Passive Defence

Vol. 16, No. 3, Autumn 2025, Serial No. 63

ISSN: 2980-8030 , E-ISSN: 2008-6849

Strategy for Enhancing the Security of Critical Infrastructure Using Artificial Intelligence

Hamed Asghari[1], Mehdi Modiri[2]*

[1]M.Sc. in Crisis Management, Faculty of Engineering and Passive Defense, Malek Ashtar University of Technology, Tehran, Iran Email Address: hasghari767@gmail.com

[2]Correspondence :Professor, Faculty of Engineering and Passive Defense, Malek Ashtar University of Technology, Tehran, Iran .Email Address: m_modiri@mut.ac.ir

ARTICLE INFO

Article history:

Article Type: Research paper

Received: 24 November 2024

Received in revised form: 18 May 2025

Accepted: 20 September 2025

Available online: 22 October 2025

Keywords:

Rule-based Artificial Intelligence Word

Cybersecurity

Critical Infrastructure

Intelligent Decision-Making Modeling

Attack Analysis

ABSTRACT

Critical Infrastructure (CI) includes the essential systems, assets, and services that are vital for the functioning and well-being of society and the economy. However, the rapid growth of cyber threats in digital environments poses serious risks to the efficiency of these infrastructures and presents significant challenges to public safety, economic stability, and national security. This growing threat landscape highlights the urgent need for effective cybersecurity solutions, particularly in the domains of automation and intelligent decision-making, where AI-based modeling can play a crucial role. In this regard, our discussion focuses on comparing rule-based artificial intelligence systems, as this approach offers greater transparency, interpretability, and trustworthiness compared to deep learning methods, enabling human analysts to examine and validate decisions—a critical and unavoidable requirement in cybersecurity. This research analyzes multi-layer rule-based AI systems designed to facilitate human-understandable decision-making alongside automated processes in critical infrastructure environments. It also categorizes various rule generation techniques and explores both knowledge-based and data-driven approaches for extracting meaningful insights from data. Such insights empower security analysts to identify threats, investigate attacks, and make informed decisions across various sectors. Furthermore, the study examines how these methods can address cybersecurity challenges in key sectors such as energy, defense, transportation, healthcare, water resources, and agriculture, thereby contributing to the enhancement of security measures. The paper concludes by identifying existing challenges, outlining future research opportunities, and proposing innovative strategies for countering emerging cyber threats.

Cite this article: H. Asghari and M. Modiri, "Strategy for Enhancing the Security of Critical Infrastructure Using Artificial Intelligence," Journal of Passive Defence, vol. 16, no. 3, pp. 1-20, 2025. DOR: 20.1001.1.20086849.1404.16.3.1.9

Publisher: Imam Hossein University.

پدافند غیرعامل

سال پانزدهم، شماره ۳، پاییز ۱۴۰۴، (پیاپی ۶۳): صص ۲۰-۱

شاپای چاپی: ۶۹۴۹-۲۰۰۸ | **شاپای الکترونیکی:** ۸۰۳۰-۲۹۸۰

راهبرد افزایش امنیت زیرساخت‌های حیاتی با هوش مصنوعی

حامد اصغری[۱]، مهدی مدیری[۲*]

[۱] کارشناسی ارشد مجتمع دانشگاهی مهندسی و پدافند غیر عامل، دانشگاه صنعتی مالک اشتر، تهران، ایران. رایانامه: hasghari767@gmail.com

[۲] استاد مجتمع دانشگاهی مهندسی و پدافند غیر عامل، دانشگاه صنعتی مالک‌اشتر، تهران، ایران. رایانامه: m_modiri@mut.ac.ir

چکیده

زیرساخت حیاتی (CI) شامل سامانه‌ها، دارایی‌ها و خدمات حیاتی است که برای عملکرد و رفاه جامعه و اقتصاد ضروری هستند. با این حال، رشد سریع تهدیدات سایبری در محیط‌های دیجیتال خطرات جدی برای کارایی این زیرساخت‌ها ایجاد می‌کند و چالش‌های قابل توجهی برای امنیت عمومی، ثبات اقتصادی و امنیت ملی به همراه دارد. این وضعیت نیاز به راه‌حل‌های مؤثر در زمینه امنیت سایبری را، به‌ویژه در حوزه اتوماسیون و تصمیم‌گیری هوشمند، تقویت می‌کند؛ جایی که مدل‌سازی مبتنی بر هوش مصنوعی می‌تواند نقش کلیدی ایفا کند. در این راستا، بحث ما بر مقایسه سامانه‌های هوش مصنوعی مبتنی بر قانون متمرکز است، زیرا این رویکرد از شفافیت، تفسیرپذیری و قابلیت اعتماد بالاتری نسبت به روش‌های یادگیری عمیق برخوردار است و امکان بررسی و اعتبارسنجی تصمیمات را توسط تحلیلگران انسانی فراهم می‌سازد؛ امری که در حوزه امنیت سایبری حیاتی و گریزناپذیر است. این پژوهش به تحلیل هوش مصنوعی مبتنی بر قوانین چندلایه می‌پردازد که هدف آن تسهیل تصمیمات قابل فهم انسانی در کنار فرآیندهای خودکار برای زیرساخت‌های حیاتی است. علاوه بر این، انواع روش‌های تولید قانون را دسته‌بندی کرده و رویکردهای مبتنی بر دانش و داده برای استخراج بینش‌های معنادار از اطلاعات بررسی می‌شود. این فهم به تحلیلگران امنیتی کمک می‌کند تا تهدیدات را شناسایی کرده، حملات را بررسی کنند و تصمیمات آگاهانه‌ای در بخش‌های مختلف بگیرند. همچنین به این موضوع پرداخته می شود که چگونه این روش‌ها می‌توانند به چالش‌های امنیت سایبری در بخش‌های حیاتی مانند انرژی، دفاع، حمل‌ونقل، بهداشت، منابع آب و کشاورزی پاسخ دهند و در نتیجه به بهبود تدابیر امنیتی کمک کنند. این مقاله با شناسایی چالش‌های موجود، فرصت‌های تحقیقاتی آینده و ارائه راهبردهای نوآورانه برای مقابله با تهدیدات سایبری آینده به پایان می‌رسد.

مشخصات مقاله

تاریخچه مقاله:

نوع مقاله: علمی پژوهشی

دریافت: ۱۴۰۳/۰۹/۰۴

بازنگری: ۱۴۰۴/۰۲/۲۸

پذیرش: ۱۴۰۴/۰۶/۲۹

ارائه آنلاین: ۱۴۰۴/۰۷/۳۰

کلیدواژه‌ها:

هوش مصنوعی مبتنی بر قوانین

امنیت سایبری

زیرساخت‌های حیاتی

مدل‌سازی تصمیم‌گیری هوشمند

تحلیل حملات

استناد: اصغری، حامد، مدیری، مهدی، " راهبرد افزایش امنیت زیرساخت‌های حیاتی با هوش مصنوعی"، نشریه پدافند غیرعامل، دوره ۱۶، شماره۳، صفحات ۲۰-۱، ۱۴۰۴. DOR: 20.1001.1.20086849.1404.16.3.1.9

ناشر: دانشگاه جام امام حسین(ع).

۱- مقدمه

زیرساخت‌های حیاتی شامل تمامی سامانه‌ها و دارایی‌های فیزیکی و دیجیتال هستند [۱] که برای حفظ عملکرد کلی یک جامعه یا کشور ضروری‌اند. این زیرساخت‌ها شامل شبکه‌های ارتباطی، فناوری اطلاعات و زنجیره‌های تأمین است که هر گونه آسیب به آن‌ها می‌تواند تبعات جدی بر رفاه اجتماعی و امنیت ملی به همراه داشته باشد [۲]. از این رو، امنیت سایبری باید در اولویت اصلی کشورها قرار گیرد، زیرا هرگونه اختلال در این زیرساخت‌ها می‌تواند آسیب جدی به امنیت عمومی و ثبات اقتصادی وارد کند؛ با گسترش تهدیدات سایبری و پیچیدگی آن‌ها در دنیای دیجیتال، روش‌های سنتی دفاعی به تنهایی کافی نیستند [۳]؛ بنابراین، ضروری است که به سمت اتوماسیون و تصمیم‌گیری هوشمندانه حرکت شود، در حالی که شفافیت و قابلیت تفسیر مدل‌ها نیز از اهمیت بالایی برخوردار است تا بتوان نیازهای امنیتی زیرساخت‌های حیاتی را به شکل مؤثری برآورده کرد.

علاوه بر این، یک رویکرد مؤثر در امنیت سایبری زیرساخت‌های حیاتی، استفاده از فناوری‌های نوین مانند هوش مصنوعی و یادگیری ماشین است که می‌تواند به شناسایی و پیش‌بینی تهدیدات بالقوه کمک کند [۴]. این فناوری‌ها با تحلیل داده‌های بزرگ و شناسایی الگوهای غیرمعمول، قادرند هشدارهایی به موقع ارائه دهند که مانع بروز حملات سایبری می‌شود. به‌علاوه، ترکیب راهکارهای خودکار با قابلیت واکنش به تهدیدات می‌تواند زمان پاسخ به این موارد را به شدت کاهش دهد و از آسیب‌های احتمالی جلوگیری کند. برای ایجاد قابلیت‌های موثر در برابر تهدیدات پیشرفته، نیاز به آموزش و آگاهی کارکنان نیز حیاتی است؛ زیرا اقدامات انسانی در کنار فناوری‌های پیشرفته می‌تواند به تقویت لایه‌های امنیتی کمک کند. در نتیجه، ایجاد یک سامانه جامع و یکپارچه که شامل فناوری‌های نوین، آموزش مستمر و به‌کارگیری مشاوره‌های امنیتی تخصصی باشد، برای حفاظت از زیرساخت‌های حیاتی در دنیای پیچیده و در حال تحول امروز ضروری است [۵ و ۶].

پیشرفت‌های اخیر در هوش مصنوعی (AI)، به ویژه در زمینه تکنیک‌های مدل‌سازی علم داده (DS) و یادگیری ماشین (ML)، به طرز چشمگیری روش‌های تحلیل داده و استفاده از دانش استخراج‌شده برای اتوماسیون و تصمیم‌گیری هوشمند در حوزه‌های مختلف، از جمله امنیت سایبری، را متحول کرده است [۷-۹]. در حالی که روش‌های یادگیری شبکه‌های عصبی عمیق دارای قدرت محاسباتی قابل توجهی هستند، درک و تفسیر نتایج آن‌ها برای انسان و همچنین قابلیت اعتماد به مدل‌های مبتنی بر هوش مصنوعی در حل مسائل امنیتی زیرساخت‌های حیاتی از اهمیت بالایی برخوردار است. بنابراین، توسعه مدل‌های هوش مصنوعی که شفاف و قابل تفسیر باشند، می‌تواند به طور خاص برای تحلیلگران سایبری مؤثرتر باشد و امکان اجرای راه‌حل‌های امنیتی هوشمندانه و قابل اعتماد را فراهم آورد. برای این منظور، در این تحقیق به بررسی مدل‌سازی هوش مصنوعی مبتنی بر قانون پرداخته شده است که در آن الگوها، وابستگی‌ها و دانش قابل تفسیر از داده‌ها کشف می‌شود. این رویکرد نه تنها برای توسعه مدل‌هایی با کارایی بیشتر مفید است، بلکه می‌تواند به عنوان یک راه‌حل برتر برای غلبه بر چالش‌های مدل‌سازی سنتی هوش مصنوعی در زمینه‌های متنوع کاربردی، از جمله امنیت سایبری، عمل کند. با چنین پیشرفت‌هایی، امکان بهبود قابل توجهی در دقت و کارایی راهبردهای امنیتی فراهم می‌شود و تحلیلگران می‌توانند با اعتماد بیشتری به داده‌ها و نتایج مدل‌ها تکیه کنند [۱۰].

همچنین، در زمینه امنیت سایبری، توضیحات قابل فهم و منطقی از تصمیمات مدل‌ها می‌تواند به تحلیلگران این توانایی را بدهد که به سرعت واکنش نشان دهند و راهکارهای مناسبی برای مقابله با تهدیدات در حال ظهور ارائه دهند [۱۱]. در عصر اطلاعات، جایی که حملات سایبری به طور فزاینده‌ای پیچیده و متنوع می‌شوند، بکارگیری روش‌های شفاف و قابل تفسیر در هوش مصنوعی می‌تواند به عنوان یک مزیت رقابتی حیاتی برای سازمان‌ها عمل کند. به همین دلیل، سرمایه‌گذاری در توسعه و بهینه‌سازی چنین مدل‌هایی نه تنها ضروری، بلکه یک گام پیشرفته در راستای تحقق اهداف امنیتی و حفاظت از داده‌ها محسوب می‌شود [۱۲]. بر این اساس، نیاز به یک رویکرد جامع در ترکیب هوش مصنوعی با امنیت سایبری بیشتر از هر زمان دیگری احساس می‌شود، تا بتوان به شکل مؤثری با چالش‌های پیچیده دنیای امروز مقابله کرد.

۱-۱- بیان مسئله

امنیت زیرساخت‌های حیاتی به عنوان یکی از مهم‌ترین ارکان جامعه، با چالش‌های متعددی مواجه است. به‌طوری‌که، طبق گزارش‌های جهانی، ۳۵ درصد از سازمان‌های زیرساختی در سال ۲۰۲۲ حداقل یک حمله سایبری را تجربه کرده‌اند، که این آمار نسبت به سال قبل ۱۵ درصد افزایش یافته است. همچنین، بر اساس برآوردهای موسسه NOAA، بلایای طبیعی در ایالات متحده

به‌تنهایی باعث خسارتی بالغ بر ۹۲ میلیارد دلار در سال ۲۰۲۱ شدند. از سوی دیگر، حملات فیزیکی به زیرساخت‌های حیاتی از جمله مسائل جدی و نگران‌کننده‌ای هستند که می‌توانند تبعات گسترده‌ای برای امنیت و سلامت جامعه داشته باشند. یکی از نمونه‌های بارز این نوع حملات، حمله به تاسیسات نفتی عربستان سعودی در سپتامبر ۲۰۱۹ بود که آسیب به شرکت آرامکو، بزرگترین شرکت نفتی جهان، به کاهش تولید روزانه حدود ۵ میلیون بشکه نفت منجر شد و در نتیجه قیمت جهانی نفت به شدت افزایش یافت. این حمله از سوی حوثی‌ها و با استفاده از پهپادها انجام شد و نشان‌دهنده آسیب‌پذیری زیرساخت‌های انرژی در برابر حملات دقیق و سازمان‌یافته است.

یک مورد دیگر در هند و در سال ۲۰۱۶ رخ داد، جایی که تاسیسات زیرساخت‌های آبرسانی در یک حمله تروریستی مورد هدف قرار گرفت و منجر به تخریب و اختلال در خدمات آبرسانی به بیش از ۱ میلیون نفر شد. این نوع حملات نه تنها به زیرساخت‌ها آسیب می‌زند، بلکه عواقب جدی اجتماعی و اقتصادی نیز به همراه دارد، زیرا باعث بی‌نظمی و نارضایتی عمومی می‌شود.

این مثال‌ها نشان می‌دهند که حملات فیزیکی به زیرساخت‌ها می‌توانند عواقب زیادی بر امنیت ملی و ثبات اقتصادی کشورها داشته باشند و نیاز به تقویت حفاظت و امنیت زیرساخت‌ها روز به روز بیشتر احساس می‌شود. با توجه به تجارب اخیر، بهبود امنیت این زیرساخت‌ها باید به عنوان یک اولویت در دستور کار دولت‌ها و سازمان‌های مربوطه قرار گیرد.

در راستای مقابله با این تهدیدات، کشورهای مختلف در سال‌های اخیر به سرمایه‌گذاری در فناوری‌های نوین پرداخته‌اند. برای مثال، انتظار می‌رود که بازار امنیت سایبری زیرساخت‌های حیاتی تا سال ۲۰۲۶ به ارزش ۲۷ میلیارد دلار برسد که نشان‌دهنده توجه روزافزون به این حوزه است. همچنین، بیش از ۷۰ درصد از سازمان‌ها تأکید می‌کنند که آموزش و آگاهی کارکنان در زمینه امنیت ضروری است و دست‌کم ۸۰ درصد از حوادث سایبری ناشی از خطای انسانی بوده است. به این ترتیب، پیشنهاد می‌شود که سرمایه‌گذاری در زیرساخت‌ها و به‌روزرسانی سامانه‌ها همراه با آموزش مستمر کارکنان، به عنوان دو اولویت اساسی در تقویت امنیت زیرساخت‌های حیاتی در نظر گرفته شود.

۱-۲- مدل‌سازی هوش مصنوعی

مدل‌سازی هوش مصنوعی مبتنی بر قوانین در حوزه امنیت سایبری به عنوان ابزاری اصلی برای شناسایی تهدیدات امنیتی به شمار می‌آید که می‌تواند فرایندهای امنیتی را به شکل موثری بهینه‌سازی کند. این مدل‌ها با تحلیل داده‌های امنیتی و استخراج قوانین و الگوهای پیچیده، قادر به شناسایی ناهنجاری‌هایی هستند که ممکن است در روش‌های سنتی نادیده گرفته شوند. به عنوان مثال، این مدل‌ها با ادغام داده‌ها از منابع مختلف، می‌توانند رفتارهای مشکوک را شناسایی کرده و تهدیدات ناشناخته‌ای را فاش کنند که نیاز به واکنش فوری دارند.

از دیگر مزایای این نوع مدل‌سازی، قابلیت یادگیری مداوم آن‌هاست که به روزرسانی و سازگاری با تهدیدات نوظهور را ممکن می‌سازد. به همین دلیل، این مدل‌ها می‌توانند به طور قابل توجهی دقت و سرعت در پاسخ به تهدیدات را افزایش دهند. همچنین، آن‌ها به تحلیل روابط و وابستگی‌های موجود در داده‌ها کمک کرده و به کاهش نتایج مثبت کاذب می‌انجامند، به طوری که بینش‌های عمیق‌تری درباره تهدیدات قانونی و پروتکل‌های امنیتی ارائه می‌دهند.

در دنیای به سرعت در حال تحول تهدیدات سایبری امروز، مدل‌سازی مبتنی بر قوانین می‌تواند به عنوان یک مزیت رقابتی برای سازمان‌ها عمل کرده و به افزایش اتوماسیون، هوشمندی و شفافیت در فرایندهای امنیتی کمک کند. این مدل‌ها همچنین با ایجاد شفافیت در مورد نحوه تصمیم‌گیری خود، اعتماد لازم را برای نظارت انسانی و اطمینان از پاسخگویی برقرار می‌سازند. علاوه بر این، قابلیت انطباق‌پذیری این مدل‌ها در فرآیند مدل‌سازی، امکان افزودن، حذف و به‌روزرسانی قوانین را فراهم می‌کند و بدین ترتیب اطمینان حاصل می‌شود که دانش سامانه همیشه با داده‌های جدید همگام است. این ویژگی به مدیریت بهینه سامانه کمک کرده و فهم و تبیین نتایج را تسهیل می‌کند.

علاوه بر مزایای ذکر شده، مدل‌سازی مبتنی بر قوانین به سازمان‌ها این امکان را می‌دهد که با کاهش وابستگی به مداخله انسانی، کارایی و سرعت پاسخگویی به تهدیدات را افزایش دهند. این اتوماسیون باعث می‌شود که منابع انسانی به فعالیت‌های تحلیلی و استراتژیک بیشتری معطوف شوند، در حالی که سامانه به صورت خودکار تهدیدات شناسایی و اقدامات لازم را انجام می‌دهد. همچنین، با استفاده از روش‌های یادگیری ماشین و تحلیل پیشرفته، این مدل‌ها می‌توانند پیش‌بینی‌هایی درباره تهدیدات آینده ارائه دهند و سازمان‌ها را آماده سازند تا با چالش‌های جدید به شکلی موثرتر مقابله کنند. در نتیجه، مدل‌سازی مبتنی بر قوانین نه تنها به

تقویت امنیت سایبری کمک می‌کند بلکه به تسهیل تصمیم‌گیری‌های آگاهانه و بهبود قابلیت‌های مدیریتی در سطح کلان نیز می‌انجامد [۱۲-۱۴].

۱-۳- امنیت سایبری زیرساخت‌های حیاتی

در سال‌های اخیر، تمرکز بر روی امنیت زیرساخت‌های حیاتی (CI) به عنوان یکی از چالش‌های مهم در عرصه فناوری اطلاعات و سایبری مورد توجه قرار گرفته است. این زیرساخت‌ها که شامل سامانه‌های حیاتی مانند برق، آب، و ارتباطات می‌شوند، به شدت در برابر حملات سایبری آسیب‌پذیرند. پژوهش‌ها به بررسی نقاط ضعف این سامانه‌ها و تحلیل ابزارهای دفاعی موجود پرداخته‌اند، به ویژه در زمینه سامانه‌های کنترل صنعتی که مدیریت آن‌ها به صورت خودکار و از راه دور صورت می‌گیرد. همچنین، گسترش اینترنت اشیا و پیوند آن با زیرساخت‌های حیاتی، تهدیدات جدیدی را به وجود آورده که نیازمند روش‌های نوین برای مقابله با آن‌هاست. این تحقیقات به تدوین راهبردهای امنیتی و ایجاد سامانه‌های محافظتی بیشتر کمک کرده و به درک بهتری از چالش‌های موجود در این حوزه می‌انجامد [۱۵].

با این وجود، هنوز هم نیاز به توجه بیشتر به راه‌حل‌های مبتنی بر هوش مصنوعی، به ویژه مدل‌سازی هوش مصنوعی مبتنی بر قوانین برای امنیت زیرساخت‌های حیاتی وجود دارد. برای درک بهتر از چالش‌های موجود و ارائه راهکارهای موثر، پنج سوال کلیدی مطرح شده است که شامل ضرورت‌های اتوماسیون و هوشمندی در امنیت سایبری، ویژگی‌ها و مزایای مدل‌سازی هوش مصنوعی مبتنی بر قوانین، تولید قوانین چندوجهی، کاربردهای عملی این مدل‌ها در بخش‌های مختلف، و چالش‌های موجود در کشف دانش و روش‌های مبتنی بر قوانین می‌شود. این تحقیق هدف دارد تا با تحلیل و بررسی عمیق این ابعاد، راهکارهای نوآورانه‌ای برای تقویت امنیت زیرساخت‌های حیاتی ارائه کند. اهداف این تحقیق شامل بررسی و مقایسه ادبیات موجود در زمینه اتوماسیون و هوشمندی در امنیت زیرساخت‌های حیاتی، شناسایی تهدیدات و ناهنجاری‌های بالقوه‌ای است که نیاز به توجه فوری دارند. همچنین، یک طبقه‌بندی از روش‌های هوش مصنوعی مبتنی بر قوانین ارائه خواهد شد که ضمن بحث در مورد قابلیت‌ها و پتانسیل محاسباتی آن‌ها، به تحلیل نحوه تأثیرگذاری این روش‌ها بر مدل‌سازی امنیت سایبری نیز می‌پردازد. با بررسی حوزه‌های کاربردی مختلف، از تشخیص ناهنجاری‌ها گرفته تا تقویت پاسخ به تهدیدات، این تحقیق سعی دارد چگونه این روش‌ها می‌توانند به حل مسائل سایبری در بخش‌های متعددی مانند انرژی، آب، حمل و نقل، و کشاورزی کمک کنند. در نهایت، چالش‌های اساسی و مسائل تحقیقاتی در این حوزه شناسایی و خلاصه شده و جهت‌های تحقیقاتی جدیدی برای مدل‌سازی امنیت سایبری نسل بعدی در زیرساخت‌های حیاتی تعیین می‌شود.

۲- مرور ادبیات و پیشینه تحقیق

در این بخش، به بررسی پیشینه‌ای می‌پردازیم که شامل زیرساخت‌های حیاتی (CI) و چالش‌های امنیت سایبری مرتبط با آن‌ها است. ابتدا به تعریف و اهمیت زیرساخت‌های حیاتی و تهدیداتی که ممکن است آن‌ها را تحت تأثیر قرار دهد، پرداخته شده است و سپس امنیت سایبری در این زمینه، با تأکید بر روش‌های موجود برای حفاظت از این زیرساخت‌ها، مورد تحلیل قرار گرفت. پس از آن، به امنیت سایبری مبتنی بر قواعد مبتنی بر هوش مصنوعی در CI خواهیم پرداخت و بررسی خواهیم کرد که چگونه این تکنیک‌ها می‌توانند به شناسایی و مقابله با تهدیدات کمک کنند. همچنین، بررسی‌های مرتبط با حوزه مطالعه خود را مرور می‌کنیم و تفاوت‌های کلیدی بین نتایج و رویکردهای مقاله خود و مقالات نظرسنجی موجود را مورد تحلیل قرار می‌دهیم تا شکاف‌های موجود در ادبیات فعلی را شناسایی کرده و زمینه‌های جدیدی را برای تحقیقات آینده پیشنهاد دهیم. این تحلیل جامع به ما کمک می‌کند تا چارچوبی دقیق و مستند برای پژوهش‌های آتی فراهم آوریم.

۲-۱- مبانی نظری

۲-۱-۱- زیرساخت های حیاتی

زیرساخت‌های حیاتی به مجموعه‌ای از سامانه‌ها، شبکه‌ها و دارایی‌های فیزیکی و دیجیتالی اطلاق می‌شود که برای ادامه حیات یک جامعه و پایداری اقتصاد آن ضروری هستند [۱۶]. این زیرساخت‌ها شامل دو بخش اصلی فناوری اطلاعات (IT) و فناوری عملیاتی (OT) می‌شوند. فناوری اطلاعات به سامانه‌های سردبیر و محاسباتی اشاره دارد که برای پردازش، ذخیره‌سازی و تبادل اطلاعات در سازمان‌ها استفاده می‌شوند. به‌عنوان نمونه، سرورها، کامپیوترها، لپ‌تاپ‌ها و دیگر دستگاه‌های ارتباطی در این دسته قرار می‌گیرند. از سوی دیگر، فناوری عملیاتی به سامانه‌ها و ابزارهایی مربوط می‌شود که وظیفه نظارت و کنترل عملیات فیزیکی در بخش‌هایی همچون انرژی، حمل‌ونقل و آب را بر عهده دارند [۱۷ و ۱۸]. نمونه‌هایی از این سامانه‌ها شامل SCADA، DCS، ICS و

PLC ها هستند که به طور خاص برای مدیریت حوزه‌های مختلف زیرساخت‌ها طراحی شده‌اند [۱۹-۲۱].

اهمیت این زیرساخت‌ها در تأمین خدمات کلیدی برای جامعه و هم‌چنین تأثیرگذاری آن‌ها بر رفاه عمومی غیرقابل انکار است. آن‌ها در حال فراهم آوردن خدماتی هستند که پایه‌های اقتصادی و اجتماعی را تقویت می‌کند و به فعالیت‌های حیاتی چون انرژی، حمل و نقل و ارتباطات کمک می‌کند. با این حال، زیرساخت‌های حیاتی به‌سادگی در برابر تهدیدات و بلایای مختلف آسیب‌پذیر هستند، که این آسیب‌پذیری می‌تواند عواقب جدی برای امنیت عمومی و ثبات اقتصادی به همراه داشته باشد. به همین دلیل، محافظت از این زیرساخت‌ها در برابر تهدیدات سایبری و فیزیکی امری حیاتی است تا علاوه بر حفظ خدمات کلیدی، سلامت جامعه و امنیت ملی به خطر نیفتد.

۲-۱-۲- تهدیدات زیرساخت های حیاتی

زیرساخت‌های حیاتی در جوامع مدرن با طیف وسیعی از تهدیدات فیزیکی و سایبری مواجه هستند که می‌توانند خدمات ضروری را مختل کرده و امنیت و رفاه جامعه را به خطر بیندازند. مهاجمان ممکن است سامانه‌های فناوری اطلاعات (IT) و فناوری عملیاتی (OT) را هدف قرار دهند تا به داده‌های حساس دسترسی پیدا کرده، اختلال ایجاد کنند یا فرآیندهای حیاتی را دستکاری کنند. از این رو، حفاظت از هر دو نوع شبکه برای تأمین امنیت زیرساخت‌ها بسیار حائز اهمیت است؛ زیرا این دو سامانه به‌طور مستمر با یکدیگر در ارتباط‌اند و نقاط ضعف یکی می‌تواند به دیگری آسیب برساند. بنابراین، نیاز به طراحی استراتژی‌های امنیتی یکپارچه و همکاری میان نهادهای مختلف برای مقابله با این تهدیدات ضروری است [۲۲ و ۲۳].

۲-۱-۳- امنیت سایبری

امنیت سایبری شامل مجموعه‌ای از روش‌ها و فناوری‌هاست که برای حفاظت از دارایی‌های دیجیتال و پیشگیری از تهدیدات سایبری طراحی شده‌اند. با پیشرفت تکنولوژی و افزایش پیچیدگی حملات سایبری، چالش‌های بیشتری در دفاع از سامانه‌های دیجیتال بروز کرده است. این وضعیت نیاز به درک عمیق‌تری از نوع جدیدی از جرایم رایانه‌ای را ایجاب می‌کند که به طور خاص شامل جرایم سایبری و هوش مصنوعی می‌شود. به عنوان مثال، جرایم سایبری به فعالیت‌های غیرقانونی انجام‌شده از طریق اینترنت اشاره دارد، در حالی که جرایم مبتنی بر هوش مصنوعی، شامل بهره‌برداری از این فناوری‌ها برای ارتکاب اقدامات مجرمانه می‌شوند [۲۴].

زیرساخت‌های حیاتی (CI)، با دیجیتالی شدن و اتصال روزافزون به شبکه‌ها، به اهداف جذابی برای مجرمان سایبری تبدیل شده‌اند. این تهدیدات می‌توانند پیامدهای جدی از قبیل خسارت مالی، خطرات برای ایمنی عمومی و تأثیرات امنیت ملی به همراه داشته باشند. در نتیجه، تضمین امنیت سایبری برای حفاظت از این زیرساخت‌ها و جلوگیری از حملات سایبری، به یک موضوع حیاتی تبدیل شده است که نیاز به توجه و سرمایه‌گذاری مداوم دارد. برقراری امنیت در این حوزه نه تنها برای حفظ خدمات حیاتی جامعه، بلکه برای تضمین ثبات اقتصادی و اجتماعی نیز ضروری است [۲۵ و ۲۶].

۲-۱-۴- نقش هوش مصنوعی در حفاظت از زیرساخت‌های حیاتی

امنیت سایبری مبتنی بر قواعد هوش مصنوعی به عنوان یک راه حل پیشرفته، به‌منظور محافظت از زیرساخت‌های حیاتی در برابر تهدیدات سایبری طراحی شده است. این رویکرد، ترکیبی از مزایای سامانه‌های مبتنی بر قوانین سنتی و قابلیت‌های هوش مصنوعی، از جمله علم داده و یادگیری ماشین را ارائه می‌دهد. استفاده از این تکنیک‌ها امکان شناسایی و پاسخ به تهدیدات را به‌طور مؤثرتری فراهم می‌آورد. همچنین، مدل‌های مبتنی بر قانون به‌طور دوره‌ای به‌روزرسانی می‌شوند تا دانش جدید و تجربیات به‌دست‌آمده را در نظر بگیرند، به گونه‌ای که بهینه‌سازی مستمر عملکرد آنها حاصل شود [۲۷]. به‌روزرسانی سامانه‌های امنیتی نیازمند رویکردی راهبردی و پویا است که شامل افزودن قوانین تازه و تجدید نظر در قوانین موجود می‌شود [۲۹]. این فرایند نه تنها به شناسایی و ثبت تهدیدات جدید کمک می‌کند، بلکه امکان تنظیم دقیق‌تر واکنش‌ها به تغییرات محیط امنیتی را نیز فراهم می‌آورد. از سوی دیگر، حذف قواعدی که دیگر کاربردی نیستند، می‌تواند عملکرد سامانه را بهبود بخشد و تعداد هشدارهای اشتباه را کاهش دهد. این به‌روزرسانی‌های مستمر باعث افزایش دقت سامانه و کاهش نگرانی‌های مربوط به وجود قوانین غیر مرتبط می‌شود و به آن اجازه می‌دهد که به سرعت به تهدیدات جدید پاسخ دهد و همچنین با تغییرات محیطی سازگار شود.

علاوه بر این، امنیت سایبری مبتنی بر قوانین هوش مصنوعی در پیشبرد سامانه‌های خودکار، هوشمند و شفاف به‌ویژه اهمیت دارد. توانایی این مدل‌ها در گنجاندن دانش جدید و درک واضح از نحوه

کارکرد آنها، اعتماد کاربران و نظارت انسانی را تسهیل می‌کند [۲۹]. مدل‌های قانونی که از ساختارهای آسان برای تفسیر مانند قوانین IF-THEN استفاده می‌کنند، نه تنها شفافیت را افزایش می‌دهند بلکه پایه‌گذار توسعه هوش مصنوعی مسئولانه و قابل توضیح هستند. این ویژگی‌ها در نهایت می‌توانند به ایجاد یک محیط امنیتی قوی‌تر و پایدارتر در برابر تهدیدات سایبری کمک کنند [۳۰ و ۳۱].

۲-۲- پیشینه تحقیق

پیشینه تحقیق در زمینه حملات سایبری به زیرساخت‌های حیاتی و سامانه‌های عملیاتی[1] شامل مطالعات و مقالات متعدد است که به تحلیل چالش‌ها، تهدیدات و راهکارهای امنیتی می‌پردازند.

تحقیقات در زمینه حملات سایبری به زیرساخت‌های حیاتی و سامانه‌های عملیاتی از دهه ۲۰۰۰ آغاز شد، زمانی که با رشد فناوری‌های دیجیتال و اتصال شبکه‌ای، توجه به امنیت سامانه‌های کنترل صنعتی بیشتر شد. مطالعات اولیه نشان دادند که این سامانه‌ها، به ویژه سامانه‌های اسکادا[2]، به دلیل کمبود امنیت در طراحی و پیاده‌سازی، آسیب‌پذیر هستند [۳۲]. یکی از حملات در این حوزه، حمله استاکس‌نت[3] در سال ۲۰۱۰ بود که زیرساخت‌های هسته‌ای ایران را هدف قرار داد و نشان داد که اختلال در عملیات فیزیکی می‌تواند عواقب جدی به همراه داشته باشد [۳۳]. در سال‌های اخیر، پژوهش‌های متمرکز بر چرخه حیات امنیت سایبری و مراحل پیش‌بینی، حفاظت، شناسایی و مدیریت حوادث، به‌ویژه در زمینه زیرساخت‌های عملیاتی، شکل گرفته‌اند و به شناسایی الگوهای تهدید و روش‌های مقابله با آن‌ها کمک کرده‌اند [۳۴]. همچنین، پذیرش فناوری‌های نوین مانند هوش مصنوعی و یادگیری ماشین در امنیت سایبری برای شناسایی تهدیدات و تجزیه و تحلیل رفتار سامانه‌ها در حال افزایش است [۳۵]. نهایتاً، تحقیقات بر اهمیت آموزش و آگاهی‌سازی کارکنان تأکید دارند، زیرا بسیاری از حملات سایبری به دلیل خطاهای انسانی رخ می‌دهند و افزایش آگاهی در این زمینه می‌تواند به کاهش این خطرات کمک کند [۳۶]. این پیشینه پژوهشی، غنای شیوه‌های ایمن‌سازی زیرساخت‌های حیاتی و توسعه روش‌های نوین در این حوزه را نشان می‌دهد و به‌طور مستمر در حال گسترش و به‌روزرسانی است.

همچنین، تحقیقات اخیر به بررسی همکاری‌های بین‌سازمانی و تبادل اطلاعات در زمینه تهدیدات سایبری پرداخته‌اند. به‌ویژه در سطح ملی و بین‌المللی، ایجاد پلتفرم‌ها و شبکه‌های همکاری برای اشتراک‌گذاری تهدیدات و بهترین شیوه‌ها، به سازمان‌ها کمک می‌کند تا به طور مؤثرتری در برابر حملات سایبری واکنش نشان دهند. این رویکرد تعاملی می‌تواند به شناسایی زودهنگام الگوهای حملات و افزایش آمادگی در سطح زیرساخت‌های حیاتی منجر شود [۳۷]. علاوه بر این، استفاده از مدل‌سازی ریاضی و شبیه‌سازی برای پیش‌بینی سناریوهای حمله و ارزیابی تأثیر آن‌ها بر سامانه‌های عملیاتی، به عنوان ابزاری مؤثر در تعیین نقاط ضعف و توسعه استراتژی‌های دفاعی مطرح شده است [۳۸]. این مدل‌ها می‌توانند به مدیران سازمان‌ها در اتخاذ تصمیمات استراتژیک و تخصیص منابع مناسب برای تقویت امنیت سایبری کمک کنند.

در ادامه، توجه به عزم دولت‌ها و نهادهای مسئول نیز اهمیت ویژه‌ای دارد. بسیاری از دولت‌ها طی سال‌های اخیر اقداماتی برای تقویت امنیت سایبری زیرساخت‌های حیاتی خود انجام داده‌اند. این اقدامات شامل تدوین سیاست‌ها و استراتژی‌های جامع، تشکیل تیم‌های واکنش به حوادث سایبری و تهیه دستورالعمل‌های امنیتی است. در برخی کشورها، مانند ایالات متحده و اتحادیه اروپا، برنامه‌های آموزشی و تخصصی برای پرسنل IT و امنیت سایبری طراحی شده است تا بهبود مهارت‌ها و دانش فنی آنها را تضمین کند [۳۹].

در عین حال، پژوهشگران به بررسی تأثیرات اجتماعی و اقتصادی حملات سایبری نیز پرداخته‌اند. تحقیقات نشان می‌دهد که حملات سایبری می‌توانند منجر به خسارات مالی هنگفت، اختلال در خدمات عمومی و از بین رفتن اعتماد عمومی به سامانه‌ها و نهادهای دولتی شوند [۴۰ و ۴۱]. بنابراین، بررسی ابعاد اقتصادی امن‌سازی زیرساخت‌ها و ارزیابی سرمایه‌گذاری‌های لازم در این حوزه به‌منظور حداکثر کردن بازده مالی و اجتماعی، از جمله موارد مهمی است که نیاز به توجه دارد. علاوه بر این، چالش‌هایی مانند هک‌های مبتنی بر هوش مصنوعی و تهدیدهای ناشی از فناوری‌های نوین مانند بلاک‌چین و سامانه‌های توزیع‌شده، نیازمند رویکردهای جدید و نوآورانه در امنیت سایبری هستند. این فناوری‌ها می‌توانند هم به عنوان ابزارهایی برای تقویت امنیت و هم به عنوان کانال‌هایی برای ایجاد تهدیدات جدید عمل کنند [۴۲].

همچنین، در مواجهه با تهدیدات سایبری که به صورت روزافزونی پیچیده‌تر و هوشمندتر می‌شوند، نیاز به ظرفیت‌سازی در سطح فردی و سازمانی برای شناسایی و پاسخ به این تهدیدات بیش از پیش احساس می‌شود. ایجاد فرهنگ امنیت سایبری در

[1] Operational Technology
[2] Supervisory Control and Data Acquisition
[3] Stuxnet

سازمان‌ها، شامل آموزش‌های مستمر به کارکنان و شناسایی قابلیت‌های بالقوه در مبارزه با تهدیدات، می‌تواند به طور قابل توجهی از وقوع حملات جلوگیری کند [۴۳].

در نهایت، فردای حملات سایبری و اقدامات امنیتی به طور فزاینده‌ای در حال تغییر است و تکنیک‌های جدیدی مانند تحلیل داده‌های بزرگ[1]، یادگیری عمیق[2] و فناوری‌های بلاک‌چین برای شناسایی و پیشگیری از تهدیدات به کار گرفته می‌شوند. استفاده از این فناوری‌ها امکان تحلیل رفتاری مخاطرات و پیش‌بینی الگوهای حمله را فراهم می‌کند و به سازمان‌ها در تصمیم‌گیری‌های آگاهانه‌تر کمک می‌کند [۴۴-۴۷].

در نهایت، با توجه به اینکه امنیت سایبری به یک دغدغه جهانی تبدیل شده است، توجه به نوآوری‌های فناوری و به‌کارگیری شیوه‌های کارآمد برای مقابله با تهدیدات آینده، ضروری به نظر می‌رسد. این رویکردهای جدید می‌توانند به خلق مدل‌های پیشرفته‌تر و کارآمدتر در مدیریت تهدیدات سایبری منجر شده و در نهایت استحکام و تاب‌آوری زیرساخت‌های حیاتی را در برابر حملات سایبری افزایش دهند.

۳- روش تحقیق

در این بخش، به بررسی روش‌های هوش مصنوعی مبتنی بر قواعد چند جنبه‌ای برای مدل‌سازی امنیت سایبری در زیرساخت‌های حیاتی[3] پرداخته و با استفاده از شکل (۱)، یک طبقه‌بندی جامع ارائه شده است. این روش‌ها به سه دسته کلی تقسیم می‌شوند[۴۸]: (الف) رویکرد دانش‌محور که بر پایه‌ی تخصص و دانش فنی در زمینه امنیت سایبری استوار است و به تحلیل متون و داده‌های مرتبط با تهدیدات می‌پردازد [۴۸]؛ (ب) رویکرد مبتنی بر داده که از الگوهای داده‌ای و یادگیری ماشین برای شناسایی و پیشگیری از تهدیدات استفاده می‌کند[۴۹ و ۵۰]؛ (ج) رویکرد ترکیبی که از هر دو روش قبلی بهره می‌برد تا مزایای هر یک را به حداکثر برساند و به یک مدل جامع و مقاوم در برابر تهدیدات سایبری دست یابد [۵۱]؛ و (د) رویکرد تصمیم گیری مبتنی بر منطق فازی، معادلات (۱-۹). در ادامه، به تحلیل دقیق‌تر این سه رویکرد پرداخته شده است. رویکرد دانش‌محور معمولاً شامل استفاده از قواعد منطقی و مدل‌های تجربی است که بر مبنای دانش و تخصص‌های موجود شکل گرفته‌اند و به شناسایی و مدیریت تهدیدات امنیتی کمک می‌کنند. از سوی دیگر، رویکرد مبتنی بر داده با بهره‌گیری از فن‌آوری‌های نوین مانند یادگیری ماشین، بر روی تحلیل داده‌های بزرگ و شناسایی الگوهای غیرطبیعی متمرکز است که می‌تواند به شناسایی حملات سایبری جدید و پیچیده کمک کند. نهایتاً، رویکرد ترکیبی با ترکیب اینسایتس[4] به دست آمده از هر دو رویکرد، سعی دارد یک سامانه امنیتی قدرتمندتر و تطبیق‌پذیرتر ارائه دهد که بتواند به سرعت به تغییرات در زمینه تهدیدات واکنش نشان دهد و نیازهای متنوع امنیتی زیرساخت‌های حیاتی را برآورده کند.

$$xa_{ij}^{n} = \left(a_{ij}^{n} - minc_{ij}^{n}\right)/\Delta_{min}^{max} \quad (۱)$$

$$xb_{ij}^{n} = \left(b_{ij}^{n} - minc_{ij}^{n}\right)/\Delta_{min}^{max} \quad (۲)$$

$$xc_{ij}^{n} = \left(c_{ij}^{n} - minc_{ij}^{n}\right)/\Delta_{min}^{max} \quad (۳)$$

$$Where\ \Delta_{min}^{max} = \left(maxa_{ij}^{n} - minc_{ij}^{n}\right) \quad (۴)$$

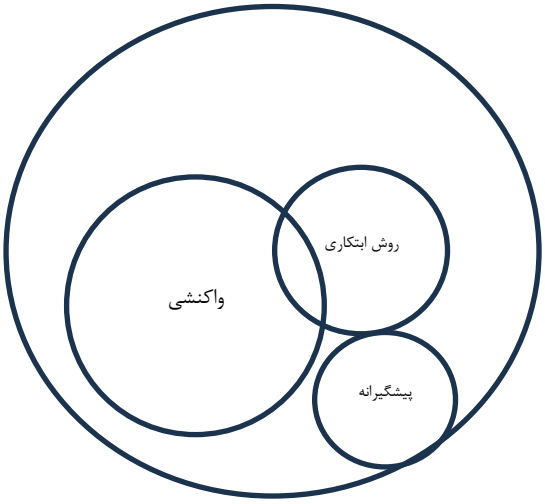
$$xas_{ij}^{n} = xa_{ij}^{n}/\left(1 + xa_{ij}^{n} - xb_{ij}^{n}\right) \quad (۵)$$

$$xcs_{ij}^{n} = xb_{ij}^{n}/\left(1 + xb_{ij}^{n} - xc_{ij}^{n}\right) \quad (۶)$$

$$x_{ij}^{n} = \left[xcs_{ij}^{n}\left(1 - xcs_{ij}^{n}\right) + xas_{ij}^{n}\ X\ xas_{ij}^{n}\right] / \left[1 - xcs_{ij}^{n} + xas_{ij}^{n}\right] \quad (۷)$$

$$u_{ij}^{n} = minc_{ij}^{n} + x_{ij}^{n}\ X\ \Delta_{min}^{max} \quad (۸)$$

$$u_{ij} = 1/p\left(u_{ij}^{1} + u_{ij}^{2} + \cdots + u_{ij}^{p}\right) \quad (۹)$$



شکل (۱): حالت‌های دفاع سایبری [۴۸].

۴- تجزیه و تحلیل یافته‌ها

۴-۱- رویکرد دانش محور

برای تدوین قوانین مؤثر در مدل‌سازی امنیت سایبری، ضروری است که فرآیند توسعه این قوانین به‌طور مداوم با تغییرات فناوری و

[1] Big Data
[2] Deep Learning
[3] Critical Infrastructure
[4] Insights

تهدیدات نوظهور به‌روز شود، به طوری که نه تنها از دانش و تجربیات کارشناسان بهره‌برداری کند، بلکه به‌طور فعال به نظرات و بازخوردهای کاربرانی که در دامنه‌های مختلف مشغول به کار هستند نیز توجه داشته باشد. این رویکرد فراگیر، قابلیت انطباق و اثربخشی قوانین امنیتی را افزایش می‌دهد و در نهایت به حفاظت بهتر از سامانه‌های اطلاعاتی در برابر حملات سایبری کمک می‌کند [۵۲].

۴-۱-۱- تخصص انسانی

برای مقابله با چالش‌های ناشی از تغییرات مداوم و ویژگی‌های متنوع تهدیدات امنیت سایبری، لازم است که قوانین و الگوهای شناسایی به‌طور مرتب به‌روزرسانی شوند، زیرا به‌روز نبودن این قوانین می‌تواند منجر به ناتوانی در شناسایی تهدیدات جدید و پیچیده گردد. بر اساس تحقیقات کلک و همکاران [۵۳]، استفاده از ترکیب هوش مصنوعی و یادگیری ماشین در فرآیند شناسایی تهدیدات می‌تواند به‌طور چشمگیری قابلیت‌های تشخیصی را ارتقا بخشد و نیاز به به‌روزرسانی‌های دستی را کاهش دهد، اما برای تحقق این امر، همچنان لازم است که دانش کارشناسان انسانی در ترسیم و ارائه الگوهای کارآمد به‌طور ترکیبی به کار رود. به‌این‌ترتیب، یک رویکرد جامع و پویا که شامل تعامل اطلاعاتی بین سامانه‌های هوش مصنوعی و تخصص انسانی است، می‌تواند به بهبود امنیت سایبری کمک شایانی کند و سازگاری با تهدیدات رو به رشد را تضمین نماید [۵۴].

۴-۱-۲- دانش بازنمایی

استفاده از تکنیک‌های بازنمایی دانش رسمی در مدل‌سازی امنیت سایبری، امکان جمع‌آوری و بیان دانشی تخصصی را فراهم می‌آورد که به عنوان مبنای ایجاد قوانین برای سامانه‌های امنیت سایبری به کار می‌رود. این روش‌ها بر ساختاردهی و تفسیر دانش تمرکز دارند و به این ترتیب تدوین قوانین مطابق با تخصص‌های حوزه را تسهیل می‌کنند. در نتیجه، این تکنیک‌ها به دقت و کارایی بیشتر در مدیریت امنیت سایبری و انطباق قوانین کمک می‌کنند [۱۲].

• تولید قوانین مبتنی بر هستی شناسی:

تولید قوانین مبتنی بر هستی‌شناسی در امنیت سایبری، امکان شناسایی و تعریف موجودیت‌ها، تهدیدها، آسیب‌پذیری‌ها، الگوهای حمله و مکانیسم‌های دفاعی خاص یک حوزه را فراهم می‌آورد. به عنوان مثال، سید و همکاران یک هستی‌شناسی آسیب‌پذیری امنیت سایبری[1] را برای مدیریت آسیب‌پذیری‌ها معرفی کرده‌اند که هم‌چنین می‌تواند به ادغام داده‌ها از منابع ساختاریافته و بدون ساختار کمک کند. با توجه به روابط و محدودیت‌های تعریف‌شده در این هستی‌شناسی‌ها، قوانین امنیت سایبری می‌توانند تولید شوند که قابلیت‌های استدلالی و تصمیم‌گیری را بهبود می‌بخشند [۵۵].

• تولید قواعد مبتنی بر نمودار دانش:

نمودارهای دانش در حوزه امنیت سایبری به عنوان ابزاری کارآمد برای سازمان‌دهی و تجزیه و تحلیل اطلاعات پیچیده عمل می‌کنند و می‌توانند روابط متعدد و وابستگی‌های موجود بین عناصر مختلف مانند دارایی‌ها، تهدیدات و آسیب‌پذیری‌ها را به صورت بصری و ساختاریافته نمایش دهند. به طور مثال، با استفاده از یک چارچوب مبتنی بر نمودار، پژوهشگران می‌توانند به کشف الگوهای جدید و روابط ناشناخته میان داده‌ها بپردازند که در نتیجه آن، قابلیت‌های پیش‌بینی و تصمیم‌گیری به شکل چشمگیری افزایش می‌یابد. این رویکرد نه تنها شفافیت بیشتری در تحلیل داده‌های امنیت سایبری ایجاد می‌کند، بلکه توانایی درک عمیق‌تری از دینامیک و ساختار پیچیده تهدیدات سایبری را نیز فراهم می‌سازد، که به بهبود استراتژی‌ها و شیوه‌های مقابله با این تهدیدات منجر می‌شود. در نتیجه، ترکیب نمودارهای دانش با تکنیک‌های یادگیری ماشین می‌تواند به توسعه راهکارهایی منجر شود که به طور پویا به تغییرات محیطی و تهدیدات جدید پاسخ دهند [۵۶].

۴-۲- رویکرد داده محور

یک رویکرد مبتنی بر داده برای امنیت سایبری بر این اصل استوار است که می‌توان از طریق تجزیه و تحلیل دقیق داده‌های موجود، الگوهای مشهود و ناشناخته را شناسایی و قوانین کاربردی خلق کرد. این رویکرد به جای تکیه بر دانش قبلی یا چارچوب‌های نظری، از تکنیک‌های پیشرفته الگوریتمی استفاده می‌کند تا به صورت خودکار به استخراج اطلاعات ارزشمند از داده‌ها بپردازد. در این راستا، می‌توان به بررسی روش‌های نوآورانه‌ای پرداخت که قادر به شناسایی تهدیدات و نقاط ضعف در سامانه‌های اطلاعاتی هستند و در نهایت، راهکارها و قواعد موثری را برای تقویت سامانه‌های امنیت سایبری ارائه دهند [۱۲ و ۵۷].

۴-۲-۱- یادگیری ماشین

با استفاده از روش‌های یادگیری ماشین، می‌توان به‌صورت خودکار

[1] Cyber Vulnerability Opportunity

الگوهای پیچیده، همبستگی‌ها و قوانین را از داده‌ها استخراج کرد. این رویکرد به ویژه در زمینه‌هایی که تدوین دستی قوانین به دلیل میزان و پیچیدگی داده‌ها دشوار و زمان‌بر است، بسیار مؤثر به نظر می‌رسد. برای نمونه، در مجموعه‌های بزرگ و پیچیده داده‌های زیرساخت‌های حیاتی، یادگیری ماشین می‌تواند به شناسایی الگوهای ناواضح و استخراج بینش‌هایی منجر شود که به تصمیم‌گیری آگاهانه‌تر و بهینه‌تر کمک می‌کند و نیاز به دخالت انسانی را به حداقل می‌رساند [۵۸]. به عنوان مثال:

• یادگیری قوانین انجمنی: یادگیری قوانین انجمنی یکی از تکنیک‌های موثر در شناسایی ارتباطات و وابستگی‌های کلیدی میان رویدادها و ویژگی‌های مختلف است. در حوزه امنیت سایبری، این نوع تجزیه و تحلیل می‌تواند به شناسایی زنجیره‌های حمله و بررسی همبستگی‌ها کمک شایانی کند. به عنوان مثال، الگوریتمی مانند آپریوری[1] می‌تواند به بررسی ترافیک شبکه، گزارش‌ها و داده‌های رویداد سامانه بپردازد تا الگوهای رفتاری مشکوک یا اقداماتی که ممکن است به نقض‌های امنیتی منجر شوند، شناسایی کند. دیگر روش‌ها مانند اف پی گروث[2]، اکلات[3] و آر ای آر اِم[4] نیز می‌توانند در استخراج قوانین مهم از داده‌ها به کار گرفته شوند. هرچند این تکنیک‌ها قادر به تولید قواعد زیادی هستند، اما ممکن است به تداخل و دشواری در تصمیم‌گیری نیز منجر شوند. با بهره‌گیری از تحلیل‌های انجمنی، سازمان‌ها می‌توانند به درک عمیق‌تری از تهدیدات امنیتی و زنجیره‌های حمله دست یابند و ریشه‌های حوادث را بهتر شناسایی کنند، که در نهایت موجب تقویت مدل‌های امنیتی آن‌ها خواهد شد [۵۹].

• یادگیری قوانین متوالی: استخراج قوانین متوالی در امنیت سایبری به شناسایی سناریوهای حمله پیچیده کمک می‌کند که شامل یک دنباله از رویدادها در طول زمان می‌شود. این روش تمرکز خود را بر روی درک توالی زمانی وقوع رویدادها قرار می‌دهد تا الگوهای پنهانی را کشف کند که ممکن است در روش‌های تحلیل مرسوم ناپیدا بمانند. به عنوان نمونه، به گفته اونیشچنکو [۶۰] یک مطالعه از هوساک و همکارانش به بررسی یک رویکرد قانون‌کاوی متوالی برای پیش‌بینی آگاهی موقعیتی سایبری و ارائه فهرست سیاه شخصی‌سازی شده پرداخته است. همچنین، کیم و همکارانش از استخراج قوانین متوالی در مدل پیش‌بینی مبتنی بر نمودار حمله استفاده کردند تا به درک بهتری از ترتیب وقوع رویدادها دست یابند و این ترتیب را در تحلیل‌های خود لحاظ کنند. این رویکردها بر اهمیت تجزیه و تحلیل توالی رویدادها در ارائه بینش‌های عمیق‌تر درباره تهدیدات سایبری تأکید می‌کنند.

• یادگیری قوانین طبقه بندی: سامانه‌های یادگیری نظارت شده مانند درخت‌های تصمیم و جنگل‌های تصادفی در حوزه امنیت سایبری به شناسایی و تمیز دادن رفتارهای عادی از مشکوک کمک می‌کنند. این الگوریتم‌ها می‌توانند با تجزیه و تحلیل الگوهای ترافیک شبکه و فعالیت‌های کاربر، ناهنجاری‌های احتمالی را به سرعت شناسایی کنند و از این طریق به پیشگیری از تهدیدات کمک کنند. الگوریتم‌هایی مانند جنگل‌های تصادفی با یادگیری از داده‌های تاریخی و تشخیص الگوهای غیرمعمول، به کارشناسان امنیتی توانایی پیش‌بینی و شناسایی حملات در مراحل اولیه را می‌دهند. این سامانه‌ها همچنین قابلیت به‌روزرسانی مداوم برای تطبیق با تغییرات جدید را دارند، که در دنیای پر مخاطره امنیت سایبری ضروری است. نهایتاً، ترکیب این تکنیک‌ها با مدیریت ریسک می‌تواند به بهبود امنیت سامانه‌ها و حفاظت از اطلاعات حساس کمک کند [۶۱].

• یادگیری قوانین مبتنی بر خوشه: خوشه‌بندی به‌عنوان یک روش تحلیل داده در حوزه امنیت سایبری به شناسایی تهدیدات و الگوهای غیرعادی کمک شایانی می‌کند. این تکنیک می‌تواند با شناسایی الگوهای مشترک در داده‌ها، به کارشناسان امنیتی کمک کند تا تهدیدات نوظهور را شناسایی کنند و به تجزیه و تحلیل رفتارهای مرتبط بپردازند. با استفاده از رویکردهایی نظیر کی-مدویدز[5]، می‌توان حملات سایبری را در سامانه‌ها و شبکه‌ها طبقه‌بندی کرده و نتایج جامع‌تری به دست آورد که برای پیش‌بینی و مقابله با تهدیدات بعدی مفید است. علاوه بر این، خوشه‌بندی می‌تواند به انتخاب ویژگی‌های کلیدی برای تمرکز روی داده‌های مهم کمک کند و به طور کلی به بهبود تصمیم‌گیری در مورد اقدامات امنیتی موثر منجر شود. با این حال، لازم است بر روی جنبه‌های مرتبط با مقیاس‌پذیری و تفسیر نتایج نیز توجه ویژه‌ای صورت گیرد تا اطمینان حاصل شود که رویکردهای مورد استفاده هم‌راستا با نیازهای دنیای واقعی هستند [۶۲].

• یادگیری قوانین مبتنی بر ناهنجاری: ناهنجاری‌ها به رفتارهایی اشاره دارند که از الگوهای عادی و متعارف منحرف می‌شوند و

[1] Apriori
[2] FP-Growth
[3] Eclat
[4] RARM
[5] K-means

می‌توانند نشانه‌ای از تهدیدات یا مشکلات در سامانه‌ها باشند. برای نمونه، شناسایی ایمیل‌های هرزنامه یا ترافیک غیرمعمول شبکه می‌تواند نشان‌دهنده دسترسی غیرمجاز یا حملات سایبری باشد. برای شناسایی این ناهنجاری‌ها، می‌توان از الگوریتم‌های یادگیری ماشین و روش‌های آماری استفاده کرد، مانند الگوریتم‌های ماشین بردار پشتیبان[1] و جنگل‌های تصادفی[2]. این ابزارها به سامانه‌های امنیتی این امکان را می‌دهند که به طور فعال به فعالیت‌های مشکوک واکنش نشان دهند و الگوهای غیرعادی را تحلیل کنند، به طوری که با یادگیری قوانین خاص، شناسایی نفوذها و تهدیدات احتمالی تسهیل شود [۶۳].

۴-۲-۲- مهندسی ویژگی

یکی از مؤلفه‌های کلیدی استخراج قوانین، مهندسی ویژگی است [۶۴] که می‌توان آن را به دو دسته کلی تقسیم کرد: (۱) استخراج مبتنی بر ویژگی دست ساز، و (ب) استخراج مبتنی بر ویژگی علم داده که در زیر مورد بحث قرار می‌گیرد:

• استخراج مبتنی بر ویژگی دست ساز: در فرآیند تحلیل خطرات امنیتی، بسیاری از ویژگی‌ها و پارامترها بر اساس تجربه انسانی و دانش تخصصی تحلیلگران تعیین می‌شوند. این متخصصان با توجه به درک عمیق خود از خبیث‌ترین تهدیدات و روش‌های حمله، قادر به انتخاب و طراحی ویژگی‌های کارآمد هستند. با این حال، این روش دستی می‌تواند زمان‌بر بوده و در مقیاس‌های بزرگ، به ویژه در هنگام پردازش داده‌های متغیر، به چالش‌های قابل توجهی بینجامد. این عدم توانایی در تولید ویژگی‌ها به‌طور خودکار می‌تواند نیز باعث بروز سوگیری‌هایی در نتایج تحلیل شود یا اطلاعات مهمی را از دست بدهد. بنابراین، بهره‌گیری از ابزارها و روش‌های علمی داده‌کاوی و یادگیری ماشین می‌تواند به بهبود این فرآیند کمک کند و قابلیت مقیاس‌پذیری و دقت تحلیل‌ها را افزایش دهد [۶۵].

• استخراج مبتنی بر ویژگی علم داده: روش‌های مدرن در تحلیل داده‌ها توانایی استخراج ویژگی‌های کلیدی را به صورت خودکار از داده‌های خام دارند، که این ویژگی به ویژه در مواجهه با حجم بالای داده‌های پیچیده اهمیت دارد. این فرآیند به طور مداوم ویژگی‌های مرتبط را شناسایی و توسعه می‌دهد، همچنین شامل مراحل تبدیل داده‌ها به فرمت‌های قابل استفاده و ادغام درک تخصصی از حوزه‌های مربوطه است. این رویکرد پویا، منجر به شناسایی و تجسم الگوهای بنیادین در داده‌ها می‌شود که می‌تواند به تصمیم‌گیری‌های آگاهانه‌تر و کارآمدتر کمک کند. در نتیجه، این سامانه‌ها به طور مداوم در حال بهبود و به‌روزرسانی هستند، که کارایی و دقت تحلیل‌ها را افزایش می‌دهد [۶۶].

انتخاب ویژگی یکی از مراحل حیاتی در مدل‌سازی داده‌ها به شمار می‌آید، به‌ویژه در سناریوهایی که با داده‌های با ابعاد بالا سروکار داریم. در این شرایط، وجود ویژگی‌های نامناسب می‌تواند نه‌تنها دقت پیش‌بینی مدل را تحت تأثیر قرار دهد بلکه باعث پیچیدگی بیشتر مدل و نیاز به زمان طولانی‌تری برای آموزش می‌شود. به این ترتیب، متخصصان می‌توانند از تکنیک‌های مختلفی برای کاهش تعداد ویژگی‌ها استفاده کنند، از جمله استفاده از نظر کارشناسان حوزه یا بهره‌گیری از الگوریتم‌های خاص مانند حذف تدریجی ویژگی‌ها، خوشه‌بندی یا روش‌های آماری نظیر تحلیل همبستگی. برای نمونه، در یک تحقیق مشخص، یک گروه از پژوهشگران توانستند با بهره‌گیری از متدهای مبتنی بر همبستگی، سامانه تشخیص نفوذی طراحی کنند که نه تنها کارایی آن را افزایش داد بلکه توانست میزان فالس پازیتیو[3] را نیز کاهش دهد. این نوع انتخاب ویژگی نه‌تنها به بهبود عملکرد سامانه‌های امنیتی کمک می‌کند، بلکه به تصمیم‌گیری‌های سریع‌تر و دقیق‌تر نیز منجر می‌شود [۶۷].

در بسیاری از سناریوهای واقعی، ویژگی‌های اولیه موجود به تنهایی برای ساخت مدل‌های پیش‌بینی قوی کافی نیستند. در این مواقع، نیاز به تولید ویژگی‌های جدید از دل ویژگی‌های موجود احساس می‌شود که می‌تواند به بهبود نمایش داده‌ها و کارایی مدل‌های تحلیلی کمک کند. این فرآیند می‌تواند شامل مجموعه‌ای از تکنیک‌ها باشد، به‌عنوان مثال، استفاده از محاسبات ریاضی برای تجمیع اطلاعات، استخراج ویژگی‌های مخصوص به یک حوزه خاص، و یا به‌کارگیری روش‌های پیش‌پردازش داده‌ها مانند خوشه‌بندی، با توجه به نوع داده‌ها [۶۷]. به‌عنوان نمونه، در تحقیقات اخیر، استفاده از تکنیک‌های خوشه‌بندی به شناسایی ویژگی‌های نماینده‌ای انجامیده که به عنوان ابزارهایی قوی در تشخیص نفوذ عمل می‌کنند. همچنین، تجزیه و تحلیل مؤلفه‌های اصلی[4] با کاهش ابعاد مجموعه داده‌ها و حفظ اطلاعات کلیدی، می‌تواند به حل مسائل پیچیده کمک شایانی کند. به عنوان مثال، در یک مطالعه مشخص، ویژگی‌های جدید برای شناسایی ناهنجاری‌ها با استفاده از تحلیل

[1] Support Vector Machine
[2] Random Forest
[3] False positive
[4] Principal Component Analysis

مؤلفه‌های اصلی استخراج شد که اثربخشی روش‌های تشخیصی را به طور قابل توجهی افزایش داد. این چنین ابتکاراتی نه تنها دقت مدل‌ها را بالا می‌برد، بلکه منجر به کارایی بیشتر در تجزیه و تحلیل داده‌ها می‌شود [۶۸].

گسسته‌سازی یکی از روش‌های کلیدی در پیش‌پردازش داده‌هاست که به‌خصوص در زمینه تجزیه و تحلیل داده‌های پیچیده کاربرد فراوانی دارد. این فرآیند به تبدیل ویژگی‌های پیوسته به دسته‌های مشخص و مجزا می‌پردازد، که می‌تواند به سادگی استخراج قوانین و همچنین بهبود قابلیت تفسیر آن‌ها کمک کند. روش‌های مختلفی برای گسسته‌سازی وجود دارد، از جمله روش‌های ایستا و پویا، نظارت‌شده و بدون نظارت، و همچنین استراتژی‌های تقسیم و ادغام [۶۹]. برای نمونه، بررسی‌های اخیر نشان داده است که از تفکیک‌کننده‌های بدون نظارت مانند ای اف بی[1] و ای دبلیو بی[2] و نیز تفکیک‌کننده‌های نظارت شده‌ای مانند ام دی ال پی[3] و چی مرج[4] می‌توان در مطالعات یادگیری ماشین بهره گرفت [۱۲]. همچنین، پژوهشگران دیگر به نتایج مثبتی در زمینه امنیت مدل‌های یادگیری ماشین در برابر حملات خصمانه با استفاده از روش‌های گسسته‌سازی دست یافته‌اند. این نوع رویکردها با ایجاد یک ساختار منسجم و ساده در داده‌ها، نه تنها به بهبود دقت مدل‌ها کمک می‌کند، بلکه فهم و تفسیر نتایج را نیز تسهیل می‌نماید [۷۰-۷۲].

یکپارچه‌سازی دانش تخصصی در فرآیند مهندسی ویژگی می‌تواند به بهبود درک مسائل دنیای واقعی و دستیابی به نتایج دقیق‌تر کمک کند. برای مثال، در حوزه‌های حساس مانند امنیت سایبری، ادغام دانش تخصصی می‌تواند تأثیر بسزایی در شناسایی و جلوگیری از تهدیدات و آسیب‌های اطلاعاتی داشته باشد. کارشناسان در این زمینه می‌توانند بینش‌ها و مشاوره‌های کلیدی در مورد ویژگی‌های مهم، الگوهای پنهان و تغییرات لازم برای بهینه‌سازی مدل‌ها را ارائه دهند. این مشارکت می‌تواند به ایجاد ویژگی‌های بهینه‌تری منجر شود که با نیازمندی‌ها و چالش‌های خاص یک پروژه مرتبط باشد. به همین ترتیب، هنگامی که مهندسان ویژگی از چنین دانشی بهره‌مند می‌شوند، می‌توانند به استخراج قوانین و الگوهای معنادار از داده‌ها به روشی کارآمدتر و مؤثرتر دست یابند. یعین، همکاری بین فناوری و تخصص انسانی می‌تواند ارزش‌های افزوده قابل توجهی در فرآیندهای تحلیل داده ایجاد کند [۷۳].

به طور کلی، فرآیند مهندسی ویژگی می‌تواند به‌طرز چشمگیری بر افزایش کارایی مدل‌های یادگیری ماشین و شفافیت نتایج اثرگذار باشد. با شناسایی و ایجاد ویژگی‌هایی که به‌طور خاص با داده‌های امنیت سایبری سازگار هستند، می‌توان به استخراج قوانین عملی از داده‌های خام امنیتی پرداخت. این پروسه نه‌تنها دقت مدل‌ها را بالا می‌برد، بلکه باعث بهبود فهم و قابلیت تعمیم آن‌ها نیز می‌شود. در سناریوهای واقعی، استفاده از ترکیب دانش انسانی و تحلیل داده می‌تواند نتایج بهتری به همراه داشته باشد. با این حال، باید به چالش‌های موجود مانند نیاز به منابع بالا، خطرات ناشی از برازش بیش از حد، و حساسیت به کیفیت داده‌ها توجه ویژه‌ای شود. این مسائل می‌توانند بر خروجی نهایی تأثیرگذار باشند و نیازمند توجه و مدیریت دقیق هستند تا از حداکثر پتانسیل مهندسی ویژگی بهره‌برداری شود.

۴-۲-۳- استخراج قوانین مبتنی بر عدم قطعیت

در فرآیند مدل‌سازی مبتنی بر قانون، توجه به معیارهای عدم قطعیت و اطلاعات احتمالاً می‌تواند تأثیر قابل‌توجهی بر کیفیت پیش‌بینی‌ها داشته باشد. به همین منظور، هدف ما ارزیابی و اندازه‌گیری سطوح مختلفی از عدم قطعیت در مدل‌های گوناگون است که در ادامه به بررسی آن‌ها خواهیم پرداخت. این ارزیابی از طریق تحلیل جنبه‌های مختلف مدل‌ها، شامل پارامترهای ورودی، ساختار قوانین و نحوه تعامل آن‌ها با داده‌های دریافتی انجام می‌شود. با این کار، می‌توانیم درک بهتری از عوامل تأثیرگذار بر عدم قطعیت ایجاد کنیم و روش‌های ممکن برای بهبود دقت پیش‌بینی‌ها را شناسایی نماییم. در نهایت، این تحلیل می‌تواند به بهینه‌سازی مدل‌ها و افزایش قابلیت اطمینان نتایج منجر شود [۷۴].

• قواعد کاوی احتمالی: به جای استفاده از قوانین قطعی، تکنیک‌های مبتنی بر قواعد کاوی احتمالی به ما این امکان را می‌دهند که در کنار شناسایی الگوها، به قوانین امتیاز اطمینان و احتمالات نیز اختصاص دهیم. این رویکرد به ما اجازه می‌دهد تا به جای یک نتیجه ثابت، میزان اطمینان هر قانون را مشخص کنیم. به عنوان نمونه، پژوهشگران مانند هوساک و همکارانش از این نوع امتیازات برای توسعه قوانین تسلسلی به منظور پیش‌بینی وضعیت‌های امنیتی سایبری بهره برده‌اند. این روش‌ها می‌توانند احتمال صحت یک قانون خاص یا دقت پیش‌بینی‌های ناشی از آن را

[1] EFB
[2] EWB
[3] MDLP
[4] ChiMerge

نشان دهند، که از این طریق می‌توان تصمیم‌گیری‌های بهتری انجام داد. یکی از ابزارهای رایج در این زمینه، شبکه‌های بیزی است که به تحلیل و استنتاج احتمال با استفاده از روابط پیچیده میان متغیرها کمک می‌کند. همچنین، تحقیقات اخیر که توسط ژانگ و همکاران انجام شده، نشان‌دهنده ترکیب مدل‌های مختلف برای پیش‌بینی حوادث و ارزیابی ریسک در سامانه‌های کنترلی صنعتی است. در حالی که این رویکردها قدرت کمیابی برای مدیریت عدم قطعیت و ارزیابی ریسک دارند، باید به چالش‌های مرتبط با پیچیدگی مدل‌ها و نیازهای داده‌ها نیز توجه کرد تا حداکثر کارایی آن‌ها تضمین شود [۷۵].

• کاوی قواعد فازی: منطق فازی به ما این امکان را می‌دهد که فراتر از قوانین سخت و صریح، درجات مختلفی از وابستگی را در مدل‌سازی امنیت سایبری لحاظ کنیم. این رویکرد، از طریق روش‌هایی همچون درخت‌های تصمیم فازی و استخراج قوانین انجمن فازی، به ما اجازه می‌دهد تا عدم قطعیت موجود در داده‌ها را بهتر منتقل کنیم و مدل‌های جامع‌تری برای تحلیل رویدادهای امنیتی ایجاد کنیم. به عنوان نمونه، پژوهش‌هایی مانند کار آلالی و همکارانش، رویکردهای مبتنی بر سامانه‌های استنتاج فازی را برای ارزیابی ریسک در حوزه امنیت سایبری مطرح کرده‌اند. این نوع استخراج قوانین فازی، به دلیل قابلیت انعطاف‌پذیری بالای زبان و توانایی در بیان شرایط مبهم، ابزاری مؤثر برای مدیریت داده‌های پیچیده امنیتی به شمار می‌آید. با این حال، افزایش تعداد اصطلاحات و قوانین می‌تواند به پیچیدگی و چالش‌های جدیدی در تفسیر و نگهداری این سامانه‌ها منجر شود [۷۶]. بنابراین، پیش از پیاده‌سازی چنین رویکردهایی، توجه به مشکلات محاسباتی، مفاهیم مورد استفاده و خطرات مربوط به تفسیر نادرست ضروری است تا از بروز اشتباهات در نتیجه‌گیری‌ها جلوگیری شود.

• مبنای قانون باور: نظریه دمپستر-شفر چارچوبی قوی برای مقابله با داده‌های نامطمئن و نامشخص فراهم می‌کند و به ما این امکان را می‌دهد که با استفاده از ترکیبی از شواهد موجود تصمیمات آگاهانه‌تری بگیریم. قوانین استخراج شده از این نظریه، می‌توانند نه‌تنها بر پایه دانش تخصصی، بلکه بر اساس داده‌های تاریخی نیز بنا شوند و به مدل‌سازی امنیت سایبری یاری رسانند. به عنوان مثال، در مطالعاتی مانند کارهای اول و همکارانش، مدلی برای تشخیص ناهنجاری‌ها با استفاده از قوانین اعتقادی طراحی شده که می‌تواند عدم قطعیت در داده‌های حسگر را مدیریت کند. همچنین، تحقیقاتی نظیر آنچه توسط او و همکاران ارائه شده، به بررسی خرابی‌های موجود در شبکه‌های حسگر بی‌سیم پرداخته و روش‌هایی برای تحلیل مؤثر آنها بر اساس اصول اعتقادی به کار گرفته‌اند. این رویکرد مبتنی بر قوانین اعتقادی علاوه بر توانایی در مدیریت عدم قطعیت، قابلیت انعطاف و درهم تنیدگی در فرآیند تصمیم‌گیری را نیز فراهم می‌آورد. با این حال، افزایش تعداد متغیرها و پیچیدگی‌های موجود در این مدل‌ها می‌تواند به دشواری‌هایی در تفسیر و مدیریت صحیح آن‌ها منجر شود [۷۷]. در نتیجه، ضروری است که هنگام پیاده‌سازی سامانه‌های مبتنی بر قوانین اعتقادی با دقت به چالش‌های موجود در تفسیر، خطرات مربوط به تطابق بیش از حد و پیچیدگی‌های مدل‌ها توجه کنیم تا از بروز مشکلات جدی در فرآیند تصمیم‌گیری جلوگیری شود.

۴-۲-۴- روش‌های مبتنی بر افزایش داده‌ها

تقویت داده‌ها در حوزه امنیت سایبری نقش حیاتی را ایفا می‌کند و می‌تواند به بهبود توانایی سامانه‌ها در شناسایی تهدیدات و ناهنجاری‌ها کمک کند [۷۸]. این فرآیند شامل استفاده از تکنیک‌هایی است که نه تنها حجم داده‌های آموزشی را افزایش می‌دهند، بلکه کیفیت و تنوع آن‌ها را نیز بهبود می‌بخشند. با بهره‌گیری از روش‌های تبدیل، مانند نرمال‌سازی و همچنین ترکیب داده‌ها از منابع مختلف، می‌توان به مجموعه‌ای جامع و غنی از داده‌ها دست یافت که به تقویت مدل‌های یادگیری ماشین کمک می‌کند. به‌ویژه در شرایطی که داده‌های موجود ممکن است ناکافی یا غیر متعارف باشند، این رویکرد می‌تواند به کشف دقیق‌تر و کارآمدتر رفتارهای مشکوک در سامانه‌های امنیتی منجر شود. به عبارت دیگر، تقویت داده‌ها به کارایی بالاتر الگوریتم‌ها و تصمیم‌گیری‌های هوشمند در شناسایی و پاسخ به تهدیدات دنیای واقعی کمک می‌کند و در نهایت به ایجاد محیط‌های دیجیتال امن‌تر منتهی می‌شود [۷۹].

• تبدیل داده: تبدیل داده‌ها در حوزه‌های مختلف تحلیل می‌تواند به بهبود قابلیت‌های مدل‌های امنیت سایبری کمک شایانی کند. این فرآیند نه تنها شامل تغییر در ویژگی‌های داده‌ها است، بلکه می‌تواند بر نمونه‌های آموزشی نیز تأثیر بگذارد. در زمینه امنیت سایبری، استفاده از تکنیک‌های تبدیل داده برای افزایش کیفیت و کارایی اطلاعات بسیار مهم است. به‌عنوان مثال، با ایجاد ویژگی‌های جدید از طریق تحلیل ویژگی‌های موجود، می‌توان دیدگاه عمیق‌تری به تفاوت‌های بین رفتارهای معمول و مخرب پیدا کرد. به همین ترتیب، شبکه‌های عصبی کانولوشنال می‌توانند نقش مؤثری در

تحلیل و استخراج ویژگی‌های مرتبط داشته باشند. علاوه بر این، فضای ورودی نیز می‌تواند با بهره‌گیری از راهکارهای خاصی مانند تکنیک‌های نمونه‌برداری، به‌ویژه در شرایطی که داده‌ها نامتوازن هستند، غنی‌تر شود. به‌عنوان مثال، روش اسموت[1] می‌تواند برای تقویت داده‌ها در تحلیل فیشینگ یا تشخیص تقلب به کار رود. همچنین، استفاده از تکنیک‌های نمونه‌برداری در مطالعات مختلف، مانند تشخیص نفوذ، نشان‌دهنده پتانسیل بالای این روش‌ها در ارتقای دقت مدل‌هاست. با این حال، باید به این نکته توجه داشت که در حالی که تبدیل داده‌ها می‌تواند به ملت‌های غنی از اطلاعات منتهی شود، تبدیل‌های غیرضروری یا نادرست ممکن است به عملکرد کلی سامانه آسیب بزند و باعث کاهش دقت در نتایج نهایی شود [۷۹].

• سنتز داده ها: در سناریوهای خاص، تولید داده‌های مصنوعی می‌تواند به تقویت مدل‌های یادگیری ماشینی کمک کند، بخصوص زمانی که داده‌های واقعی محدود هستند. مدل‌های مولدی مانند شبکه‌های متخاصم تولیدی[2] و رمزگذارهای خودکار متغیر قادرند الگوهای نزدیک به داده‌های واقعی خلق کنند. به‌عنوان مثال، پژوهش‌ها نشان داده‌اند که استفاده از شبکه‌های متخاصم تولیدی در شناسایی ناهنجاری‌ها بسیار مؤثر بوده است. با این حال، باید به خطرات احتمالی ناشی از داده‌های تقویت‌شده توجه کرد؛ زیرا اگر الگوهای تولید شده به‌درستی به واقعیت‌های امنیت سایبری مرتبط نباشند، ممکن است موجب بیش‌برازش و کاهش دقت در شناسایی تهدیدهای واقعی شوند [۸۰]. استفاده از تکنیک‌های افزایش داده‌ها در زمینه قواعد کاوی به‌ویژه در امنیت سایبری یک رویکرد مؤثر برای تقویت دقت و قابلیت‌های مدل‌ها است. این روش به محققان و متخصصان امنیتی این امکان را می‌دهد که با شبیه‌سازی سناریوها و طراحی داده‌های مجازی مختلف، توانایی شناسایی تهدیدات را بهبود بخشند. ایجاد مجموعه‌های داده گسترده‌تر باعث می‌شود تا الگوها و ویژگی‌های بیشتری از رفتارهای مخرب شناسایی شود و در نتیجه قوانین کارآمدتری برای مقابله با حملات و نقایص امنیتی توسعه یابد. با این وجود، در پیاده‌سازی این تکنیک‌ها، چالش‌هایی همچون خطر بیش‌برازش، مشکلات درزمینه شفافیت مدل‌ها و مسائل مربوط به حریم خصوصی باید به دقت بررسی و مدیریت شود تا کارایی و امنیت اطلاعات حفظ گردد.

[1]SMOTE
[2]Generative Adversarial Network

۴-۲-۵- تکنیک‌های به‌روزرسانی مفهوم و قوانین

سعید و همکاران [۸۱] تغییرات سریع در محیط‌های دیجیتال می‌تواند بر کارایی مدل‌های امنیت سایبری تأثیر بگذارد و نیاز به به‌روزرسانی مداوم قوانین را به وجود می‌آورد. هنگامی که تهدیدات جدید یا تغییرات در رفتار سامانه بروز می‌کند، افزودن مکانیسم‌های هوشمند برای تعدیل و اصلاح مدل‌ها ضروری می‌شود. این روش‌ها می‌توانند شامل به‌کارگیری الگوریتم‌های یادگیری فعال باشند که به طور دینامیک و بر اساس داده‌های جدید، الگوهای مؤثر را شناسایی و قوانین امنیتی را به‌روز می‌کنند. همچنین، تجزیه و تحلیل مستمر داده‌ها برای شناسایی نقاط ضعف و تعدیل دقیق قوانین می‌تواند به کاهش تعداد هشدارهای کاذب کمک کند و دقت کلی مدل‌ها را تقویت نماید. در نهایت، بررسی منظم و انطباق سریع با وضعیت‌های جدید امنیتی، کلید حفظ کارایی و اطمینان از موفقیت مدل‌های امنیت سایبری است. در اینجا تعدادی از روش‌های مرسوم برای به‌روزرسانی قوانین در حوزه مدل‌سازی امنیت سایبری ارائه شده است:

• یادگیری افزایشی: تکنیک‌های یادگیری تدریجی نقش مهمی در توسعه مدل‌های مبتنی بر قانون ایفا می‌کنند و به این مدل‌ها این امکان را می‌دهند که بدون نیاز به آموزش کامل از ابتدا، به‌طور مؤثر با داده‌های جدید تطابق پیدا کنند. این تکنیک به مدل‌ها اجازه می‌دهد که تنها بخش‌های مرتبط را به‌روز کنند و بدین ترتیب زمان و منابع لازم برای فرآیند یادگیری را کاهش دهند. به‌عنوان نمونه، پژوهش‌ها نشان داده‌اند که استفاده از این رویکرد می‌تواند به افزایش توان مدل‌ها در شناسایی حملات در سامانه‌های پیچیده کمک کند. الگوریتم‌های یادگیری تدریجی می‌توانند تغییراتی در وزن قوانین یا آستانه‌های شناسایی تطبیق دهند تا به اطلاعات جدید واکنش نشان دهند. این انعطاف‌پذیری به مدل‌ها این امکان را می‌دهد که با سرعت بیشتری خود را با تهدیدات تازه به‌روز کنند و در نتیجه همچنان مؤثر و کاملاً مرتبط باقی بمانند [۸۲].

• تازگی داده ها و کاوی مبتنی بر تازگی: روش‌های استخراج قواعد مبتنی بر تازگی در امنیت سایبری به ایجاد قوانین کارآمدی کمک می‌کنند که بتوانند به‌سرعت به تهدیدات در حال تغییر واکنش نشان دهند. این رویکرد به داده‌های جدید اهمیت بیشتری می‌دهد و سعی دارد تا تأثیر تحولات اخیر را بر تصمیم‌گیری در مورد تهدیدات را به حداکثر برساند. به‌طور خاص، تکنیک‌هایی همچون پنجره‌های کشویی یا روش‌های تقسیم‌بندی زمانی می‌توانند در این

زمینه به کار گرفته شوند تا وزن بیشتری به داده‌های اخیر داده شود و نقش آن‌ها در شناسایی الگوهای مشکوک توضیح بیشتری یابد. این فرآیند، در کنار تضمین بروز بودن مدل، اطلاعاتی را فراهم می‌کند که می‌تواند در شناسایی حملات جدید و بهره‌برداری از رفتار کاربر حائز اهمیت باشد. با این حال، لازم به ذکر است که این روش‌ها ممکن است خطراتی را به همراه داشته باشند، از جمله خطر بیش‌برازش به داده‌های جدید و نادیده گرفتن الگوهای طولانی‌مدت که می‌تواند منجر به کاهش دقت در شناسایی تهدیدات شود [۸۳]. در نهایت، ایجاد تعادل بین استفاده از داده‌های جدید و حفظ بافت تاریخی برای موفقیت این رویکردها ضروری است.

• به‌روزرسانی‌های بازخورد محور: مدل‌های مبتنی بر قانون با بهره‌گیری از چرخه‌های بازخورد، به‌طور مستمر بهینه می‌شوند، به‌طوری‌که نظرات و پیشنهادات کاربران و کارشناسان در فرآیند یادگیری این مدل‌ها نقش بسزایی دارند. این بازخورد نه‌تنها مشخص می‌کند که کجا اشتباهات وجود دارد، بلکه نقاط قوت و ضعف مدل را نیز روشن می‌کند. بر اساس اطلاعات جمع‌آوری‌شده، می‌توان به بازنگری مقررات موجود پرداخت، به‌طوری‌که وزن بعضی از قوانین کاهش یابد یا آستانه‌های شناسایی بهینه شوند، تا دقت تصمیم‌گیری افزایش یابد. علاوه بر این، تحلیل بازخوردها می‌تواند زمینه‌ساز اضافه کردن قوانین جدیدی شود که عملکرد بهتری در شرایط خاص داشته باشند [۸۴]. چنین رویکردی نه‌تنها منجر به ارتقای کیفیت عملکرد مدل می‌شود، بلکه اعتماد به سامانه را نیز افزایش می‌دهد، زیرا کاربران شاهد بهبود مستمر و تطبیق مدل با نیازهای عملی خود خواهند بود.

به‌روزرسانی قوانین در سامانه‌های امنیت سایبری نه‌تنها به انطباق سریع‌تر با تهدیدات جدید کمک می‌کند، بلکه به بهبود کارایی و دقت تشخیص نیز منجر می‌شود. با به‌روزرسانی مداوم قوانین، این سامانه‌ها قادر به پردازش اطلاعات جدید و سازگاری با شرایط متغیر محیطی می‌شوند، که این امر به آنها قدرت می‌دهد تا عملکرد خود را در برابر حملات پیچیده تر حفظ کنند. اما برای دستیابی به این به‌روزرسانی مؤثر، نیاز است که به چالش‌هایی مانند خطرات ناشی از بیش‌برازش به داده‌های جدید و همچنین پیچیدگی فزاینده الگوریتم‌ها توجه شود. همچنین، باید منابع لازم برای نگهداری و به‌روزرسانی این قوانین در نظر گرفته شود تا از کارایی سامانه کاسته نشود. در نهایت، مدیریت این جوانب به‌منظور حفظ تعادل بین تطبیق‌پذیری و دقت، از اهمیت ویژه‌ای برخوردار است.

۴-۳- رویکرد ترکیبی

برای توسعه قوانینی مؤثر و قابل تطبیق در حوزه تشخیص تهدیدات سایبری، استفاده از رویکردهای چندگانه در شکل‌گیری این قوانین ضروری است. این فرآیند شامل ترکیبی از روش‌های مبتنی بر داده و دانش است که به غنای تحلیل و دقت تصمیم‌گیری کمک می‌کند. به‌عنوان مثال، رویکردهای داده‌محور می‌توانند با استخراج الگوها و اطلاعات معنی‌دار از مجموعه‌های بزرگ داده‌های تاریخی، به شناسایی رفتارهای مشکوک بپردازند. از سوی دیگر، روش‌های دانش‌محور که بر اساس تجربیات و تخصص کارشناسان عمل می‌کنند، می‌توانند زمینه‌های کلیدی و تهدیدات خاص را شناسایی کنند که داده‌ها به‌تنهایی قادر به شفاف‌سازی آنها نیستند. این هم‌افزایی بین داده‌های کمی و دانش کیفی، به طراحی قوانین قوی‌تری منجر می‌شود که نه‌تنها توانایی شناسایی تهدیدات فعلی را دارند، بلکه قابلیت انطباق با خطرات نوظهور را نیز خواهند داشت.

۴-۳-۱- رویکرد دانش محور

عملکرد مؤثر در زمینه امنیت سایبری نیازمند یک چارچوب جامع است که شامل ترکیب دانش و تخصص از منابع مختلف باشد. در این راستا، ابزارهایی چون هستی‌شناسی و نمودارهای دانش نقش کلیدی دارند. هستی‌شناسی به تبیین دقیق مفاهیم، روابط بین آن‌ها و ویژگی‌های هر مورد پرداخته و بدین ترتیب یک ساختار مفهومی واضح فراهم می‌آورد. به‌علاوه، نمودارهای دانش با نمایش ارتباطات عمیق و پیچیده بین موجودیت‌های مختلف، درک بهتری از نحوه تعامل تهدیدات و آسیب‌پذیری‌ها به ما می‌دهند. این روش‌شناسی جامع، به تولید قوانین مؤثرتر و مدل‌های تحلیلی دقیق‌تر کمک می‌کند که می‌توانند به سرعت به تهدیدات پیچیده و متغیر واکنش نشان دهند. در نتیجه، بهره‌گیری از تکنیک‌های دانش محور نه‌تنها دقت مدل‌ها را افزایش می‌دهد، بلکه آنها را برای درک بهتر رفتارهای تهدید نیز آماده‌تر می‌سازد.

۴-۳-۲- مجموعه داده محور

استفاده از رویکردهای متنوع مبتنی بر داده برای شکل‌گیری مجموعه‌ای جامع از قوانین مربوط به تشخیص تهدیدات سایبری، اساس کار در این حوزه را تشکیل می‌دهد. این رویکردها به ما اجازه می‌دهند تا از توانایی‌های تحلیل داده‌ها بهره‌برداری کنیم و الگوهای مهم، روابط و ناهنجاری‌ها را در میان داده‌های وسیع شناسایی کنیم. به‌عنوان نمونه، مدل‌های مبتنی بر یادگیری ماشین می‌توانند با

استفاده از روش‌های انتخاب ویژگی و تکنیک‌های پیشرفته داده‌کاوی، دقت بالایی در شناسایی خطرات ارائه دهند. علاوه بر این، به‌کارگیری روش‌هایی نظیر رأی‌گیری یا ترکیب وزنی به ما این امکان را می‌دهد که قوانین استخراج‌شده از تکنیک‌های مختلف را به‌طور مؤثر ادغام کنیم و یک چارچوب تصمیم‌گیری قوی‌تر ایجاد کنیم. با این کار، می‌توانیم به نتایج بهتری در پیگیری و شناسایی تهدیدات دست یابیم و در عین حال قابلیت انطباق مدل را با وضعیت‌های جدید افزایش دهیم.

۴-۳-۳- مجموعه چند وجهی

ترکیب قابلیت‌های روش‌های داده‌محور با تخصص دامنه‌ای خاص امکان ایجاد مجموعه‌ای از قوانینی را فراهم می‌آورد که نه‌تنها سازگار و منعطف هستند، بلکه قابلیت شناسایی تهدیدات سایبری را نیز تقویت می‌کنند. به‌عنوان نمونه، پژوهشگران مانند چی و همکاران [۸۵] از تکنیک‌های یادگیری ماشینی برای توسعه نمودارهای دانش استفاده کردند که در آن، اطلاعات مربوط به موجودیت‌ها به‌طور مؤثر جمع‌آوری شده و در یک پایگاه دانش مرتبط با امنیت سایبری سازماندهی می‌شود. به‌علاوه، روش‌های یادگیری عمیق می‌توانند برای شناسایی روابط پیچیده میان این موجودیت‌ها به کار گرفته شوند و بدین ترتیب نمودارهای دانش را تقویت کنند. این ادغام بین تکنیک‌های نوین داده‌محور و دانش ساختاریافته، به ما این امکان را می‌دهد که به‌طور جامع‌تری به رمزگشایی مفاهیم و تعاملات داخلی در حوزه امنیت سایبری پرداخته و در نتیجه، بتوانیم استراتژی‌های مؤثرتری را برای شناسایی و تحلیل تهدیدات طراحی کنیم.

۴-۴- تجزیه و تحلیل عملکرد

در حوزه امنیت سایبری، استفاده از روش‌های متنوع می‌تواند به توسعه مدل‌های مبتنی بر قانون کمک کند که به‌طور خاص به چالش‌های مختلف و ویژگی‌های خاص داده‌ها پاسخ می‌دهند. در حالی که دقت داده‌ها یکی از معیارهای تعیین‌کننده برای ارزیابی عملکرد مدل‌ها محسوب می‌شود، دیگر معیارهای مهم نیز وجود دارند که باید مد نظر قرار گیرند؛ از جمله نرخ تشخیص، تعداد مثبت‌های کاذب و منفی‌های کاذب، و همچنین محاسبه خطا. این معیارها به ما کمک می‌کنند تا عملکرد مدل‌ها را به‌طور جامع‌تری ارزیابی کنیم و درک بهتری از نقاط قوت و ضعف آن‌ها به‌دست آوریم، که در نهایت موجب بهبود استراتژی‌های امنیتی و کارایی سامانه‌ها می‌شود.

در طراحی مدل‌های مبتنی بر قانون برای امنیت سایبری، تأثیر فاکتورهای مختلفی از جمله انتخاب ویژگی‌ها و نوع الگوریتم طبقه‌بندی روشن است. تحقیقات نشان می‌دهند که نرخ تشخیص ممکن است به‌طور قابل توجهی وابسته به مجموعه ویژگی‌های انتخابی باشد و انواع مختلف مسائل (باینری در مقابل چندکلاسه) می‌توانند دقت را تحت تأثیر قرار دهند. به‌علاوه، ویژگی‌هایی مانند تنوع و تعداد قوانین، نوع قوانین (کلی یا خاص) و کامل بودن آن‌ها در تعیین کیفیت مدل نقشی کلیدی دارند. برای ایجاد یک مدل مؤثر، لازم است که این عوامل با هم ترکیب شوند و دانش عمیق در حوزه، تخصص انسانی و قابلیت‌های هوش مصنوعی به‌کار گرفته شوند تا مدلی جامع و پاسخگو به تهدیدات سایبری شکل گیرد.

این ادغام به توسعه یک رویکرد چندجانبه منجر می‌شود که می‌تواند به بهینه‌سازی عملکرد مدل کمک کند. به‌ویژه، برای ساخت مدل‌های مؤثر امنیت سایبری، ضروری است که به چگونگی تعامل این عواملی چون دقت و پیچیدگی نیز توجه شود. برای مثال، یک مدل ممکن است از دقت بالایی برخوردار باشد، اما اگر پیچیدگی قوانین آن بیش از حد باشد، در عمل قابل استفاده نخواهد بود. همچنین، از آن جا که تهدیدات سایبری به‌طور مداوم در حال تغییرند، تعمیم‌پذیری قوانین نیز باید در نظر گرفته شود تا مدل بتواند به شرایط جدید واکنش نشان دهد. در نهایت، توجه به این نکات می‌تواند به محققان و متخصصان کمک کند تا به شیوه‌ای مؤثرتر با چالش‌های امنیتی روبرو شوند و راه‌حل‌هایی پایدار ارائه دهند که قابلیت ارتقاء و کدگشایی در برابر تهدیدات در حال ظهور را دارا باشند.

۵- نتیجه گیری

در این تحقیق، به بررسی مدل‌سازی هوش مصنوعی مبتنی بر قوانین چندجانبه پرداخته شده است که می‌تواند در حفاظت از زیرساخت‌های حیاتی نقش بسزایی ایفا نماید. این مطالعه به طبقه‌بندی روش‌های تولید قوانین پرداخته و دو رویکرد اصلی دانش‌محور و داده‌محور را در فرآیند ایجاد قوانین مورد بررسی قرار داده است. همچنین، قابلیت‌های این مدل‌ها در مواجهه با تهدیدات سایبری، اعم از شناسایی و پیش‌بینی، به‌صورت شفاف نشان داده شده است. دلیل اصلی اتخاذ راهبرد مبتنی بر قانون، ایجاد ساختاری شفاف، قابل تفسیر و انعطاف‌پذیر است که امکان واکنش سریع و دقیق به تهدیدات سایبری را برای متخصصان فراهم آورده و مدیریت

و به‌روزرسانی قوانین را تسهیل می‌کند. برخلاف مدل‌های داده‌محور با عملکرد سیاه‌باکس، این مدل‌ها با ارائه منطق قابل فهم پشت تصمیمات، موجب افزایش اعتماد به سامانه شده و زمینه‌ای مناسب برای تلفیق دانش تخصصی انسانی با داده‌ها فراهم می‌آورند.

با وجود مزایای مذکور، لازم است توجه داشت که حوزه امنیت سایبری به‌طور مستمر در حال تغییر و تحول است؛ از این‌رو، اتکا صرف به قوانین ثابت، کافی نخواهد بود. بنابراین، ضروری است علاوه بر قوانین شفاف و مستحکم، از تکنیک‌های پیشرفته‌ای نظیر یادگیری ماشین و تحلیل رفتار برای تقویت توان دفاعی سامانه‌های امنیت سایبری بهره گرفته شود.

مدل‌های هوش مصنوعی مبتنی بر قانون، با ارائه ساختاری شفاف و قابل فهم برای فرایند تصمیم‌گیری، به ویژه در حوزه امنیت سایبری، نقشی کلیدی در شناسایی و واکنش به تهدیدات ایفا می‌کنند. این مدل‌ها با استفاده از الگوی "اگر-آنگاه"[1] شرایط و اقدامات لازم را تعریف می‌نمایند که این امر به متخصصان امکان می‌دهد منطق پشت اقدامات اتخاذ شده را به سهولت درک کنند. بر این اساس، واکنش سریع به تهدیدات، مانند مسدودسازی آدرس‌های آی‌پی[2] مشکوک یا ارسال هشدار به تیم‌های امنیتی، امکان‌پذیر می‌شود. افزون بر این، قابلیت به‌روزرسانی و اصلاح قوانین در پی توسعه دانش نوین، فرآیند مدیریت را تسهیل کرده و اعتماد به سامانه را تقویت می‌نماید. به طور کلی، این نوع مدل‌سازی با شفافیت و قابلیت تفسیر خود، به‌صورت مؤثری از مدل‌های پیچیده‌تر و غیرقابل تفسیر هوش مصنوعی متمایز می‌گردد و در بهبود ایمنی زیرساخت‌های حیاتی سهم قابل توجهی دارد.

در کاربری‌های بلادرنگ که با مجموعه‌ای گسترده و پیچیده از قوانین مواجه هستند، مدیریت زمان و اجرای سریع این قوانین اهمیت ویژه‌ای پیدا می‌کند. در چنین سناریوهایی، کارایی سامانه به شدت وابسته به بهینه‌سازی فرآیند تحلیل و واکنش به تهدیدات است. استفاده از روش‌های بهینه‌سازی الگوریتمی، پردازش موازی، تقسیم‌بندی قوانین و اولویت‌بندی آنها، می‌تواند به کاهش زمان تأخیر و افزایش سرعت پاسخ‌دهی کمک شایانی نماید. علاوه بر این، ترکیب مدل‌های مبتنی بر قوانین با تکنیک‌های یادگیری ماشین و تحلیل رفتار، ضمن حفظ شفافیت تصمیم‌گیری، توانمندی سامانه در مواجهه با تهدیدات نوظهور را افزایش می‌دهد.

این مدل‌ها نه تنها در شناسایی و اولویت‌بندی تهدیدات سایبری مؤثرند، بلکه فرآیندهای کاهش ریسک و پاسخ به حوادث را نیز بهبود می‌بخشند. از طریق تحلیل داده‌ها و استخراج قوانین قابل فهم، متخصصان قادرند ریشه‌های تهدیدات را شناسایی کرده و منطق پشت توصیه‌های خود برای کاهش ریسک را ارائه دهند. همچنین، با بهره‌گیری از پیش‌بینی‌های مبتنی بر الگوهای تاریخی، امکان شناسایی تهدیدات نوظهور پیش از وقوع فراهم می‌شود که به اتخاذ تصمیمات مؤثرتر در مدیریت آسیب‌پذیری‌ها کمک می‌کند. علاوه بر این، ارائه درکی عمیق از عوامل مؤثر بر رفتارهای مشکوک، توانایی تشخیص ناهنجاری‌ها را ارتقاء می‌دهد. در نهایت، تلفیق دانش استخراج شده با تخصص تیم‌های امنیت سایبری، سازمان‌ها را قادر می‌سازد واکنش سریع‌تر و مؤثرتری نسبت به تهدیدات داشته و تاب‌آوری خود را در برابر خطرات سایبری افزایش دهند. بنابراین، به‌کارگیری مدل‌های مبتنی بر قوانین می‌تواند به طور چشمگیری کیفیت و اثربخشی اقدامات پیشگیرانه و واکنشی را بهبود بخشد. این رویکرد نه تنها به متخصصان امکان می‌دهد با شفافیت بیشتری به شناسایی و کاهش تهدیدات بپردازند، بلکه توانایی تیم‌های امنیتی را در شناسایی و مدیریت تهدیدات نوظهور افزایش می‌دهد. با استفاده از دانش حاصل از تحلیل داده‌ها و استخراج قوانین، سازمان‌ها می‌توانند اقدامات خود را نه صرفاً مبتنی بر واکنش به حوادث، بلکه مبتنی بر پیش‌بینی و تثبیت زیرساخت‌های امنیتی مبتنی بر اطلاعات به انجام رسانند. بدین ترتیب، این مدل‌ها به‌عنوان چرخه‌ای مستمر، دانش و توانمندی‌های انسانی را تقویت نموده و تاب‌آوری کلی سازمان‌ها در برابر تهدیدات سایبری را ارتقاء می‌دهند.

اگرچه مدل‌سازی امنیت سایبری با بهره‌گیری از هوش مصنوعی و الگوریتم‌های مبتنی بر قوانین، نویدبخش بهبود قابل توجهی در اقدامات دفاعی زیرساخت‌های حیاتی است، اما همچنان نیازمند تحقیقات گسترده‌تری در برخی جنبه‌ها می‌باشد. از جمله الزامات کلیدی، توسعه چارچوبی جامع و هماهنگ است که تعامل مؤثر بین داده‌های جمع‌آوری شده و تخصص انسانی را فراهم آورد. چنین تعاملی می‌تواند به افزایش دقت و کارایی مدل‌ها یاری رسانده و در سطح کلان، امنیت سایبری در بخش‌های حیاتی نظیر انرژی، سلامت و دفاع را تقویت نماید. شناخت عمیق‌تر روابط و الگوهای موجود در داده‌های امنیتی به تحلیلگران امکان طراحی کاربردهای مؤثرتر برای مدل‌های مبتنی بر قوانین را می‌دهد.

با توجه به پیچیدگی‌های روزافزون تهدیدات سایبری و محدودیت‌های مدل‌های مبتنی بر قوانین و یادگیری عمیق به‌صورت مجزا، پژوهش‌های آینده باید بر توسعه چارچوب‌های ترکیبی تمرکز

[1] IF-THEN
[2] IP blocking

کنند که مزایای هر دو رویکرد را در هم ادغام کنند. این چارچوب‌ها می‌توانند ضمن حفظ شفافیت و قابلیت تفسیر مدل‌های قانون‌محور، از قدرت یادگیری عمیق در شناسایی الگوهای پیچیده بهره‌مند شوند. همچنین بهینه‌سازی پردازش بلادرنگ و ارتقاء همکاری بین تحلیلگران انسانی و سامانه‌های هوشمند از اولویت‌های اصلی در این زمینه خواهد بود. توصیه می‌شود مطالعات تجربی و آزمایش‌های میدانی با داده‌های واقعی و در محیط‌های زیرساخت‌های حیاتی انجام شود تا کارایی و اثربخشی این روش‌های نوین به‌صورت جامع ارزیابی گردد.

۶- مراجع

[1] S. A. Argyroudis et al., "Digital technologies can enhance climate resilience of critical infrastructure," Climate Risk Management, vol. 35, p. 100387, 2022, doi: https://doi.org/10.1016/j.crm.2021.100387.

[2] M. Chen, Y. Jiang, E. Wang, Y. Wang, and J. Zhang, "Measuring Urban Infrastructure Resilience via Pressure-State-Response Framework in Four Chinese Municipalities," Applied Sciences, vol. 12, no. 6, p. 2819, Mar. 2022, doi: https://doi.org/10.3390/app12062819.

[3] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," Computers & Security, vol. 120, no. 1, p. 102820, Sep. 2022, doi: https://doi.org/10.1016/j.cose.2022.102820.

[4] A. Alqudhaibi, M. Albarrak, A. Aloseel, S. Jagtap, and K. Salonitis, "Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations," Sensors, vol. 23, no. 9, p. 4539, Jan. 2023, doi: https://doi.org/10.3390/s23094539.

[5] N. A. Samson, "Exploring security, performance and privacy in the internet of things: A comprehensive survey," GSC Advanced Research and Reviews, vol. 21, no. 1, pp. 280–319, Oct. 2024, doi: https://doi.org/10.30574/gscarr.2024.21.1.0388.

[6] Oluwatobiloba Okusi, "Leveraging AI and Machine Learning for the Protection of Critical National Infrastructure," Asian Journal of Research in Computer Science, vol. 17, no. 10, pp. 1–11, Sep. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i10505.

[7] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," Journal of Big Data, vol. 7, no. 1, Jul. 2020, Available: https://link.springer.com/article/10.1186/s40537-020-00318-5.

[8] A. Ajala, C. Okoye, None Onyeka Chrisanctus Ofodile, A. Arinze, and D. Daraojimba, "Review of AI and machine learning applications to predict and Thwart cyber-attacks in real-time," Magna Scientia Advanced Research and Reviews, vol. 10, no. 1, pp. 312–320, Feb. 2024, doi: https://doi.org/10.30574/msarr.2024.10.1.0037.

[9] Merve Ozkan-Ozay et al., "A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions," IEEE Access, vol. 12, pp. 12229–12256, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3355547.

[10] K. Yu et al., "Securing Critical Infrastructures: Deep-Learning-Based Threat Detection in IIoT," IEEE Communications Magazine, vol. 59, no. 10, pp. 76–82, Oct. 2021, doi: https://doi.org/10.1109/MCOM.101.2001126.

[11] I. H. Sarker, "Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects," Annals of Data Science, vol. 10, pp. 1473–1498, Sep. 2022, doi: https://doi.org/10.1007/s40745-022-00444-2.

[12] I. H. Sarker, H. Janicke, Mohamed Amine Ferrag, and Alsharif Abuadbba, "Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures," Internet of Things, pp. 101110–101110, Feb. 2024, doi: https://doi.org/10.1016/j.iot.2024.101110.

[13] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," SN Computer Science, vol. 2, no. 3, Mar. 2021, doi: https://doi.org/10.1007/s42979-021-00557-0.

[14] I. H. Sarker, "Multi aspects AI based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview," SECURITY AND PRIVACY, vol. 6, no. 5, Jan. 2023, doi: https://doi.org/10.1002/spy2.295.

[15] Z. A. Sheikh, Y. Singh, P. K. Singh, and K. Z. Ghafoor, "Intelligent and secure framework for critical infrastructure (CPS): Current trends, challenges, and future scope," Computer Communications, vol. 193, pp. 302–331, Sep. 2022, doi: https://doi.org/10.1016/j.comcom.2022.07.007.

[16] A. V. Gheorghe, D. V. Vamanu, P. F. Katina, and R. Pulfer, Critical Infrastructures, Key Resources, Key Assets. Springer Nature (Netherlands), 2018. doi: https://doi.org/10.1007/978-3-319-69224-1.

[17] A. Kok, A. Martinetti, and J. Braaksma, "The impact of integrating information technology with operational technology in physical assets: a literature review," IEEE Access, pp. 1–1, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3442443.

[18] [۱۸] K. Stouffer, "Guide to Operational Technology (OT) Security," Jan. 2023, doi: https://doi.org/10.6028/nist.sp.800-82r3.

[19] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," International Journal of Critical Infrastructure Protection, vol. 9, pp. 52–80, Jun. 2015, doi: https://doi.org/10.1016/j.ijcip.2015.02.002.

[20] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," Computers & Security, vol. 89, p. 101677, Feb. 2020, doi: https://doi.org/10.1016/j.cose.2019.101677.

[21] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," International Journal of Critical Infrastructure Protection, vol. 34, p. 100433, Sep. 2021, doi: https://doi.org/10.1016/j.ijcip.2021.100433.

[22] M. Abdullahi et al., "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," Electronics, vol. 11, no. 2, p. 198, Jan. 2022, doi: https://doi.org/10.3390/electronics11020198.

[23] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure," Applied Sciences, vol. 11, no. 10, p. 4580, May 2021, doi: https://doi.org/10.3390/app11104580.

[24] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," Sustainability, vol. 15, no. 18, p. 13369, Jan. 2023, doi: https://doi.org/10.3390/su151813369.

[25] M. Lehto, "Cyber-Attacks Against Critical Infrastructure," Computational Methods in Applied Sciences, vol. 56, pp. 3–42, 2022, doi: https://doi.org/10.1007/978-3-030-91293-2_1.

[26] Y. C. Tok and S. Chattopadhyay, "Identifying threats,

[41]M. F. Franco, F. Künzler, J. von der Assen, C. Feng, and B. Stiller, “RCVaR: An economic approach to estimate cyberattacks costs using data from industry reports,” Computers & Security, vol. 139, p. 103737, Apr. 2024, doi: https://doi.org/10.1016/j.cose.2024.103737.
[42]H. Arif, A. Kumar, M. Fahad, and H. K. Hussain, “Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research,” International Journal of Multidisciplinary Sciences and Arts, vol. 2, no. 2, pp. 242–251, 2023, doi: https://doi.org/10.47709/ijmdsa.v2i2.3452.
[43]T. K. Vashishth, V. Sharma, K. K. Sharma, S. Vidyant, and A. Bhardwaj, “Future Trends and Challenges in Pharmaceutical Microbiology with the Integration of Artificial Intelligence,” Advances in Medical Technologies and Clinical Practice, pp. 315–344, Sep. 2024, doi: https://doi.org/10.4018/979-8-3693-3212-2.ch012.
[44]D. Krause, “Generative AI in FinTech: Transforming Financial Activities through Advanced Technologies,” Jan. 2024, doi: https://doi.org/10.2139/ssrn.4923224.
[45]J. Pfeiffer, J. F. Lachenmaier, O. Hinz, and van, “New Laws and Regulation,” Business & Information Systems Engineering, Oct. 2024, doi: https://doi.org/10.1007/s12599-024-00902-6.
[46] S. Shepherd and A. A. Jacob, “A Detailed Investigation on Digital Technology and AI in Social Sectors,” Advances in computational intelligence and robotics book series, pp. 33–62, Sep. 2024, doi: https://doi.org/10.4018/979-8-3693-5533-6.ch002.
[47] Roumen Trifonov, Evgeni Sabev, G. Pavlova, and Kamelia Raynova, “Analysis of deep learning methods for cybersecurity in industry 4.0,” AIP conference proceedings, Jan. 2024, doi: https://doi.org/10.1063/5.0193712.
[48]G. Wang, P. Liu, J. Huang, H. Bin, X. Wang, and H. Zhu, “KnowCTI: Knowledge-based Cyber threat intelligence entity and relation extraction,” Computers & security, vol. 141, pp. 103824–103824, Jun. 2024, doi: https://doi.org/10.1016/j.cose.2024.103824.
[49]AI-Powered Data-Driven Cybersecurity Techniques: Boosting Threat Identification and Reaction,” Nanotechnology Perceptions, vol. 20, no. S10, Aug. 2024, doi: https://doi.org/10.62441/nano-ntp.v20is10.25.
[50]F. Al-Quayed, Z. Ahmad, and M. Humayun, “A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0,” IEEE access, pp. 1–1, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3372187.
[51]M. N. Halgamuge, “Leveraging Deep Learning to Strengthen the Cyber-Resilience of Renewable Energy Supply Chains: A Survey,” IEEE Communications Surveys and Tutorials, pp. 1–1, Jan. 2024, doi: https://doi.org/10.1109/comst.2024.3365076.
[52]S. C. Phillips, S. Taylor, M. Boniface, S. Modafferi, and M. Surridge, “Automated Knowledge-Based Cybersecurity Risk Assessment of Cyber-Physical Systems,” IEEE Access, pp. 1–1, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3404264.
[53]M. Z. Kolk, S. Ruipérez-Campillo, A. A. Wilde, R. E. Knops, S. M. Narayan, and F. V. Tjong, “Prediction of sudden cardiac death using artificial intelligence: Current status and future directions,” Heart Rhythm, Sep. 2024, doi: https://doi.org/10.1016/j.hrthm.2024.09.003.
[54]C. Obi, V. Akagha, S. Onimisi, A. Chigozie, None Shedrack Onwusinkwue, and A. Ibrahim, “COMPREHENSIVE REVIEW ON CYBERSECURITY: MODERN THREATS AND ADVANCED DEFENSE STRATEGIES,” Computer science & IT research journal, vol. 5, no. 2, pp. 293–310, Feb. 2024, doi: https://doi.org/10.51594/csitrj.v5i2.758.
[55]Davy Preuveneers and Wouter Joosen, “An Ontology-Based cybercrime and digital forensic opportunities in Smart City Infrastructure via threat modeling,” Forensic Science International: Digital Investigation, vol. 45, p. 301540, Jun. 2023, doi: https://doi.org/10.1016/j.fsidi.2023.301540.
[27] I. H. Sarker, “AI for Critical Infrastructure Protection and Resilience,” pp. 153–172, Jan. 2024, doi: https://doi.org/10.1007/978-3-031-54497-2_9.
[28] J. Govea, W. Gaibor-Naranjo, and W. Villegas-Ch, “Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence,” Systems, vol. 12, no. 5, p. 165, May 2024, doi: https://doi.org/10.3390/systems12050165.
[29]M. Roshanaei, M. R. Khan, and N. N. Sylvester, “Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions,” Journal of Information Security, vol. 15, no. 3, pp. 320–339, May 2024, doi: https://doi.org/10.4236/jis.2024.153019.
[30] W. Ding, M. Abdel-Basset, H. Hawash, and A. M. Ali, “Explainability of Artificial Intelligence Methods, Applications and Challenges: A Comprehensive Survey,” Information Sciences, Oct. 2022, doi: https://doi.org/10.1016/j.ins.2022.10.013.
[31] X. Gu, J. Han, Q. Shen, and P. Angelov, “Autonomous learning for fuzzy systems: a review,” Artificial Intelligence Review, vol. 56, no. 8, pp. 7549–7595, Dec. 2022, doi: https://doi.org/10.1007/s10462-022-10355-6.
[32] P. Butala and A. Sluga, “Autonomous Work Systems in Manufacturing Networks,” Jan. 2006, doi: https://doi.org/10.1016/s0007-8506(07)60473-9.
[33] A. Dolunay, F. Kasap, and G. Keçeci, “Freedom of Mass Communication in the Digital Age in the Case of the Internet: ‘Freedom House’ and the USA Example,” Sustainability, vol. 9, no. 10, p. 1739, Oct. 2017, doi: https://doi.org/10.3390/su9101739.
[34]K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, “Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures,” IoT, vol. 2, no. 1, pp. 163–186, Mar. 2021, doi: https://doi.org/10.3390/iot2010009.
[35]F. A. Adelani, E. S. Okafor, B. S. Jacks, and O. A. Ajala, “THEORETICAL FRAMEWORKS FOR THE ROLE OF AI AND MACHINE LEARNING IN WATER CYBERSECURITY: INSIGHTS FROM AFRICAN AND U.S. APPLICATIONS,” Computer Science & IT Research Journal, vol. 5, no. 3, pp. 681–692, Mar. 2024, doi: https://doi.org/10.51594/csitrj.v5i3.928.
[36]A. Pollini et al., “Leveraging human factors in cybersecurity: an integrated methodological approach,” Cognition, Technology & Work, vol. 24, no. 2, Jun. 2021, doi: https://doi.org/10.1007/s10111-021-00683-y.
[37]A. Mehmood, G. Epiphaniou, C. Maple, N. Ersotelos, and R. Wiseman, “A Hybrid Methodology to Assess Cyber Resilience of IoT in Energy Management and Connected Sites,” Sensors, vol. 23, no. 21, p. 8720, Jan. 2023, doi: https://doi.org/10.3390/s23218720.
[38]D. Kim, Myung kil Ahn, S. Lee, D. Lee, M. Park, and D. Shin, “Improved Cyber Defense Modeling Framework for Modeling and Simulating the Lifecycle of Cyber Defense Activities,” IEEE Access, vol. 11, pp. 114187–114200, Jan. 2023, doi: https://doi.org/10.1109/access.2023.3324901.
[39]S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, and K.-K. Raymond Choo, “The role of national cybersecurity strategies on the improvement of cybersecurity education,” Computers & Security, vol. 119, no. 1, p. 102754, Aug. 2022, doi: https://doi.org/10.1016/j.cose.2022.102754.
[40]M. Bada and J. R. C. Nurse, “The social and psychological impact of cyberattacks,” Emerging Cyber Threats and Cognitive Vulnerabilities, pp. 73–92, 2020, doi: https://doi.org/10.1016/b978-0-12-816203-3.00004-6.

024-00886-w.
[69]Pranali Dhawas, Abhishek Dhore, D. Bhagat, Ritu Dorlikar Pawar, Ashwini Kukade, and Kamlesh Kalbande, “Big Data Preprocessing, Techniques, Integration, Transformation, Normalisation, Cleaning, Discretization, and Binning,” Advances in business information systems and analytics book series, pp. 159–182, Dec. 2023, doi: https://doi.org/10.4018/979-8-3693-0413-6.ch006.
[70]S. N. Ashraf, R. Siddiqi, and H. Farooq, “Auto encoder-based defense mechanism against popular adversarial attacks in deep learning,” PLOS ONE, vol. 19, no. 10, p. e0307363, Oct. 2024, doi: https://doi.org/10.1371/journal.pone.0307363.
[71]D. Vasan and M. Hammoudeh, “Enhancing Resilience Against Adversarial Attacks in Medical Imaging Using Advanced Feature Transformation Training,” Current Opinion in Biomedical Engineering, pp. 100561–100561, Oct. 2024, doi: https://doi.org/10.1016/j.cobme.2024.100561.
[72]X. Yuan, S. Han, W. Huang, H. Ye, X. Kong, and F. Zhang, “A Simple Framework to Enhance the Adversarial Robustness of Deep Learning-based Intrusion Detection System,” arXiv (Cornell University), Dec. 2023, doi: https://doi.org/10.1016/j.cose.2023.103644.
[73]Yuvaraja Thangavel, H. Garg, Manjunathan Alagarsamy, and D. Pradeep, “Revolutionizing breast cancer diagnosis with a comprehensive approach using digital mammogram-based feature extraction and selection for early-stage identification,” Biomedical signal processing and control, vol. 94, pp. 106268–106268, Aug. 2024, doi: https://doi.org/10.1016/j.bspc.2024.106268.
[74]M. Wasim, A. R. Singh, A. Pandian, R. S. Rathore, M. Bajaj, and I. Zaitsev, “A hybrid approach using support vector machine rule-based system: detecting cyber threats in internet of things,” Scientific Reports, vol. 14, no. 1, Nov. 2024, doi: https://doi.org/10.1038/s41598-024-78976-1.
[75] Arash Mahboubi et al., “Evolving techniques in cyber threat hunting: A systematic review,” Journal of Network and Computer Applications, pp. 104004–104004, Aug. 2024, doi: https://doi.org/10.1016/j.jnca.2024.104004.
[76]Ayo Rotibi, N. Saxena, and P. Burnap, “Winning the battle with cyber risk identification tools in industrial control systems: A review,” IET Cyber-Physical Systems Theory & Applications, Nov. 2024, doi: https://doi.org/10.1049/cps2.12105.
[77]N. Ullah, S. Rahman, and Sharmine Akther Liza, “Cyber-susiliency index: A comprehensive resiliency-sustainability-cybersecurity index for healthcare supply chain networks,” Decision Analytics Journal, vol. 9, pp. 100319–100319, Dec. 2023, doi: https://doi.org/10.1016/j.dajour.2023.100319.
[78]P. Ranka, A. Shah, N. Vora, A. Kulkarni, and N. Patil, “Computer Vision-Based Cybersecurity Threat Detection System with GAN-Enhanced Data Augmentation,” Communications in Computer and Information Science, pp. 54–67, 2024, doi: https://doi.org/10.1007/978-3-031-53728-8_5.
[79]R. Mohammad, F. Saeed, A. A. Almazroi, F. S. Alsubaei, and A. A. Almazroi, “Enhancing Intrusion Detection Systems Using a Deep Learning and Data Augmentation Approach,” Systems, vol. 12, no. 3, p. 79, Mar. 2024, doi: https://doi.org/10.3390/systems12030079.
[80]L. K. Nwobodo, C. S. Nwaimo, A. E. Adegbola, L. K. Nwobodo, C. S. Nwaimo, and A. E. Adegbola, “Enhancing cybersecurity protocols in the era of big data and advanced analytics,” GSC Advanced Research and Reviews, vol. 19, no. 3, pp. 203–214, 2024, doi: https://doi.org/10.30574/gscarr.2024.19.3.0211.
[81]G. Agrawal, A. Kaur, and S. Myneni, “A Review of Generative Models in Generating Synthetic Attack Data for Cybersecurity,” Electronics, vol. 13, no. 2, p. 322, Jan. 2024, doi: https://doi.org/10.3390/electronics13020322.
Cybersecurity Framework for AI-Enabled Systems and Applications,” Future internet, vol. 16, no. 3, pp. 69–69, Feb. 2024, doi: https://doi.org/10.3390/fi16030069.
[56] Andrei Chiş, O. I. Stoica, Ana-Maria Ghiran, and R. A. Buchmann, “A Knowledge Graph Approach to Cyber Threat Mitigation Derived from Data Flow Diagrams,” 2022 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), vol. 8, pp. 1–6, May 2024, doi: https://doi.org/10.1109/aqtr61889.2024.10554074.
[57]J. Oloyede, “AI-Driven Cybersecurity Solutions: Enhancing Defense Mechanisms in the Digital Era,” SSRN Electronic Journal, Jan. 2024, doi: https://doi.org/10.2139/ssrn.4976103.
[58]A. Mehmood, A. Shafique, Moatsum Alawida, and Abdul Nasir Khan, “Advances and Vulnerabilities in Modern Cryptographic Techniques: A Comprehensive Survey on Cybersecurity in the Domain of Machine/Deep Learning and Quantum Techniques,” IEEE access, pp. 1–1, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3367232.
[59]F. Wang, Z. Ding, K. Liu, L. Xin, Y. Zhao, and Y. Zhou, “Multi-Relation Extraction for Cybersecurity Based on Ontology Rule-Enhanced Prompt Learning,” Electronics, vol. 13, no. 12, pp. 2379–2379, Jun. 2024, doi: https://doi.org/10.3390/electronics13122379.
[60]V. Onishchenko, Oleksandr Puchkov, and I. Subach, “Investigation of associative rule search method for detection of cyber incidents in information management systems and security events using CICIDS2018 test data set,” Collection Information technology and security, vol. 12, no. 1, pp. 91–101, Jun. 2024, doi: https://doi.org/10.20535/2411-1031.2024.12.1.306275.
[61]A. K. Sah and Venkatesh K, “Anomaly-Based Intrusion Detection in Network Traffic using Machine Learning: A Comparative Study of Decision Trees and Random Forests,” vol. 9, pp. 1–7, Apr. 2024, doi: https://doi.org/10.1109/icnwc60771.2024.10537451.
[62]Z. Aziz and R. Bestak, “Insight into Anomaly Detection and Prediction and Mobile Network Security Enhancement Leveraging K-Means Clustering on Call Detail Records,” Sensors, vol. 24, no. 6, p. 1716, Jan. 2024, doi: https://doi.org/10.3390/s24061716.
[63]Alsamir Alsamir and Hanan AlShaher, “Anomaly-Based Intrusion Detection Systems Using Machine Learning,” Journal of Cybersecurity and Information Management, vol. 14, no. 1, pp. 20–33, Jan. 2024, doi: https://doi.org/10.54216/jcim.140102.
[64]A. Mumuni and F. Mumuni, “Automated data processing and feature engineering for deep learning and big data applications: a survey,” Journal of Information and Intelligence, Jan. 2024, doi: https://doi.org/10.1016/j.jiixd.2024.01.002.
[65]D. Patil, N. L. Rane, P. Desai, and J. Rane, “Machine learning and deep learning: Methods, techniques, applications, challenges, and future research opportunities,” Trustworthy Artificial Intelligence in Industry and Society, Oct. 2024, doi: https://doi.org/10.70593/978-81-981367-4-9_2.
[66]Y. Chen et al., “Development and application of Few-shot learning methods in materials science under data scarcity,” Journal of Materials Chemistry A, Jan. 2024, doi: https://doi.org/10.1039/d4ta06452f.
[67]H. Hassani, Ehsan Hallaji, Roozbeh Razavi-Far, and M. Saif, “Learning from high-dimensional cyber-physical data streams: a case of large-scale smart grid,” International Journal of Machine Learning and Cybernetics, Sep. 2024, doi: https://doi.org/10.1007/s13042-024-02365-3.
[68]Md. Alamin Talukder et al., “Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction,” Journal of Big Data, vol. 11, no. 1, Feb. 2024, doi: https://doi.org/10.1186/s40537-

[82] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, “Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations,” Sensors, vol. 23, no. 15, p. 6666, Jul. 2023, doi: https://doi.org/10.3390/s23156666.

[83] A. A. Aliyu, J. Liu, and E. Gilliard, “A Decentralized and Self-Adaptive Intrusion Detection Approach Using Continuous Learning and Blockchain Technology,” Journal of Data Science and Intelligent Systems, 2024, doi: https://doi.org/10.47852/bonviewjdsis42023803.

[84] A. E. Topcu, Y. I. Alzoubi, E. Elbasi, and E. Camalan, “Social Media Zero-Day Attack Detection Using TensorFlow,” Electronics, vol. 12, no. 17, p. 3554, Jan. 2023, doi: https://doi.org/10.3390/electronics12173554.

[85] Preeja Pradeep, M. Caro-Martínez, and Anjana Wijekoon, “A practical exploration of the convergence of Case-Based Reasoning and Explainable Artificial Intelligence,” Expert Systems with Applications, vol. 255, pp. 124733–124733, Jul. 2024, doi: https://doi.org/10.1016/j.eswa.2024.124733.

[86] Y. Qi et al., “Cybersecurity knowledge graph enabled attack chain detection for cyber-physical systems,” vol. 108, pp. 108660–108660, May 2023, doi: https://doi.org/10.1016/j.compeleceng.2023.108660.