فصلنامه علمی آماد و فناوری دفاعی، سال ششم، شماره بیستم، زمستان ۱۴۰۲

# بررسی الزامات زنجیره تأمین دفاعی تاب آور با تأکید بر فناوری‌های نوظهور صنعت ۴

علی پارسا[۱]، سید حسین خادم[۲]، حمیدرضا رضائی*[۳] و ابراهیم محمودزاده[۴]

تاریخ دریافت:۱۴۰۲/۰۸/۱۹ تاریخ پذیرش: ۱۴۰۲/۱۱/۲۳

## چکیده

**فرصت‌های فناورانه، قابلیت‌ها و دستاوردهای انقلاب صنعتی نسل چهارم منشأ تحولات و اثرات مثبتی در فرآیندها و جریان‌های زنجیره‌های تأمین هستند اما حرکت شتاب‌زده به سمت آن‌ها زمینه‌ساز اختلال‌ها و پیامدهای نامطلوب در این حوزه خواهد شد. زنجیره تأمین دفاعی هم که وظیفه ایجاد بستر توسعه پایدار و ابعاد مختلف امنیت ملی در بخش دفاع را، با پشتیبانی یکپارچه و مداوم از نیروهای مسلح ج.ا.ایران به عهده دارد به دلیل ویژگی‌های پیچیدگی و محرمانگی، دائماً در معرض مخاطرات متنوع سخت‌افزاری و نرم‌افزاری واقع‌شده و انتخاب رویکردی تاب‌آور برای مدیریت اختلالات این زنجیره، امری گریزناپذیر است. این پژوهش تلاش دارد تأثیر فناوری‌های نوظهور صنعت نسل چهارم بر تاب‌آوری زنجیره تأمین دفاعی را ضمن بررسی نظام‌مند مطالعات صورت گرفته پیشین، با تأکید بر مفهوم امنیت سایبری با روش فراترکیب نتایج موردبررسی قرار دهد. پس از بررسی مقالات مرتبط و انتخاب مقالات معتبر و جدید و انجام فراترکیب نتایج حاصل از مقالات، نتایج حاصل از این تحقیق مؤید این واقعیت است که مهم‌ترین**

[۱] دکترای فناوری اطلاعات و ارتباطات دانشگاه اصفهان -پژوهشگرحوزه صنعت ۴ Email:a.parsa2580@gmail.com

[۲] دانشجوی دکتری فناوری اطلاعات-کسب و کار هوشمند از دانشگاه آزاد اسلامی واحد تهران جنوب Email:h.khadem@sndu.ac.ir

[۳] دانش آموخته دکترای علوم دفاعی راهبردی( سیاست دفاعی)نویسنده مسئول Email:rezaee55@chmail.ir

[۴] استاد مدیریت راهبردی و عضو هیئت علمی دانشگاه صنعتی مالک اشتر Email:maheb20@mut.ac.ir

**الزامات زنجیره تأمین دفاعی تاب‌آور با تأکید بر فناوری‌های نوظهور صنعت ٤ شامل: «رؤیت پذیری زنجیره تأمین دفاعی» با بیش‌ترین تأثیرپذیری از قابلیت‌های انقلاب صنعتی چهارم و «تجزیه و تحلیل داده‌های حجیم»، تأثیرپذیرترین فناوری تعیین می‌گردد.**

**واژه‌های کلیدی:** **الزامات، امنیت سایبری، انقلاب صنعتی چهارم، تاب‌آوری، زنجیره تأمین دفاعی، فراترکیب**

## مقدمه

زنجیره تأمین، سامانه‌ای متشکل از سازمان‌های مرتبط با تأمین، افراد دخیل، فعالیت‌ها عملیات و درنهایت منابع اطلاعاتی آن‌ها است که در انتقال یک کالا یا خدمات از عرضه‌کننده به متقاضی نهایی درگیر و فعال هستند (هاگز،۲۰۱۸). این زنجیره شامل جریان فیزیکی (تبدیل، جابه‌جایی و ذخیره‌سازی کالاها و مواد)، جریان اطلاعات (هماهنگی درخواست‌ها و ردیابی جریان فیزیکی روزانه کالا) و جریان‌های مالی و مشارکتی، به همراه خدمات است که به صورت کاملاً هماهنگ فعال، همه این فعالیت‌ها و جریان‌ها از طریق مبادلات داده‌ها در یک زنجیره تأمین، یکپارچه شده است. ویژگی‌های خاص هر صنعت توجه ویژه طراحان و مدیران را به بخش‌های مختلفی از زنجیره تأمین، معطوف می‌کند. در این بین، زنجیره تأمین دفاعی حائز ویژگی‌های خاصی است که آن را از زنجیره‌های تأمین تجاری متمایز کرده است و به‌تبع آن نحوه نگرش به مسائل و اهمیت جنبه‌های مختلف را نیز تحت تأثیر قرار داده است. مهم‌ترین تفاوت متمایزکننده زنجیره تأمین دفاعی از انواع تجاری آن، هدف و رسالت این زنجیره است. در نوع تجاری، هدف عمده تمامی فعالیت‌ها تحقق سودآوری بیشتر است. اما در زنجیره تأمین دفاعی، ایجاد قدرت بازدارندگی با حفظ آمادگی دفاعی نیروهای مسلح است که بسترساز توسعه پایدار و ابعاد مختلف امنیت ملی است. از طرف دیگر، یک زنجیره تأمین دفاعی بیش از زنجیره‌های تأمین تجاری، به دلیل پیچیدگی و وسعت مأموریتی و محرمانگی بالا در اطلاعات و تجهیزان و سرمایه‌های انسانی، هدف مخاطرات و عدم قطعیت‌های محیطی قرار می‌گیرد. بدین جهت، حفظ مداومت و توانایی پاسخگویی زنجیره تأمین دفاعی در برابر اختلال‌های احتمالی، ضروری به نظر می‌رسد. علی‌رغم مزایای بسیاری که می‌توان برای استفاده از فناوری‌های نوین در زنجیره تأمین برشمرد، این مسئله دسته‌ای از چالش‌ها را در حوزه امنیت سایبری به وجود می‌آورد که غیرقابل‌اغماض هستند (Creazza et al., 2021). با توجه به فعالیت‌های خاص زنجیره تأمین دفاعی و سطح حساسیت آن، نیاز به پرداختن به چالش‌های امنیتی و راهکارهای مقابله با آن‌ها ضروری به نظر می‌رسد (موحدی صفت، ۱۴۰۱). در همین جهت، پژوهش حاضر به بررسی تأثیرات

فناوری‌های نوظهور در صنعت ٤ برتاب‌آوری زنجیره تأمین دفاعی، با تأکید بر موضوع امنیت سایبری می‌پردازد.

## پیشینه تحقیق و مروری بر ادبیات مسئله

در این بخش سعی می‌شود ادبیات مرتبط با پژوهش به صورت مختصر بیان شود. این مفاهیم در قالب ۲ دسته کلی جایگاه تاب‌آوری در زنجیره تأمین دفاعی و تأثیرات صنعت ٤ بر تاب‌آوری زنجیره تأمین، سازمان‌دهی شده‌اند.

### جایگاه تاب‌آوری در زنجیره تأمین دفاعی

به صورت کلی مفهوم تاب‌آوری[1] زنجیره تأمین به توانایی و آمادگی آن در مقابل رخدادهای غیرمنتظره و پاسخگویی به اختلالات[2] اشاره می‌کند. با توجه به وجود عدم قطعیت‌های[3] مختلف در فرآیندهای زنجیره تأمین، بروز اختلال به عنوان یک رخداد اجتناب‌ناپذیر شناخته می‌شود. با توجه به این موضوع، یک زنجیره تأمین تاب‌آور با شناخت نقاط محتمل اختلال، می‌کوشد در مواجه با این رخداد، همچنان به عملکرد مطلوب خود ادامه دهد (کریمی زارچی و همکاران،۱۳۹۹). توجه به غیرقابل‌انکار بودن نقش فناوری اطلاعات در تمام شئون زندگی بشر، گویای این واقعیت است که ورود فناوری اطلاعات به هر صنعتی، مزایای عمومی مانند افزایش دقت، سرعت، کاهش هزینه‌ها و خسارت‌ها را دنبال دارد. در این بین، به صورت خاص تلفیق فناوری اطلاعات در فعالیت‌های یک زنجیره تأمین می‌تواند مزایای بسیاری به دنبال داشته باشد که از مهم‌ترین آن‌ها می‌توان به شفافیت جریان اطلاعات، افزایش کیفیت و صحت اطلاعات واصله به تصمیم‌سازان و کاهش مدت زمان دسترسی متقاضیان به کالاها اشاره نمود (Hammi et al., 2023). ظهور و بروز مزایای ادغام فرآیندهای صنعتی با فناوری اطلاعات از یک‌طرف و ظهور مفاهیمی مانند اینترنت اشیا[4] از طرف دیگر، جهان را با مفهومی تحت

[1] Resiliency
[2] Disruptions
[3] Uncertainties
[4] Internet of Things

عنوان صنعت چهارم [1] آشنا کرده است که در آن، فناوری اطلاعات به عنوان قلب فرآیندهای صنعتی شناخته می‌شود. در همین جهت، زنجیره تأمین چهارم[2] نیز باهدف بازنگری و طراحی مجدد فرآیندها و جریان‌های زنجیره تأمین با تأکید ویژه بر مفاهیم و ابزارهای انقلاب صنعتی نسل چهارم، مطرح می‌گردد (Ozenc et al., 2022).

زنجیره‌های تأمین که به صورت ذاتی با رایج‌ترین مخاطرات[3] همچون تقاضای نامشخص، وقفه در عرضه، نوسان نرخ ارز، بی‌ثباتی سیاسی، بازارهای مصرف پویا و حتی رویدادهای غیرمنتظره مانند حوادث کاری، بلایای طبیعی و تروریسم مواجه هستند (Ozenc et al., 2022) اولین گام در رویارویی با این مخاطرات، تبیین مفهوم مخاطره است. به صورت کلی یک مخاطره به مفهوم قرار گرفتن زنجیره تأمین درمعرض خطر[4] و یا ضرر[5] است. در مفهومی گسترده‌تر مخاطره، احتمال یا تهدید آسیب[6]، جراحت[7]، مسئولیت[8]، ضرر یا سایر رویدادهای منفی است که ناشی از آسیب‌پذیری‌های داخلی هر سازمان است و ممکن است از طریق اقدام پیشگیرانه از آن اجتناب شود. تعاریف دیگری نیز وجود دارند که جنبه‌های دیگری از مخاطرات زنجیره تأمین را مشخص می‌کنند. از کنار هم قرار دادن این تعاریف می‌توان این نکات را برداشت نمود که اولاً، یک مخاطره، به معنی وجود یک احتمال بالقوه برای رخدادهای نامطلوب در زنجیره تأمین است و در ثانی، در صورت وقوع یک مخاطره، سازمان‌ها متحمل ضررهایی از قبیل ضررهای مالی، اعتباری و یا خدشه به اهداف بنیادین خود می‌شوند. لذا همواره سازمان‌ها می‌کوشند تا زنجیره تأمین خود را از مخاطرات، محافظت کنند (Louis & Pagell, 2018). به همین جهت، مدیریت مخاطرات زنجیره تأمین،[9] که یک رویکرد

[1] Industry 4.0
[2] Supply Chain 4.0
[3] Risks
[4] Danger
[5] Loss
[6] Damage
[7] Injury
[8] Liability
[9] Supply Chain Risk Management

سامانمند جهت شناسایی، ارزیابی و تخفیف اثر مخاطرات در زنجیره‌های تأمین است همواره در شمار اساسی‌ترین وظایف مدیریت زنجیره تأمین قرار می‌گیرد (Kara et al., 2020).

ظهور مفهوم زنجیره تأمین نسل چهارم که به معنای بازنگری فرآیندها و عملکردهای زنجیره تأمین به منظور استفادهٔ هرچه بیشتر از فناوری‌های نوین در بستر تحول دیجیتال در زنجیره تأمین است هم‌سال‌هاست به مفهومی آشنا در حوزه صنعت تبدیل‌شده‌اند. این مفهوم عمدتاً بر ایجاد اتصال بین افراد، فرآیندها و تجهیزات، استوار است که به افزایش تبادل داده‌ها و اطلاعات در طول زنجیره تأمین منجر می‌شود. اگرچه اشتراک بیشتر اطلاعات و در دسترس بودن بیشتر داده‌ها منشأ اثرات مثبتی هستند، اما مخاطراتی را نیز ایجاد می‌کنند که نمی‌توان آن‌ها را نادیده گرفت (Creazza et al., 2021). انواع جدیدی از مخاطرات با به‌کارگیری فناوری‌های انقلاب صنعت چهارم ایجاد می‌شوند که مخاطرات زنجیره تأمین ٤.٠ نامیده می‌شوند. این مخاطرات عمدتاً اطلاعات در حوزه حملات سایبری، امنیت اطلاعات و تهدیدات امنیتی سامانه‌های رایانه‌ای ظاهر می‌شوند. نظر به گستردگی روزافزون اهمیت فناوری‌های جدید، پرداختن به مخاطرات حوزه امنیت سایبری و مدیریت این دسته از مخاطرات با رویکرد تاب‌آوری در این زنجیره بااهمیت ویژه‌ای مطرح می‌گردد (Ozenc et al., 2022). معمولاً مفهوم تاب‌آوری به بررسی قابلیت انعطاف‌پذیری زنجیره تأمین در توانایی برای مقابله با پیامدهای حاصل از مخاطرات اجتناب‌ناپذیر، به منظور بازگشت به حالت عملیاتی اولیه یا حرکت به وضعیت جدید و مطلوب‌تر پس از اختلال می‌پردازد. مارینگانی و همکاران (۲۰۲۳) در پژوهش خود به جامع‌ترین تعریف از تاب‌آوری این‌گونه اشاره داشته‌اند که توانایی زنجیره تأمین برای آماده شدن برای رویدادهای مخاطرهٔ غیرمنتظره، واکنش سریع و بازیابی سریع از اختلالات احتمالی شبکه تأمین زمانی تاب‌آور است به‌گونه‌ای که بتواند به اختلالات غیرمنتظره پاسخ دهد و توانایی بازگشت به حالت اولیه یا رفتن به حالت جدید و مطلوب‌تر پس از اختلال را داشته تا عملیات عادی شبکه تأمین را بازیابی کند با حفظ تداوم عملیات در سطح مطلوب اتصال و کنترل بر ساختار و عملکرد. حال این سؤال پیش بیاید که چه عواملی سبب می‌شوند یک زنجیره تأمین، حائز ویژگی تاب‌آوری شود؟

محققان، عوامل بسیاری را برای ایجاد قابلیت تاب‌آوری در زنجیره تأمین، نام‌برده‌اند. فهرست این مؤلفه‌ها به همراه تعریف هر کدام در جدول ۲ ارائه شده است (Marinagi et.al,2023).

**جدول ۱- مؤلفه‌های تأثیرگذار در تاب‌آوری زنجیره تأمین (Marinagi et.al,2023)**

| عنوان | تعریف |
|---|---|
| **پیکره‌بندی و طراحی شبکه زنجیره تأمین** | توانایی بازطراحی دوباره زنجیره تأمین |
| **افزونگی** | نگهداری ظرفیت‌های اضافی برای مواقع ضروری |
| **انعطاف‌پذیری** | ظرفیت زنجیره تأمین برای تطبیق با تغییراتی که در سطح منابع فروشگاه، کارخانه یا در سطح کل شبکه |
| **رؤیت پذیری** | توانایی دیدن زنجیره تأمین به صورت سراسری و یافتن محل رویداد مخرب |
| **همکاری** | توانایی برنامه‌ریزی و اجرای عملیات زنجیره تأمین به‌طور مشترک با سایر شرکت‌ها. اعتماد متقابل و تمایل به اشتراک‌گذاری اطلاعات در این بخش، موردنیاز است |
| **چابکی**[1] | توانایی واکنش سریع به یک تغییر غیرقابل‌پیش‌بینی در عرضه و/یا تقاضا |
| **آگاهی از وضعیت** | توانایی درک آسیب‌پذیری‌های زنجیره تأمین و برنامه‌ریزی برای رویدادهای اختلال |
| **اشتراک اطلاعات** | توانایی به اشتراک‌گذاری اطلاعات دارایی‌های سازمان یا رویدادهای آن قبل/ در حین / پس از اختلال |
| **فرهنگ مدیریت مخاطرات** | درک مخاطرات، درک ساختار زنجیره تأمین، یادگیری مدیریت مخاطرات زنجیره تأمین |
| **امنیت** | امنیت فیزیکی، امنیت اطلاعات یا امنیت حمل‌ونقل |

[1] Agility

| | |
|---|---|
| **استحکام**[1] | **توانایی زنجیره تأمین برای مقاومت در برابر تغییرات و پیش‌بینی پیشگیرانه تغییر** |
| **مدیریت مخاطرات** | **اقداماتی پیش‌بینی کننده برای مخاطره، پاسخگویی یا بازیابی از اثرات اختلال ناشی از وقوع مخاطره** |
| **مدیریت دانش**[2] | **پیش از اختلال (توانایی کسب دانش از تجربیات گذشته برای آماده شدن برای یک اختلال در آینده)**<br>**پس از اختلال (توانایی یادگیری چگونگی ایجاد راه‌حل‌های بهتر پس از بروز اختلال)** |
| **سرعت** | **سرعت انجام سازگاری‌های انعطاف‌پذیر و بازیابی از یک اختلال** |

## تأثیر مفاهیم و فناوری‌های صنعت ٤ بر تاب‌آوری زنجیره تأمین

در انقلاب صنعتی اول و عصر تولید مکانیکی پس از ظهور ماشین بخار (۱۷٦۰)، انرژی حاصل از تبدیل بخار برای تأمین انرژی مورداستفاده قرار می‌گرفت. ورود برق در قرن ۱۹، باعث ایجاد شیوه‌های جدید سازمان‌دهی تولید انبوه شد (انقلاب صنعتی دوم). در نیمه دوم قرن بیستم، توسعه نیمه‌هادی‌ها و معرفی کنترل‌کننده‌های الکترونیکی آغاز عصر خودکارسازی بود و انقلاب صنعتی سوم را رقم زد. در نمایشگاه هانوفر در سال ۲۰۱۱، هنینگ کاگرمن، ولف-دیتر لوکاس و ولفگانگ والستر اصطلاح انقلاب صنعتی نسل چهارم را که بر پایه استفاده از قابلیت‌های آخرین فناوری‌های دیجیتال بود، مطرح کردند. به صورت کلی انتظار می‌رود، در انقلاب صنعتی ٤، اتصال یا ادغام تولید با فناوری اطلاعات و ارتباطات، ادغام داده‌های متقاضی با داده‌های ماشین‌های عملیاتی، استفاده از قابلیت ارتباط ماشین‌ها با ماشین‌ها و مدیریت تولید به صورت مستقل به شیوه‌ای انعطاف‌پذیر، کارآمد و همراه باصرفه جویی در منابع، اجرا شوند (Nath et al., 2020). این مرحله از فرآیند صنعتی شدن، و همچنین سه مرحله

[1] Robustness
[2] Knowledge Management

قبلی، تحت سلطه نوآوری‌های فنی است (Bartodziej, 2017). فناوری‌های متعددی که به مفهوم انقلاب صنعتی نسل چهارم عینیت می‌بخشند عبارت‌اند از اینترنت اشیا، هوش مصنوعی[1]، محاسبات ابری[2]، داده‌های حجیم و آنالیز[3] و زنجیره‌های بلوکی[4] که در این بخش به‌اختصار هریک از آن‌ها را شرح خواهیم داد.

**اینترنت اشیا** مفهوم جدیدی است که در سناریوی ارتباطات بی‌سیم مدرن به سرعت در حال گسترش است. ایده اصلی این مفهوم، حضور فراگیر اشیاء مختلفی - مانند برچسب‌های شناسایی فرکانس رادیویی[5]، حسگرها، محرک‌ها، تلفن‌های همراه و غیره - در اطراف ماست که از طریق طرح‌های آدرس‌دهی منحصربه‌فرد می‌توانند برای رسیدن به اهداف مشترک با یکدیگر و سایر موجودیت‌های پیرامون، تعامل کنند. اینترنت اشیا دنیایی است که در آن اشیاء فیزیکی به‌طور یکپارچه در شبکه اطلاعات ادغام می‌شوند و در آن اشیاء فیزیکی می‌توانند به شرکت‌کنندگان فعال در فرآیندهای تجاری تبدیل شوند. خدماتی برای تعامل با این «اشیاء هوشمند» از طریق اینترنت، پرس‌وجو کردن وضعیت آن‌ها و هرگونه اطلاعات مرتبط با آن‌ها، با در نظر گرفتن مسائل امنیتی و حریم خصوصی، امکان‌پذیر است (Sadhu et al., 2022).

**رایانش ابری** مدلی است برای امکان دسترسی راحت، بر حسب تقاضا و بدون محدودیت زمانی و مکانی، به یک مجموعه مشترک از منابع محاسباتی قابل تنظیم (مانند شبکه‌ها، سرورها، ذخیره‌سازی، برنامه‌ها و خدمات) که می‌تواند به سرعت تهیه‌شده و با حداقل تلاش مدیریت شوند. در ابتدای همه‌گیری سامانه‌های کامپیوتری، هر سازمان به‌کارگیرنده می‌بایست به صورت مستقل اقدام به سرمایه‌گذاری در حوزه فناوری اطلاعات کند. پس از اجرای سامانه موردنظر، فرآیند نگهداری زیرساخت آغاز می‌شود. این مسئله، ورود سازمان‌ها به مقوله فناوری اطلاعات را بسیار دشوار کرده و

[1] Artificial Intelligence
[2] Cloud Computing
[3] Big Data and Analytics
[4] Blockchain
[5] Radio Frequency Identification

هزینه‌هایی که سازمان‌ها برای به‌کارگیری سامانه‌های فناوری اطلاعات، متحمل می‌شوند، هزینه‌های سرمایه‌ای[1] است (Gammelgaard & Nowicka, 2023).

**هوش مصنوعی** به استفاده از رایانه برای انجام کارهایی که عموماً با کمک هوش انسانی انجام می‌شوند اطلاق می‌شود. این وظایف می‌تواند شامل ادراک با استفاده از ورودی‌های بصری، صوتی و لمسی، تشخیص الگو در داده‌های دریافتی از حسگرهای حرکتی/محیطی، جستجو در فضای حالت یک مسئله بهینه‌سازی و یا تصمیم‌گیری باشد. یادگیری ماشین زیرمجموعه‌ای از هوش مصنوعی است که با استفاده از مفاهیم حوزه علوم کامپیوتر و همچنین مفاهیم حوزه آمار و احتمالات، سعی در کشف روابط در یک مجموعه داده‌های ورودی دارد (Nath et al., 2022). در یک دسته‌بندی کلی، می‌توان از هوش مصنوعی انتظار پاسخگویی به مسائل زیر را داشت:

- حل مسائل بهینه‌سازی به عنوان قلب فرآیندهای مهندسی و همچنین فرآیندهای تجاری (Jang et al., 2023)؛
- پردازش تصویر و بینایی ماشین با ایجاد این قابلیت برای رایانه‌ها برای طراحی الگوریتم هوش مصنوعی در تشخیص سالم و یا معیوب بودن قطعات جدید (Ambore et al., 2022)؛
- پردازش زبان طبیعی با ایجاد قابلیت فهم و پردازش مفاهیم معنایی توسط رایانه‌ها (Helo & Hao, 2021)؛
- پیش‌بینی صحیح با استفاده از سوابق درست تقاضای مشتریان و افزایش میزان بهره‌وری (Helo & Hao, 2021).

**زنجیره بلوکی** یک فناوری پیشرفته، غیرمتمرکز و توزیعی است که محرمانه بودن، یکپارچگی و در دسترس بودن همه تراکنش‌ها و داده‌ها را حفظ می‌کند. درواقع زنجیره بلوکی یک دفتر کل دیجیتال[2] مشترک است که در شبکه توزیع می‌شود. هر صنعت با توجه به حفظ حریم خصوصی و کنترل‌های

[1] Capital Expenditure
[2] Digital Ledger

امنیتی موردپذیرش، نیازهای متفاوتی دارد. برای پاسخگویی به نیازهای مختلف، زنجیره بلوکی می‌تواند دارای ۳ ساختار عمومی، خصوصی و کنسرسیوم (هیبرید) باشد (Dutta et al., 2020). رمز ارزها یک نمونه مشهور از کاربردهای زنجیره بلوکی است که در آن، نیاز به واسطه‌ها در معاملات از بین می‌رود. به صورت کلی، می‌توان کاربردهای زنجیره بلوکی را در حذف مرکزگرایی در سازوکارهای امنیتی و انجام عملیات به صورت توزیع‌شده، دانست. فناوری زنجیره بلوکی این قابلیت را دارد که حملات امنیتی مختلف را مدیریت کند زیرا می‌تواند نیاز به وجود یک موجودیت متمرکز را برای انجام عملیات مختلف، برطرف کند (Bodkhe et al., 2020).

از جمع‌بندی نظرات می‌توان این‌گونه برداشت نمود که ابزارهای صنعت ٤ به خودی خود، عاملی برای ارتقاء تاب‌آوری زنجیره تأمین به شمار نمی‌روند اما مؤلفه‌های تاب‌آوری زنجیره تأمین به‌شدت از انقلاب صنعت چهارم و مفاهیم مرتبط با آن تأثیر می‌پذیرند (Marinagi et.al,2023). فناوری‌های صنعت نسل ٤ می‌توانند رؤیت پذیری و یکپارچگی میان اعضاء و شرکای زنجیره تأمین را افزایش داده و با اشتراک‌گذاری اطلاعات، میزان اعتماد و همکاری را در زنجیره تأمین در همه جنبه‌ها و رؤیت پذیری زنجیره تأمین را افزایش می‌دهد و می‌توانند اقدامات را در واکنش به‌موقع در خصوص رفع اختلالات توسط قابلیت‌های تاب‌آوری را زنجیره تأمین، پیش‌بینی کنند (Qader et al., 2022).

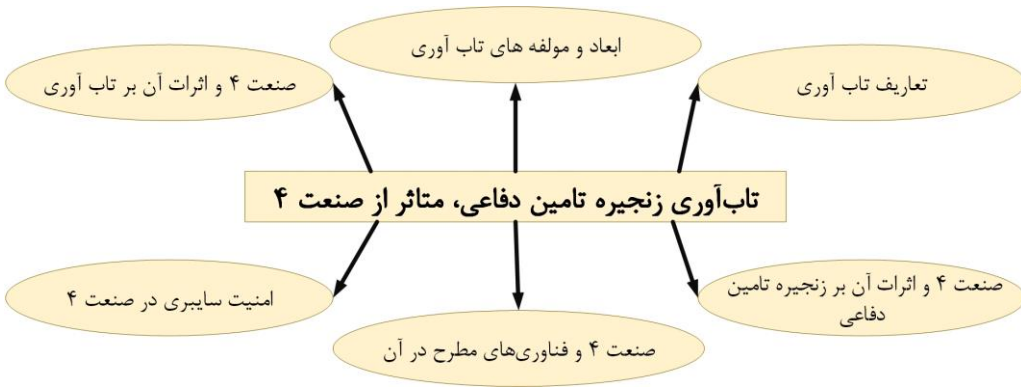
فناوری‌های مختلف توانمند ساز صنعت ٤ هم پتانسیل افزایش رؤیت پذیری و سرعت را در مقیاس وسیع دارند. طراحی زنجیره تأمین و درک آن، منبع یابی و فرهنگ مدیریت مخاطرات نیز می‌تواند تحت تأثیر مؤثر صنعت ٤ همچون تجزیه و تحلیل داده‌های حجیم باشد. درحالی‌که تمام فناوری‌های موردبحث، پتانسیل پشتیبانی از تاب‌آوری زنجیره تأمین را دارند، تجزیه و تحلیل داده‌های حجیم، کاربردی‌ترین و بالغ‌ترین آن‌ها است (Spieske & Birkel, 2021).

## امنیت سایبری زنجیره تأمین نسل ٤

جهت بقای سازمان، همواره محافظت از منابع سرمایه‌ای و ارزشمند، ضروری اهمیت بسزایی دارد. تا قبل از گسترش سامانه‌های کامپیوتری، این محافظت به شیوه‌های فیزیکی انجام می‌شد. به‌عنوان‌مثال، اسناد ارزشمند یک شرکت در گاوصندوق‌هایی نگهداری می‌شد تا هم در مقابل آسیب‌های فیزیکی

مانند آتش‌سوزی و هم در مقابل دسترسی افراد غیرمجاز به آن اسناد در امان باشند. با ظهور و گسترش سامانه‌های کامپیوتری، بسیاری از منابع سازمان‌ها به صورت الکترونیکی خود تبدیل شدند و در همین جهت، شیوه محافظت از آن‌ها نیز باید دست‌خوش تغییراتی می‌شد. ازاین‌رو امروزه مفهوم امنیت سایبری[1]، جایگاه ویژه‌ای پیدا کرده است و به یکی از مفاهیم غیرقابل‌اغماض تبدیل شده است (Sarker et al., 2020). انقلاب صنعتی ٤ و فناوری‌های مطرح در آن می‌توانند منشأ اثرات مثبت فراوانی بر روی کارایی صنعت‌ها داشته باشند. در این بین، چالش‌هایی وجود دارد که به عنوان موانع بر سر راه پیاده‌سازی ابزارهای نوین، شناخته می‌شوند (Sony & Naik, 2019). به دلیل وابستگی کسب‌وکارها به این محیط جدید، هر حمله امنیتی می‌تواند اثرات مخربی در حوزه اقتصادی برجای بگذارد و صنایع را از رسیدن به اهداف خود دور کند (Corallo & Lezzi, 2020). معمولاً خدمات امنیتی به منظور حفاظت از خصیصه‌های امنیتی سازمان‌ها و زیرساخت‌های فناوری اطلاعات آن‌ها طراحی می‌شوند. یک مدل پذیرفته‌شده برای خصیصه‌های امنیتی یک سامانه، مدلی موسوم به «سی آی آ» است. نام این مدل از کنار هم قرار دادن ابتدای سه واژه محرمانگی[2]، جامعیت[3] و دسترس‌پذیری[4] تشکیل‌شده است که با استفاده از این سه مفهوم می‌توان حملات امنیتی را طبقه‌بندی نمود. هدف هر حمله امنیتی، نقض یکی از این سه ویژگی خواهد بود (Ham,2021). در ادامه این مقاله از این مدل برای تفسیر آسیب‌پذیری‌های امنیتی فناوری‌های صنعت ٤ استفاده می‌شود. شکل ۱، نمایی از چارچوب نظری پژوهش را نشان می‌دهد.

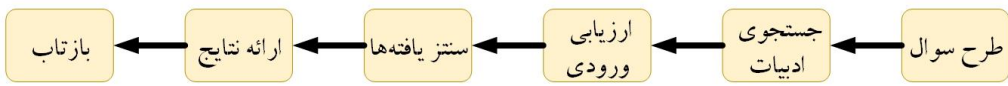
[1] Cybersecurity
[2] Confidentiality
[3] Integrity
[4] Availability




شکل ۱- چارچوب نظری پژوهش

## روش تحقیق

نوع پژوهش حاضر بر اساس هدف، توسعه ای-کاربردی، بر اساس ماهیت داده، کیفی و بر اساس روش‌های گردآوری داده و اطلاعات، اسنادی است. روش انجام پژوهش، تحلیلی – توصیفی بوده و داده‌های کیفی از روش فراترکیب جمع‌آوری می‌شود. در سالیان گذشته، پژوهش‌های کیفی، عمدتاً بر پایه بررسی و خلاصه‌سازی مطالعات پیشین انجام می‌شدند. افزایش شمار محققان و پژوهش‌های انجام‌شده توسط آنان سبب شده است تا روش‌های گذشته، کارایی خود را از دست بدهند. لذا امروزه محققان به دنبال روش‌هایی هستند که قابلیت استفاده در فضای پژوهش حاضر را داشته باشند. روش فراترکیب یکی از روش‌های جدید سنتز در حوزه مطالعات کیفی است که می‌تواند در گسترش و خلق نظریه‌ها، محققان را یاری رساند (عابدی جعفری و امیری، ۱۳۹۸). در این بخش سعی می‌شود با استفاده از روش فراترکیب، به منظور مقایسه، تفسیر، تبدیل و ترکیب مفاهیم اولیه و مؤلفه‌ها، شاخص‌های پژوهش بر مبنای یافته‌های حاصل از پژوهش‌های پیشین و مرتبط با اهداف پژوهش استخراج گردد. شکل ۲ به صورت شماتیک، مراحل انجام عملیات فراترکیب را نشان می‌دهد.




**شکل ۲- مراحل انجام عملیات فراترکیب (عابدی جعفری و امیری، ۱۳۹۸)**

## مرحله اول- تعیین هدف و طرح سؤالات تحقیق

در گام اول اجرای تحقیق با روش فراترکیب، نیاز است تا هدف اصلی پژوهش آشکار شود. هدف اصلی این پژوهش، همان‌طور که قبلاً اشاره شد؛ بررسی الزامات زنجیره تأمین دفاعی تاب‌آور با تأکید بر فناوری‌های نوظهور صنعت نسل چهارم تعیین‌شده است. سپس با مطرح کردن سؤالات تحقیق به عنوان نقطه ورودی روش فراترکیب، مورداستفاده قرار می‌گیرد. برای پژوهش حاضر، یک سؤال اصلی و چهار سؤال فرعی به شرح جدول ۳ مطرح می‌شود:

**جدول ۲- سؤالات پژوهش**

| ردیف | سؤال | کد |
|---|---|---|
| ۱ | مفاهیم، جایگاه، معیارهای کارایی و عوامل تأثیرگذار برتاب‌آوری زنجیره تأمین دفاعی کدامند؟ | RQ1 |
| ۲ | تأثیرات، مفاهیم و ابزارهای انقلاب صنعتی نسل ۴ مؤثر برتاب‌آوری زنجیره تأمین دفاعی کدامند؟ | RQ2 |
| ۳ | تهدیدات نوپدید تحمیل‌شده از سوی شبکه‌های رایانه‌ای به زنجیره‌های تأمین، دسته‌بندی و اولویت‌بندی آن‌ها کدامند؟ | RQ3 |
| ٤ | چه راهکارهایی برای دفع و یا تخفیف اثر تهدیدات مترتب بر زنجیره تأمین دفاعی وجود دارد؟ | RQ4 |

با استفاده از سؤالات پژوهش، کلیدواژه‌های موردنیاز برای جستجو در پایگاه‌های استنادی، استخراج گردیدند. جدول ٤ این کلیدواژه‌ها را نشان می‌دهد.

جدول ۳- کلیدواژه‌های پژوهش

| کلیدواژه | معادل لاتین | کد |
|---|---|---|
| زنجیره تأمین دفاعی | (Defense Supply Chain) | W1 |
| زنجیره تأمین ۴ | (Supply Chain 4.0) | W2 |

| | | |
|---|---|---|
| زنجیره تأمین تاب‌آور | (Resilient Supply Chain) | W3 |
| صنعت ۴ | (Industry 4.0) | W4 |
| چالش‌های امنیت سایبری | (Cyber Security Challenges) | W5 |

## مرحله دوم: جمع‌آوری ادبیات پژوهش

با استفاده از کلیدواژه‌های مندرج در جدول ٤، پایگاه‌های استنادی داخلی شامل سیویلیکا و sid و همچنین پایگاه‌های استنادی خارجی شامل google scholar، emerald، Taylor & Francis، ScienceDirect و IEEE explore موردبررسی قرار گرفتند. از این بررسی‌ها مجموعاً ۱۵۰ عنوان مقاله استخراج گردید که به منظور بررسی بیشتر، موردمطالعه قرار می‌گیرند.

## مرحله سوم: ارزیابی ورودی‌ها

در این مرحله، سعی می‌شود، مقالات یافته شده، با استفاده از یک سری شروط، مورد پالایش قرار گیرند تا درنهایت، مرتبط‌ترین منابع به دست آیند. اولین شرط پالایش، لحاظ کردن بازه زمانی انتشار مقالات است. برای مقالات فارسی بازه زمانی سال ۱۳۹۷ به بعد و مقالات لاتین بازه زمانی سال ۲۰۱۸ به بعد در نظر گرفته شده است. با مطالعه بخش چکیده، تعداد مقالات مرتبط به ۷۰ مقاله و با مطالعه بخش مقدمه، به ۳۰ مقاله تقلیل پیدا کردند. نهایتاً این ۳۰ مقاله موردمطالعه قرار گرفتند و با مطالعه کامل آن‌ها ۱۵ مقاله که ارتباط بسیار نزدیکی با موضوع و اهداف پژوهش داشتند، به عنوان مبنای انجام عملیات فرا ترکیب، مورداستفاده قرارگرفته و به مرحله بعد، وارد شدند. با مطالعه این مقالات، و انجام جمع‌بندی، مبانی نظری پژوهش حاضر به دست می‌آید. جدول ۵ نشان‌دهنده تقسیم‌بندی موضوعی ادبیات پژوهش به همراه درصد تکرار هریک از موضوعات مرتبط است.

جدول ٤- تقسیم‌بندی موضوعی پژوهش

| مضمون | مقوله | کد | تکرار (درصد) |
|---|---|---|---|
| **تاب‌آوری زنجیره تأمین** | مدل‌سازی مؤلفه‌های تاب‌آوری زنجیره تأمین | A1 | ۲۰ |
| | طراحی زنجیره‌های تأمین تاب‌آور | A2 | ۲۰ |
| | نقش انقلاب صنعتی نسل ۴ در تاب‌آوری زنجیره تأمین | A3 | ۲۰ |

| | | | |
|---|---|---|---|
| **انقلاب صنعتی نسل ٤** | فناوری‌های مطرح در انقلاب صنعتی نسل ۴ | A4 | ۲۰ |
| | نقش فناوری‌های انقلاب صنعتی نسل ۴ در زنجیره تأمین | A5 | ۵۰ |
| **امنیت سایبری** | امنیت سایبری در انقلاب صنعتی نسل ۴ | A6 | ۳۰ |
| | امنیت سایبری زنجیره تأمین | A7 | ۳۰ |
| **زنجیره تأمین دفاعی** | الزامات زنجیره تأمین دفاعی | A8 | ۳۰ |
| | تاب‌آوری زنجیره تأمین دفاعی | A9 | ۳۰ |

### مرحله چهارم: سنتز یافته‌ها

در این بخش، یافته‌های حاصل از مقالات منتخب، جهت انجام عملیات سنتز، تجزیه و تحلیل می‌شوند. جدول؟ لیست مقالات نهایی را به همراه کلیدواژه‌های مرتبط با آن‌ها نشان می‌دهد.

**جدول ۵- لیست مقالات استفاده‌شده در فرآیند سنتز به همراه کلیدواژه‌های مرتبط با آن‌ها**

| آدرس | کد مرجع | W1 | W2 | W3 | W4 | W5 |
|---|---|---|---|---|---|---|
| **باقری منش و همکاران (۱۳۹۸)** | P1 | * | | * | | |
| **رحیمی و همکاران (۱۳۹۷)** | P2 | * | | * | | |
| **کریمی زارچی و همکاران (۱۳۹۹)** | P3 | * | | * | | |
| **Fatorachian & Kazemi(2020)** | P4 | | * | | * | |
| **Frederico et. al(2019)** | P5 | | * | | | |
| **Ghadge et. al(2019)** | P6 | | | | | * |
| **Ghobakhloo(2020)** | P7 | | | | * | |
| **Hassija et. al(2019)** | P8 | | | | | * |
| **Queiroz et. al(2019)** | P9 | | * | | * | |
| **Sob et.al (2020)** | P10 | | * | | | * |
| **Sony et.al(2019)** | P11 | | | | * | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Culot et.al(2019) | P12 | | | | * | * |
| Corallo & Lezzi(2020) | P13 | | | | * | * |
| Marinagi et.al(2023) | P14 | | * | * | * | |
| Tortorella et al. (2021) | P15 | | * | * | * | |

یافته‌های حاصل از بررسی مقالات جدول ۵، در جدول ٦ مشاهده می‌شوند.

جدول ٦- یافته‌های حاصل از بررسی مقالات منتخب

| گزاره | آدرس | استنباط | کد |
|---|---|---|---|
| افزایش یا کاهش یادگیری سازمانی در افزایش یا کاهش تاب‌آوری زنجیره تأمین مؤثر است. به بیان دقیق‌تر، افزایش سطح یادگیری سازمانی به افزایش نوآوری کمک می‌کند و این مسئله به بهبود عوامل تأثیرگذار در تاب‌آوری زنجیره تأمین که شامل افزونگی، انعطاف‌پذیری، شفافیت و همکاری هستند، کمک می‌کند. | باقری منش و همکاران (۱۳۹۸) | یادگیری سازمانی به مفهوم توانایی سازمان‌ها در اصلاح فرآیندهای خود در مقابل تغییرات محیطی و تطبیق هرچه بیشتر با آن‌ها به منظور حفظ کارایی، تأکید دارد. از این منظر، این مفهوم، با تاب‌آوری زنجیره تأمین، اشتراکاتی دارد. چراکه یک زنجیره تأمین تاب‌آور، می‌کوشد در مواجه با تغییرات محیطی، مقاوم باشد. عوامل مختلفی ممکن است بر تاب‌آوری زنجیره تأمین، اثرگذار باشند | R1 |
| مؤلفه‌های مختلفی در ایجاد تاب-آوری زنجیره تأمین، اثرگذارند که به‌عنوان‌مثال مهم‌ترین آن‌ها می‌توان به افزونگی[1]، چابکی[2]، یادگیری[3]، انعطاف‌پذیری[4] و امنیت[5] اشاره کرد. در جهت ایجاد | رحیمی و همکاران (۱۳۹۷) کریمی زارچی و همکاران (۱۳۹۹) | جهت ایجاد قابلیت تاب‌آوری در زنجیره تأمین، اقدامات مختلفی شناسایی‌شده است. فارغ از تأثیرات مجزای هریک از این اقدامات در افزایش تاب‌آوری زنجیره تأمین، اثرات متقابل هریک از این اقدامات و روابط بین آن‌ها برای ایجاد یک زنجیره تأمین تاب‌آور، | R2 |

[1] Redundancy
[2] Agility
[3] Learning
[4] Flexibility
[5] Security

| | | | |
|---|---|---|---|
| تاب‌آوری در زنجیره تأمین، باید به جمیع این عوامل و ارتباطات بین آن‌ها توجه نمود. | | ضروری است. در این جهت، پژوهش‌هایی انجام‌شده است که هریک به نحوی، در شناسایی و مدل‌سازی میزان اهمیت هریک از مؤلفه‌های تاب‌آوری و همچنین میزان تأثیرپذیری آن‌ها از یکدیگر، فعالیت کرده‌اند. | |
| فناوری‌های فعال ساز[1] انقلاب صنعتی نسل ۴ امکان بهبود معیارهای کارایی زنجیره تأمین را با فراهم آوری سطح بالایی از یکپارچه‌سازی[2] و اتصال[3]، ایجاد می‌کنند. | Fatorachian & Kazemi(2020) | جهت سنجش کارایی زنجیره تأمین، نیاز است معیارهایی تعریف شود، تا فضای کیفی، به فضایی کمی تبدیل شود. این معیارها در سطوح مختلفی تعریف می‌شوند و هریک، جنبه خاصی از زنجیره تأمین را موردبررسی قرار می‌دهند. بر اساس یافته‌های حاصل از این پژوهش، استفاده از فناوری‌های صنعت نسل چهارم، موجب بهبود معیارهای کلیدی کارایی در زنجیره‌های تأمین، خواهد شد که منشأ این بهبودها را می‌توان در افزایش قابلیت یکپارچه‌سازی و بهبود اتصال بین بخش‌های مختلف زنجیره تأمین دانست. | R3 |
| زنجیره تأمین عمدتاً به دلیل ایجاد قابلیت یکپارچه‌سازی و اشتراک اطلاعات[4]، از فناوری اطلاعات استفاده می‌کند. این مسئله باعث بروز ورود برخی چالش‌های | Ghadge et. al(2019) | استفاده از هر فناوری جدید، مستلزم سنجش جنبه‌های مختلف اثرگذار بر مسئله است. عمدتاً دیده می‌شود که با ورود یک فناوری جدید، پژوهشگران، توجه ویژه‌ای به جنبه‌های مثبت مطرح‌شده توسط آن دارند بر بهبودهای | R4 |

[1] Enabler
[2] Integration
[3] Connectivity
[4] Information Sharing

| | | | |
|---|---|---|---|
| حوزه فناوری اطلاعات، مانند مسائل امنیت سایبری[1]، به حوزه زنجیره‌های تأمین شده است. | | حاصل از آن تمرکز می‌کنند. این در حالی است که عدم شناخت نسبت به یک فناوری جدید و چالش‌های مترتب بر آن، می‌تواند اثراتی منفی به دنبال داشته باشد و مانع از ظهور بهبودهای حاصل از آن فناوری شود. در این بین، استفاده از فناوری‌های جدید حوزه ارتباطات و پردازش اطلاعات که در قالب فناوری‌های صنعت نسل ۴، می‌تواند منشأ بهبودهای فراوانی در حوزه زنجیره تأمین باشد. اما قبل از به‌کارگیری آن‌ها باید اطلاعات دقیقی در مورد چالش‌های اساسی وارد بر این حوزه کسب شود. | |
| مخاطرات حوزه سایبری می‌توانند منشأ بروز اتلاف‌های مالی و نارضایتی مشتریان در کوتاه مدت و همچنین خدشه به اعتبار سازمان، در درازمدت شوند. | Ghadge et. al(2019) | هریک از مخاطرات مطرح در زنجیره تأمین، فارغ از منشأ بروز آن‌ها، در صورت محقق شدن، اثرات نامطلوبی بر زنجیره تأمین و همچنین کلیت سازمان، خودند داشت. با توجه به ماهیت عملکرد زنجیره‌های تأمین دفاعی، اثرات مخرب ناشی از مخاطرات، تنها به اتلاف مالی محدود نخواهد شد و ممکن است اثرات جبران‌ناپذیری در کشور برجای بگذارد. لذا شایسته است در این مورد، سطح بالاتری از حساسیت، در نظر گرفته شود. | R5 |
| فناوری‌های فعال ساز انقلاب صنعتی نسل ۴، فرصت‌های بسیاری برای ایجاد بهبود در زنجیره‌های تأمین ایجاد کرده‌اند. اما استفاده از آن‌ها مستلزم در نظر | Sob et.al (2020) | دستیابی کامل به فرصت‌های موجود در استفاده از فناوری‌های صنعت نسل ۴ مستلزم شناسایی چالش‌های عمده موجود برای آن است. مسائل امنیت سایبری، در شمار مهم‌ترین چالش‌های مطرح برای به‌کارگیری مفاهیم صنعت نسل ۴، | R6 |

[1] Cyber Security

| | | | |
|---|---|---|---|
| گیری مسائل حوزه امنیت سایبری است. | | عنوان می‌شوند. اهمیت امنیت سایبری، با توجه به اهداف و شرایط کاری خاص زنجیره تأمین دفاعی، بیشتر از زنجیره تأمین تجاری است. | |
| در مورداستفاده از فناوری‌های فعال ساز انقلاب صنعتی نسل ۴، و امنیت سایبری آن‌ها، توجه به ۳ نکته، حائز اهمیت است:<br>• درنظرگیری ویژگی‌های خاص فناوری<br>• بررسی محیط پیاده‌سازی آن‌ها<br>• ارزیابی و توجیه مخاطرات سایبری | Sob et.al (2020) | علاوه بر شناسایی چالش‌های عمومی حوزهٔ امنیت سایبری صنعت نسل ۴، هریک از فناوری‌های مطرح در آن، ویژگی‌ها و شرایط کاری و همچنین مخاطرات خاصی دارند که باید موردتوجه قرار گیرد. میزان اهمیت این مخاطرات با توجه به صنعت موردمطالعه می‌تواند متفاوت باشد و لذا این تفاوت‌ها باید موردتوجه قرار گیرد. همواره در بحث مدیریت مخاطرات، در نظر گیری تمام مخاطرات موجود، با توجه به منابع محدودی که در اختیار سازمان قرار دارد، غیرممکن است. لذا باید یک برنامه اولویت‌بندی مخاطرات تدوین گردد تا به آن دسته از مخاطرات که اهمیت بیشتری دارند، توجه ویژه‌ای معطوف گردد. | R7 |
| به دلیل تفاوت‌های موجود میان زنجیره تأمین دفاعی (نظامی) و انواع تجاری آن، و همچنین اهمیت روزافزون امنیت سایبری، ارگان‌های دفاعی (نظامی) باید مجهز به ابزارهایی باشند که بتوانند به درستی، تأثیرات استفاده از فناوری‌های جدید را بسنجند. | Sob et.al (2020) | وجود ابزارهایی در جهت سهل‌الوصول بودن استفاده از یافته‌های حاصل از پژوهش‌های علمی، بسیار مهم است. از این نظر می‌توان مدل‌سازی را به عنوان روشی جهت ایجاد همسان فهمی بین پژوهشگر و مخاطبان اصلی پژوهش دانست. در پژوهش حاضر، استفاده از یک مدل در خروجی پژوهش، می‌تواند به استفادهٔ بهتر از یافته‌های حاصل از آن، کمک کند. | R8 |

| | | | |
|---|---|---|---|
| آمادگی[1] سازمان‌ها از مسائل مهمی است که قبل از پیاده‌سازی مفاهیم انقلاب صنعتی نسل ۴ باید موردتوجه مدیران قرار گیرد. | Sony et.al(2019) | ورود فناوری‌های جدید به هر سامانه، می‌تواند نویدبخش ظهور بهبودهای فراوانی در کارایی آن سامانه باشد. اما لازم است تا قبل از اجرایی شدن، تمامی چالش‌ها به نحو مؤثری موردبررسی قرار گیرند تا مزایای حاصل از به‌کارگیری فناوری‌های نوین به صورت کامل برای سازمان‌ها محقق شود. | R9 |
| برطرف کردن تمامی مخاطرات حوزه امنیت سایبری، به‌طور کامل، امکان‌ناپذیر است. با توجه به این موضوع، باید برنامه‌ریزی و اولویت‌بندی‌های لازم بر اساس نوع سازمان و نحوهٔ نگرش آن به موضوع امنیت سایبری، در دستور کار قرار گیرد. | Culot et.al(2019) | همواره در مدیریت مخاطرات، لزوم وجود برنامه‌های اولویت‌بندی مخاطرات، در اولویت قرار دارد. چراکه سازمان‌ها بودجه و منابع محدودی دارند و با توجه به این مسائل، پرداختن به تمامی مخاطرات، خارج از توان سازمان خواهد بود. مسائل و مخاطرات حوزه امنیت سایبری هم از این قاعده مستثنا نیستند و باید در مورد آن‌ها برنامه‌های اولویت‌بندی و همچنین تخفیف اثر مخاطرات، در نظر گرفته شود. | R10 |
| تهدیدات امنیت سایبری مترتب بر فناوری‌های انقلاب صنعتی نسل چهارم، هریک تأثیرات متفاوتی بر صنایع دارند که این تأثیرات باید برآورد و دسته‌بندی شوند. | Corallo & Lezzi(2020) | اجرای برنامه‌های اولویت‌بندی مخاطرات حوزه امنیت سایبری نیازمند وجود اطلاعات کافی از میزان هزینه تحمیل‌شده بر سازمان‌ها است. | R11 |
| فناوری‌های نوین مطرح در انقلاب صنعتی نسل ۴ به صورت مستقیم در تاب‌آوری زنجیره تأمین تأثیر ندارند اما مؤلفه‌های تاب‌آوری زنجیره تأمین، | Marinagi et.al(2023) | این پژوهش به بررسی تأثیرات مثبت فناوری‌های مطرح در انقلاب صنعتی نسل ۴ در تاب‌آوری زنجیره تأمین پرداخته است. این در حالی است که برخی از چالش‌ها نیز از طرف این فناوری‌ها به زنجیره تأمین تحمیل می‌شوند | R12 |

[1] Readiness

| | | | |
|---|---|---|---|
| می‌توانند به‌شدت تحت تأثیر انقلاب صنعتی نسل ۴ قرار بگیرند. | | که می‌توانند تاب‌آوری آن را تحت تأثیر قرار دهند. | |
| فناوری‌های مطرح در انقلاب صنعتی نسل چهارم، به طراحی زنجیره‌های تأمین تاب‌آور کمک می‌کنند. | Tortorella et al. (2021) | طراحی یک زنجیره تأمین تاب‌آور مستلزم در نظر گیری برخی ویژگی‌ها است که فناوری‌های نوین، می‌توانند در ایجاد آن‌ها مؤثر واقع شوند. در کنار این مسئله، توجه به چالش‌های عمده استفاده از فناوری‌های نوین، به عنوان یک موضوع اصلی باید مورد توجه قرار گیرد. | R13 |

## مرحله پنجم: یافته‌های پژوهش

در این مرحله سعی می‌شود پاسخ‌های مناسبی برای سؤالات پژوهش، بر اساس یافته‌های حاصل از پژوهش‌های بررسی‌شده، و همچنین انجام تحلیل بر روی آن‌ها، صورت‌بندی شود. در پاسخ به سؤال اول (RQ1)، جدول ۲ به معرفی مؤلفه‌های ۱۳ گانه تأثیرگذار در تاب‌آوری که شامل زنجیره تأمین می‌پردازد. همچنین پژوهش‌هایی مانند رحیمی و همکاران (۱۳۹۷) و کریمی زارچی و همکاران (۱۳۹۹) به بررسی و اولویت‌بندی این مؤلفه‌ها و ترسیم ارتباطات بین آن‌ها پرداخته‌اند. پس از شناسایی مؤلفه‌های تاب‌آوری زنجیره تأمین، اکنون به بررسی سؤال دوم که به ارتباط بین این مؤلفه‌ها و فناوری‌های صنعت ٤ اختصاص دارد، می‌پردازیم. اکثر پژوهش‌های پیشین بر این باورند که صنعت ٤ به خودی خود، عاملی جهت افزایش تاب‌آوری زنجیره تأمین نیست ولی مؤلفه‌های تاب‌آوری زنجیره تأمین به‌شدت تحت تأثیر صنعت ٤ و فناوری‌های آن هستند. در این بین، مؤلفه رؤیت پذیری، بیش‌ترین تأثیر را از مفاهیم صنعت ٤ می‌پذیرد و فناوری تجزیه و تحلیل داده‌های حجیم، به عنوان کاربردی‌ترین و بالغ‌ترین فناوری شناخته می‌شود. در پاسخ سؤال ۳ (RQ3) می‌توان گفت که مباحث مربوط به امنیت سایبری صنعت ٤، دارای اهمیت بالایی هستند و توجه به آن‌ها ضروری است. این

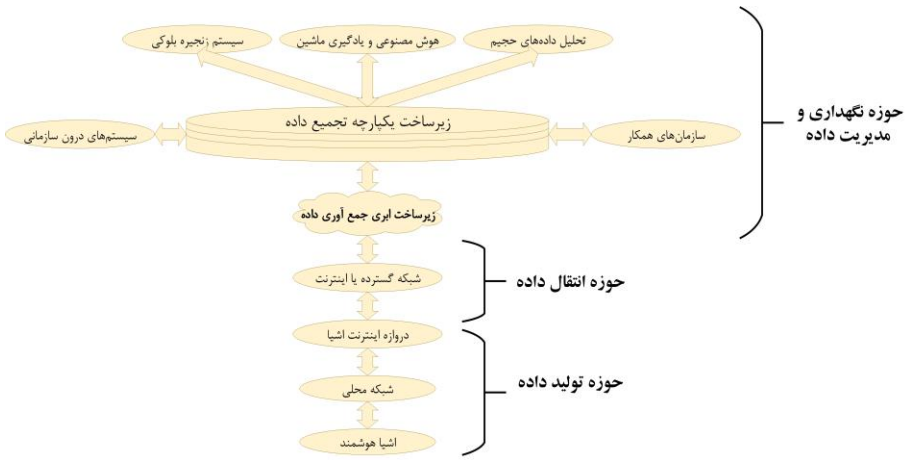
مباحث را می‌توان با توجه به ماهیت هر فناوری و همچنین مدل امنیتی سی آی آ دسته‌بندی نمود. جدول ٦ خلاصه این دسته‌بندی را نشان می‌دهد.

**جدول ۷-طبقه‌بندی تهدیدات وارد بر فناوری‌های صنعت ٤**

| عنوان فناوری | تهدید امنیتی | محرمانگی | جامعیت | دسترس‌پذیری |
|---|---|---|---|---|
| اینترنت اشیا | مسائل مربوط به احراز اصالت | * | * | |
| | حریم خصوصی | * | | |
| | آسیب‌پذیری‌های نرم‌افزاری | | | * |
| رایانش ابری | نشت داده | * | | |
| | آسیب‌پذیری‌های محیط مجازی | | | * |
| تحلیل داده‌های حجیم | حریم خصوصی | * | | |
| هوش مصنوعی و یادگیری ماشین | حریم خصوصی | * | | |
| زنجیره بلوکی | حریم خصوصی | * | | |
| | حملات کسوف | | | * |

آن گونه که از بررسی موارد امنیتی مترتب بر استفاده از فناوری‌های صنعت ٤ برمی‌آید، عمدهٔ این فناوری‌ها ریسک مربوط به کاهش محرمانگی اطلاعات را ایجاد نموده و با توجه به ایجاد وابستگی بین زنجیره تأمین دفاعی و فناوری‌های جدید، مخاطرات مربوط به نقض سرویس می‌تواند موجب بروز اختلال در فرایندها و جریان‌های زنجیره تأمین شود. نهایتاً سؤال چهارم (RQ4) به دنبال بررسی روش‌های موجود برای مقابله و کاهش اثر آسیب‌پذیری امنیت سایبری فناوری‌های صنعت چهارم است، علاوه بر شناسایی ویژگی‌های تک‌تک این فناوری‌ها، شناخت نحوهٔ ارتباط یا اثرگذاری آن‌ها نیز از اهمیت ویژه‌ای برخوردار است. لذا قبل از ورود به بحث اصلی این بخش، سعی می‌شود،

معماری کلی کاربردهای حاصل از صنعت ٤ به تصویر کشیده شود. شکل ۳ این معماری را نشان می‌دهد.




**شکل ۳- معماری اجزا مختلف در کاربردهای صنعت ٤**

همان‌گونه که در شکل ۲ قابل‌مشاهده است، داده‌های حاصل از اشیا هوشمند از طریق شبکه محلی و سپس از طریق دروازه اینترنت اشیا، به سمت شبکه اینترنت، هدایت می‌شوند. این داده‌ها در زیرساخت ابری تجمیع می‌شوند تا درنهایت کاربردهای لایه‌های بالاتر مورداستفاده قرار گیرند. همچنین داده‌های سامانه‌های داخلی سازمان، نظیر سامانه برنامه‌ریزی سازمانی به همراه داده‌های سازمان‌های همکار نیز باید برای ایجاد یک دید سرتاسری از زنجیره تأمین، در دسترس باشند. لذا وجود زیرساخت یکپارچه تجمیع داده، ضروری به نظر می‌رسد.

حال می‌توان به تفکیک هر بخش، مسائل مرتبط با امنیت سایبری را موردبررسی قرار داد. بر اساس جدول ٦، نگرانی عمده در زمینه استفاده از فناوری‌های نوین، بحث محرمانگی داده‌ها است. با توجه به این مسئله، استفاده از روش‌های مناسب رمزنگاری در سطوح مختلف، می‌تواند این مخاطره را تا حد زیادی کاهش دهد. این رمزنگاری باید در تمام مراحل اعم از تولید، انتقال و نگهداری داده‌ها وجود داشته باشد. جدول ۷ به صورت خلاصه، روش‌های امن سازی را در هر بخش نشان می‌دهد.

جدول ۸- راهکارهای حفظ محرمانگی داده‌ها در صنعت ٤

| حوزه | مرحله | گزینه موجود | ملاحظات |
|---|---|---|---|
| **اینترنت اشیا** | تولید داده | تولیدکنندگان معتبر و بزرگ | رعایت استانداردها<br>هزینه بالا |
| | | استفاده از روش‌های رمزنگاری در شبکه محلی | سرباره محاسباتی |
| **شبکه گسترده** | انتقال داده | استفاده از تونل امن و رمزگذاری شده | • افزایش حجم انتقالی<br>• سرباره‌های محاسباتی |
| | | استفاده از شبکه خصوصی گسترده | • سطح امنیت بسیار بالا<br>• هزینه‌های بسیار بالا |
| **پردازش ابری** | نگهداری داده | زیرساخت خصوصی پردازش ابری | • امنیت بالا<br>• هزینه بالای تأمین زیرساخت<br>• هزینه بالای نگهداری زیرساخت<br>• دشواری همکاری با سازمان‌های همکار |
| | | رمزگذاری داده‌های ذخیره‌شده | • نیاز به منابع بیشتر<br>• دشواری استفاده |

## نتیجه‌گیری

زنجیره‌های تأمین در معرض مخاطرات اجتناب‌ناپذیری هستند و انتخاب رویکردی تاب‌آور جهت رویارویی مؤثر با این مخاطرات، اقدامی حیاتی است که به بررسی چگونگی بازیابی وضعیت عملیاتی زنجیره تأمین، پس از بروز یک اختلال می‌پردازد. تمایل به استفاده از مفاهیم و فناوری‌های صنعت نسل چهارم می‌تواند نویدبخش مزایای فراوانی برای زنجیره‌های تأمین باشد. اما ایجاد یک رویکرد جامع نسبت به این مسئله و لحاظ نمودن اثرات جانبی مترتب بر آن، در هنگام سیاست‌گذاری‌های کلان در حوزه زنجیره تأمین، امری ضروری است که یکی از اثرات جانبی این کار، تأثیرگذاری بر تاب‌آوری زنجیره تأمین می‌باشد. در این پژوهش با توجه به محرمانگی و پیچیدگی زنجیره تأمین

دفاعی به بررسی رویکرد تاب‌آوری در این زنجیره پرداخته شد. هرچند قابلیت‌های صنعت نسل چهارم و مفاهیم مطرح در آن، به عنوان یک عامل ایجاد تاب‌آوری شناخته نمی‌شوند اما مؤلفه‌های ایجاد تاب‌آوری زنجیره تأمین دفاعی از فناوری‌های نسل چهارم تأثیر می‌پذیرند. پس از تحلیل به‌عمل‌آمده در این حوزه مشخص گردید که ویژگی «رؤیت پذیری»، بیش‌ترین تأثیرپذیری را از فناوری‌های صنعت نسل چهارم دارد و همچنین، «تحلیل داده‌های حجیم»، بیش‌ترین اثرگذاری را بر تاب‌آوری زنجیره تأمین ایجاد می‌نماید. به‌وضوح روشن است که مسئله امنیت سایبری، با ورود فناوری‌های صنعت نسل چهارم در زنجیره تأمین دفاعی، اهمیتی بیش از پیش پیدا نموده و بر همین اساس، حملات مربوط به نقض محرمانگی داده‌ها و نقض سرویس، مهم‌ترین حملات نوپدید حاصل از صنعت نسل چهارم در زنجیره تأمین دفاعی هستند و در این بین، مسئله محرمانگی داده‌ها بیش از سایر مسائل حوزه امنیت سایبری، باید موردتوجه قرار گیرد. در این پژوهش، حفظ محرمانگی در سه سطح تولید، انتقال و ذخیره‌سازی داده‌ها معرفی‌شده و راهکارهای لازم جهت پیاده‌سازی و همچنین ملاحظات مربوط به هریک از این راهکارها مطرح گردید. هریک از این راهکارها، هزینه‌هایی را برای سازمان‌ها ایجاد می‌کنند و مدیران، با توجه به سطح محرمانگی داده‌های خود باید نسبت به انتخاب روش مناسب برای سازمان متبوع، اقدام نمایند.

پیشنهاد اجرایی: اداره‌های فناوری اطلاعات سازمان‌های نیروهای مسلح، ضمن تأکید بر سیاست‌گذاری لازم در خصوص استقرار کلان داده در بستر امن سایبری با حفظ موازین محرمانگی و تعریف سطوح دسترسی متقاضیان و تأمین‌کنندگان ملزومات و مایحتاج نظامی در همه سطوح بهره‌بردار، تدابیر لازم را برای دفع مخاطراتی همچون حملات مربوط به نقض محرمانگی داده‌ها و نقض سرویس، اتخاذ نموده تا ارتقاء تاب‌آوری در زنجیره تأمین دفاعی فراهم گردد.

پیشنهاد پژوهشی: پیشنهاد می‌شود در ادامه این پژوهش، مدلی به جهت ارزیابی میزان تأثیرگذاری هریک از راهکارهای موجود از نقطه‌نظر سطح امنیت، تأثیر در تاب‌آوری زنجیره تأمین دفاعی کشور و همچنین میزان هزینه‌ای که پیاده‌سازی آن برای سازمان‌ها دارد، تبیین شود.

## منابع

رحیمی، اکبر، راد، عباس، عالم تبریز، اکبر، و موتمنی، علیرضا. (۱۳۹۷). **ارائه مدل ساختاری تفسیری زنجیره تأمین تاب‌آور در صنایع دفاعی ایران. مدیریت نظامی**، ۱۸(۷۱)، ۷۰-۳۱.

کریمی زارچی، محمد، معبودی، حامد، فتحی، محمدرضا و خسروی، ابوالفضل. (۱۳۹۹). «**ارائه مدل زنجیره تأمین دفاعی تاب‌آور با رویکرد مدل‌سازی ساختاری- تفسیری (موردمطالعه صندوق حمایت از فناوری)**». بهبود مدیریت، ۱٤(۲)، ٦۷-۹۱.

عابدی جعفری، عابد و امیری، مجتبی. (۱۳۹۸). **فرا ترکیب، روشی برای سنتز مطالعات کیفی. روش‌شناسی علوم انسانی**، ۲۵(۹۹)، ۸۷-۷۳.

مبینی دهکردی، علی، کشتکارهراتکی، مهران، (۱۳۹۵)، **فراترکیب مدل‌های نوآوری اجتماعی**، فصلنامه برنامه‌ریزی رفاه و توسعه اجتماعی، سال هفتم، شماره ۲٦، بهار ۱۳۹۵

Ambore, B., Gupta, A. D., Rafi, S. M., Yadav, S., Joshi, K., & Sivakumar, R. (2022). A Conceptual Investigation on the Image Processing using Artificial Intelligence and Tensor Flow Models through Correlation Analysis. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*.

Bartodziej, C. J. (2017). The Concept Industry 4.0. In *Springer eBooks*. Lu, D. (2011). *Fundamentals of Supply Chain Management*.

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for Industry 4.0: A Comprehensive Review. *IEEE Access*, *8*, 79764–79800.

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2021). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management*, *27*(1), 30–53.

Corallo, A., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, *114*, 103165.

Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing Industry 4.0 Cybersecurity Challenges. *IEEE Engineering Management Review*, *47*(3), 79–86.

Deepa, N., Pham, Q., Nguyen, D. C., Bhattacharya, S., Prabadevi, B., Gadekallu, T. R., Maddikunta, P. K. R., Fang, F., & Pathirana, P. N. (2022). A survey on blockchain for big data: Approaches, opportunities, and future directions. *Future Generation Computer Systems*, *131*, 209–226.

Dutta, P., Choi, T., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation Research Part E-logistics and Transportation Review*, *142*, 102067.

Gammelgaard, B., & Nowicka, K. (2023). Next generation supply chain management: the impact of cloud computing. *Journal of Enterprise Information Management*.

Hugos, M. H. (2018). Essentials of supply chain management: John Wiley & Sons.

Ham, J. V. D. (2021). Toward a better understanding of "Cybersecurity". Digital Threats: Research and Practice, 2(3), 1-3.

Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys*, *55*(14s), 1–40.

Helo, P., & Hao, Y. (2021). Artificial intelligence in operations management and supply chain management: an exploratory case study. *Production Planning & Control*,

*33*(16), 1573–1590.

Jang, S., Jeong, J., Lee, J. H., & Choi, S. (2023). Digital Twin for intelligent network: data lifecycle, digital replication, and AI-based optimizations. *IEEE Communications Magazine*, 1–7.

Louis, M., & Pagell, M. (2018). Categorizing Supply Chain Risks: review, integrated typology and future research. In *Springer series in supply chain management* (pp. 329–366).

Marinagi, C., Reklitis, P., Trivellas, P., & Sakas, D. P. (2023). The Impact of Industry 4.0 Technologies on Key Performance Indicators for a Resilient Supply Chain 4.0. *Sustainability*, *15*(6), 5185.

Nath, S. V., Dunkin, A., Chowdhary, M., & Patel, N. (2020). *Industrial Digital Transformation: Accelerate Digital Transformation with Business Optimization, AI, and Industry 4. 0*. Packt Publishing.

Ozenc, S. C. Y., Er, M., & Fırat, S. Ü. O. (2022). Risks in Supply Chain 4.0: A Literature review study. In *Springer eBooks* (pp. 163–177).

Qader, G., Junaid, M., Abbas, Q., & Mubarik, M. S. (2022). Industry 4.0 enables supply chain resilience and supply chain performance. *Technological Forecasting and Social Change*, *185*, 122026.

Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and Solutions Survey. *Sensors*, *22*(19), 7433.

Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). IntruDTree: a machine learning based Cyber security intrusion detection model. *Symmetry*, *12*(5), 754.

Sony, M., & Naik, S. R. (2019). Ten Lessons for Managers While Implementing Industry 4.0. *IEEE Engineering Management Review*, *47*(2), 45–52.

Spieske, A., & Birkel, H. (2021). Improving supply chain resilience through industry 4.0: A systematic literature review under the impressions of the COVID-19 pandemic. *Computers & Industrial Engineering*, *158*, 107452.

Vaidya, S., Ambad, P. M., & Bhosle, S. (2018). Industry 4.0 – A Glimpse. *Procedia Manufacturing*, *20*, 233–238