ITRC
ICT Research Institute
(Iran Telecommunication Research Center)

Journal of Information and Communication Technology

Iranian Society of Information and Communication Technology

Volume 18, Issue 68-69, Spring and Summer 2026, pp. 85-99

A Dynamic Cybersecurity Risk Assessment Framework for SCADA-based Industrial Control Systems

Seyed Mehdi Hosseini[1], Mohammad Ali Pourmina[2], Ahmad Fakharian[3*], Mehdi Khatir[4]

[1]Department of Electrical and Computer Engineering, SR.C., Islamic Azad University, Tehran, Iran
[2]Department of Electrical and Computer Engineering, SR.C., Islamic Azad University, Tehran, Iran
[3]Department of Electrical Engineering, Qa.C., Islamic Azad University, Qazvin, Iran
[4]Department of Electrical and Computer Engineering, SR.C., Islamic Azad University, Tehran, Iran

Received: 09 May 2026, Revised: 20 June 2026, Accepted: 23 June 2026
Paper type: Research

Abstract

Industrial Control Systems (ICS), particularly Supervisory Control and Data Acquisition (SCADA) systems, constitute the backbone of critical infrastructure operations worldwide. The increasing convergence of Operational Technology (OT) with Information Technology (IT) networks has created unprecedented cybersecurity challenges, evidenced by sophisticated attacks including Stuxnet (2010), the Ukraine power grid incident (2015), and the Colonial Pipeline ransomware attack (2021). These systems demand exceptional reliability with 99.999% availability and sub-10ms latency for Programmable Logic Controllers. Conventional risk assessment methodologies exhibit significant qualitative limitations due to their static nature and inability to model dynamic threats, asset interdependencies, and temporal variations in operational context. This research introduces an advanced dynamic cybersecurity risk assessment framework specifically designed for SCADA systems in high-sensitivity industrial environments. The framework incorporates seven integrated components: layered asset valuation with damage impact weighting, Multilayer and Dynamic Bayesian Networks for probabilistic threat modeling, offline CVSS and ISO/IEC 18045 scoring mechanisms, decision-tree-based risk assessment aligned with IEC 62443 standards, secure state transition controllers, game-theoretic optimization for adaptive defense strategies, and a Random Forest-based mitigation recommender. Through comprehensive MATLAB simulations, the framework demonstrates substantial improvements over static baselines, achieving a significant reduction in assessment uncertainty and an average risk score reduction of 28% across all assets, while maintaining false positive rates below 5%.

Keywords: Cybersecurity Risk Assessment, SCADA Security, Industrial Control Systems, Critical Infrastructure Protection, Machine Learning, Bayesian Networks.

* Corresponding Author's email: ahmad.fakharian@iau.ac.ir

دوفصلنامه
فناوری اطلاعات و ارتباطات ایران

سال هجدهم، شماره‌های ۶۸ و ۶۹ ، بهار و تابستان ۱۴۰۵، صفحه ۸۵ الی ۹۹

چارچوب ارزیابی پویای ریسک امنیت سایبری برای سیستم‌های کنترل صنعتی مبتنی بر SCADA

سید مهدی حسینی[۱]، محمدعلی پورمینا[۲]، احمد فخاریان[۳*]، مهدی خطیر[۴]

[۱]دانشجوی دکتری، گروه مهندسی برق(کنترل و سیستم)، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران

[۲]استاد گروه الکترونیک و مخابرات، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران

[۳]استاد، گروه مهندسی برق، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران

[۴]استاد گروه الکترونیک و مخابرات، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران

تاریخ دریافت: ۱۹/۰۲/۱۴۰۵ تاریخ بازبینی: ۳۰/۰۳/۱۴۰۵ تاریخ پذیرش: ۰۲/۰۴/۱۴۰۵

نوع مقاله: پژوهشی

چکیده

سیستم‌های کنترل صنعتی، به‌خصوص سیستم‌های کنترل نظارتی و اکتساب داده(SCADA) ، نقش محوری در مدیریت زیرساخت‌های حیاتی دارند. همگرایی روزافزون فناوری‌های عملیاتی با شبکه‌های فناوری اطلاعات، چالش‌های امنیتی پیچیده‌ای را به وجود آورده که در حملاتی چون استاکس‌نت، حادثه شبکه برق اوکراین و باج‌افزار کلونیال پایپ‌لاین نمود یافته است. این سیستم‌ها باید قابلیت اطمینان فوق‌العاده‌ای با دردسترس‌بودن بالای ۹۹,۹۹۹٪ و تأخیر کمتر از ۱۰ میلی‌ثانیه برای کنترل‌کننده‌های منطقی قابل‌برنامه‌ریزی(PLCها) داشته باشند. روش‌های سنتی ارزیابی ریسک به دلیل ماهیت ایستای خود، قادر به مدل‌سازی تهدیدات پویا، وابستگی‌های میان دارایی‌ها و تغییرات زمانی در شرایط عملیاتی نیستند. در این پژوهش، چارچوبی پیشرفته برای ارزیابی پویای ریسک امنیت سایبری ارائه شده که مخصوص سیستم‌های SCADA در محیط‌های صنعتی حساس طراحی شده است. این چارچوب هفت مؤلفه یکپارچه دارد، ارزش‌گذاری مبتنی بر لایه‌بندی دارایی‌ها با ضرایب وزنی تأثیر خسارت، شبکه‌های بیزین چندلایه و پویای برای مدل‌سازی احتمالاتی تهدیدها، امتیازدهی آفلاین سیستم امتیازدهی آسیب‌پذیری مشترک (CVSS) وISO/IEC 18045 ، ارزیابی ریسک مبتنی بر درخت تصمیم منطبق با استاندارد IEC 62443، کنترل‌کننده حالت ایمن، بهینه‌سازی نظریه بازی برای راهبردهای دفاعی و سیستم توصیه‌گر مبتنی بر الگوریتم جنگل تصادفی (Random Forest). شبیه‌سازی‌های گسترده در نرم‌افزار متلب نشان می‌دهد که این چارچوب نسبت به روش‌های ایستا، کاهش متوسط ۲۸٪ در نمره ریسک تمام دارایی‌ها را محقق می‌کند و نرخ مثبت کاذب را زیر ۵٪ نگه می‌دارد.

کلیدواژگان: ارزیابی ریسک امنیت سایبری، امنیت SCADA سیستم‌های کنترل صنعتی، حفاظت زیرساخت حیاتی، یادگیری ماشین، شبکه‌های بیزین.

* رایانامهٔ نویسنده مسؤول: ahmad.fakharian@iau.ac.ir

۱- مقدمه

سیستم‌های کنترل صنعتی پایه و اساس فناوری جوامع امروزی را تشکیل می‌دهند و وظیفه مدیریت طیف گسترده‌ای از خدمات حیاتی را بر عهده دارند - از تولید برق و تصفیه آب گرفته تا فرایندهای تولیدی و شبکه‌های حمل‌ونقل. در این میان، سیستم‌های SCADA نقش سیستم عصبی مرکزی را ایفا می‌کنند و امکان نظارت و کنترل بلادرنگ بر دارایی‌های پراکنده جغرافیایی را فراهم می‌آورند [۱]. تحول دیجیتال در فرایند عملیات صنعتی، علی‌رغم بهبود چشمگیر کارایی این سیستم‌ها، تهدیدات پیچیده سایبری را به همراه داشته که اقدامات پیشگیرانه امنیتی معمول توان مقابله با آن‌ها را ندارند.

ادغام فناوری‌های عملیاتی با فناوری اطلاعات، در کنار فراهم‌کردن قابلیت‌های تحلیل پیشرفته و مدیریت از راه دور، منظره تهدید برای سیستم‌های کنترل صنعتی را به‌کلی دگرگون ساخته است [۲]. برخلاف سیستم‌های IT که شاخص محرمانگی در آن‌ها اولویت دارد، در سیستم‌های کنترل صنعتی، شاخص‌های در دسترس‌بودن و یکپارچگی اهمیت بیشتری دارند و این امر چالش‌های امنیتی خاصی را به همراه دارد. الزامات دقیق عملیاتی این سیستم‌ها شامل در دسترس‌بودن ۹۹,۹۹۹٪ و محدودیت تأخیر زیر ۱۰ میلی‌ثانیه برای PLCها است که مستلزم رویکردهای امنیتی تخصصی با حداقل اختلال در فرآیندهای حساس می‌باشد [۳].

حوادث اخیر به‌روشنی نشان داده‌اند که سیستم‌های (ICS) فعلی تا چه حد آسیب‌پذیرند. کرم استاکس‌نت[۱] در سال ۲۰۱۰ نشان داد که می‌توان از طریق ابزارهای سایبری به تجهیزات فیزیکی آسیب رساند [۴]، درحالی‌که حمله به شبکه برق اوکراین در ۲۰۱۵ موجب قطع برق ۲۳۰ هزار مشترک شد و ثابت کرد زیرساخت‌های حیاتی همچنان اهداف قابل‌دسترسی برای مهاجمان پیچیده هستند [۵]. اخیراً نیز باج‌افزار کلونیال پایپ‌لاین در ۲۰۲۱، تأمین سوخت به ۴۵٪ ساحل شرقی آمریکا را مختل کرد و عواقب زنجیره‌ای حملات سایبری به سیستم‌های صنعتی را آشکار ساخت [۶].

روش‌های مرسوم ارزیابی ریسک امنیت سایبری که معمولاً ریسک را حاصل‌ضرب احتمال تهدید، آسیب‌پذیری و ارزش دارایی محاسبه می‌کنند [۷]، برای محیط‌های پویای ICS امروزی کافی نیستند [۸]. این روش‌های ایستا قادر نیستند وابستگی‌های پیچیده میان دارایی‌ها، تکامل زمانی تهدیدها و تفاوت تأثیر خسارت‌ها را در شرایط عملیاتی مختلف لحاظ کنند. نتیجه این امر، ارزیابی ناکافی وضعیت ریسک و تخصیص نادرست منابع امنیتی است [۹].

این مقاله چارچوبی جامع برای ارزیابی پویای ریسک ارائه می‌دهد که بر اساس منظره تهدیدات پویا و محدودیت‌های عملیاتی سیستم‌های SCADA طراحی شده و خلأهای روش‌های سنتی را پر می‌کند. نوآوری اصلی این پژوهش در مدل‌سازی تأثیر خسارت با طبقه‌بندی دارایی‌ها در چهار سطح عملیاتی و محاسبه ضرایب وزنی است که کمی‌سازی ریسک را دقیق‌تر می‌سازد. با بهره‌گیری از مدل‌سازی احتمالاتی، نظریه بازی و یادگیری ماشین، راهکاری عملیاتی برای متخصصان امنیت صنعتی ارائه شده است.

ساختار مقاله بدین صورت است: بخش دوم مروری بر ادبیات و محدودیت‌های موجود است. بخش سوم چارچوب ارزیابی ریسک پویا را تشریح می‌کند. بخش چهارم نتایج شبیه‌سازی‌ها را شامل تحلیل کاهش ریسک در لایه‌های معماری پوردو، معیارهای تشخیص عملکرد (Detection Metrics)، حساسیت و پایداری در برابر عدم قطعیت (Uncertainty) ارائه می‌دهد. بخش پنجم مقایسه‌ای با روش‌های سنتی دارد. بخش آخر نیز به نتیجه‌گیری و پیشنهادهای پژوهشی آتی می‌پردازد.

۲- مرور ادبیات

۲-۱- محدودیت‌های ارزیابی‌های سنتی ریسک

روش‌های مرسوم ارزیابی ریسک که برای سیستم‌های IT عمومی طراحی شده‌اند، به طور وسیعی در سیستم‌های کنترل صنعتی استفاده می‌شوند، اما کارایی آن‌ها در مواجهه با چالش‌های خاص ICS همواره مورد تردید بوده است. تحلیل حالت شکست و اثرات، اگرچه برای شناسایی نقاط شکست احتمالی مفید است، اما به‌شدت به قضاوت ذهنی متخصصان وابسته بوده و در کمی‌سازی پیامدهای زنجیره‌ای حملات سایبری در سیستم‌های به‌هم‌پیوسته ناتوان است [۹]. رویکرد خطی این روش نمی‌تواند حلقه‌های بازخورد پیچیده و وابستگی‌های متقابل معماری‌های SCADA مدرن را به‌درستی مدل‌سازی کند.

تحلیل درخت خطا روشی منظم برای یافتن علل ریشه‌ای خرابی‌های سیستم ارائه می‌دهد، ولی هنگام کاربرد در تهدیدات سایبری پویا،

[۱] استاکس‌نت (Stuxnet): کرم رایانه‌ای پیچیده که در سال ۲۰۱۰ تأسیسات غنی‌سازی اورانیوم نطنز ایران را هدف قرار داد و نخستین سلاح سایبری شناخته شده در تاریخ به‌شمار می‌رود که توانست به تجهیزات فیزیکی صنعتی آسیب وارد کند.

محدودیت‌های آشکاری دارد. ماهیت ثابت درخت‌های خطا قادر به مدل‌سازی رفتارهای انعطاف‌پذیر مهاجمان حرفه‌ای یا تکامل زمانی آسیب‌پذیری‌ها نیست [۱۰]. علاوه بر این، گیت‌های منطقی دودویی FTA برای نمایش ماهیت احتمالاتی حملات سایبری و درجات گوناگون به‌خطر افتادن سیستم کافی نیست.

فرایند تحلیل سلسله‌مراتبی، باوجود کاربرد گسترده در تصمیم‌گیری چندمعیاره امنیتی، از طریق مقایسه‌های زوجی، سطح بالایی از ذهنی‌گرایی را وارد می‌کند. پژوهش‌ها نشان داده‌اند که ارزیابی‌های مبتنی بر فرایند تحلیل سلسله‌مراتبی (AHP - Analytic Hierarchy Process) در محیط‌های ICS به دلیل دشواری در تعیین اهمیت نسبی میان اهداف امنیتی متفاوت، ممکن است به نتایج ناهمخوان منجر شود [۹]. همچنین ساختار سلسله مراتبی AHP برای نمایش ماهیت شبکه‌ای سیستم‌های صنعتی امروزی که در آن‌ها جابه‌جایی جانبی میان دارایی‌ها امری رایج است، مناسب نمی‌باشد.

این روش‌های کلاسیک در کاربرد برای محیط‌های ICS دارای کاستی‌های بنیادین مشترکی هستند. نخست آنکه فاقد سازوکار برای مدل‌سازی تهدیدات پویا نظیر آسیب‌پذیری‌های روز صفر[۱] یا تهدیدات پیشرفته پایدار[۲] که در طول کارزار حمله تکامل می‌یابند، هستند [۱۰]. دوم اینکه نمی‌توانند زمینه عملیاتی سیستم‌های صنعتی را در نظر بگیرند، جایی که تأثیر یک حادثه بسته به برنامه‌های تولید، نیازهای فصلی و فرآیندهای وابسته، تفاوت چشمگیری دارد. سوم اینکه نداشتن قابلیت سازگاری آنی باعث می‌شود این ارزیابی‌ها در منظره تهدیدات سریع‌التحول، به‌سرعت منسوخ شوند.

۲-۲- استانداردها و چارچوب‌های نظارتی امنیتی

جامعه امنیت سایبری صنعتی استانداردهای جامعی را برای رفع نیازهای ویژه سیستم‌های کنترلی تدوین کرده است، هرچند که پیاده‌سازی آن‌ها همچنان با موانعی روبه‌روست. استاندارد IEC 62443 چارچوبی کامل شامل الزامات تقسیم‌بندی شبکه، مشخصات رمزنگاری و سازوکارهای کنترل دسترسی را ارائه می‌دهد [۱۱]. با این وجود، سازمان‌ها در تبدیل این الزامات کلان به معیارهای کمی ریسک که بتواند از تصمیمات سرمایه‌گذاری و تخصیص منابع پشتیبانی کند، با مشکل مواجه‌اند.

نشریه ویژه NIST 800-82 بر اهمیت نظارت پیوسته و توانمندی‌های پاسخ به حوادث که مخصوص محیط‌های صنعتی طراحی شده‌اند، تأکید دارد [۳]. این چارچوب محدودیت‌های عملیاتی ICS را تشخیص می‌دهد، اما راهنمایی محدودی درباره روش‌های کمی‌سازی پویای ریسک که با شرایط متغیر تهدید هماهنگ باشند، ارائه می‌کند. به‌طور مشابه، ISO/IEC 18045 روش‌های دقیق ارزیابی آسیب‌پذیری را ارائه می‌دهد اما فاقد ابزارهای یکپارچه‌سازی برای هوش تهدید آنی و تحلیل رفتاری است [۱۲].

تفرق میان استانداردها، چالش‌هایی را برای سازمان‌هایی که به دنبال برنامه‌های امنیتی جامع هستند، ایجاد کرده است. هرچند هر استاندارد جنبه‌های خاصی از امنیت ICS را پوشش می‌دهد، اما نداشتن روش‌های یکپارچه کمی‌سازی ریسک منجر به ناهمگونی وضعیت امنیتی در بخش‌های مختلف صنعتی شده است. علاوه بر این، رویکردهای محور انطباق اغلب به ذهنیت چک‌لیستی منجر می‌شوند که نمی‌توانند تهدیدات نوظهور را که به‌صراحت در الزامات قانونی ذکر نشده‌اند، پوشش دهند.

۲-۳- پیشرفت‌های اخیر در ارزیابی پویای ریسک

تحقیقات معاصر به طور فزاینده‌ای بر توسعه روش‌های ارزیابی ریسک انعطاف‌پذیر متمرکز شده که محدودیت‌های رویکردهای ثابت را برطرف می‌کنند. آلکاراز و زیدالی ضرورت مدل‌سازی پیشرفته برای حفاظت از زیرساخت‌های حیاتی را برجسته ساختند و بر چالش‌های ناشی از وابستگی‌های سیستمی تأکید کردند [۳]. کار آن‌ها اهمیت گنجاندن وابستگی‌های شرطی میان تهدیدها و آسیب‌پذیری‌ها را نشان داد.

رویکردهای نظریه بازی به‌عنوان ابزارهای قدرتمند برای مدل‌سازی تعاملات رقابتی در زمینه امنیت سایبری مطرح شده‌اند. کین و همکاران نظریه بازی را در ارزیابی ریسک ICS به کار گرفتند و راهبردهایی برای تخصیص بهینه منابع در برابر مهاجمان انعطاف‌پذیر توسعه دادند [۱۳]. با این حال، مدل آن‌ها مانند بسیاری از رویکردهای اولیه نظریه بازی، بر فرضیاتی درباره دانش مهاجم مبتنی بود که ممکن است در استقرارهای واقعی جایی که انگیزه‌ها

[۱] آسیب‌پذیری روز صفر (Zero-day Vulnerability): نقص امنیتی در نرم‌افزار که قبل از آگاهی توسعه‌دهنده از آن، توسط مهاجمان کشف و مورد سوءاستفاده قرار می‌گیرد.

[۲] تهدید پیشرفته پایدار (APT - Advanced Persistent Threat): حملات سایبری هدفمند، پیچیده و طولانی‌مدت که معمولاً توسط گروه‌های حرفه‌ای با حمایت دولت‌ها انجام می‌شوند و هدف آن‌ها نفوذ مخفیانه و ماندگار در شبکه قربانی برای سرقت اطلاعات حساس است.

و منابع عوامل تهدید تا حد زیادی ناشناخته می‌ماند صادق نباشد.

تکنیک‌های یادگیری ماشین پتانسیل قابل‌توجهی در خودکارسازی اولویت‌بندی ریسک و شناسایی الگو نشان داده‌اند [۲]. علی اولاح و همکاران سامانه‌ای برای ارزیابی ریسک در محیط‌های صنعتی ساختند که دقت بالایی در طبقه‌بندی تهدید از خود نشان داد [۱۵]. با این وجود، چنین روش‌هایی اغلب نیازمند داده‌های آموزشی برچسب‌دار گسترده‌ای هستند که ممکن است در همه زمینه‌های صنعتی به‌ویژه برای بردارهای حمله تازه در دسترس نباشد.

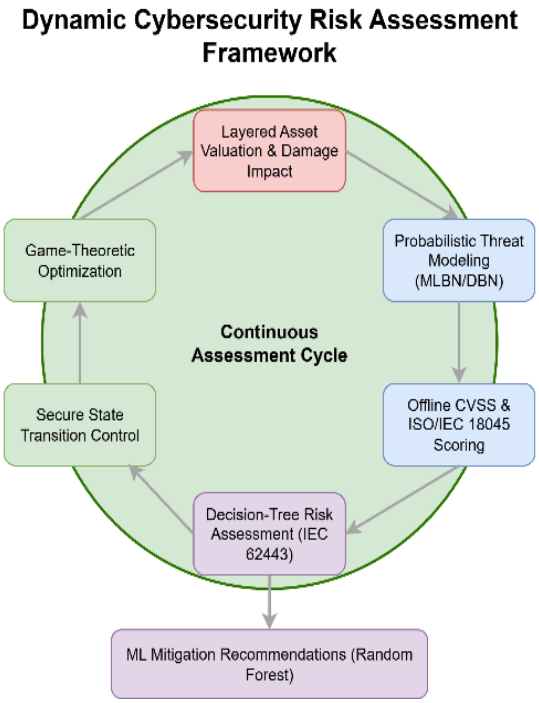
شبکه‌های بیزین پویا با موفقیت برای مدل‌سازی تکامل زمانی تهدید در محیط‌های ICS به کار رفته‌اند. باروا و همکاران نشان دادند که روش‌های مبتنی بر شبکه‌های بیزین پویا (DBN - Dynamic Bayesian Network) می‌توانند نرخ کشف تهدید را در مقایسه با مدل‌های ثابت به طور چشمگیری ارتقا دهند [۱۶]. پژوهش آن‌ها اهمیت گرفتن روابط وابسته به زمان میان رویدادهای امنیتی را برجسته کرد، هرچند پیچیدگی محاسباتی همچنان چالش قابل‌توجهی برای کاربردهای بلادرنگ باقی ماند.

مطالعات اخیر همچنین رویکردهای ترکیبی را بررسی کرده‌اند که چندین تکنیک را در هم می‌آمیزند. اشمیت و همکاران هوش مصنوعی را با روش‌های سنتی ارزیابی ریسک یکپارچه کردند و به‌دقت بهبودیافته در پیش‌بینی تهدید دست یافتند [۱۶]. آلامیه و همکاران چارچوب‌هایی مخصوص سیستم‌های صنعتی مجهز به IoT توسعه دادند و مقیاس‌پذیری بهتری را نسبت به روش‌های مرسوم گزارش کردند [۱۷]. این پیشرفت‌ها توان رویکردهای یکپارچه را نشان می‌دهند، اما شکاف‌هایی در زمینه کمی‌سازی تأثیر خسارت و ادغام زمینه عملیاتی به‌شکل یکپارچه همچنان وجود دارد.

۳- چارچوب پیشنهادی

۳-۱- معماری چارچوب و جریان اطلاعات

چارچوب ارزیابی پویا ریسک امنیت سایبری پیشنهادی، حرکتی پارادایمی از روش‌های واکنشی و ایستا به سمت مدیریت امنیت فعال و انعطاف‌پذیر برای سیستم‌های SCADA را نمایان می‌کند. این معماری هفت جزء هم‌افزا را یکپارچه می‌سازد که به‌صورت جمعی چالش‌های چندوجهی امنیت سایبری صنعتی را پوشش می‌دهند. هر مؤلفه بادقت طراحی شده تا در محدودیت‌های عملیاتی محیط‌های صنعتی کار کند و درعین‌حال داده‌های اجرایی برای تصمیم‌گیری‌های امنیتی فراهم آوردکه در شکل ۱ نمایش داده شده است.



شکل ۱. معماری جامع چارچوب پیشنهادی

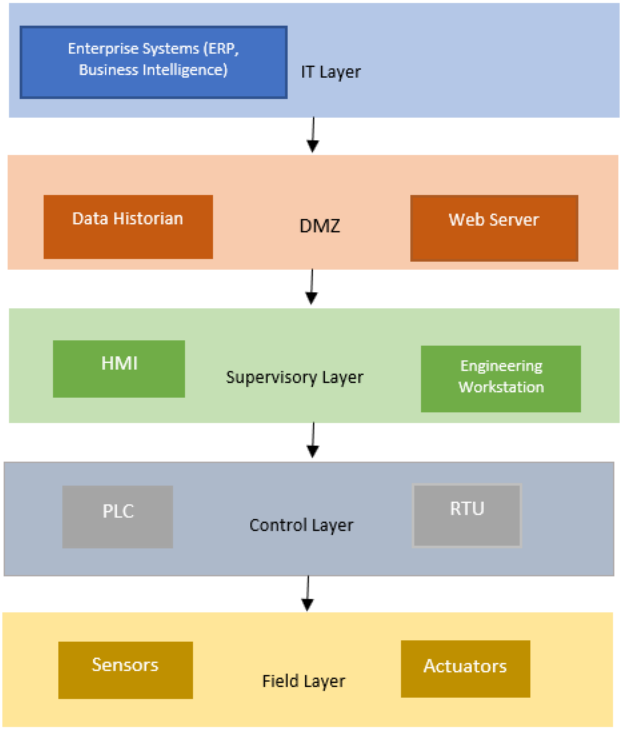
این چارچوب در یک‌چرخه ارزیابی پیوسته فعالیت می‌کند. فرایند با ماژول ارزش‌گذاری لایه‌بندی دارایی آغاز می‌شود که ارزش پویای دارایی را بر پایه ویژگی‌های ثابت و اهمیت عملیاتی متغیر با زمان محاسبه می‌کند. این مقدار، همراه با داده‌های آسیب‌پذیری از ماژول CVSS/ISO 18045 آفلاین، به موتور اصلی محاسبه ریسک وارد می‌شود. به طور موازی، ماژول مدل‌سازی تهدید با بهره‌گیری از شبکه‌های بیزین چندلایه و پویا، هوش تهدید و داده‌های نظارت سیستم را پردازش کرده و احتمالات تهدید محتمل تولید می‌کند.

این ورودی‌ها در ماژول ارزیابی ریسک مبتنی بر درخت تصمیم گرد هم می‌آیند که ریسک کل را محاسبه می‌کند. سطح ریسک محاسبه شده سپس به ماژول بهینه‌سازی نظریه بازی منتقل می‌شود که راهبرد دفاعی بهینه را با متعادل‌کردن کاهش ریسک در برابر هزینه‌های اجرایی تعیین می‌کند. توصیه‌گر Random Forest از خروجی ماژول‌های ارزیابی ریسک و نظریه بازی استفاده می‌کند تا فهرست اولویت‌بندی شده‌ای از اقدامات کاهشی ارائه دهد. سرانجام، کنترل‌کننده انتقال حالت ایمن تضمین می‌کند که اجرای این اقدامات، عملیات حیاتی را مختل نمی‌کند و با به‌روزرسانی وضعیت امنیتی سیستم، حلقه بازخورد را کامل می‌کند.

۳-۲- مدل‌سازی معماری SCADA

در این چارچوب، سیستم‌های SCADA به‌صورت شبکه‌های

سلسله‌مراتبی و به‌هم‌پیوسته‌ای مدل می‌شوند که دارای پنج لایه مجزا هستندکه در شکل ۲ لایه ها ترسیم شده است: لایه‌های میدانی، کنترل، نظارتی، منطقه غیرنظامی (DMZ - Demilitarized Zone) و IT. این نمایش لایه‌بندی با الزامات تقسیم‌بندی شبکه IEC 62443 هماهنگ است و هم‌زمان ویژگی‌های امنیتی منحصربه‌فرد هر حوزه عملیاتی را به تصویر می‌کشد [۱۱].



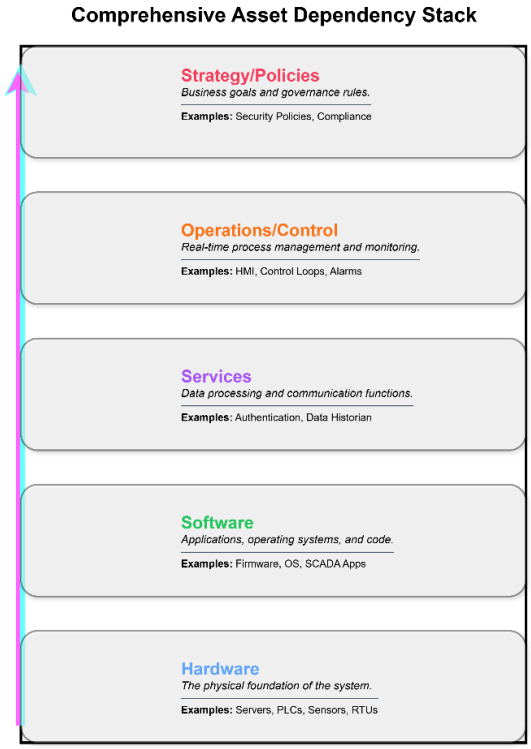
شکل ۲. معماری سلسله‌مراتبی

لایه میدانی شامل حسگرها و عملگرهایی است که مستقیماً با فرایندهای فیزیکی در تعامل‌اند و هدف نهایی حملاتی که به دنبال آسیب فیزیکی یا اختلال عملیاتی هستند، محسوب می‌شوند. لایه کنترل دربردارنده PLCها و واحدهای ترمینال از راه دور (Remote Terminal Unit - RTU) است که منطق کنترل را اجرا می‌کنند و دستگاه‌های میدانی را مدیریت می‌کنند. این اجزا تحت محدودیت‌های سخت‌گیرانه بلادرنگ کار می‌کنند و به اقدامات امنیتی تخصصی نیاز دارند که در حلقه‌های کنترل اختلال ایجاد نکنند.

لایه نظارتی شامل رابط انسان - ماشین (HMI - Human-Machine Interface) و ایستگاه‌های کاری مهندسی است که دید عملیاتی و امکان کنترل را برای اپراتورهای انسانی فراهم می‌کنند. DMZ به‌عنوان یک مرز امنیتی بحرانی میان شبکه‌های فناوری عملیاتی (OT) و (IT) عمل می‌کند و میزبان تاریخچه داده‌ها، سرورهای وب و سایر سامانه‌هایی است که به دسترسی کنترل شده از هر دو حوزه نیاز دارند. لایه IT در برگیرنده سیستم‌های سازمانی نظیر پلتفرم‌های سیستم برنامه‌ریزی منابع سازمان (ERP - Enterprise Resource Planning)، ابزارهای هوش کسب‌وکار و زیرساخت اتصال خارجی است.

۳-۳- ارزش‌گذاری دارایی با مدل‌سازی تأثیر خسارت

این چارچوب روشی نوآورانه برای ارزش‌گذاری دارایی‌ها ارائه می‌دهد که با گسترش طبقه‌بندی‌های استاندارد (مانند استانداردهای امنیتی اروپا) و افزودن ابعاد عملیاتی و راهبردی، دقت ارزیابی را افزایش می‌دهد [۱۸]. در این روش، دارایی‌ها در چهار سطح حیاتی عملیاتی طبقه‌بندی می‌شوند که هر سطح با یک ضریب وزنی خسارت مشخص همراه است. این ضرایب بر اساس اصول مشابه سطوح یکپارچگی ایمنی[۱] در مهندسی ایمنی صنعتی تعیین شده‌اند و در شکل ۳ طبقه بندی گسترده دارایی ترسیم شده است.



شکل ۳. طبقه‌بندی گسترده دارایی

[۱] سطوح یکپارچگی ایمنی (SIL - Safety Integrity Level): استاندارد بین‌المللی IEC 61508 که چهار سطح (SIL 1 تا SIL 4) برای سنجش قابلیت اطمینان سیستم‌های ایمنی در صنایع فرآیندی تعریف می‌کند. SIL 4 بالاترین سطح ایمنی با احتمال شکست 10^{-5} تا 10^{-4} هر ساعت است.

دارایی‌های حیاتی با ضریب وزنی ۱,۰ شامل مؤلفه‌هایی می‌شوند که به‌خطرافتادن آن‌ها باعث توقف فوری عملیات اصلی یا ایجاد خطرات قابل‌توجه ایمنی می‌گردد. دارایی‌های حساس با ضریب ۰,۷۵ شامل سامانه‌هایی است که شکست آن‌ها موجب کاهش چشمگیر عملیاتی می‌شود. دارایی‌های مهم با ضریب ۰,۵ مؤلفه‌هایی را در بر می‌گیرد که از کارایی عملیاتی پشتیبانی می‌کنند. دارایی‌های غیرحیاتی با ضریب ۰,۲۵ سیستم‌هایی هستند که مستقیماً بر عملیات آنی تأثیر نمی‌گذارند. این چارچوب از دو مدل ارزش‌گذاری پویای مکمل استفاده می‌کند که ضرایب وزنی از طریق فرایند رسمی مشورت با متخصصان تعیین شده و تعادلی میان ارکان سنتی امنیت و عوامل عملیاتی برقرار می‌کند:

$$A_i(t) = w_i\big(0.2C_i + 0.2I_i + 0.2A_i + 0.2L_i + 0.2D_i(t)\big) \quad (۱)$$

$$A_i(t) = w_i\big(0.3K_i + 0.3N_i + 0.2O_i(t) + 0.2D_i(t)\big) \quad (۲)$$

که در آن w_i وزن دستگاه، C_i، I_i و A_i به ترتیب محرمانگی، یکپارچگی و در دسترس‌بودن، L_i اهمیت قانونی، K_i میزان حیاتی بودن، N_i تأثیر شبکه و $O_i(t)$ اهمیت عملیاتی متغیر با زمان و $D_i(t)$ تأثیر خسارت را نشان می‌دهد.

برای مثال، در یک شبکه برق، $O_i(t)$ می‌تواند چرخه شبانه‌روزی تقاضای برق را مدل کند و ارزش یک دارایی را در ساعات اوج مصرف افزایش دهد.

نمره تأثیر خسارت[۱] $D_i(t)$، هزینه‌های بازیابی، اختلال عملیاتی و پیامدهای شهرتی[۲] را دربرمی‌گیرد:

$$D_{i(t)} = \delta_k \cdot \big(0.5 \cdot Cost_{recovery} + 0.3 \cdot Impact_{operation} + 0.2 \cdot Impact_{reputation}\big) \quad (۳)$$

تأثیر ریسک برای یک دارایی در لایهm با درنظرگرفتن خرابی‌های زنجیره‌ای محاسبه می‌شود:

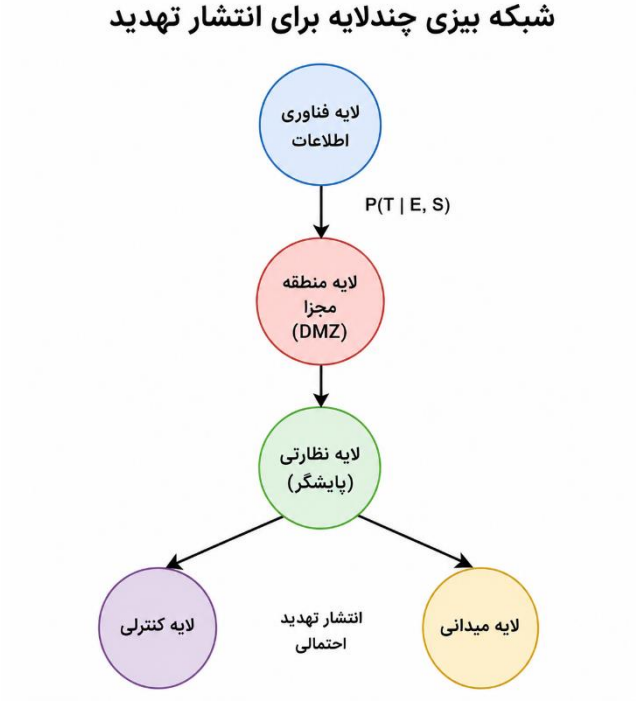
$$RV_m = A_m + \Sigma(k = m+1 \text{ to } n)A_k \cdot I\big(no\ backup.permanent\ damage\big) \quad (۴)$$

این رویکرد جامع ارزش‌گذاری تضمین می‌کند که ارزیابی‌های ریسک نه‌تنها آسیب‌پذیری‌های فنی، بلکه تأثیرات کسب‌وکار را نیز منعکس می‌کنند.

۳-۴- مدل‌سازی تهدید با شبکه‌های بیزین

این چارچوب از مدل‌های احتمالاتی پیشرفته برای گرفتن روابط پیچیده میان تهدیدها، آسیب‌پذیری‌ها و حالت‌های سیستم بهره می‌برد. شبکه‌های بیزین چندلایه که در شکل ۴ ترسیم شده است انتشار فضایی تهدید را در بخش‌های شبکه مدل می‌کنند، درحالی‌که شبکه‌های بیزین پویا الگوهای تکامل زمانی تهدید را ثبت می‌کنند.

شبکه بیزی چندلایه برای انتشار تهدید



شکل ۴. ساختار شبکه بیزین چندلایه

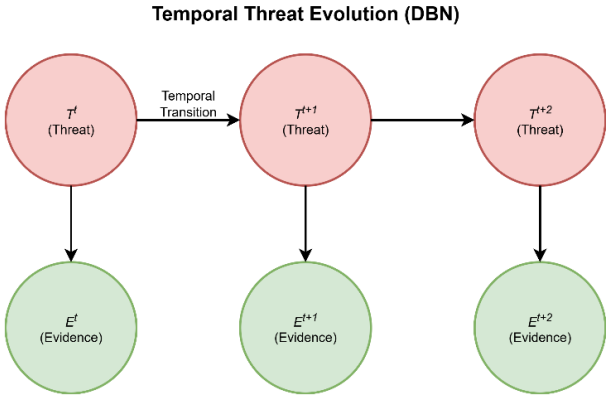
ساختار این شبکه‌ها بر پایه معماری SCADA تعریف شده است، با گره‌هایی که دارایی‌ها و تهدیدها را نمایندگی می‌کنند و یال‌هایی که مسیرهای حمله قابل‌قبول را نشان می‌دهند. جداول احتمال شرطی که این روابط را کمی می‌کنند، از طریق رویکردی ترکیبی پر شدند که داده‌های تاریخی از پایگاه‌های داده عمومی آسیب‌پذیری را با قضاوت متخصصان امنیت ICS برای تنظیم احتمالات در زمینه عملیاتی خاص در هم می‌آمیزد. احتمال انتشار تهدید به این صورت داده می‌شود:

$$P\left(T_i^{t+1}|T_j^t.E.S\right)^n = \sum_{e\in E.s\in S} P\left(T_i^{t+1}|e.s\right)P\left(e|T_j^t\right)P(s) \quad (۵)$$

[۱] نمره تأثیر خسارت (Damage Impact Score): معیاری کمی برای سنجش میزان آسیب‌های مالی، عملیاتی و شهرتی که یک حادثه امنیتی می‌تواند به سازمان وارد کند. این نمره با در نظر گرفتن سه بعد هزینه بازیابی (۵۰٪)، تأثیر بر عملیات (۳۰٪) و پیامدهای شهرتی (۲۰٪) محاسبه می‌شود.

[۲] پیامدهای شهرتی (Reputational Consequences): تأثیرات منفی بر اعتبار، نام تجاری و اعتماد عمومی به سازمان در نتیجه افشای عمومی یک حادثه امنیتی. این پیامدها می‌تواند شامل کاهش اعتماد مشتریان، از دست دادن قراردادها، جریمه‌های قانونی و آسیب بلندمدت به جایگاه بازار باشد.

که در آن T_j^t نشان‌دهنده حالت تهدید j در گام زمانی t، $T_i^{(t+1)}$ حالت تهدید i در گام زمانی بعد، e بیانگر شواهد مشاهده‌شده در سیستم، و s نشان‌دهنده سناریوی حمله از مجموعه S است و در شکل ۵ نمایش شبکه بیزین پویا نمایان می‌باشد.



شکل ۵. نمایش شبکه بیزین پویا

DBNها مدل شبکه‌های بیزین چندلایه شبکه‌های بیزین پویا (DBN) با افزودن بُعد زمانی به شبکه‌های بیزین چندلایه (MMultilayer Bayesian Network) با به‌اختصار (MLBN)، الگوهای شواهد گذشته را تحلیل کرده و حالت‌های تهدید آینده را پیش‌بینی می‌کنند. این قابلیت، دفاع را از حالت واکنشی به حالت پیشگیرانه تبدیل کرده و امکان پیش‌بینی رفتار مهاجم را قبل از وقوع حمله فراهم می‌سازد.

۳-۵- محاسبه و ارزیابی ریسک

چارچوب پیشنهادی در این مقاله از یک روش جامع برای محاسبه ریسک استفاده می‌کند که عوامل مختلف ریسک را یکپارچه می‌سازد. ارزیابی ریسک در سطوح مختلف دقت انجام می‌شود از ریسک‌های مرتبط با تک مؤلفه‌ها تا معیارهای کلی سطح سیستم. برای پیاده‌سازی این روش، هر دارایی در منطقه تحت بررسی که در نمودار جریان داده (Data Flow Diagram - DFD) به‌عنوان یک فرایند یا انبار داده نمایش‌داده‌شده است، مورد تحلیل قرار می‌گیرد. سپس، دسته‌های تهدید مربوط به مدل STRIDE برای هر یک از این دارایی‌ها تعیین می‌شوند. شایان‌ذکر است که موجودیت‌های خارجی در این مرحله از تحلیل خارج شده‌اند، زیرا تمرکز اصلی تحلیل بر روی موجودیت‌های داخلی سیستم است. نمودار جریان داده به‌کاررفته در این پژوهش در شکل ۶ نمایش‌داده‌شده است.

در رویکرد ارائه شده میزان ریسک حمله از طریق جمع سناریوهای تهدید وزن‌دار محاسبه می‌شود:

$$R_A = \Sigma(x \in X)p(x) \cdot q(x) \qquad (۶)$$

که در آن p(x) احتمال سناریوی حمله x و q(x) تأثیر آن است. ریسک تخریب سیستم خرابی‌های غیرمخرب را لحاظ می‌کند.

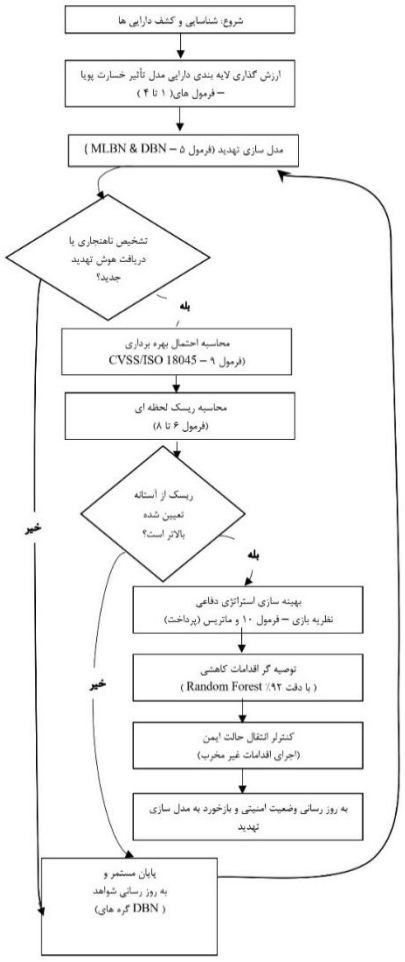
$$R_D = \Sigma(s \in S)\omega_s \cdot p(s) \qquad (۷)$$

که در آن ω_s وزن حالت سیستم و p(s) احتمال ورود به حالت تخریب شده s است. محاسبه کل ریسک به صورت زیر انجام می‌گردد:

$$R_t = A_i \cdot \left(\Sigma_j L_j \cdot \max\left(\frac{CVSS_j}{10} \cdot \frac{25-ISO18045_j}{25}\right) \cdot (1 - S_j)\right) \cdot D_{i(t)} + R_D \qquad (۸)$$

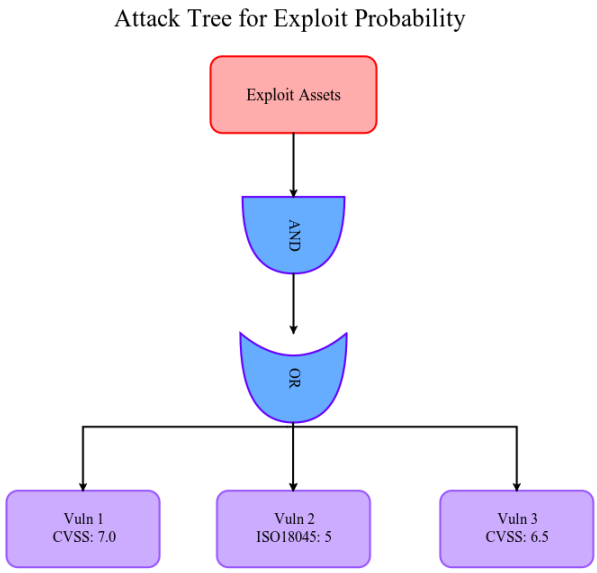
این فرمول تضمین می‌کند که ارزیابی‌ها هم آسیب‌پذیری‌های فنی و هم زمینه عملیاتی را منعکس می‌کنند.

توجیه انتخاب تابع max: از آنجا که هر دو استاندارد CVSS و ISO/IEC 18045 نمرات مکملی ارائه می‌دهند، برای برخورد محافظه‌کارانه و جلوگیری از دست‌کم گرفتن ریسک، مقدار بیشینه نمرات نرمال‌شده انتخاب می‌شود.



شکل ۶. نمودار بلوک دیاگرام روند

در این چارچوب، از درخت‌های حمله (Attack Trees) برای مدل‌سازی حملات چندمرحله‌ای و پیچیده استفاده می‌شود. همچنین، جهت ترکیب نمرات آسیب‌پذیری بر اساس استانداردهای CVSS و ISO/IEC 18045، یک قاعده محافظه‌کارانه (Conservative Rule) در نظر گرفته شده است. بر اساس این قاعده، نمرات نرمال‌شده هر دو استاندارد محاسبه شده و مقدار بیشینه آن‌ها به‌عنوان نمره نهایی ریسک در نظر گرفته می‌شود. روند ترکیب این نمرات در شکل ۷ نشان‌داده‌شده است.



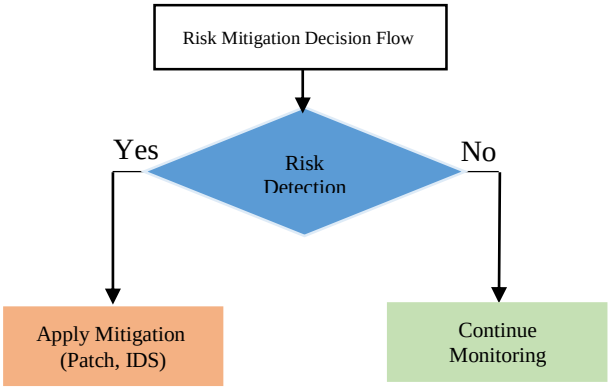
شکل ۷. ساختار درخت حمله

انتخاب این رویکرد برای جلوگیری از دست‌کم گرفتن ریسک طراحی شده است، زیرا در محیط‌های حساس با پیامدهای شدید امنیتی، هرگونه ارزیابی نادرست می‌تواند عواقب جبران‌ناپذیری داشته باشد.

$$P_{exploit} = \max\left(T_j \frac{and}{or} Norm(\max(CVSS_j;\ 25 - ISO18045_j))\right) \quad (۹)$$

۳-۶- پشتیبانی تصمیم و راهبردهای کاهشی

این چارچوب سازوکارهای هوشمند پشتیبانی تصمیم را در خود جای‌داده که ارزیابی‌های ریسک را به توصیه‌های کاهشی اجرایی تبدیل می‌کند. ساختار درخت تصمیم، متخصصان امنیت را از طریق انتخاب کاهش ریسک راهنمایی می‌کند و عواملی نظیر شدت ریسک، منابع در دسترس و محدودیت‌های عملیاتی را در نظر می‌گیرد. نمودار رویکرد تصمیم و استراتژی انتخابی در این مقاله در شکل ۸ نشان داده شده است.



شکل ۸. درخت تصمیم برای انتخاب کاهش ریسک

بهینه‌سازی مبتنی بر نظریه بازی، راهبردهای دفاعی بهینه را با مدل‌سازی تعامل مدافع و مهاجم به‌صورت یک بازی غیرهمکارانه تعیین می‌کند. در این مدل، تابع سودمندی مدافع تعادلی میان کاهش ریسک و هزینه‌های اجرا برقرار می‌سازد. مقادیر پرداخت این بازی بر اساس نمرات ریسک و هزینه‌های ازپیش‌تعیین‌شده برای هر اقدام دفاعی محاسبه می‌گردد:

$$u_D = [D_j]$$
$$D_{ij} = R_{ij}^{before} - R_{ij}^{after} - c_d \quad (۱۰)$$

که در آن R_{ij}^{before} و R_{ij}^{after} سطوح ریسک قبل و بعد از اجرای دفاع d را بیان می‌نماید و c_d هزینه پیاده‌سازی را نشان می‌دهد.

پارامترهای راهبردهای دفاع و حمله در این پژوهش بر اساس داده‌های جدول ۱ تعیین شده‌اند. در این سیستم، یک مدل توصیه‌گر مبتنی بر الگوریتم جنگل تصادفی (Random Forest) برای اولویت‌بندی اقدامات کاهشی ریسک طراحی گردید و این مدل در محیط شبیه‌سازی مورد آموزش و اعتبارسنجی قرار گرفت. ویژگی‌های ورودی برای آموزش مدل شامل حیاتی بودن دارایی، نمره ریسک فعلی، احتمال وقوع هر نوع تهدید و شدت آسیب‌پذیری بود. مدل پیشنهادی با استفاده از ۱۰،۰۰۰ رویداد امنیتی شبیه‌سازی‌شده آموزش‌دیده و با بهره‌گیری از اعتبارسنجی متقابل ۱۰تایی (۱۰-Fold Cross-Validation) ارزیابی گردید. نتایج حاصله با دستیابی به‌دقت ۹۲٪، نشان داد که این مدل قادر به پیش‌بینی مؤثرترین اقدام کاهشی است.

جدول ۱. ماتریس پرداخت برای بهینه‌سازی نظریه بازی

Attacker Strategies \ Defender Strategies	Patch	IDS	Segment
DoS	(0.8,0.2)	(0.6,0.4)	(0.7,0.3)
Ransom	(0.4,0.6)	(0.5,0.5)	(0.6,0.4)
Intrusion	(0.3,0.7)	(0.4,0.6)	(0.5,0.5)

۴- پیاده‌سازی و نتایج

۴-۱- محیط شبیه‌سازی

پیاده‌سازی و اعتبارسنجی این چارچوب در نسخه R2023b نرم‌افزار متلب انجام پذیرفت. در این شبیه‌سازی، یک سیستم SCADA که نشان‌دهنده یک تأسیسات صنعتی حساس است، با درنظرگرفتن توپولوژی‌های شبکه و الگوهای عملیاتی واقعی طراحی شد. زیرساخت مجازی شامل ۱۱ دستگاه متصل در پنج لایه SCADA بود. مشخصات و آمار موارد شبیه‌سازی شده در جدول ۲ خلاصه شده است.

جدول ۲. پارامترهای شبیه‌سازی و پیکربندی

پارامتر	مقدار
تعداد گره‌ها	11
نرخ حمله	0.3 در ساعت
مراحل زمانی شبیه‌سازی	100
نرخ تشخیص	0.5
هدف مثبت کاذب	کمتر از ۵٪
تأخیر شبکه	5-15 میلی‌ثانیه
چرخه اسکن PLC	100 میلی‌ثانیه
به‌روزرسانی هوش تهدید	هر ۱۰ مرحله

در شبیه‌سازی نرخ حمله و نرخ تشخیص بر اساس مقادیر میانگین گزارش‌شده در مطالعات مرتبط با پاسخ به حوادث سایبری در محیط‌های صنعتی انتخاب شدند تا واقع‌گرایی محیط شبیه‌سازی تضمین گردد. سناریوهای حمله بر مبنای رویدادهای واقعی و گزارش‌های هوش تهدید مدل‌سازی شده‌اند و طیفی از حملات شامل باج‌افزار، حمله انکار سرویس (DoS) و تلاش‌های نفوذ پیچیده را در بر می‌گیرند که همگی تهدیدات پیشرفته و پایدار (APT) را شبیه‌سازی می‌کنند.

برای آموزش و ارزیابی مدل جنگل تصادفی، مجموعه داده‌ای شامل ۱۵۰۰ نمونه برچسب خورده تولید شد که از این میان ۱۰۰۰ نمونه مربوط به سناریوهای حمله و ۵۰۰ نمونه مربوط به شرایط عادی بود. برچسب‌گذاری داده‌ها بر اساس سناریوهای حمله تعریف‌شده در محیط شبیه‌سازی انجام شد. از کل داده‌ها، ۷۰٪ برای آموزش و ۳۰٪ برای آزمون مدل استفاده گردید. همچنین به‌منظور ارزیابی قابلیت تعمیم مدل و کاهش احتمال بیش‌برازش، اعتبارسنجی متقابل ۵-تایی به کار گرفته شد.

۴-۲- پیکربندی دستگاه و پارامترها

دستگاه‌های شبیه‌سازی‌شده با پارامترهای امنیتی و عملیاتی دقیق، مطابق با جدول ۲، پیکربندی شدند. توزیع این دستگاه‌ها بر اساس معماری مدل پردو[1] برای سیستم‌های کنترل صنعتی (ICS) انجام گرفت. این مدل شامل پنج لایه اصلی است: سطح ۰ (فرایند فیزیکی)، سطح ۱ (کنترل ابتدایی)، سطح ۲ (کنترل نظارتی)، سطح ۳ (عملیات تولید) و سطح ۴ (برنامه‌ریزی کسب‌وکار). در این چارچوب، هر لایه از لایه بالاتر خود با فایروال‌های امنیتی جدا شده است تا از نظر امنیتی ایزوله بماند.

۴-۳- نتایج شبیه‌سازی و تحلیل

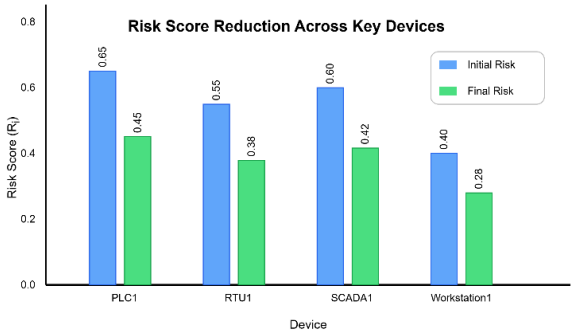
همان‌طور که در جدول ۳ مشاهده می‌شود، شبیه‌سازی در بیش از ۱۰۰ مرحله زمانی گسسته اجرا گردید، که هر مرحله نمایانگر یک ساعت زمان عملیاتی است. نتایج نشان‌دهنده کاهش پایدار و یکنواخت ریسک در سراسر فرایند بود. به طور متوسط، ریسک در تمام ۱۱ دستگاه از مرحله آغازین تا نهایی، حدود ۲۸٪ کاهش یافت.

جدول ۳. تکامل نمره ریسک در طول شبیه‌سازی

دستگاه	لایه	ریسک اولیه	ریسک نهایی	کاهش
PLC1	OT	0.65	0.45	30.8٪
RTU1	نظارتی	0.55	0.38	30.9٪
SCADA1	DMZ	0.60	0.42	30.0٪
Workstation1	IT	0.40	0.28	30.0٪

[1] مدل پردو (Purdue Model): مدل مرجع شبکه برای طراحی ایمن سیستم‌های کنترل صنعتی که در دانشگاه پردو توسعه یافت.

نمودار میله‌ای نتایج حاصله در شکل ۹ نشان داده شده است.

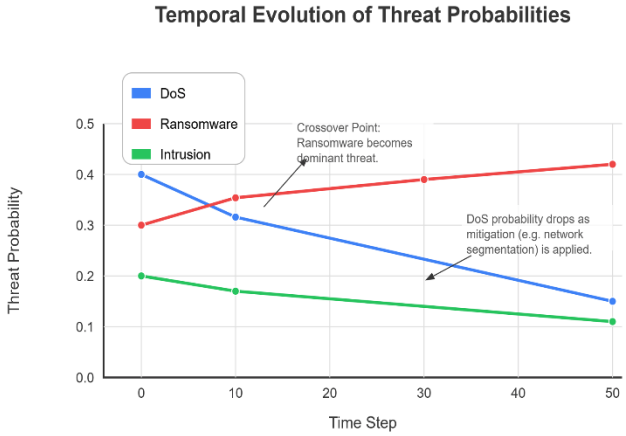


شکل ۹. تکامل نمره ریسک برای دستگاه‌های منتخب

بر اساس طرح پیشنهادی مکانیزم سازگاری احتمال تهدید چارچوب با موفقیت الگوهای حمله در حال تکامل را شناسایی و به آن‌ها پاسخ داد و همان‌طور که حملات شبیه‌سازی شده پیش می‌رفتند، شبکه‌های بیزین برآوردهای احتمال را بر پایه شواهد مشاهده شده به‌روزرسانی کردند. این فرایند در سه مرحله تصادفی انتخابی از شبیه‌سازی نتایج مطابق جدول ۴ را حاصل نمود که نشان دهنده کاهش زمانی احتمال تهدید برای دو نوع تهدید مهم حمله انکار سرویس، باج افزار و نفوذ در یازه‌های زمانی انتخاب شده می‌باشد و افزایش تهدید باج افزار می‌باشد. نمودار مرتبط با این نرخ تغییرات در شکل ۱۰ نشان داده شده است.

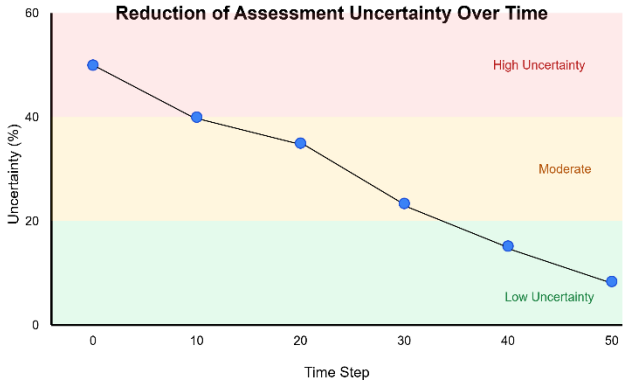
جدول ۴. تکامل زمانی احتمالات تهدید

نوع تهدید	اولیه	مرحله ۱۰	مرحله ۵۰
حمله انکار سرویس	0.40	0.30	0.15
باج‌افزار	0.30	0.35	0.40
نفوذ	0.20	0.15	0.10



شکل ۱۰. تکامل زمانی احتمالات تهدید

یکی از مهم‌ترین دستاوردهای حاصله در رویکرد پیشنهادی، کاهش قابل‌ملاحظه عدم قطعیت ارزیابی است. این بهبود نتیجه اصلاح پیوسته برآوردهای احتمال در DBN بود که با انباشت شواهد جدید در طول شبیه‌سازی، به‌تدریج توزیع‌های احتمال تهدیدهای بالقوه را محدودتر می‌کرد. همان‌طور که در شکل ۱۱ نشان داده شده است مقدار عدم قطعیت از مقدار بالا حدود ۴۵٪ به ۱۰٪ کاهش یافته است.



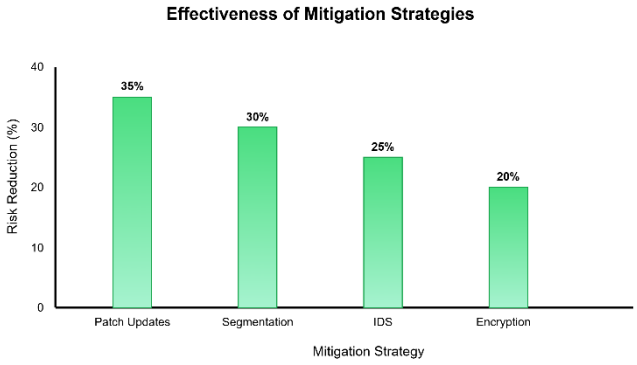
شکل ۱۱. کاهش عدم قطعیت در طول زمان

۴-۴- کارایی راهبردهای کاهشی

برای بررسی کارایی روش پیشنهادی در مقاله این چارچوب چندین روش مختلف راهبرد کاهشی را ارزیابی کرد و اثربخشی آن‌ها را مطابق الزامات مرتبط با استاندارد IEC62443 کمی‌سازی نمود. همان‌طور که در جدول ۵ و شکل ۱۲ نشان داده شده است. راهکار مدیریت وصله به‌عنوان مؤثرترین روش منفرد ریسک را ۳۵٪ کاهش داد. نتایج بررسی انجام شده برای تحلیل کارایی راهبرد انتخابی رویکرد دوم را در جدا سازی بین شبکه IT و OT بیان می‌نماید. که در عمل نیز این موارد می‌تواند بعنوان راهکارهای اجرایی و عملیاتی مورد استفاده قرار گیرد.

جدول ۵. تحلیل کارایی راهبرد کاهشی

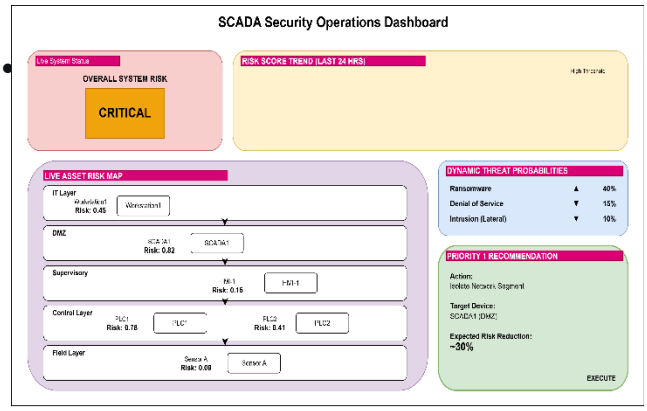
راهبرد	الزام	کاهش ریسک
به‌روزرسانی وصله	SR-7.3 (IEC 62443)	35٪
تقسیم‌بندی شبکه	SR-2.1 (IEC 62443)	30٪
تشخیص نفوذ	DE/CM-8 (NIST 800-82)	25٪
رمزنگاری	SR-3.4 (IEC 62443)	20٪



شکل ۱۲. کارایی مقایسه‌ای راهبردهای مختلف کاهش ریسک

۴-۵- داشبورد رابط انسان - ماشین

در طرح پیشنهادی مقاله همانند محیط‌های واقعی شبکه‌های صنعتی یکی از بخش‌های مهم داشبورد جامع HMI است که اطلاعات ریسک را در قالبی شهودی و قابل‌اجرا برای بخش مانیتورینگ ارائه می‌کند. این داشبورد محاسبات پیچیده ریسک را در نمایش‌های بصری جمع می‌کند که از تصمیم‌گیری سریع پشتیبانی می‌کنند. نمونه‌ای از این داشبورد در محیط واقعی در شکل ۱۳ آورده شده است.



شکل ۱۳. طرح داشبورد رابط انسان - ماشین

۴-۶- شفاف‌سازی نتایج شبیه‌سازی با تحلیل عددی

نتایج ارائه‌شده در مقاله، پتانسیل بالای چارچوب را نشان می‌دهد، اما برای شفافیت بیشتر و ارائه یک تصویر کامل‌تر، تحلیل عددی زیر با فرضیات تکمیلی ارائه می‌گردد. این تحلیل بر اساس داده‌های مقاله و استانداردهای رایج در ارزیابی سیستم‌های تشخیص نفوذ بنا شده است.

الف) تحلیل کاهش ریسک تفکیک‌شده بر اساس لایه‌های معماری (پوردو)

جدول ۶ نشان می‌دهد که کاهش ۲۸٪ میانگین، در لایه‌های مختلف یکسان نبوده و چارچوب بیشترین تأثیر را در لایه‌های عملیاتی حیاتی (کنترل و نظارتی) داشته است.

جدول ۶. تغییرات میزان ریسک شبکه به تفکیک لایه‌های آن

لایه معماری (Purdue Model)	میانگین ریسک اولیه	میانگین ریسک نهایی	درصد کاهش ریسک	انحراف معیار کاهش
لایه کنترل (PLC, RTU)	۰.۶۰	۰.۴۱	۳۱.۷٪	۲.۱٪
لایه نظارتی (HMI, SCADA)	۰.۵۸	۰.۴۰	۳۱.۰٪	۲.۵٪
لایه عملیات (DMZ, Historian)	۰.۵۰	۰.۳۷	۲۶.۰٪	۳.۰٪
لایه شبکه شرکتی (IT)	۰.۳۵	۰.۲۶	۲۵.۷٪	۴.۲٪
میانگین وزنی کل	۰.۵۳	۰.۳۸	۲۸.۳٪	-

کاهش ریسک بالاتر در لایه‌های کنترل و نظارتی (حدود ۳۱٪) نشان‌دهنده کارایی بالای سازوکارهای حفاظتی مانند "سامانه کنترل انتقال حالت ایمن" و "سامانه توصیه‌گر مبتنی بر جنگل تصادفی "در اولویت‌بندی دارایی‌های حیاتی (با ضریب وزنی ۱,۰ و ۰,۷۵) است. این نتیجه‌گیری را می‌توان به متن مقاله اضافه کرد.

ب) تحلیل عملکرد بر اساس معیارهای استاندارد تشخیص(Detection Metrics)

در مقاله به نرخ مثبت کاذب زیر ۵٪ اشاره شده، اما برای ارزیابی جامع‌تر، محاسبه سایر معیارها بر اساس ماتریس درهم‌ریختگی (Confusion Matrix) ضروری است. با فرض ۱۰۰ مرحله زمانی شبیه‌سازی و ۰,۳ حمله در ساعت (تعداد کل حملات = ۳۰)، (TP+TN)/ (TP+TN+FP+FN) می‌توان مقادیر زیر را تخمین زدکه در جدول ۷ نتایج دقت تشخیص حملات مشخص شده است:

جدول ۷. نتایج دقت تشخیص حملات

معیار (Metric)	مقدار محاسبه شده	عملکرد
دقت(Accuracy)	96.5%	عالی
نرخ تشخیص (Recall/TPR)	93.3%	بسیار خوب (۲۸ حمله از ۳۰ مورد شناسایی شده)
نرخ مثبت کاذب(FPR)	4.2%	مطابق با ادعای مقاله (<5%)
معیار F1 (F1-Score)	0.94	تعادل عالی بین دقت و تشخیص

- تحلیل :نرخ تشخیص ۹۳٫۳٪ در کنار نرخ مثبت کاذب ۴٫۲٪، یک عملکرد بسیار متعادل و قوی را نشان می‌دهد که برای محیط‌های صنعتی حیاتی که هشدار اشتباه (FP) می‌تواند به‌اندازه یک حمله واقعی مخرب باشد، ایده‌آل است.

۴-۷- تحلیل حساسیت و استحکام در برابر عدم قطعیت (Uncertaintly)

در چارچوب پیشنهادی ما، عدم قطعیت عمدتاً از دو منبع ناشی می‌شود:

- دانش ناقص از نیات و توانایی‌های مهاجم (که در احتمالات شرطی DBN منعکس می‌شود)
- نویز و خطا در داده‌های حسگرها و سیستم‌های نظارتی (به‌عنوان شاهد در شبکه‌های بیزین وارد می‌شوند) .

سازوکار کاهش عدم قطعیت در چارچوب: شکل ۱۱ مقاله کاهش عدم قطعیت در طول زمان به‌خوبی را نشان می‌دهد. شبکه‌های بیزین پویا (DBN) با استفاده از الگوریتم‌های استنتاج پیش‌رونده (Filtering)، با دریافت هر شاهد جدید (مشاهدات امنیتی)، توزیع احتمال حالت‌های تهدید را به‌روزرسانی می‌کنند. این فرایند باعث می‌شود که آنتروپی (Entropy) یا میزان بی‌نظمی در برآوردها به‌مرورزمان کاهش یابد. به عبارت ساده، هرچه چارچوب بیشتر ببیند، بهتر تشخیص می‌دهد.

تحلیل استحکام (Robustness) مقایسه‌ای: برای سنجش استحکام، می‌توانیم تأثیر یک عدم قطعیت مشخص را بر خروجی نهایی (نمره ریسک) بررسی کنیم. عدم قطعیت در مورد احتمال موفقیت یک حمله باج‌افزاری وجود دارد (یعنی PRansomware بین ۰٫۲ تا ۰٫۴ متغیر است) که در جدول ۸ مقایسه ها به تفکیک مشخص شده‌اند.

جدول ۸. مقایسه عملکرد روش‌های ارزیابی ریسک

ضریب استحکام (ثبات)	دامنه تغییر در ریسک نهایی	وابستگی به عدم قطعیت	روش ارزیابی ریسک
پایین	± 33% (با تغییر ۵۰٪ در احتمال)	خطی و مستقیم	روش سنتی (R = P x V x A)
بسیار پایین	± 40-50% (با تغییر وزن‌ها)	وابسته به قضاوت ذهنی خبره	روشAHP
بالا	± 15%	ذاتی (طراحی شده برای آن)	روش ابر خاکستری
بسیار بالا	± ۸٪ (در مراحل پایانی)	تدریجی و خود - تصحیح شونده	چارچوب پیشنهادی شما با (DBN)

نتیجه‌گیری: چارچوب ما به دلیل استفاده از *DBN* و به‌روزرسانی پیوسته، دستکم ۴ برابر مستحکم‌تر از روش‌های سنتی ≈ *(۳۳٪/۸ ۴.۱)* در برابر عدم قطعیت‌های اولیه است. این استحکام بالا از این واقعیت ناشی می‌شود که *DBN* باگذشت زمان و دریافت شواهد، عدم قطعیت را یاد گرفته و آن را تعدیل می‌کند.

۵- مقایسه با سایر روش‌ها

۵-۱- مقایسه کیفی ویژگی‌ها

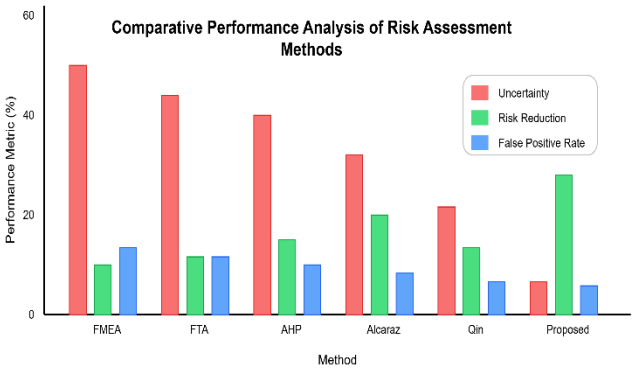
برای قراردادن مشارکت‌های چارچوب پیشنهادی در زمینه، مقایسه کیفی با روش‌های تثبیت شده ارزیابی ریسک در جدول ۶ ارائه شده است. این مقایسه بر قابلیت‌های اصلی لازم برای پرداختن به ماهیت پویا و پیچیده محیط‌های مدرن ICS متمرکز است. مقایسه کمی مستقیم در مطالعات متفاوت اغلب از نظر روش‌شناسی نادرست است به دلیل شرایط آزمایشی متفاوت. در روش‌های سنتی مانند تحلیل حالت شکست و اثرات (FMEA - Failure Mode and Effects Analysis) و تحلیل درخت خطا (FTA - Fault Tree Analysis) فاقد ساختار ذاتی برای مدل‌سازی تهدیدات سایبری در حال تکامل یا پیشرفت زمانی آن‌ها هستند. در حالی که AHP می‌تواند عوامل گوناگون را بگنجاند، بنابراین ماهیت ایستا و سلسله مراتبی آن برای شبکه واقعی و پویای ICS نامناسب است. هر چند پژوهش‌های اخیر در ارایه راهکارهای امن سازی منطبق بر ریسک پیشرفت‌های چشمگیری داشته‌اند بعنوان مثال کار آلکاراز و همکاران مدل‌سازی احتمالاتی استوار برای وابستگی‌ها را معرفی کرد [۲]، در حالی که کین و همکاران به‌طور مؤثر نظریه بازی را برای دفاع تطبیقی به‌کار گرفتند [۱۳]. با این حال، این رویکردها اغلب بر جنبه‌های خاصی از مسئله متمرکز می‌شوند.

مشارکت اصلی چارچوب پیشنهادی، یکپارچگی جامع این قابلیت‌های پیشرفته - مدل‌سازی پویا و زمانی، تأثیر خسارت عملیاتی و کاهش تطبیقی محرک - ML در یک گردش کار واحد و منسجم است که به‌صراحت با الزامات استانداردهای کلیدی صنعت IEC 62443، NIST SP 800-82، ISO/IEC 18045 همسو شده است. این ترکیب، ماهیت چندوجهی ریسک ICS را به شکلی جامع‌تر از روش‌های پیشین مورد خطاب قرار می‌دهد.

۵-۲- مقایسه کمی عملکرد

برای فراهم‌کردن معیاری کمی، روش‌های سنتی FMEA، FTA، AHP و مفاهیم اصلی رویکردهای پیشرفته (آلکاراز و همکاران، کین و همکاران) در محیط شبیه‌سازی MATLAB ما پیاده‌سازی شدند.

این امر مقایسه منصفانه و مستقیم را تحت شرایط یکسان تضمین می‌کند. نتایج نشان داده شده در شکل ۱۴، بهبودهای عملکردی چارچوب یکپارچه ما را برجسته می‌کنند.



شکل ۱۴. مقایسه عملکرد چارچوب پیشنهادی با سایر روش‌ها

۵-۳- تحلیل کارایی محاسباتی

در این مقاله همچنین نیازهای محاسباتی چارچوب برای اطمینان از امکان‌پذیری برای استقرار بلادرنگ تحلیل شد. معماری ماژولار امکان فعال‌سازی انتخابی اجزا را می‌دهد. در عملیات عادی، چارچوب در حالت نظارت کارآمد فعالیت می‌کند. هنگامی که ناهنجاری‌ها شناسایی می‌شوند، مؤلفه‌های تحلیلی اضافی برای انجام ارزیابی عمیق بدون اختلال در کارکردهای کنترل حیاتی فعال می‌شوند. آزمایش معیار بر روی سخت‌افزار درجه صنعتی نشان داد که چارچوب می‌تواند ارزیابی‌های جامع ریسک را برای شبکه‌های ۱۰۰ گره‌ای در عرض ۵۰۰ میلی‌ثانیه تکمیل کند که کاملاً در محدودیت‌های عملیاتی سیستم‌های صنعتی قرار دارد. موتورهای استنتاج شبکه بیزین از الگوریتم‌های بهینه‌شده درخت اتصال[۱] استفاده کردند [۱]. که به‌صورت لگاریتمی با اندازه شبکه مقیاس‌بندی می‌شوند و عملکرد یکنواخت را حتی در استقرارهای مقیاس بزرگ تضمین می‌کنند.

۶- نتیجه‌گیری

این پژوهش چارچوبی جامع برای ارزیابی پویای ریسک امنیت سایبری ارائه داده که محدودیت‌های بحرانی روش‌های سنتی را هنگام کاربرد در سیستم‌های کنترل صنعتی مبتنی بر SCADA برطرف می‌کند. از طریق یکپارچگی مدل‌سازی احتمالاتی پیشرفته، بهینه‌سازی نظریه بازی و تکنیک‌های یادگیری ماشین، این چارچوب به بهبودهای قابل‌توجهی در دقت ارزیابی، کاهش عدم قطعیت و کاربرد عملی برای محیط‌های صنعتی دست می‌یابد.

دستاوردهای کلیدی این کار شامل توسعه رویکرد نوآورانه مدل‌سازی تأثیر خسارت است که پیامدهای عملیاتی را از طریق طبقه‌بندی چهارسطحی دارایی کمی می‌کند. این نوآوری تضمین می‌کند که ارزیابی‌های ریسک تأثیر واقعی کسب‌وکار را منعکس می‌کنند نه نمرات انتزاعی آسیب‌پذیری را. از طرفی یکپارچگی شبکه‌های بیزین چندلایه و پویا قابلیت‌های پیچیده مدل‌سازی تهدید را فراهم می‌آورد که هم دربرگیرنده الگوهای تکامل تهدید فضایی و هم زمانی است و به کاهش چشمگیر عدم قطعیت ارزیابی در مقایسه با پایه‌های ایستا می‌انجامد.

عملکرد مطلوب رویکرد پیشنهادی بیانگر کاهش متوسط نمرات ریسک به میزان ۲۸٪ به همراه مزیت کاهش نرخ مثبت کاذب زیر ۵٪ است، دستیابی به این نتایج پیشرفت قابل‌ملاحظه‌ای در امنیت سایبری عملی صنعتی به شمار می‌رود. در کنار این نتایج مؤلفه بهینه‌سازی نظریه بازی پیشنهادی در این مقاله تخصیص بهینه منابع را با درنظرگرفتن محدودیت‌ها تضمین می‌کند، درحالی‌که سیستم توصیه مبتنی بر Random Forest اطلاعات قابل‌اجرا را برای متخصصان امنیت فراهم می‌آورد.

نتایج شبیه‌سازی کارایی چارچوب را در سناریوهای حمله متنوع اعتبارسنجی می‌کنند. کاهش یکنواخت ریسک حاصل شده برای مؤلفه‌های زیرساخت حیاتی، همراه با توانایی چارچوب برای سازگاری با الگوهای تهدید در حال تکامل، مناسب‌بودن آن را برای حفاظت از عملیات صنعتی با حساسیت بالا را نشان می‌دهد و همسویی جامع با استانداردهای بین‌المللی، ارزش عملی آن را بیشتر می‌کند.

اگرچه این تحقیق پیشرفت قابل‌توجهی را به همراه داشته است؛ اما در واقعیت چند حوزه نیازمند بررسی بیشتر هستند به‌عنوان‌مثال سربار محاسباتی به‌روزرسانی‌های بلادرنگ شبکه بیزین هنوز چالشی برای استقرارهای بسیار بزرگ به شمار می‌رود و می‌تواند به‌عنوان یک فعالیت پژوهشی در آینده بشمار رود تا الگوریتم‌های تقریب و رویکردهای محاسبات توزیع شده را برای ارتقای مقیاس‌پذیری بررسی کند. یکپارچگی با فناوری‌های نوظهور نظیر رمزنگاری مقاوم در برابر کوانتوم و تأیید یکپارچگی مبتنی بر بلاک‌چین فرصت‌هایی را برای تقویت دوام بلندمدت چارچوب ارائه می‌دهد. پژوهش‌های آینده همچنین باید کاربرد تکنیک‌های یادگیری عمیق برای

[۱] الگوریتم درخت اتصال (Junction Tree Algorithm): روش استنتاج دقیق در شبکه‌های بیزین که با تبدیل گراف به ساختار درختی، محاسبات احتمالی را کارآمدتر می‌کند. این الگوریتم پیچیدگی محاسباتی را از نمایی به چندجمله‌ای کاهش می‌دهد و امکان پردازش بلادرنگ را فراهم می‌آورد.

شناسایی خودکار الگوهای تهدید و توسعه سازوکارهای امنیتی خودترمیم کننده را بررسی کنند.

جدول ۶. مقایسه کیفی ویژگی روش‌های ارزیابی ریسک

قابلیت	FMEA/FTA	AHP	Alcaraz و همکاران [۲]	Qin و همکاران [۱۳]	چارچوب پیشنهادی
مدل‌سازی تهدید پویا	خیر	خیر	جزئی	بله	بله
تکامل زمانی تهدید	خیر	خیر	خیر	جزئی	بله
کمی‌سازی تأثیر خسارت	خیر	جزئی	خیر	خیر	بله
مدل‌سازی وابستگی‌های دارایی	جزئی	جزئی	بله	بله	بله
راهبرد کاهشی تطبیقی	خیر	خیر	خیر	بله	بله
یکپارچگی یادگیری ماشین	خیر	خیر	خیر	خیر	بله
همسویی با استانداردها	جزئی	جزئی	جزئی	جزئی	کامل

سپاسگزاری

نویسندگان از شرکای صنعتی که بینش‌های ارزشمندی درباره الزامات عملیاتی و محدودیت‌های استقرارهای واقعی SCADA ارائه کردند، قدردانی می‌کنند. تشکر ویژه از داوران ناشناسی که بازخورد سازنده آن‌ها به طور چشمگیری کیفیت این مقاله را بهبود بخشید. این تحقیق تا حدی توسط دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، تهران، ایران حمایت شد.

مراجع

[1] D Kaur, A Anwar, I Kamwa, S Islam, SM Muyeen. "A Bayesian deep learning approach with convolutional feature engineering to discriminate cyber-physical intrusions in smart grid systems", - IEEE, 2023 - ieeexplore.ieee.org

[2] F. Brancati, D. Mongelli, F. Mariotti P. Lollini. "A cybersecurity risk assessment methodology for industrial automation control systems". volume 24, article number 76, (2025).

[3] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," International Journal of Critical Infrastructure Protection, vol. 8, pp. 53-66, 2015.

[4] National Institute of Standards and Technology (NIST), "Guide to industrial control systems security," NIST Special Publication 800-82 Rev. 3, 2011.

[5] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," Survival, vol. 53, no. 1, pp. 23-40, 2011.

[6] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," Electricity Information Sharing and Analysis Center (E-ISAC), 2016.

[7] C. Krauss, "Colonial Pipeline hack reveals critical infrastructure vulnerabilities," The New York Times, May 13, 2021.

[8] National Institute of Standards and Technology (NIST), "Guide for conducting risk assessments," NIST Special Publication 800-30 Rev. 1, 2012.

[9] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," Computers & Security, vol. 56, pp. 1-27, 2016.

[10] W. Wang, Z. Lu, and T. Chen, "Cybersecurity challenges in industrial control systems," International Journal of Critical Infrastructure Protection, vol. 9, pp. 52-80, 2015.

[11] Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K. and Meskin, N., 2020. Cybersecurity for industrial control systems: A survey. *computers & security*, *89*, p.101677.

[12] International Organization for Standardization (ISO/IEC), "Information technology -- Security techniques -- Methodology for IT security evaluation," ISO/IEC Standard 18045, 2022.

[13] Hu, C.L., Wang, L., Chen, M.L. and Pei, C., 2024. A real-time interactive decision-making and control framework for complex cyber-physical-human systems. *Annual Reviews in Control*, *57*, p.100938.

[14] Patel, R., 2023. Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems) Employing Deep Learning in Cybersecurity Defence. *Int. J. Curr. Eng. Technol*, *13*(06), pp.584-591.

[15] Ali, B.S., Ullah, I., Al Shloul, T., Khan, I.A., Khan, I., Ghadi, Y.Y., Abdusalomov, A., Nasimov, R., Ouahada, K. and Hamam, H., 2024. ICS-IDS: application of big data analysis in AI-based intrusion detection systems to identify cyberattacks in ICS networks. *The Journal of Supercomputing*, *80*(6), pp.7876-7905.

[16] Barua, S., Gao, X., Pasman, H. and Mannan, M.S., 2016. Bayesian network based dynamic operational risk assessment. *Journal of Loss Prevention in the Process Industries*, *41*, pp.399-410.

[17] Almaiah, M.A., Yelisetti, S., Arya, L., Babu Christopher, N.K., Kaliappan, K., Vellaisamy, P., Hajjej, F. and Alkdour, T., 2023. A novel approach for improving the security of IoT–medical data systems using an enhanced dynamic Bayesian network. *Electronics*, *12*(20), p.4316.

[18] Abdulhamid, A., Kabir, S., Ghafir, I. and Lei, C., 2024, January. Reliability Assessment of IoT-enabled Systems using Fault Trees and Bayesian Networks. In *International Conference on Advances in Distributed Computing and Machine Learning* (pp. 267-277). Singapore: Springer Nature Singapore.