیشن بانکی دمو ارزیابی شده و نقاط قوت و چالش‌های آن موردبحث قرار می‌گیرد. مؤسسات مالی با اجرای این مدل می‌توانند تأیید مداوم کاربران و دستگاه‌ها را بهبود بخشند و امنیت اطلاعات حساس را تضمین کنند.

نورعلی و همکاران در [۲۳] به بررسی ادغام مدل اعتماد صفر و فناوری بلاک‌چین در سیستم‌های بانکی آنلاین می‌پردازد و تأکید دارد که این رویکرد می‌تواند امنیت سایبری را به طور چشمگیری تقویت کند. مدل اعتماد صفر با تأیید مداوم درخواست‌های دسترسی، خطر دسترسی غیرمجاز را کاهش می‌دهد، درحالی‌که بلاک‌چین با ایجاد یک دفترکل غیرقابل‌تغییر، از تقلب و دست‌کاری داده‌ها جلوگیری می‌کند. این ادغام به مؤسسات مالی کمک می‌کند 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 می‌شود.

نعیم و همکاران در مقاله [۶] به تحلیل مدل امنیتی اعتماد صفر و اهمیت احراز هویت و کنترل دسترسی در زیرساخت‌های حیاتی می‌پردازد. همچنین، چالش‌ها و نیاز به تحقیقات بیشتر برای پیاده‌سازی مؤثر این مدل در محیط‌های پیچیده موردبررسی قرار می‌گیرد. همچنین سعید قاسمی و همکاران در [۲۴] به بررسی کاربردها و چالش‌های معماری اعتماد صفر می‌پردازد و نشان می‌دهد که این مدل باوجود پتانسیل بالا برای تقویت امنیت، با موانع فرهنگی و فنی قابل توجهی در پیاده‌سازی مواجه است. ادغام آن با فناوری‌های نوین مانند هوش مصنوعی می‌تواند به بهبود کارایی امنیتی کمک کند.

دیپا آجیش در [۲۵] با موضوع اهمیت هوش مصنوعی در فناوری‌های اعتماد صفر، به بررسی نقش کلیدی هوش مصنوعی در تقویت امنیت سایبری می‌پردازد. با افزایش استفاده از خدمات ابری، مدل‌های اعتماد صفر به‌عنوان راهکارهای جدید برای مقابله با تهدیدات سایبری ضروری شده‌اند. این مقاله تأکید می‌کند که هوش مصنوعی می‌تواند به شناسایی تهدیدات و بهبود فرایندهای امنیتی کمک کند. همچنین، جمع‌آوری داده‌های زمینه‌ای به هوش مصنوعی امکان می‌دهد تا واکنش‌های دقیق‌تری به رویدادهای امنیتی ارائه دهد.

یوانهانگ و همکاران در [۲۶] چالش‌ها و روندهای آینده به بررسی مدل امنیتی اعتماد صفر می‌پردازد که بر اساس تأیید هویت کاربران و دستگاه‌ها در همه شبکه‌ها طراحی شده است. این مقاله به چالش‌های 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 می‌کند.

مقاله [۲۷] به تحلیل چالش‌ها و مزایای مدل امنیت اعتماد صفر در سازمان‌ها می‌پردازد. باتوجه‌به نیاز به کار از راه دور ناشی از پاندمیCOVID19 ، این رویکرد امنیتی به‌عنوان یک راهکار ضروری برای مقابله با آسیب‌پذیری‌های جدید مطرح شده است. نویسندگان، کرنیلیوس ایتودو و مورات اوزر، یک چارچوب مفهومی جامع برای هدایت فرایند پیاده‌سازی این مدل ارائه می‌دهند که شامل ارزیابی وضعیت کنونی و آینده، نقشه‌راه پیاده‌سازی و نظارت مستمر است.

[1] Identity and Access Management - IAM

جدول ۱: مقایسه کلی مطالعات انجام شده در باره اعتماد صفر
Table 1: A synthesized comparative examination of Zero Trust research literature

| منبع | موضوع اصلی | مفاهیم کلیدی | اجزای اصلی | چالش‌ها | کاربردها و پیشنهادها |
|---|---|---|---|---|---|
| **NIST SP 800207 [4]** | معرفی و تبیین معماری اعتماد صفر | اصل "هرگز اعتماد نکن، همیشه تأیید کن"<br>تمرکز بر احراز هویت و مجوزدهی به‌جای مرزهای شبکه‌ای سنتی | احراز هویت چندعاملی (MFA)<br>میکرو قطاع‌بندی<br>زیرساخت نرم‌افزار تعریف‌شده(SDI) | پیچیدگی پیاده‌سازی<br>نیاز به تغییر فرهنگ‌سازمانی | راهنمای عملی برای معماران امنیت سایبری<br>مناسب برای مدیریت کاربران از راه دور و دارایی‌های ابری |
| **استراتژی DoD [۱۴]** | استراتژی اعتماد صفر وزارت دفاع آمریکا | چهار هدف: فرهنگ‌سازی، تأمین سیستم‌ها، شتاب‌دهی فناوری، توانمندسازی | احراز هویت چندعاملی<br>میکرو قطاع‌بندی | مقاومت سازمانی<br>نیاز به آموزش و فرهنگ‌سازی | کاهش سطح حمله<br>افزایش امنیت در برابر تهدیدات سایبری |
| **هریشکی [۱۵]** | تأثیر فناوری‌های نوظهور بر اعتماد صفر | ادغامAI ، ML، بلاک‌چین و محاسبات کوانتومی | احراز هویت مداوم<br>ارزیابی ریسک | پیچیدگی‌های فناوری جدید<br>نیاز به تطبیق مداوم | تطبیق استراتژی‌ها با پیشرفت‌های فناوری<br>تقویت امنیت سایبری |
| **مدل بلوغ CISA [۱۶]** | مدل بلوغ اعتماد صفر | پنج رکن: شناسایی، دستگاه‌ها، شبکه‌ها، برنامه‌ها، داده‌ها | احراز هویت<br>کنترل دسترسی<br>ارزیابی مداوم | همکاری بین سطوح سازمانی<br>موانع عملیاتی | پیاده‌سازی تدریجی<br>بهبود وضعیت امنیت سایبری |
| **پونام [۱۲]** | اصول و چالش‌های اعتماد صفر | اصول اساسی: عدم اعتماد پیش‌فرض، تأیید مداوم | احراز هویت<br>کنترل دسترسی<br>اتوماسیون امنیتی | موانع فنی و فرهنگی<br>پیچیدگی پیاده‌سازی | استفاده از AI و بلاک‌چین<br>تحقیقات در احراز هویت و اتوماسیون |
| **نهار و همکاران [۳]** | اعتماد صفر در شبکه‌های G۶ | نیاز به احراز هویت مداوم در شبکه‌های پیچیده | ارزیابی ریسک<br>کنترل دسترسی | افزایش پیچیدگی‌های امنیتی<br>تعداد بالای دستگاه‌ها | امنیت شبکه‌های نسل ششم<br>مدیریت دستگاه‌های متصل |
| **جان لوان [۱۷]** | اعتماد صفر در بانکداری دیجیتال | تأیید مداوم هویت‌ها<br>کاهش سطح حمله | احراز هویت<br>مدیریت دسترسی | چالش‌های تحول دیجیتال<br>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<br>کنترل دسترسی | مقاومت سازمانی<br>توازن امنیت و تجربه کاربری | استراتژی‌های مؤثر برای پیاده‌سازی |

| | | | | | |
|---|---|---|---|---|---|
| **چاندری و همکاران [۱۱]** | اعتماد صفر و بلاک‌چین در بانکداری | افزایش ۱۳۱۸٪ حملات سایبری<br>ادغام بلاک‌چین و اعتماد صفر | الگوریتم‌های اجماع بلاک‌چین<br>تأیید هویت مداوم | پیچیدگی ادغام فناوری‌ها | حفاظت از دارایی‌های بانکی<br>کاهش آسیب‌پذیری‌ها |
| **سارکار و همکاران [۲۰]** | اعتماد صفر در رایانش ابری | عدم اعتماد ضمنی به هیچ نهادی | احراز هویت<br>کنترل دسترسی | پیچیدگی‌های ابری<br>نیاز به بلوغ سازمانی | بهبود امنیت در محیط‌های ابری |
| **کتاب فصل ۱۲ [۲۱]** | اعتماد صفر در بانکداری و فین‌تک | همکاری در اکوسیستم‌هایAPI<br>اصل حداقل دسترسی | احراز هویت<br>مدیریت دستگاه و دسترسی | طراحی مناسب<br>پیچیدگی‌های محیط‌های مالی | کاهش خطرات سایبری<br>حفاظت از داده‌ها |
| **گوپتا [۲۲]** | تحول در امنیت سایبری با اعتماد صفر | تأیید مداوم در برابر تهدیدات پویا | هویت، دستگاه، شبکه، برنامه، داده<br>VPN برای ارتباطات امن | تغییر مدل‌های قدیمی<br>پیچیدگی پیاده‌سازی | تضمین امنیت داده‌ها در انتقال |
| **سلمنت [۱]** | اعتماد صفر در مؤسسات مالی | حفاظت از داده‌ها و مدیریت هویت | احراز هویت مداوم<br>امنیت دستگاه و شبکه | چالش‌های پیاده‌سازی اپلیکیشن | بهبود امنیت اطلاعات حساس |
| **نورعلی و همکاران [۲۳]** | ادغام بلاک‌چین و اعتماد صفر در بانکداری | دفترکل غیرقابل‌تغییر بلاک‌چین<br>تأیید مداوم دسترسی | احراز هویت<br>مدیریت هویت | پیچیدگی ادغام فناوری‌ها | ایجاد زیرساخت امنیتی قوی<br>حفاظت از داده‌های مشتریان |
| **نعیم و همکاران [۶]** | اعتماد صفر در زیرساخت‌های حیاتی | اهمیت احراز هویت و کنترل دسترسی | ارزیابی ریسک<br>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<br>اتوماسیون امنیتی | موانع فرهنگی و فنی | ادغام با AI برای بهبود کارایی |
| **دیپا آجیش [۲۵]** | نقش AI در اعتماد صفر | شناسایی تهدیدات با AI<br>جمع‌آوری داده‌های زمینه‌ای | تحلیل امنیتی<br>اتوماسیون | پیچیدگی ادغامAI | بهبود فرایندهای امنیتی<br>واکنش دقیق به تهدیدات |
| **یوانهانگ و همکاران [۲۶]** | چالش‌ها و روندهای آینده اعتماد صفر | تأیید هویت و کنترل دسترسی در همه شبکه‌ها | احراز هویت<br>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<br>نظارت مستمر | آسیب‌پذیری‌های کار از راه دور | نقشه راه پیاده‌سازی<br>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 به‌شدت 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،۶، 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 به‌سرعت 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 باتکیه‌بر 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 به‌سوی راهکارهای نوین را اجتناب‌ناپذیر کرده است.

معماری اعتماد صفر  به‌عنوان 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.

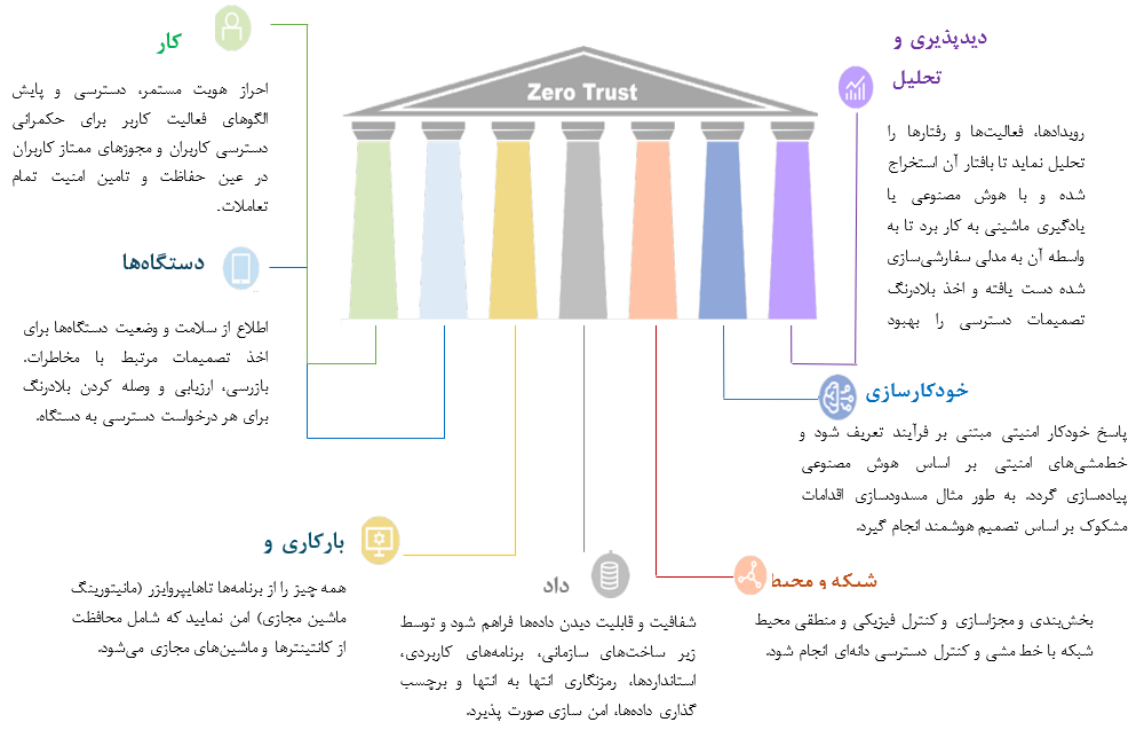
باوجود مزایای بالقوه، پیاده‌سازی معماری اعتماد صفر در سیستم‌های نظارت تصویری با چالش‌هایی نظیر نیاز به بازطراحی زیرساخت‌های امنیتی، هماهنگی میان دستگاه‌های متنوع، مدیریت هویت و دسترسی در مقیاس بزرگ، و حفظ عملکرد سیستم در حین اعمال سیاست‌های امنیتی همراه است. علاوه بر این، انطباق با الزامات قانونی و استانداردهای 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.

## ۲- مفهوم معماری اعتماد صفر و ارکان آن

معماری اعتماد صفر به‌عنوان 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، ۲،۱]

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 که در شکل ۳ نشان داده شده 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 . [۱۹، ۶۴، ۲]

یکی از اصول اصلی معماری اعتماد صفر، احراز هویت مداوم[1] 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]
Figure 2: Zero Trust Pillars [14]

[1] Continous Authentication

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]

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، قابل‌استفاده نباشند. علاوه بر این، استفاده از پروتکل‌های امن مانند TLS و VPN و همچنین مدیریت کلیدهای رمزنگاری به‌صورت 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[۱] و تحلیل رفتار کاربری[۲] 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 به‌سرعت به تهدیدات پاسخ دهند و از وقوع حملات جلوگیری کنند. استفاده از فناوری‌هایی مانند هوش مصنوعی[۳] و یادگیری ماشین[۴] برای شناسایی الگوهای تهدید و ایجاد پاسخ‌های خودکار، از جمله روش‌هایی است که به تحقق این هدف کمک می‌کند. [۱۷، ۶، ۵، ۳]

## ۳- معماری اعتماد صفر

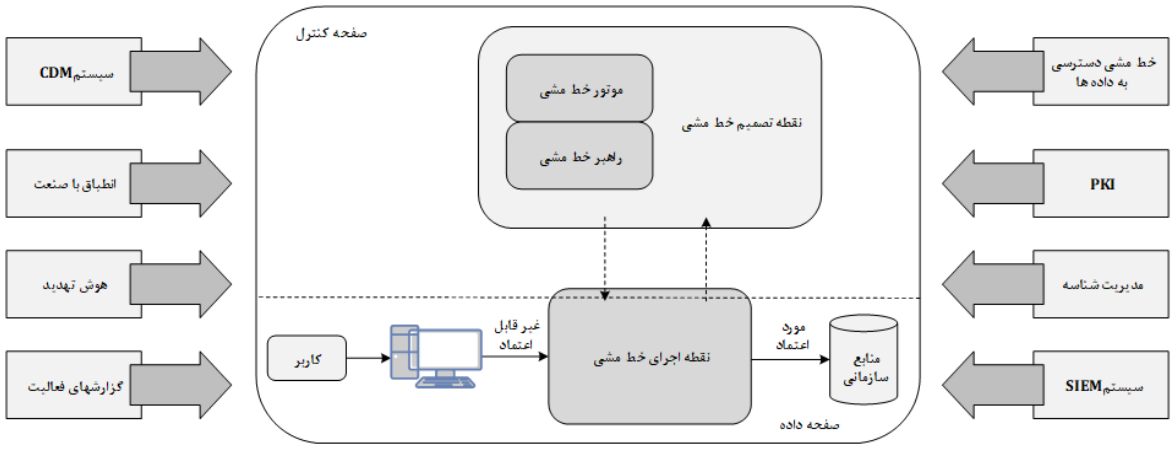
معماری اعتماد صفر به‌عنوان یکی از پیشرفته‌ترین رویکردهای امنیت سایبری، بر پایه اصل "هرگز اعتماد نکن و همیشه تأیید کن" طراحی شده است. این معماری برای مدیریت دسترسی به منابع سازمانی، از ابزارها و اجزای مختلفی استفاده می‌کند که موتور خط‌مشی[۵] و راهبر خط‌مشی[۶] از مهم‌ترین آن‌ها هستند. این دو بخش، نقش کلیدی در اجرای سیاست‌های امنیتی و مدیریت دسترسی ایفا می‌کنند. در ادامه، به بررسی جزئیات این دو مؤلفه در ادامه توضیح داده می‌شود. (شکل ۴) [۲۶، ۱۴، ۶۴، ۲]

### ۳-۱- 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. به‌طورکلی، موتور خط‌مشی وظیفه دارد که تمامی داده‌های مرتبط با درخواست دسترسی را تحلیل کرده و بر اساس سیاست‌های تعریف‌شده، تصمیم نهایی 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 به طور مؤثر به تهدیدات جدید پاسخ دهد . این موارد در شکل ۴ قابل‌بررسی است.[۶، ۴]

---

[1] Intrusion Detection Systems - IDS
[2] User Behavior Analytics - UBA
[3] Artificial Intelligence - AI
[4] Matchine learning - ML
[5] Policy Engine
[6] Policy Administrator




شکل ۴: مولفه‌های منطقی هسته معماری اعتماد صفر
Figure 3:Core logical components of a Zero Trust architecture

## ۳-۲- 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 است که اطلاعات هویتی کاربران را فراهم می‌کند. همچنین، ابزارهای مدیریت دستگاه‌های موبایل[1] و سیستم‌های تشخیص تهدید[2] نیز اطلاعاتی درباره وضعیت دستگاه‌ها و تهدیدات احتمالی ارائه می‌دهند. موتور خط‌مشی با تجمیع این داده‌ها و تحلیل آن‌ها، می‌تواند تصمیمات امنیتی دقیقی بگیرد. [۶، ۴]

## ۳-۳- 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. به‌عنوان‌مثال، 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. [۶، ۴]

## ۳-۴- 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، تصمیم نهایی 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

[1] Mobile Device Management - MDM
[2] Threat Detection Systems

آسیب‌پذیری جلوگیری کند. برای این منظور، از پروتکل‌های امن و مکانیزم‌های رمزنگاری برای ارتباط بین این دو مؤلفه استفاده می‌شود. [۲۶، ۱۹، ۵، ۴]

### ۳-۵- 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. [۲۶، ۱۹، ۵، ۴]

### ۳-۶- 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. به‌طورکلی، موتور خط‌مشی و راهبر خط‌مشی با ایجاد یک‌لایه اضافی از کنترل و نظارت، امنیت کلی سازمان را به طور قابل‌توجهی افزایش می‌دهند و به تحقق اهداف معماری اعتماد صفر کمک می‌کنند. [۲۶، ۱۹، ۵، ۴]

## ۴- روش‌های پیاده‌سازی معماری اعتماد صفر

معماری اعتماد صفر به‌عنوان یک رویکرد نوین در امنیت سایبری، به‌ویژه در دنیای پیچیده و متغیر فناوری اطلاعات امروز، به طور 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[۱]، مدل مبتنی بر کاربر[۲]، مدل مبتنی بر دستگاه[۳] و مدل ترکیبی[۴]. [۲۶، ۲۳، ۲۰، ۱۱، ۵، ۱]

### ۴-۱- مدل مبتنی بر شبکه

مدل مبتنی بر شبکه، به‌عنوان یکی از اساسی‌ترین رویکردها در معماری اعتماد صفر، بر پایه قطاع‌بندی شبکه [۵] و شبکه‌های تعریف شده مبتنی بر نرم‌افزار[۶] استوار است. قطاع‌بندی شبکه به معنای ایجاد بخش‌های کوچک‌تر و ایزوله در شبکه است که هر

[1] Network-Centric
[2] User-Centric
[3] Device-Centric
[4] Hybrid Model
[5] Micro-Segmentation
[6] Software Define Network - SDN

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.

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. به‌طورکلی، مدل مبتنی بر شبکه با کاهش سطح حمله و کنترل دقیق‌تر بر ترافیک، امنیت کلی سازمان را به طور قابل‌توجهی افزایش می‌دهد. [۲۶، ۲۳، ۲۰، ۱۱، ۵، ۱]

### ٤-۲- 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[1] 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 قابل‌توجهی 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 نه‌تنها تجربه کاربری را بهبود می‌بخشد، بلکه احتمال افشای رمز عبور را نیز کاهش می‌دهد. باتوجه‌به 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. [۲۶، ۲۳، ۲۰، ۱۱، ۵، ۱]

### ٤-۳- 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 موردبررسی قرار گیرد. این بررسی شامل ارزیابی وضعیت امنیتی، به‌روزرسانی‌های نرم‌افزاری و وجود نرم‌افزارهای مخرب می‌شود. این فرایند به‌عنوان یک‌لایه 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. به‌طورکلی، مدل مبتنی بر دستگاه با تمرکز بر اعتبارسنجی و مدیریت دستگاه‌ها، امنیت شبکه را به طور قابل‌توجهی افزایش می‌دهد. [۲۶، ۲۳، ۲۰، ۱۱، ۵، ۱]

### ٤-٤- 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. باتوجه‌به اینکه سازمان‌ها معمولاً با تهدیدات پیچیده و متنوعی مواجه هستند، استفاده از یک مدل ترکیبی می‌تواند به بهبود امنیت و کاهش ریسک‌ها کمک کند. به‌طورکلی، مدل

[1] Single Sign-On - SSO

ترکیبی به‌عنوان یک راهکار مقیاس‌پذیر و بهینه، می‌تواند به سازمان‌ها در تأمین امنیت اطلاعات و منابع خود کمک نماید. [۲۶، ۲۳، ۲۰، ۱۱، ۵، ۱]

## ۵-کاربرد معماری اعتماد صفر در دوربین‌های مداربسته

با ظهور خدمات ابری و افزایش تعداد دستگاه‌های متصل، شبکه‌ها به‌شدت پیچیده شده‌اند. جداسازی شبکه‌ها با دیوارهای آتش به دلیل این تحولات، دیگر به‌تنهایی کارآمد نیست. به‌عنوان‌مثال، 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 قابل‌اعتماد نیست. این رویکرد به سازمان‌ها این امکان را می‌دهد که هر درخواست دسترسی را به‌دقت 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 قطاع‌بندی 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. به‌این‌ترتیب، حتی اگر یک بخش از شبکه به خطر بیفتد، سایر بخش‌ها ایمن باقی می‌مانند. این رویکرد همچنین به شناسایی و محدودکردن تهدیدات کمک می‌کند. [۱۸، ۱۲، ۱]

با افزایش تعداد دستگاه‌های متصل به شبکه، تأمین امنیت آن‌ها اهمیت بیشتری پیدا می‌کند. بسیاری از دستگاه‌ها ممکن است به‌روزرسانی‌های 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 تجزیه‌وتحلیل دقیق ریسک‌ها و نیازهای خود پرداخته و استراتژی‌های مناسبی را برای پیاده‌سازی این مدل امنیتی طراحی کنند. این تغییر نه‌تنها به افزایش امنیت کمک می‌کند، بلکه می‌تواند به بهبود کارایی و بهره‌وری سازمان‌ها نیز منجر شود. جدول ۲ در باره کاربرد اعتماد صفر در سیستم های نظارت تصویری اشاره دارد. [۲۸]

با اتخاذ این رویکرد، سازمان‌ها می‌توانند تاب‌آوری 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 می‌دهیم.

### ۵-۱- روش پیشنهادی

در روش پیشنهادی باتوجه‌به مطالعات انجام شده برای شناسایی مخاطرات و تهدیدهای سیستم‌های نظارت تصویری در مقالات [۱۰ – ۸] که توسط نویسندگان تهیه شده است. رویکردی ارائه شده که باتوجه‌به روش‌های اعتماد صفرو مدل بلوغ و پیاده‌سازی تدریجی آن بتوان این راهکار را این سیستم‌ها پیاده کرد. برای این منظور مراحل و گام‌های شکل ۵ طی شده است.

جدول ۲: کاربرد اعتماد صفر در سیستم‌های نظارت تصویری
Table 2: Application of Zero Trust in Video Surveillance Systems

| 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<br>رمزنگاری داده‌ها<br>– میکرو قطاع‌بندی<br>استفاده از بلاک‌چین | حفاظت از حریم خصوصی<br>کاهش خطر نفوذ<br>انطباق با استانداردها (مانند GDPR) | [۲۸، ۲۰، ۱۸، ۱۷، ۱۲، ۵، ۲، ۱] |
| **احراز هویت چندعاملی** | استفاده از چندین روش تأیید (رمز عبور، کد یک‌بارمصرف، بیومتریک) برای جلوگیری از دسترسی غیرمجاز به سیستم‌های نظارت تصویری. | – ترکیب رمز عبور، کدهای ارسالی و بیومتریک<br>– تأیید مداوم هویت | کاهش احتمال نفوذ<br>افزایش امنیت در محیط‌های حساس | [۲۰، ۱۷، ۵، ۲] |
| **قطاع‌بندی شبکه** | جداسازی شبکه دوربین‌ها از سایر بخش‌های سازمان برای کاهش خطر نفوذ و بهبود مدیریت ترافیک شبکه. | – ایجاد شبکه مستقل برای دوربین‌ها<br>استفاده از دیواره‌های آتش و IDS/IPS<br>– میکرو قطاع‌بندی | محدودکردن گسترش تهدیدات<br>بهبود عملکرد و کنترل شبکه | [۱۹، ۱۸، ۱۴، ۱۲، ۷، ۵، ۴، ۱] |
| **کنترل دسترسی مبتنی بر نقش** | محدودکردن دسترسی کاربران به داده‌های موردنیاز بر اساس نقش‌های سازمانی برای جلوگیری از سوءاستفاده. | – تخصیص دسترسی بر اساس نقش<br>بازبینی و محدودسازی دسترسی‌ها | جلوگیری از دسترسی غیرمجاز<br>افزایش امنیت داده‌های حساس | [۲۶، ۱۴، ۷، ۵، ۴] |
| **نظارت و ثبت فعالیت‌ها** | ثبت و بررسی فعالیت‌های کاربران و دسترسی‌ها برای شناسایی تهدیدات و استفاده به‌عنوان شواهد در صورت بروز حادثه. | – ثبت زمان و نوع دسترسی‌ها<br>تحلیل رفتارهای مشکوک | شناسایی سریع تهدیدات<br>بهبود عملکرد سازمانی | [۲۴، ۲۱، ۱۴، ۴، ۱] |
| **به‌روزرسانی و وصله‌گذاری منظم** | به‌روزرسانی نرم‌افزارها و میان‌افزارهای دوربین‌ها برای رفع آسیب‌پذیری‌ها و افزایش مقاومت در برابر تهدیدات جدید. | – بررسی و اعمال پچ‌های امنیتی به‌روزرسانی منظم سیستم‌ها | کاهش خطرات امنیتی<br>بهبود عملکرد سیستم‌ها | [۲۶، ۲۴، ۲۲] |


شکل ۵: روش پیشنهادی و گام‌های طی شده
Figure 4: Proposed Method Overview

## ۵-۲- 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 قابل‌اعتماد 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 نه‌تنها 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[1] 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

[1] General Data Protection Regulation - GDPR

قوانین و استانداردها سازگار شوند. این رویکرد نه‌تنها از داده‌های حساس محافظت می‌کند، بلکه اعتماد مشتریان و کاربران را نیز جلب می‌کند. باتوجه‌به اهمیت روزافزون امنیت سایبری، امنیت اعتماد صفر برای دوربین‌ها و سایر دستگاه‌های متصل به شبکه یک ضرورت است.

### ۵-۳- 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]

### ۵-٤- قطاع‌بندی شبکه

تقسیم‌بندی یا قطاع‌بندی شبکه به معنای جداسازی بخش‌های مختلف شبکه است که دوربین‌ها و سیستم‌های نظارت تصویری در یک شبکه مستقل قرار می‌گیرند. این کار به کاهش خطر نفوذ به سایر بخش‌های سازمان کمک می‌کند. به‌عنوان‌مثال، اگر یک هکر به شبکه عمومی سازمان دسترسی پیدا کند، نمی‌تواند به‌راحتی به دوربین‌ها و داده‌های حساس دسترسی یابد. این روش همچنین به بهبود عملکرد شبکه کمک می‌کند، زیرا ترافیک مربوط به دوربین‌ها و سایر دستگاه‌ها به طور مستقل مدیریت می‌شود. با جداسازی شبکه، سازمان‌ها می‌توانند کنترل بیشتری بر دسترسی‌ها داشته باشند و در صورت بروز یک حمله، به‌سرعت اقدام کنند. این کار به‌ویژه در محیط‌های بزرگ و پیچیده که تعداد زیادی دوربین و دستگاه وجود دارد، حیاتی است. [۱۹، ۱۴، ۷، ۵، ۴]

### ۵-۵- کنترل دسترسی مبتنی بر نقش

کنترل دسترسی مبتنی بر نقش[1] روشی است که به سازمان‌ها این امکان را می‌دهد تا دسترسی به دوربین‌ها و داده‌های ضبط‌شده 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 می‌کند و امنیت کلی سیستم را افزایش می‌دهد. به‌عنوان‌مثال، یک کارمند امنیتی ممکن است به‌تمامی دوربین‌ها دسترسی داشته باشد، درحالی‌که یک کارمند اداری تنها به دوربین‌های مربوط به بخش خود دسترسی خواهد داشت. این نوع کنترل دسترسی به سازمان‌ها کمک می‌کند تا از سوءاستفاده‌های احتمالی جلوگیری کنند و اطمینان حاصل کنند که تنها افراد مجاز به اطلاعات حساس دسترسی دارند . [۲۶، ۱۴، ۷، ۵، ۴]

### ۵-٦- نظارت و ثبت فعالیت‌ها

پیاده‌سازی سیستم‌های نظارتی برای ثبت و بررسی فعالیت‌های کاربران و دسترسی‌ها به دوربین‌ها از اهمیت بالایی برخوردار است. این سیستم‌ها می‌توانند اطلاعات دقیقی درباره زمان، نوع دسترسی و فعالیت‌های انجام‌شده توسط کاربران را ثبت کنند. این اطلاعات به شناسایی و پاسخ به تهدیدات کمک می‌کند و در صورت وقوع یک حادثه، می‌توانند به‌عنوان شواهد مورداستفاده قرار گیرند. همچنین، نظارت بر فعالیت‌ها به مدیران این امکان را می‌دهد که رفتارهای مشکوک را شناسایی کنند و اقدامات لازم را

[1] Role Base Access Control - RBAC

انجام دهند. در نتیجه، این سیستم‌ها نه‌تنها به افزایش امنیت کمک می‌کنند، بلکه به بهبود عملکرد کلی سازمان نیز می‌انجامند . [۲۱، ۱۴، ۷، ۴، ۱]

### ۵-۷- به‌روزرسانی و وصله‌گذاری منظم

اطمینان از به‌روزرسانی منظم نرم‌افزار دوربین‌ها و سیستم‌های وابسته به‌منظور جلوگیری از آسیب‌پذیری‌ها و تهدیدات جدید بسیار حائز اهمیت است. باگذشت زمان، ممکن است باگ‌ها و آسیب‌پذیری‌های نرم‌افزارها توسط مهاجمان یا محققان کشف شوند که می‌تواند به نفوذگران اجازه دسترسی به سیستم را بدهد؛ بنابراین، سازمان‌ها باید به طور مداوم نرم‌افزارهای خود را بررسی و به‌روزرسانی کنند تا از جدیدترین پچ‌ها و بهبودها بهره‌مند شوند. این کار به کاهش خطرات امنیتی کمک می‌کند و اطمینان حاصل می‌کند که سیستم‌ها در برابر تهدیدات جدید مقاوم هستند. به‌علاوه، به‌روزرسانی‌های منظم می‌توانند به بهبود عملکرد دوربین‌ها و سیستم‌های نظارت تصویری نیز کمک کنند. [۲۶، ۲۴، ۲۲]

### ۶- مزایای استفاده از معماری اعتماد صفر در دوربین‌های مداربسته

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

### ۷- ارائه راهکار برای پیاده‌سازی اعتماد صفر در سیستم‌های نظارت تصویری

معماری اعتماد صفر به‌عنوان یکی از رویکردهای پیشرفته در امنیت سایبری، راهکاری جامع برای مقابله با تهدیدات پیچیده و روزافزون ارائه می‌دهد. این معماری، با اصل بنیادین "هرگز اعتماد نکن، همیشه تأیید کن"، امکان مدیریت دقیق دسترسی به منابع حساس را فراهم می‌کند. در زمینه سیستم‌های نظارت تصویری، به‌ویژه دوربین‌های مداربسته، پیاده‌سازی اعتماد صفر می‌تواند امنیت این سامانه‌ها را به طور چشمگیری بهبود بخشد. این مقاله به بررسی راهکارهای علمی و عملی برای اعمال معماری اعتماد صفر در چهار بخش کلیدی سیستم‌های نظارت تصویری شامل کاربران، دستگاه‌های دوربین، شبکه و انتقال داده‌ها می‌پردازد. [۲۲، ۲۰، ۱۶، ۱۵، ۵، ۱،۴]

کاربران، شناسایی و تأیید هویت کاربران به طور مداوم از اصول اساسی این معماری است. این فرایند نه‌تنها در زمان ورود به سیستم، بلکه در طول تعاملات کاربر با سیستم نیز باید انجام شود تا از دسترسی غیرمجاز جلوگیری گردد. دستگاه‌های دوربین، اطمینان از اینکه تنها دستگاه‌های مجاز به شبکه متصل می‌شوند، یکی دیگر از ارکان این رویکرد است. این امر به همراه استفاده از روش‌های رمزنگاری امن برای انتقال اطلاعات، به حفاظت از داده‌های حساس کمک می‌کند و امکان نفوذ به سیستم را کاهش می‌دهد. شبکه، ایجاد شبکه‌های مجزا و امن، به کاهش سطح آسیب‌پذیری کمک می‌کند. با تفکیک شبکه‌ها، حتی در صورت نفوذ به یکی از آن‌ها، امکان دسترسی به سایر بخش‌ها محدود می‌شود. انتقال داده‌ها، استفاده از پروتکل‌های امن مانند TLS برای حفاظت از داده‌ها در حین انتقال، از دیگر جنبه‌های حیاتی این معماری است. این پروتکل‌ها تضمین می‌کنند که اطلاعات در برابر حملات سایبری محافظت شده و از امنیت لازم برخوردارند. در مجموع، اجرای معماری اعتماد صفر در سیستم‌های نظارت تصویری می‌تواند به طور قابل‌توجهی امنیت این سیستم‌ها را افزایش دهد و از تهدیدات سایبری محافظت کند، به‌ویژه در دنیای امروز که حملات سایبری به طور فزاینده‌ای رایج شده‌اند. [۱۴، ۱۰، ۷، ۴]

جدول ۳: مزایای کاربری اعتماد صفر در سیستم‌های نظارت تصویری
Table 3: Operational Benefits of Zero Trust in Video Surveillance Systems

| مزیت | توضیحات | ویژگی‌های کلیدی | منابع |
|---|---|---|---|
| **افزایش امنیت** | نقاط ضعف سیستم‌های نظارت تصویری به حداقل می‌رسد و کنترل بیشتری بر دسترسی‌ها فراهم می‌شود. تنها کاربران باهویت تأییدشده (از طریق احراز هویت چندعاملی و بررسی رفتار) به داده‌های دوربین دسترسی دارند. | – احراز هویت چندعاملی (MFA)<br>– بررسی رفتار کاربران | [۲۲، ۱۵، ۱۴، ۹، ۳] |
| **کاهش خطر نفوذ** | با تأکید بر احراز هویت مداوم و نظارت مستمر بر فعالیت‌ها، خطر نفوذ به سیستم‌های دوربین کاهش می‌یابد. رفتارهای مشکوک به‌سرعت شناسایی و مدیریت می‌شوند. | – تأیید هویت مداوم<br>– نظارت مستمر بر فعالیت‌ها | [۲۷، ۲۲، ۱۴، ۹، ۳] |
| **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<br>– کاهش زمان واکنش | [۲۲، ۱۴، ۹، ۶، ۵، ۳] |
| **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<br>– حفاظت از داده‌های حساس | [۶۳، ۲۲، ۱۴، ۹] |
| **افزایش انطباق با استانداردها** | پیاده‌سازی سیاست‌های دسترسی و نظارت، انطباق با الزامات قانونی و استانداردهای امنیتی را بهبود می‌بخشد. فعالیت‌ها مستند شده و قابل‌پیگیری هستند. | – مستندسازی فعالیت‌ها<br>– انطباق با مقررات | [۲۷، ۲۲، ۱۷، ۱۴، ۹، ۴، ۲] |
| **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<br>– بهینه‌سازی منابع | [۲۲، ۲۰، ۱۵، ۵، ۴، ۱] |

## ۷-۱- شناسایی و تشخیص دارایی‌ها: پایه‌گذاری امنیت ساختاریافته

اولین گام در پیاده‌سازی معماری اعتماد صفر، شناسایی دقیق دوربین‌ها، کاربران مجاز و جریان‌های داده‌ای مرتبط است. این فرایند شامل ایجاد یک نقشه جامع از تمامی دستگاه‌ها، مسیرهای انتقال داده و نقاط دسترسی می‌شود. شناسایی مدل دوربین‌ها، نسخه‌های میان‌افزار[1]، موقعیت فیزیکی و نحوه ارتباط آن‌ها با شبکه، امکان تحلیل آسیب‌پذیری‌ها و شناسایی نقاط ضعف را فراهم می‌کند. همچنین، نقشه‌برداری از جریان داده‌ها (مانند انتقال تصاویر به سرور مرکزی یا فضای ابری) برای تعیین مکان‌های بالقوه

[1] Firmware version

نفوذ ضروری است. این مرحله به سازمان‌ها کمک می‌کند تا پایه‌ای ساختاریافته برای اعمال سیاست‌های امنیتی فراهم کنند و کنترل دقیقی بر دارایی‌های خود اعمال نمایند. [۲۲، ۲۰، ۱۵، ۵، ۴، ۱]

### ۷-۲- احراز هویت چندمرحله‌ای: 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 یک‌بارمصرف[1] ، و احراز هویت بیومتریک (مانند اثر انگشت یا تشخیص چهره)، سطح امنیتی سیستم را افزایش می‌دهد. علاوه بر این، اصل حداقل دسترسی باید اعمال شود، به‌گونه‌ای که هر کاربر تنها به داده‌ها و بخش‌هایی که برای انجام وظایف خود نیاز دارد، دسترسی داشته باشد. بازبینی دوره‌ای دسترسی‌ها و حذف دسترسی‌های غیرضروری نیز از دیگر اقدامات ضروری در این بخش است. این کنترل‌ها از سوءاستفاده احتمالی کاربران داخلی یا نفوذگران خارجی جلوگیری می‌کند. [۲۲، ۲۰، ۱۵، ۵، ۴، ۱]

### ۷-۳- ایمن‌سازی دستگاه‌های دوربین: حفاظت از نقاط انتهایی شبکه

دوربین‌های مداربسته به‌عنوان نقاط انتهایی[2] 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 منحصربه‌فرد جایگزین شوند. غیرفعال‌کردن قابلیت‌های غیرضروری مانند دسترسی از راه دور بدون رمزنگاری و پروتکل‌های ناامن (مانند Telnet یاFTP ) 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، نه‌تنها از نفوذ به دستگاه‌ها جلوگیری می‌کند، بلکه امنیت داده‌های حساس را نیز تضمین می‌نماید. [۲۲، ۲۰، ۱۵، ۵، ۴، ۱]

### ۷-۴- ایمن‌سازی شبکه: ایجاد زیرساختی مقاوم در برابر تهدیدات

شبکه‌ای که دوربین‌های مداربسته 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 دیواره‌های آتش و سیستم‌های تشخیص و پیشگیری از نفوذ[3] نیز امکان شناسایی و مسدودسازی ترافیک مشکوک را فراهم می‌کند. نظارت مداوم بر ترافیک شبکه و تحلیل فعالیت‌های غیرعادی، به‌عنوان یک‌لایه اضافی امنیتی، از اهمیت ویژه‌ای برخوردار است. [۱۵، ۱۳، ۱]

### ۷-۵- ایمن‌سازی انتقال و ذخیره‌سازی داده‌ها: حفاظت از داده‌های حساس

داده‌های تولیدشده توسط دوربین‌های مداربسته، 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 دستیاری 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

[1] One Time Password - OTP
[2] Endpoints
[3] Intrusion Detection Systems / Intrusion Prevention Systems - IDS/IPS

مداوم نظارت و بررسی گردد. این اقدامات از سرقت، دست‌کاری یا ازدست‌رفتن داده‌های حساس جلوگیری می‌کند. [۲۷، ۲۲، ۲۰، ۱۷، ۱۵، ۱۴، ۹، ۴، ۲، ۱]

## ۸- 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، می توان 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
Table 4: Maturity Concepts in Zero Trust Implementation for Video Surveillance Networks

| رکن | سنتی | ابتدایی | پیشرفته | بهینه |
|---|---|---|---|---|
| **هویت** | احراز هویت با رمز عبور یا احراز هویت چندگانه ساده، ذخیره‌سازی داخلی، دسترسی ایستا، ارزیابی دستی مخاطرات | احراز هویت چندگانه با عوامل ترکیبی، ذخیره‌سازی داخلی و ابری با یکپارچگی محدود، دسترسی موقت، ارزیابی دستی | احراز هویت چندگانه مقاوم در برابر فیشینگ، ذخیره‌سازی یکپارچه، دسترسی جلسه محور، تحلیل خودکار مخاطرات | احراز هویت مداوم، ذخیره‌سازی کاملاً یکپارچه، دسترسی پویا و 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 قطاع‌بندی، رمزگذاری جامع، مدیریت پویای ترافیک، تاب‌آوری گسترده | میکرو قطاع‌بندی 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[1] | 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 |

### ۸-۱- 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.

[1] Continuous Integration / Continuous Delivery or Continuous Deployment - CI/CD

### ۸-۲- 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 قابل‌توجهی ارتقا می‌دهد.

### ۸-۳- 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 قطاع‌بندی پویا تکامل می‌یابد. در سطح ابتدایی، رمزگذاری ترافیک داخلی و پایش مبتنی بر شاخص‌های شناخته‌شده تهدید[1] آغاز می‌گردد. در سطح پیشرفته، میکرو قطاع‌بندی (قطاع‌بندی) گسترده، رمزگذاری جامع و مدیریت پویای ترافیک با خودکارسازی تقویت می‌شود. در سطح بهینه، معماری شبکه با میکرو قطاع‌بندی 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.

### ۸-٤- 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[2]، 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.

### ۸-۵- 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 ویدئویی و مرتبط را به طور کامل تضمین می‌کند.

---

[1] Indicator of Compromise
[2] Context

## ۹- 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 قابل‌توجهی 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 امکان را می‌دهد که به‌سرعت به تهدیدات پاسخ دهند. همچنین، با بهبود مدیریت داده‌ها و افزایش انطباق با استانداردهای امنیتی، سازمان‌ها می‌توانند از نشت داده‌ها جلوگیری کرده و اعتماد مشتریان و کاربران را جلب کنند.

در نهایت، اگرچه پیاده‌سازی معماری اعتماد سفر ممکن است در ابتدا هزینه‌بر به نظر برسد، اما در بلندمدت می‌تواند به کاهش هزینه‌های امنیتی و افزایش کارایی سازمان‌ها منجر شود. باتوجه‌به افزایش روزافزون تهدیدات سایبری و اهمیت حفاظت از داده‌های حساس، استفاده از این رویکرد در سیستم‌های دوربین‌های مداربسته یک ضرورت اجتناب‌ناپذیر است. سازمان‌ها باید به طور مستمر به بررسی و به‌روزرسانی استراتژی‌های امنیتی خود بپردازند تا از منابع خود به بهترین نحو محافظت کنند و تاب‌آوری خود را در برابر حملات سایبری افزایش دهند.

## ۱۰- منابع


[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. Adebiyi, "Zero Trust Architecture: Trend and Impacton 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.