فصلنامه علوم و فنون نظامی
سال هجدهم، شماره ۶۲، زمستان ۱۴۰۱
صص ۱۰۱- ۷۵

تاریخ دریافت: ۱۴۰۱/۰۷/۰۴
تاریخ پذیرش: ۱۴۰۱/۱۲/۲۰

الزامات امنیتی کاربست لجستیک هوشمند در سازمان‌های دفاعی

حمیدرضا ضرغامی*[۱]
محمود غلامی[۲]
امیر صادقی[۳]
جعفر محققی[۴]

نوع مقاله: پژوهشی

چکیده

لجستیک هوشمند یکی از زمینه‌های پژوهشی به روز است. مبدأ بیشتر فناوری‌های نوین در حوزه‌ی فناوری اطلاعات و ارتباطات تجاری و نظامی در اختیار سازمان‌های جاسوسی و امنیتی است. لذا امنیت اطلاعات عاملی حیاتی برای سازمان‌های نظامی است. بر این مبنا در این پژوهش به بررسی و شناسایی الزامات امنیتی مرتبط با پیاده‌سازی و استفاده از این فناوری‌ها پرداخته می‌شود. روش پژوهش حاضر توصیفی- پیمایشی بوده و در تحلیل داده‌ها از آمار توصیفی و استنباطی با استفاده از نرم‌افزار اس. پی. اس. اس. استفاده شده است. پس از مرور جامع مبانی نظری و پیشینه پژوهش‌های انجام شده مرتبط با این حوزه، مدل مفهومی مربوط به الزامات امنیتی، طراحی و سپس با استفاده از پرسشنامه محقق‌ساخته به بررسی نظرات خبرگان امنیتی- لجستیکی و استادان این حوزه در یک سازمان منتخب دفاعی پرداخته شد و با توجه به نرمال نبودن داده‌ها، نتایج آزمون دوجمله‌ای نشان داد که الزامات شناسایی شده با سطح اطمینان بالای ۹۹ درصد مورد تأیید است. از جمله نتایج پژوهش می‌توان به پذیرش تمام الزامات امنیتی شناسایی شده برای استفاده از فناوری‌های نوین قابل بهره‌برداری در لجستیک هوشمند، اشاره کرد. اصلی‌ترین نوآوری پژوهش حاضر این است که علاوه بر بررسی مبانی و مفهوم‌سازی برای انجام پژوهش‌های گسترده در حوزه لجستیک هوشمند و ابعاد آن، برای اولین بار به شناسایی الزامات امنیتی موردنیاز برای استفاده فناوری‌های این حوزه در سازمان‌های دفاعی پرداخته است.

واژه‌های کلیدی:
لجستیک هوشمند، فناوری‌های نوین، سازمان دفاعی، هوش مصنوعی، اینترنت اشیاء، بلاک‌چین.

[۱] استادیار مهندسی صنایع دانشگاه علوم و فنون هوایی شهید ستاری، تهران، ایران.
[۲] استادیار مدیریت بازرگانی دانشگاه علوم و فنون هوایی شهید ستاری، تهران، ایران.
[۳] استادیار مدیریت بازرگانی دانشگاه علوم و فنون هوایی شهید ستاری، تهران، ایران.
[۴] کارشناس ارشد آماد دانشگاه علوم و فنون هوایی شهید ستاری، تهران، ایران.
* نویسنده مسئول: Email: zarghami.hamid@gmail.com

DOI: 10.22034/QJMST.2023.539824.1593

مقدمه

رشد سریع فناوری‌های نوین مانند هوش مصنوعی، زنجیره بلوکی، رایانش ابری، اینترنت اشیاء و مواردی از این دست سبب ایجاد نوآوری‌هایی در لجستیک و بروز و ظهور زنجیره‌های تأمین هوشمند شده است (Kuo et al. 2021). مقصود اساسی هوشمندی در زنجیره تأمین و لجستیک، استفاده از فناوری به منظور ارتقاء هوشمندی و ویژگی‌هایی همچون خودکارسازی[1]، شفافیت[2] و ایجاد لینک ارتباطی[3] در این عرصه است (Uckelmann, 2008).

با پیشرفت فناوری‌های حوزه هوشمندی، خدمات زنجیره تأمین و لجستیک هوشمند به صورت گسترده‌ای توسط شرکت‌ها و مؤسسات شناخته شده‌ای همچون اَپل، تِسلا، آمازون، علی بابا و مجموعه لجستیکی جَی. دی. [4] به‌کارگرفته شده است و با توجه به تأثیرات شگرف لجستیک و زنجیره تأمین هوشمند در توسعه صنایع، بسیاری از کشورها سیاست‌های حمایتی‌ای برای توسعه و حمایت از ارتقاء هوشمندی در حوزه لجستیکی انجام داده‌اند. به‌عنوان مثال در سال ۲۰۱۵، وزارت تجارت چین برنامه‌ای موسوم به «برنامه اجرایی برای توسعه سیستم‌های توزیع لجستیک هوشمند» را وضع و تعدادی از شهرهای هوشمند را برای اجرایی‌سازی این برنامه انتخاب کرده است. به ویژه در طی ۳ سال اخیر برخی کشورها همچون چین، آمریکا، آلمان، انگلستان و ژاپن نیز سیاست‌های حمایتی برای افزایش هوشمندی در زنجیره تأمین و لجستیک اتخاذ کرده‌اند (Liu et al. 2021).

از نقطه نظر پژوهش‌های دانشگاهی نیز به نظر می‌رسد که این حوزه در سالیان اخیر به یک موضوع بسیار داغ پژوهشی تبدیل شده است. با جستجوی ساده عبارت Intelligent Logistics در گوگل اسکالِر برای بازه از سال ۲۰۱۷ تاکنون، بیش از ۳۵۰۰۰ مقاله نمایه شده مشاهده می‌شود. این در حالی است که تا این تاریخ (اول مرداد ۱۴۰۰) با جستجوی عبارت «"لجستیک هوشمند" یا "زنجیره تأمین هوشمند"» در پایگاه داده یادشده، صرفاً یک مقاله به زبان فارسی یافت می‌شود که البته آن هم در حوزه لجستیک و زنجیره تأمین دفاعی است و توسط شاه‌حیدری و حضوری (۱۳۹۷) با هدف شناسایی عوامل مؤثر بر ایجاد یک زنجیره تأمین هوشمند صنعت نظامی بر پایه دفاع و اقتصاد دانش‌بنیان انجام شده است. بر اساس یافته‌های پژوهش یادشده، عوامل هزینه، فناوری، زیرساخت‌های نرم‌افزاری و سخت‌افزاری، استاندارد،

[1] Automation
[2] Transparency
[3] Connection
[4] JD

مشخصات بین‌المللی و امنیت بر هوشمندسازی زنجیره تأمین صنعت نظامی تأثیرگذار می‌باشند. بر این مبنا شکاف پژوهش در حوزه لجستیک هوشمند در کشور مشهود است.

یکی از جنبه‌های مهم در لجستیک نظامی، حفظ امنیت و هوشمندی در شرایط تبادل اطلاعات و اقلام مورد نیاز سازمان می‌باشد (شاه‌حیدری و حضوری، ۱۳۹۷). با توجه به ایجاد زیرساخت‌های هوشمندی لجستیکی در سازمان‌های نظامی به‌دلیل بهره‌گیری از فناوری‌های نوین اطلاعاتی، امنیت سایبری حوزه لجستیکی اهمیت دوچندانی پیدا کرده است. به‌گونه‌ای که خلل در عملیات لجستیکی در شرایط تولید و پشتیبانی منجر به شکست در تولید و عملیات‌های نظامی می‌گردد. از این رو در این پژوهش با استفاده از بررسی مقالات و متون علمی تدوین شده در حوزه لجستیک هوشمند و امنیت سایبری این حوزه، مؤلفه‌های مؤثر شناسایی شده و سپس با استفاده از نظرات خبرگان به تأیید و اولویت‌بندی عوامل مربوطه پرداخته خواهد شد. ضرورت پژوهش این است که با توجه به لزوم استفاده از فناوری‌های نوین و لجستیک هوشمند دربخش دفاع، حوزه امنیتی بتواند نظریه تخصصی در رابطه با ایجاد الزامات موردنیاز بهره‌برداری هوشمندانه و اثربخش و در عین حال ایمن از این قابلیت را ایجاد و در زمان لزوم مورد استفاده قرار دهد. با توجه به بررسی به عمل آمده در پایگاه‌های اطلاعاتی ایران داک[1]، مگ ایران[2]، نور مگز[3]، اس‌ای دی[4] و سیویلیکا[5] تاکنون پژوهشی با این موضوع در کشور انجام نشده است. بررسی پژوهشگران در منابع علمی مرتبط با لجستیک و لجستیک هوشمند سبب شکل‌گیری مدل مفهومی پژوهش به صورت شکل ۱ شده است. بر این مبنا لجستیک سازمان‌ها به چهاربخش استراتژیک دسته‌بندی می‌شود که عبارتند از: «لجستیک تأمین مواد اولیه»، «لجستیک انبارداری»، «لجستیک درون شرکتی (وسایل نقلیه AVG)» و «لجستیک توزیع» (محققی، ۱۳۹۹). در لایه بعدی مدل و پژوهش حاضر و مبتنی بر مبانی علمی و نظری و پیشینه پژوهش، فناوری‌های مرتبط با هر یک از این ابعاد و سپس الزامات امنیتی موردنیاز برای کاربست هر یک از فناوری‌ها در سازمان‌های دفاعی مورد بررسی و تعیین می‌شود. بنابراین سؤال‌های اصلی و فرعی پژوهش به صورت زیر است:

---

[1] https://www.irandoc.ac.ir
[2] http://magiran.com
[3] http://www.noormags.ir/
[4] http://www.sid.ir/
[5] https://www.civilica.com

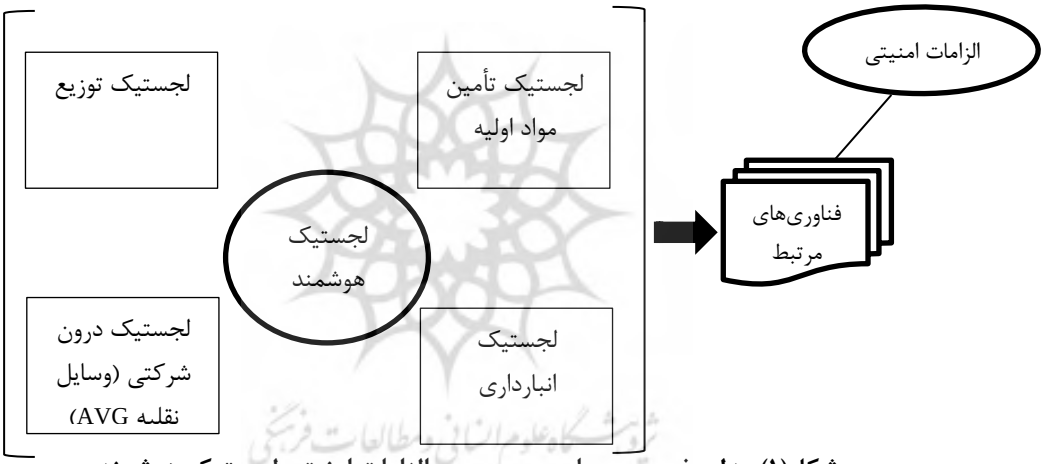
سؤال اصلی: الزامات امنیتی بهره‌برداری از لجستیک هوشمند دربخش دفاع شامل چه مواردی است؟

سؤال‌های فرعی:

۱- عوامل و الزامات امنیتی لجستیک هوشمند در سازمان‌های عمومی و دفاعی مبتنی بر مبانی نظری و مطالعات کتابخانه‌ای شامل چه مواردی است؟

۲- الزامات امنیتی بهره‌برداری از فناوری‌های مرتبط با لجستیک هوشمند دربخش دفاعی مبتنی بر نظرات خبرگان آمادی و امنیتی شامل چه مواردی است؟

۳- اولویت الزامات امنیتی بهره‌برداری از فناوری‌های مرتبط با لجستیک هوشمند دربخش دفاعی مبتنی بر نظرات خبرگان آمادی و امنیتی چگونه است؟



شکل(۱) مدل مفهومی و چارچوب محوری الزامات امنیتی لجستیک هوشمند

مبانی نظری

مدیریت زنجیره‌ی تأمین

زنجیره تأمین، یک کل به‌هم پیوسته است که واحدهای کاری مختلف اجزای تشکیل‌دهندهٔ آن به‌شمار می‌روند (طالبی و همکاران، ۱۳۹۰). در دههٔ ۱۹۵۰ کارشناسان با مطالعهٔ رابطهٔ داخلی بین انبارداری و حمل ونقل و یکپارچه‌سازی آنها توانستند موجودی انبار خود را کاهش دهند. حاصل این مطالعات مدیریت توزیع نام گرفت. با چنین نگرشی رویکرد مدیریت زنجیره تأمین پا به عرصه وجود نهاد (جعفر نژاد و همکاران، ۱۳۹۲). به عبارتی زنجیره تأمین نتیجهٔ به هم پیوستن حلقه‌های عملیاتی مختلف است که در ابتدای آن تأمین‌کنندگان و در انتهای آن مشتریان (و در سیستم‌های دفاعی یگان‌های مصرف‌کننده) قرار دارند. از نقطه‌نظر آیرس

(۱۳۹۰)، مدیریت زنجیره تأمین، طراحی، نگهداری و اجرای فرآیندهای زنجیرهٔ تأمین به منظور تأمین نیازمندی‌های مصرف‌کننده نهایی است.

لجستیک و زنجیره تأمین هوشمند

کلمه هوشمندی به مجموعه‌ای از ابزارها و امکانات و تخصص‌ها از قبیل مفاهیم مهندسی فناوری اطلاعات، فناوری‌های نرم‌افزاری، سخت‌افزاری و مخابراتی اطلاق می‌شود که به‌صورت هماهنگ و مجتمع به‌منظور بهبود کارآیی و ایمنی در سیستم لجستیک به کار گرفته می‌شود (Zhang et al. 2019).

لجستیک هوشمند عبارت است از سیستم‌های لجستیکی که فناوری‌های اطلاعات و ارتباطات و کنترل را برای بهبود عملکرد شبکه‌های لجستیکی به‌کار می‌گیرند. ابزارهای لجستیک بر مبنای سه مشخصه اطلاعات و ارتباطات و تجمیع استوار هستند که به‌مدیران شبکه‌های لجستیکی کمک می‌کنند تا تصمیمات بهتر و متناسب‌تری با شرایط موجود بگیرند. ابزارهای لجستیک هوشمند از طریق بهبود عملکرد سیستم‌ها باعث صرفه‌جویی در وقت، حفظ محصولات، و بهبود کیفیت و محیط‌زیست و افزایش کارآیی فعالیت‌های اقتصادی می‌شود.

سیستم لجستیک هوشمند به‌معنای به‌کارگیری فناوری‌های نوین از قبیل پردازش اطلاعات، الکترونیک، ارتباطات و سیستم‌های کنترل و دیگر فن‌آوری‌های ارتباطی و استراتژی‌های مدیریت به‌گونه‌ای هماهنگ و یکپارچه جهت ارتقاء سطح ایمنی و کارایی و ارزانی در لجستیک است (Zhang et al. 2019).

لجستیک و زنجیره تأمین هوشمند که با استفاده از مواردی چون داده‌های عظیم، رایانش ابری، حسگرهای ارزان قیمت (کوچک‌تر، دقیق‌تر)، هوش‌مصنوعی، اینترنت اشیاء و... توصیف می‌شود، سعی در ارتقای بهره‌وری حوزه لجستیکی با کاربست فناوری‌های نوین یادشده را دارد. لجستیک هوشمند یک صنعت عظیم است که دارای شبکه‌ی پیچیده‌ای در سراسر جهان است. درآمدهای این صنعت در حدود ۸ تریلیون دلار تخمین زده شده است. انتظار می‌رود تا سال ۲۰۲۴ افزایش داشته و به ۱۵/۵ تریلیون دلار برسد (محققی، ۱۳۹۹).

لجستیک که به‌عنوان عنصر اصلی مدیریت زنجیره تأمین شناخته می‌شود؛ با چالش‌های بسیار زیادی برای فعالیت و عملیات مواجه است. برخی از این چالش‌های اساسی به‌شرح زیر می‌باشند.

۱. کارآیی کسب‌وکار: تمرکز بر "چابکی" در زنجیره‌های تأمین صنعتی، برای کاهش هزینه و بهبود عملکرد تحویل افزایش یافته است. تلاش اصلی برای کاهش ذخایر موجودی و انتقال به سمت مدل‌های تولید به‌هنگام است.

۲. محیط عملیاتی نامطمئن: مسیرهای حمل و نقل شلوغ و دسترسی پیچیده که منجر به عدم قطعیت در زمان جمع‌آوری و تحویل کالاها می‌شود.

۳. نیازهای خصوصی شده مشتری‌ها: مشتریان نیز از نظر ترکیب سفارش و گزینه‌های تحویل خواستار تغییر سفارش‌ها پس از سفارش و حتی ارسال هستند.

۴. تغییر و تنوع در بازار: با ظهور خرید اینترنتی و خرید مستقیم از انبارهای تأمین کننده، افزایش دامنه‌های سفارش، افزایش تعداد سفارش‌های کوچک و مشتریانی که خواستار زمان تحویل دقیق با ضمانت‌های قوی هستند.

این چالش‌ها پیچیده و در بعضی مواقع متضاد هم هستند. مواجه شدن با هر یک از این چالش‌ها به تلاش قابل توجهی ازبخش ارائه دهنده لجستیک نیاز دارد که باید به سمت کارآیی اقتصادی، انعطاف‌پذیری، مشتری‌مداری و سازگاری حرکت کند.

این تغییرات و هماهنگی‌ها باید با هم ترکیب و هماهنگ باشند تا بتوان به اهداف مورد نظر رسید. هوشمندسازی لجستیک برای مواجه با این تغییرات بسیار راه‌گشا خواهد بود (McFarlane et al. 2016). در مبانی نظری پژوهش‌های این حوزه از دو واژه Smart و Intelligent به‌صورت موازی با هم استفاده شده و هر دو عبارت «زنجیره تأمین هوشمند/ SSC» و «سیستم‌های لجستیک هوشمند/ ILS» مطرح می‌باشند (Liu et al. 2021).

برخی از پژوهشگران چارچوب‌های نظام‌مند و پژوهش‌های تئوریکی برای توسعه مفاهیم مربوط به لجستیک هوشمند ارائه نموده‌اند (Chen et al. 2019 و Liu et al. , 2020). تعداد زیادی نیز به انجام پژوهش با رویکرد تجربی در این حوزه پرداخته‌اند (مانند: Zeng et al. ,2020 و Liu et al. , 2020b)، برخی دیگر به مدل‌سازی روش‌های بهینه‌سازی پرداخته‌اند (مانند: Li 2020). به‌طور خاص کاربست فناوری‌های نوظهور نیز در این عرصه در پژوهش‌های متعددی در سالیان اخیر مورد مطالعه قرار گرفته است (به عنوان مثال «رایانش ابری» توسط لی و همکاران در سال ۲۰۱۹، «اینترنت +» توسط جیان[1] و همکاران درسال ۲۰۱۹، «زنجیره بلوکی» توسط چوی[2] و همکاران در سال ۲۰۱۹، «کلان داده» توسط فِنگ و شانتی کومار[3] در سال ۲۰۱۸ و

[1] Jian
[2] Choi
[3] Feng and Shanthikumar

چوی و همکاران در سال ۲۰۱۸، «هوش مصنوعی» توسط داورن[1] درسال ۲۰۲۰، «اینترنت اشیاء» توسط وانگ[2] و همکاران در سال ۲۰۲۰، و...).

امنیت سایبری

جنگ اطلاعاتی یک اصطلاح نسبتاً جدید است که طی سال‌های گذشته به واژه‌نامه اصطلاحات نظامی وارد شده‌است. البته مفهوم استفاده از اطلاعات در جنگ قدمت طولانی دارد. ظهور اصطلاح جنگ اطلاعاتی و اهمیت روزافزون آن احتمالاً با انقلاب اطلاعات ارتباط مستقیم دارد. باور همگانی به این صورت است که چنین انقلابی آن‌قدر قدرتمند و دامنه تأثیر آن گسترده است که می‌تواند بعد جدیدی در جنگ و یا حتی سبک جدیدی از جنگ را تعریف کند. مگان برنز در سال ۱۹۹۹ تلاش کرد که مؤلفه مشترک همه تعاریف صاحب‌نظران را در یک مجموعه گردآوری کند، وی نتیجه می‌گیرد که: "جنگ اطلاعاتی، طبقه یا مجموعه‌ای از تکنیک‌ها شامل جمع‌آوری، انتقال، حفاظت، ممانعت از دسترسی، ایجاد اغتشاش و افت کیفیت در اطلاعات است که از طریق آن یکی از طرفین درگیر نسبت به دشمنان خود به مزیتی چشمگیر دست یافته و آن را حفظ می‌کند "(Kermer et al. , 2019). در دهه ۱۹۹۰ در محافل دفاعی و نظامی آمریکا یک بحث داغ درباره ضرورت تغییر دکترین و سیاست نظامی برای انطباق با الزامات و ویژگی‌های عصر اطلاعات شکل گرفت. در آن زمان هیچ تفاهمی به دست نیامد و دقیقاً معلوم نبود که چه اصطلاحات و تعاریفی مناسب‌تر از بقیه هستند. کارشناسان مختلف مفاهیم آشنای جنگ فرماندهی و کنترل، جنگ الکترونیک، عملیات اطلاعاتی، بعد پنجم جنگ درکنار چهار بعد زمین، دریا، هوا، و فضا را پیشنهاد می‌دادند و شاخه‌های مختلف نیروهای مسلح آمریکا هر یک تعریف خاص خود را تبلیغ می‌کردند (Ellram et al. 2018). البته تعریف مدنظر نیروی هوایی آمریکا، به‌عنوان یک نیروی آینده‌نگر و پیش‌رو، بیشتر جلب توجه کرده و دیگر نیروهای مسلح با آن تاحدودی موافق بودند. فرماندهان ارشد نیروی هوایی در سندی رسمی تحت عنوان «سنگ بنای جنگ اطلاعاتی»، تعریف زیر را مطرح کردند: "جنگ اطلاعاتی عبارت است از هر اقدامی در راستای ممانعت از دسترسی، بهره‌برداری، سوءاستفاده، ایجاد اختلال و فساد و در نهایت تخریب و حذف اطلاعات دشمن و کارکردهای آن و همچنین حفاظت در برابر اقدامات مشابه دشمن" (Ricci & Baggili, 2019).

[1] Dauvergne
[2] Wang

پیشینه‌های پژوهش

پژوهش‌های بسیار متنوع و متعددی با تأکید بر اهمیت استفاده از فناوری‌های نوین و مقوله‌های مرتبط با امنیت سایبری در حوزه لجستیک هوشمند انجام و به ثبت رسیده است که با توجه به وسعت و فراوانی حجم آنها، تنها به ذکر برخی از این پژوهش‌ها در قسمت‌های قبل و به‌ویژه‌بخش مربوط به لجستیک و زنجیره تأمین هوشمند، پرداخته شد[1] و در ادامه به‌صورت خلاصه چارچوب مستخرج از پژوهش‌های پیشین در جدول ۱ ارائه شده است. لازم بذکر است که چنانکه در مدل مفهومی پژوهش نیز عنوان شد، لجستیک سازمان‌ها به چهاربخش استراتژیک دسته‌بندی می‌شود که عبارتند از: «لجستیک تأمین مواد اولیه»، «لجستیک انبارداری»، «لجستیک درون شرکتی (وسایل نقلیه AVG)» و «لجستیک توزیع» (محققی، ۱۳۹۹).

جدول (۱) الزامات امنیتی مستخرج از پیشینه پژوهش

نوع لجستیک	نوع فناوری	الزامات امنیت سایبری کاربست فناوری	منابع
لجستیک تأمین مواد[2]	فناوری بلاک چین[3]	۱- استفاده از فناوری‌های نوین جهت رصد فعالیت‌های لجستیکی در سازمان	Petit, 2018; chen et al. 2021
		۲- ایجاد زیرساخت‌های مناسب در حفظ امنیت اطلاعاتی لجستیک هوشمند	Chen et al. 2021; Nasiri & Pourmohammadzade 2015
		۳- ایجاد و طرح‌ریزی زیرساخت‌های مناسب جهت بهره‌گیری از فناوری‌های بومی (استفاده از اینترانت و اینترنت‌های محلی و بومی مانند شبکه گسترده (LAN	Ku 2017; Rasouli 2019; Yuen et al. 2018
		۴- طراحی و اجرای شبکه‌های رمزنگاری شده و سلولار مناسب برای افزایش امنیت شبکه	Zhang et al. 2018
		۵- ایجاد زمینه پشتیبان‌گیری دوره‌ای از اطلاعات فعالیت‌های لجستیکی	Yuen et al. 2018

[1] پژوهشگران محترم و علاقمندان به مطالعه دقیق این پیشینه و موارد مندرج در جدول ۱، می‌توانند جزئیات نتایج این پژوهش‌ها را در پایان‌نامه محققی (۱۳۹۹) مشاهده نمایند.

[2] Procurement or Supplying Logistics

[3] Blockchain Technology

نوع لجستیک	نوع فناوری	الزامات امنیت سایبری کاربست فناوری	منابع
		۶- ایجاد زمینه دسترسی به اطلاعات مورد نیاز لجستیک هوشمند با استفاده از بسترهای فناوری اطلاعات برای اعضای زنجیره تأمین	Xu et al. 2018a; Yuen et al. 2018
		۷- اجرا و پیاده‌سازی مدیریت دانش در تجزیه و تحلیل داده‌های لجستیکی	Xu et al. 2018a
		۸- استفاده از فناوری‌های نوین ماهواره‌ای بومی در مراکز حیاتی	Yuen et al. 2018
	فناوری اینترنت اشیاء	۹- طراحی و اجرای سیستم ارزیابی و کنترل دوره‌ای مناسب از حسگرهای اینترنت اشیاء	Rasouli 2019; Zhang et al. 2018
		۱۰- استفاده از دیواره‌های آتش[1] مناسب و بومی	Khoo. 2019
		۱۱- استفاده از پروتکل‌های رمزنگاری شده مانند بلاک‌چین[2]	Poster. 2018
		۱۲- توسعه خطوط اینترانت در سطوح لجستیکی سازمان	Ku. 2017
		۱۳- استفاده از سیستم ماهواره‌ای داخلی	مارکلائی(۱۳۹۵)
		۱۴- استفاده از سیستم‌های back up در توسعه خطوط ارتباطی	Tao. 2014
		۱۵- نصب دستگاه‌های تولید فرکانسی مناسب (خارج از استاندارد)	Zhang et al. 2018;
		۱۶- ایجاد بستر و سدهای امنیتی مناسب جهت جلوگیری از نفوذ اطلاعاتی در سیستما	Zhang et al. 2018;
		۱۷- طراحی و اجرای زیرساخت‌های پوشش بافرهای امنیتی[3] در فرآیند لجستیک هوشمند	Xu et al. 2018b

[1] firewall
[2] block chain
[3] Security Buffers Overflow

نوع لجستیک	نوع فناوری	الزامات امنیت سایبری کاربست فناوری	منابع
لجستیک انبارداری	فناوری RFID	۱۸- طراحی و اجرای آموزش مفاهیم اینترنت اشیاء و سطح دسترسی به اطلاعات در فرآیندهای لجستیکی بین اعضای زنجیره تأمین	افشاری ۱۳۹۶ ; Khoo Huang & Yan 2019 ; 2018
		۱۹- ایجاد زیرساخت‌های انتقال نتایج ارزیابی‌ها به گیرنده‌ها و اعضای زنجیره تأمین و رصد دقیق و برخط تگ‌های اطلاعاتی	افشاری ۱۳۹۶ ; Zhang et al. 2018
		۲۰- استفاده از تگ‌ها و حسگرهای بومی‌سازی شده	Barron et al. 2016; Zhang et al. 2018;
		۲۱- ایجاد بستر مناسب تمرکز و توجه به عمر حسگرهای اطلاعاتی برای رصد محصولات لجستیکی در طول زنجیره تأمین	Zhang et al. 2018;
		۲۲- ایجاد بستر ارزیابی و کنترل خطاهای سیگنال‌های ارسالی در حسگرهای بومی جهت تطابق با حد استاندارد جهانی	Zhang et al. 2018;
		۲۳- استفاده از رمزنگاری و سخت‌افزارهای لازم در سطح درگاه	Poster 2018; Yep 2015
	گستره فضای وب ۲.۰	۲۴- ایجاد بستر سرعت مناسب شبکه‌های اینترانت برای انتقال اطلاعات	Yuen et al. 2018
		۲۵- به روزرسانی فایروال‌های امنیتی و اجرای تست مقاوم بودن در برابر ویروس‌های جدید به‌صورت دوره‌ای	Rasouli 2019; Zhou et al. 2015
		۲۶- انجام کدینگ و رمزنگاری اطلاعاتی مناسب برای جلوگیری از سرقت و تحریف اطلاعاتی	Rasouli 2019
		۲۷- تعریف سطح دسترسی و رصد تک تک کارهای کاربران اطلاعاتی در جهت تشخیص انحراف از مسیر انجام کار	Zhang et al. 2018;
	فناوری RFID	۲۸- مهندسی معکوس تگ‌های RFID	Zelbst et al. 2017
		۲۹- توسعه تگ‌های بی‌سیم جهت کنترل پیوسته	James et al. 2005
		۳۰- استفاده از سیستم کدینگ اطلاعاتی تگ‌ها	Barron et al. 2012
		۳۱- بومی‌سازی دستگاه‌های لیبل خوان	Xu et al. 2012

نوع لجستیک	نوع فناوری	الزامات امنیت سایبری کاربست فناوری	منابع
		۳۲- توسعه فرکانسی سطح بالای دستگاه‌های لیبل خوان	Yip et al. 2015
		۳۳- بومی‌سازی دستگاه‌های لیبل خوان متناسب با فضای کاربری داخلی	Yip et al. 2015
	لجستیک همه منظوره	۳۴- استفاده از شبکه‌های پروتکلی با IP خصوصی نسل جدید (مانند ۱۷۲. ۲۰. ۲۰. ۲۰)	Gunawan 2017; Rasouli 2019
		۳۵- استفاده از محیط‌های دلفی کاربر پسند و رابط کاربری ساده	Yep 2015
		۳۶- پشتیبان‌گیری از اطلاعات فعالیت‌های لجستیکی (مانند پشتیبان گیری در فضای ابری)	Tao et al. 2014; Yep 2015
		۳۷- برخورداری از سرعت مناسب شبکه‌های اینترانت در انتقال اطلاعات	Ku 2017
		۳۸- استفاده از فضای مشترک شبکه‌ای برای تسهیل ارتباطات بین فردی	صراف ۱۳۹۱ ; Zhang et al. 2018
	پیمانکاری در لجستیک	۳۹- استفاده از پروتکل‌های ایمن برای تبادل اطلاعاتی (مانند https)	Poster 2018
		۴۰- انجام کدینگ و رمزنگاری اطلاعاتی مناسب برای جلوگیری از سرقت و تحریف اطلاعاتی	Yep 2015
		۴۱- استفاده از فناوری بلاک‌چین	Poster 2018
	واقعیت افزوده شده در لجستیک	۴۲- محافظت و مبهم‌سازی اطلاعات کدگذاری شده در فرآیندهای لجستیک هوشمند	Rasouli 2019
		۴۳- تعریف سطح دسترسی و رصد تک‌تک کارهای کاربران اطلاعاتی در جهت تشخیص انحراف از مسیر انجام کار	Huang & Yan 2018
	خودروهای خودران یا رباتیک در لجستیک	۴۴- استفاده از فناوری هوش مصنوعی در تحلیل اطلاعات	Zhang & Liu 2019
		۴۵- ارزیابی منطقی و منظم بودن تحلیل‌های هوش مصنوعی	Zhang & Liu 2019

نوع لجستیک	نوع فناوری	الزامات امنیت سایبری کاربست فناوری	منابع
فناوری‌های لجستیک توزیع		۴۶- ارائه منابع اطلاعاتی و بانک دانش طبقه‌بندی شده به کاربران	Xu et al. 2018a; Yuen et al. 2018
		۴۷- استفاده از فضای ابری بومی در راستای حفاظت اطلاعات	Zhang & Liu 2019
		۴۸- نصب و اجرای دستگاه‌های تولید فرکانسی مناسب (خارج از استاندارد)	;Zhang et al. 2018
		۴۹- توسعه و کاربست حسگرهای ارزان قیمت با محدوده فرکانسی فعال داخلی	Zhang & Liu 2019
		۵۰- توسعه و کاربست وسایل حمل و نقل خودران	Zhang & Liu 2019
		۵۱- استفاده از فناوری‌های نوین ماهواره‌ای بومی در مراکز حیاتی	Yuen et al. 2018
		۵۲- استفاده از فناوری هوش مصنوعی در تحلیل اطلاعات	Zhang & Liu 2019
		۵۳- بررسی و ارزیابی منطقی و منظم بودن تحلیل‌های هوش مصنوعی در صنعت تحت پوشش	Zhang & Liu 2019
		۵۴- استفاده از برنامه‌نویسی دفاع چند لایه‌ای در رصد نفوذ و مقابله	Zhang et al. 2018
		۵۵- ایجاد زمینه کسب اطمینان از فعال بودن سطوح فرمان هشدار نفوذ	Winkelhaus & Grosse 2019
		۵۶- پیاده‌سازی زیرساخت‌های مخابراتی برای مدیریت دانش	Xu et al. 2018a; Zhang & Liu 2019;
عمومی و کلی در تمام فناوری‌ها		۵۷- صحت و اعتبارسنجی اطلاعاتی در هوش مصنوعی	Boyes 2015; Huang & Yan 2018
		۵۸- استفاده از فناوری بلاک‌چین در ارتقای امنیت تمامی فناوری‌ها	Parn & Edwards 2019; Poster 2018

روش‌شناسی پژوهش

از آنجا که این تحقیق در جستجوی مسائل مربوط به الزامات امنیت سایبری لجستیک هوشمند در سامانه آمادی‌بخش دفاع می‌باشد و نتایج حاصل از آن برای تعیین بسترها و الزامات امنیتی

و حل مسائل و چالش‌های سازمانی این حوزه قابل اجراست، می‌توان گفت که تحقیق حاضر از نظر هدف کاربردی است. همچنین پژوهش حاضر بر اساس شیوه اجرا و نحوه گرده‌آوری اطلاعات، یک پژوهش میدانی است. با توجه به اینکه این تحقیق براساس شیوه‌های آماری و نظرسنجی از خبرگان انجام می‌شود و متغیرها مشاهده و اندازه‌گیری و توصیف می‌شوند؛ لذا نوع تحقیق از این حیث، توصیفی- پیمایشی است.

جامعه آماری این تحقیق شامل متخصصان خبره (استادان دانشگاهی حوزه لجستیک و آماد) و خبرگان حوزه امنیت اطلاعات در سامانه امنیتی سازمان دفاعی موردمطالعه می‌باشد که در تهران فعال هستند. به‌دلیل رعایت اصول محرمانگی، حجم جامعه عنوان نمی‌شود؛ ولیکن با رعایت اصول علمی نمونه‌گیری، به تعداد ۵۰ نفر پرسشنامه توزیع شد (۳۵ نفر طبقه اول و ۱۵ نفر طبقه دوم)، که در نهایت، تعداد ۳۹ پرسشنامه (۷۸٪) برگشت داده شد و تحلیل‌ها نیز بر آن مبنا صورت پذیرفت.

در تحقیق حاضر از دو شیوه کتابخانه‌ای و میدانی جهت گرداوری اطلاعات استفاده شده است. ابتدا در روش کتابخانه‌ای و اسنادی، به‌منظور بررسی و کسب اطلاعات هر چه بیشتر و شناخت دقیق‌تر موضوع مورد پژوهش و استفاده از یافته‌های تحقیقات انجام شده در این زمینه، به بررسی و مطالعه پایان‌نامه‌ها، کتب منتشر شده خارجی و ایرانی، نشریات فارسی و انگلیسی پرداخته شد. سپس، فاکتورهای شناسایی شده در معرض قضاوت تعداد ۷ نفر از صاحبنظران کلیدی این حوزه قرار گرفت و پرسشنامه‌ای منطبق بر شاخص‌های درج شده در جدول ۱ طراحی و توسط خبرگان تکمیل و در نهایت مورد تجزیه و تحلیل قرار گرفت.

برای تحلیل داده‌ها از آمار توصیفی و استنباطی با کمک نرم‌افزارهای اکسل و اس. پی. اس. اس. استفاده شد. دربخش آمار توصیفی از شاخص‌های مرکزی و پراکندگی (میانگین و واریانس) و در آمار استنباطی با توجه به نرمال نبودن توزیع داده‌ها از آزمون دوجمله‌ای استفاده شد. همچنین آزمون فریدمن برای بررسی تفاوت اولویت الزامات شناسایی شده مورد استفاده قرار گرفت.

تجزیه و تحلیل داده‌ها

نتایج تحلیل جمعیت‌شناختی

نتایج تحلیل ویژگی‌های جمعیت‌شناختی خبرگان موردمطالعه در جدول ۲ درج شده است. لازم به ذکر است که تعداد خبرگان پژوهش که پرسشنامه را تکمیل کرده‌اند، ۳۹ نفر بوده است که تعداد ۴ نفر از آنان به ویژگی‌های جمعیت‌شناختی پاسخی نداده‌اند. بر این مبنا تقریباً ۹۷ درصد از خبرگان این پژوهش دارای تحصیلات کارشناسی ارشد و بالاتر بوده‌اند. تقریباً ۸۵ درصد از خبرگان در

مشاغل سازمانی مدیریت و فرماندهی ارشد مشغول فعالیت می‌باشند. تمام خبرگان دارای سابقه خدمت بیش از ۱۰ سال بوده و بیش از ۷۰ درصد آنان نیز بالای ۲۰ سال خدمت داشته‌اند. بر این اساس، افراد مطالعه شده، دارای تجارب سازمانی بالایی از حیث ارتباط با سازمان بوده‌اند. قریب به ۹۰ درصد از خبرگان مطالعه شده، آشنایی بالاتر از حد متوسط با تخصص آماد و پشتیبانی داشته‌اند. بنابراین، افراد مورد مطالعه، شناخت مطلوبی از تخصص آماد و پشتیبانی داشته‌اند. نزدیک به ۹۰ درصد از خبرگان پژوهش، آشناییِ بالاتر از حد متوسط با مباحث این حوزه داشته‌اند. بر این اساس، افراد مطالعه شده، شناخت مطلوبی از حوزه دانشی لجستیک هوشمند داشته‌اند. بیش از ۹۷ درصد از خبرگان، آشناییِ بالاتر از حد متوسط با مباحث امنیت اطلاعات داشته‌اند. بر این اساس، افراد مطالعه شده، شناخت مطلوبی از امنیت اطلاعات نیز داشته‌اند.

جدول (۲) ویژگی‌های جمعیت‌شناختی خبرگان مورد مطالعه

ویژگی جمعیت شناختی	رده	فراوانی	درصد فراوانی
سن	زیر ۳۰ سال	۰	۰
	۳۱-۴۰	۹	۷.۲۵
	۴۱-۵۰	۲۶	۳.۷۴
	بالای ۵۰ سال	۰	۰
سطح تحصیلات	کارشناس	۱	۹.۲
	کارشناسی ارشد	۱۸	۴.۵۱
	دکتری تخصصی	۱۶	۷.۴۵
سمت سازمانی	کارشناس	۵	۷.۱۴
	جانشین مدیریت	۵	۷.۱۴
	مدیر میانی	۱۳	۲.۳۸
	فرمانده ارشد	۱۱	۴.۳۲
سابقه ارتباط با سازمان (حوزه لجستیک یا امنیتی)	زیر ۱۰ سال	۰	۰
	۱۰-۲۰	۱۰	۶.۲۸
	۲۰-۳۰	۲۱	۶۰
	بالای ۳۰	۴	۴.۱۱
سابقه آشنایی خبرگان مورد مطالعه با تخصص آماد و پشتیبانی	خیلی کم	۱	۹.۲
	کم	۳	۶.۸
	متوسط	۱۱	۴.۳۱
	زیاد	۱۴	۴۰
	خیلی زیاد	۶	۱.۱۷
سابقه آشنایی خبرگان با لجستیک هوشمند	خیلی کم	۲	۷.۵
	کم	۲	۷.۵

ویژگی جمعیت شناختی	رده	فراوانی	درصد فراوانی
	متوسط	۱۲	۳ .۳۴
	زیاد	۱۷	۶ .۴۸
	خیلی زیاد	۲	۷ .۵
سابقه آشنایی خبرگان با امنیت اطلاعات	خیلی کم	۰	۰
	کم	۱	۹ .۲
	متوسط	۱۲	۳ .۳۴
	زیاد	۱۶	۷ .۴۵
	خیلی زیاد	۶	۱ .۱۷

نتایج مربوط به بررسی سؤالات پژوهش

سؤال فرعی اول با شناسایی الزامات امنیتی پیاده‌سازی لجستیک هوشمند بر مبنای مطالعات کتابخانه‌ای و پژوهش‌های پیشین مرتبط است که نتایج تفصیلی این بررسی در پیشینه پژوهش ارائه شد. در ادامه تنها به بررسی نتایج پیمایش انجام‌شده مبتنی بر نظرات خبرگان موضوع پرداخته می‌شود. لازم به‌ذکر است که قبل از توزیع پرسشنامه‌ها، علاوه بر تأیید اعتبار و روایی پرسشنامه بر مبنای نظر تعداد ۴ نفر از خبرگان دانشگاهی و ۳ نفر از خبرگان امنیتی، قبل از هر چیز عوامل اولیه شناسایی شده در مطالعات کتابخانه‌ای در معرض قضاوت و ارزیابی ۷ نفر از خبرگان امنیتی و دانشگاهی مرتبط با مدیریت زنجیره تأمین قرار گرفت و پس از تعدیل به شرح جدول ۱ مورد تأیید قرار گرفت. در ادامه، به بررسی نتایج مرتبط با نظرات خبرگان بر روی الزامات امنیتی شناسایی شده مستخرج از مبانی نظری پژوهش پرداخته می‌شود.

آزمون نرمال بودن توزیع داده‌ها

به منظور بررسی نرمال بودن داده‌ها، از آزمون کولموگوروف – اسمیرنوف[1] استفاده شد. فرض صفر و فرض مقابل آماری برای این آزمون عبارت است از:

H_0: توزیع داده‌های مربوط به الزامات امنیتی شناسایی شده نرمال است.

H_1: توزیع داده‌های مربوط به الزامات امنیتی شناسایی شده نرمال نیست.

از آنجا که سطح معنی‌داری آزمون برای اکثر متغیرهای مورد بررسی کمتر از ۰.۰۵ بدست آمد، بنابراین فرض صفر آماری رد شده و ادعای نرمال بودن توزیع الزامات شناسایی شده تأیید نمی‌شود. بر این مبنا از آزمون‌های ناپارامتریک برای تحلیل داده‌ها استفاده می‌شود.

بررسی تأیید الزامات امنیتی شناسایی شده توسط خبرگان

[1] Kolmogorov-Smirnov

به‌منظور بررسی پذیرش یا عدم پذیرش هر یک از الزامات امنیتی شناسایی شده برای پیاده‌سازی لجستیک هوشمند در سامانه آمادی منطبق برنظرات خبرگان، از آزمون دوجمله‌ای[1] استفاده شد. بدین منظور فرض صفر و فرض مقابل آماری به‌صورت زیر برای هر یک از متغیرها تعریف می‌شوند:

$$\begin{cases} H_1: p > 0.5 \\ H_0: p \leq 0.5 \end{cases}$$

لازم به ذکر است که p نسبت خبرگانی است که نظری مبنی بر تأثیر بیش از حد متوسط عوامل شناسایی شده بر روی موضوع مورد بررسی داشته‌اند.

از آنجایی که سطح معنی‌داری آزمون برای تمام عوامل شناسایی شده به عنوان الزامات امنیتی پیاده‌سازی لجستیک هوشمند در سامانه آمادی ۰. ۰۰۰ به‌دست آمد. بنابراین برای کلیه موارد فرض صفر بالا رد شده و فرض مقابل آماری پذیرفته می‌شود. یعنی اکثر خبرگان الزامات امنیتی شناسایی شده را بیش از حد متوسط (متوسط، زیاد و خیلی زیاد) برای پیاده‌سازی لجستیک هوشمند در سامانه آمادی‌بخش دفاعی ضروری دانسته‌اند و بنابراین الزامات شناسایی شده پذیرفته می‌شود.

جزئیات نتایج مربوط به نتایج آزمون دوجمله‌ای برای سه سؤال اول در جدول ۳ درج شده است. لازم به‌ذکر است که کمترین میزان درصد مشاهدات برای سؤالات در گروه ۲ (اعتقاد به لزوم بیش از میزان متوسط الزامات) ۸۶ درصد بوده است که نشان می‌دهد توافق بالایی درخصوص پذیرش الزامات شناسایی شده در بین خبرگان وجود دارد.

جدول (۳) نتایج مرتبط با آزمون دوجمله‌ای

سؤال(الزام)	گروه	طبقه	تعداد	درصد مشاهدات	درصد قابل پذیرش	سطح معناداری
Q1	گروه ۱	<= 2	0	.00	.50	.000a
	گروه ۲	> 2	39	1.00		
Q2	گروه ۱	<= 2	0	.00	.50	.000a
	گروه ۲	> 2	39	1.00		
Q3	گروه ۱	<= 2	1	.03	.50	.000a
	گروه ۲	> 2	38	.97		

[1] Binominal test

نتایج مرتبط با اولویت‌بندی الزامات امنیتی پیاده‌سازی لجستیک هوشمند

به منظور بررسی یکسان بودن اهمیت (رتبه‌بندی) الزامات پیاده‌سازی لجستیک هوشمند در هر یک از انواع فناوری‌های نوین مورد مطالعه، از آزمون فریدمن[1] استفاده شد، بدین منظور فرض صفر و فرض مقابل آماری به‌صورت زیر تعریف می‌شوند:

H0: اولویت الزامات امنیتی شناسایی شده در فناوری مورد مطالعه (بلاک‌چین / اینترنت اشیاء / وب ۲ /...) یکسان است.

H1: اولویت الزامات امنیتی شناسایی شده در فناوری مورد مطالعه (بلاک‌چین / اینترنت اشیاء / وب ۲ /...) متفاوت است.

از آنجا که میزان سطح معنی‌داری آزمون ۰/۰۰۱ به‌دست آمد و چون این میزان کمتر از ۰/۰۵ است، فرض صفر رد شد. نتایج حاصل از اولویت‌بندی و میانگین رتبه هر یک از الزامات امنیتی مرتبط با فناوری بلاک‌چین بر اساس نظرات خبرگان مورد مطالعه در جدول ۴ نمایش داده شده است. بر این مبنا ضمن تأکید بر این نکته که تمام الزامات این بعد با میانگین بالایی مورد پذیرش قرار گرفته‌اند می‌توان عنوان داشت که اگر بخواهد تأکید و ترتیبی بر اولویت و تقدم الزامات برای اخذ مجوز امنیتی لجستیک هوشمند در سامانه آمادی صورت پذیرد، ترتیب و اولویت عوامل بر حسب میانگین به شرح جدول ۴ است.

جدول (۴) اولویت الزامات امنیتی مرتبط با فناوری بلاک‌چین

رتبه	الزام	کد الزام در جدول ۱	میانگین رتبه
۱	ایجاد زیرساخت‌های مناسب در حفظ امنیت اطلاعاتی لجستیک هوشمند	Q2	۵/۴۷
۲	استفاده از فناوری‌های نوین جهت رصد فعالیت‌های لجستیکی در سازمان	Q1	۵/۰۹
۳	طراحی و اجرای شبکه‌های رمزنگاری شده و سلولار مناسب برای افزایش امنیت شبکه	Q4	۴/۷۹
۴	ایجاد و طرح‌ریزی زیرساخت‌های مناسب جهت بهره‌گیری از فناوری‌های بومی (استفاده از اینترانت و اینترنت‌های محلی و بومی مانند شبکه گسترده LAN)	Q3	۴/۵۴
۵	اجرا و پیاده‌سازی مدیریت دانش در تجزیه و تحلیل داده‌های لجستیکی	Q7	۴/۴۱
۶	ایجاد زمینه پشتیبان‌گیری دوره‌ای از اطلاعات فعالیت‌های لجستیکی	Q5	۴/۱۸

[1] Friedman Test

رتبه	الزام	کد الزام در جدول ۱	میانگین رتبه
۷	استفاده از فناوری‌های نوین ماهواره‌ای بومی در مراکز حیاتی	Q8	۳/۸۶
۸	ایجاد زمینه دسترسی به اطلاعات مورد نیاز لجستیک هوشمند با استفاده از بسترهای فناوری اطلاعات برای اعضای زنجیره تأمین	Q6	۳/۶۵

نتایج حاصل از اولویت‌بندی و میانگین رتبه هر یک از الزامات امنیتی مرتبط با فناوری اینترنت اشیاء بر اساس نظرات خبرگان مورد مطالعه در جدول ۵ نمایش داده شده است. بر این مبنا ضمن تأکید بر این نکته که تمام الزامات این بعد با میانگین بالایی مورد پذیرش قرار گرفته‌اند، ترتیب و اولویت عوامل بر حسب میانگین به شرح جدول ۵ است.

جدول (۵) اولویت الزامات امنیتی مرتبط با فناوری اینترنت اشیاء

رتبه	عنوان الزام	کد الزام	میانگین رتبه
۱	ایجاد بستر و سدهای امنیتی مناسب جهت جلوگیری از نفوذ اطلاعاتی در سیستم‌ها	Q11	۷/۰۹
۲	ایجاد بستر مناسب تمرکز و توجه به عمر حسگرهای اطلاعاتی برای رصد محصولات لجستیکی در طول زنجیره تأمین	Q16	۶/۴۰
۳	طراحی و اجرای زیر ساخت‌های پوشش بافرهای امنیتی در فرآیند لجستیک هوشمند	Q12	۵/۷۷
۴	طراحی و اجرای آموزش مفاهیم اینترنت اشیاء و سطح دسترسی به اطلاعات در فرآیندهای لجستیکی بین اعضای زنجیره تأمین	Q13	۵/۶۷
۵	استفاده از رمزنگاری و سخت افزارهای لازم در سطح درگاه	Q18	۵/۶۷
۶	استفاده از تگ‌ها و حسگرهای بومی‌سازی شده	Q15	۵/۴۴
۷	ایجاد بستر ارزیابی و کنترل خطاهای سیگنال‌های ارسالی در حسگرهای بومی جهت تطابق با حد استاندارد جهانی	Q17	۵/۲۴
۸	ایجاد زیرساخت‌های انتقال نتایج ارزیابی‌ها به درگاه‌ها و اعضای زنجیره تأمین و نیز رصد دقیق و برخط تگ‌های اطلاعاتی	Q14	۵/۲۰
۹	طراحی و اجرای سیستم ارزیابی و کنترل دوره‌ای مناسب از حسگرهای اینترنت اشیاء	Q9	۴/۷۳
۱۰	نصب دستگاه‌های تولید فرکانسی مناسب (خارج از استاندارد)	Q10	۳/۷۹

نتایج حاصل از اولویت‌بندی و میانگین رتبه هر یک از الزامات امنیتی مرتبط با گستره فضای وب ۲.۰ بر اساس نظرات خبرگان مورد مطالعه در جدول ۶ نمایش داده شده است. بر این مبنا ضمن تأکید بر این نکته که تمام الزامات این بعد با میانگین بالایی مورد پذیرش قرار گرفته‌اند، ترتیب و اولویت عوامل بر حسب میانگین به شرح جداول ۶ است.

جدول (۶) اولویت الزامات امنیتی مرتبط با فناوری فضای وب ۲. ۰

رتبه	عنوان الزام	کد الزام	میانگین رتبه
۱	انجام کدینگ و رمزنگاری اطلاعاتی مناسب برای جلوگیری از سرقت و تحریف اطلاعاتی	Q21	۲/۷۸
۲	تعریف سطح دسترسی و رصد تک تک کارهای کاربران اطلاعاتی در جهت تشخیص انحراف از مسیر انجام کار	Q22	۲/۶۲
۳	به روزرسانی فایروال‌های امنیتی و اجرای تست مقاوم بودن در برابر ویروس‌های جدید به‌صورت دوره‌ای	Q20	۲/۳۷

الزامات امنیتی مرتبط با لجستیک همه‌منظوره بر اساس نظرات خبرگان مورد مطالعه که در جدول ۷ نمایش داده شده است به لحاظ آماری دارای اولویت یکسان هستند. بر این مبنا می‌توان گفت که تمام الزامات این بعد نیز با میانگین بالایی مورد پذیرش قرار گرفته‌اند.

جدول (۷) اولویت الزامات امنیتی مرتبط با لجستیک همه‌منظوره

ردیف	عنوان الزام	کد الزام	میانگین رتبه
۱	استفاده از شبکه‌های پروتکلی با IP خصوصی نسل جدید(مانند ۱۷۲. ۲۰. ۲۰. ۲۰)	Q23	۲/۸۸
۲	استفاده از محیط‌های دلفی کاربر پسند و رابطه کاربری ساده	Q24	۲/۵۹
۳	پشتیبان‌گیری از اطلاعات فعالیت‌های لجستیکی (مانند پشتیبا گیری در فضای ابری)	Q25	۳/۱۲
۴	برخورداری از سرعت مناسب شبکه‌های اینترانت در انتقال اطلاعات	Q26	۳/۳۱
۵	استفاده از فضای مشترک شبکه‌ای رای تسهیل ارتباطات بین فردی	Q27	۳/۰۹

نتایج حاصل از اولویت‌بندی و میانگین رتبه هر یک از الزامات امنیتی مرتبط با فناوری پهپادها در لجستیک بر اساس نظرات خبرگان مورد مطالعه در جدول ۸ نمایش داده شده است. بر این مبنا ضمن تأکید بر این نکته که تمام الزامات این بعد با میانگین بالایی مورد پذیرش قرار گرفته‌اند، ترتیب و اولویت عوامل بر حسب میانگین به شرح جدول ۸ است.

جدول (۸) اولویت الزامات امنیتی مرتبط با فناوری پهپادها در لجستیک

رتبه	عنوان الزام	کد الزام	میانگین رتبه
۱	انجام کدینگ و رمزنگاری اطلاعاتی مناسب برای جلوگیری از سرقت و تحریف اطلاعاتی	Q29	۲/۲۲
۲	استفاده از پروتکل‌های ایمن برای تبادل اطلاعاتی(مانند https)	Q28	۱/۹۶
۳	استفاده از فناوری بلاک چین	Q30	۱/۸۲

در تحلیلی اولویت الزامات امنیتی واقعیت افزوده شده در لجستیک، از آنجا که میزان سطح معنی‌داری آزمون ۰/۵۹۳ به‌دست آمد و چون این میزان بیشتر از ۰/۰۵است، فرض صفر پذیرفته

شد. بر این مبنا، الزامات امنیتی مرتبط با واقعیت افزوده شده در لجستیک بر اساس نظرات خبرگان مورد مطالعه که در جدول ۹ نمایش داده شده است به لحاظ آماری دارای اولویت یکسان هستند. بر این مبنا می‌توان گفت که تمام الزامات این بعد نیز با میانگین بالایی مورد پذیرش قرار گرفته‌اند.

جدول (۹) اولویت الزامات امنیتی مرتبط با واقعیت افزوده شده در لجستیک

ردیف	عنوان الزام	کد الزام	میانگین رتبه
۱	محافظت و مبهم‌سازی اطلاعات کدگذاری شده در فرآیندهای لجستیک هوشمند	Q31	۱/۴۷
۲	تعریف سطح دسترسی و رصد تک تک کارهای کاربران اطلاعاتی در جهت تشخیص انحراف از مسیر انجام کار	Q32	۱/۵۳

از آنجا که میزان سطح معنی‌داری آزمون در خصوص الزامات امنیتی خودروهای خودران یا رباتیک در لجستیک ۰/۲۵۷ به‌دست آمد و چون این میزان بیشتر از ۰/۰۵است، فرض صفر پذیرفته شد. بر این مبنا، الزامات امنیتی مرتبط با خودروهای خودران یا رباتیک در لجستیک بر اساس نظرات خبرگان مورد مطالعه که در جدول ۱۰ نمایش داده شده است به لحاظ آماری دارای اولویت یکسان هستند. بر این مبنا می‌توان گفت که تمام الزامات این بعد نیز با میانگین بالایی مورد پذیرش قرار گرفته‌اند.

جدول (۱۰) اولویت الزامات امنیتی مرتبط با خودروهای خودران یا رباتیک در لجستیک

ردیف	عنوان الزام	کد الزام	میانگین رتبه
۱	استفاده از فناوری هوش مصنوعی در تحلیل اطلاعات	Q33	۱/۳۴
۲	ارزیابی منطقی و منظم بودن تحلیل‌های هوش مصنوعی	Q34	۱/۴۶

نتایج حاصل از اولویت‌بندی و میانگین رتبه هر یک از الزامات امنیتی مرتبط با لجستیک توزیع بر اساس نظرات خبرگان مورد مطالعه در جدول ۱۱ نمایش داده شده است. بر این مبنا ضمن تأکید بر این نکته که تمام الزامات این بعد با میانگین بالایی مورد پذیرش قرار گرفته‌اند، ترتیب و اولویت عوامل بر حسب میانگین به شرح جدول (۱۱) است.

جدول (۱۱) اولویت الزامات امنیتی مرتبط با لجستیک توزیع

رتبه	عنوان الزام	کد الزام	میانگین رتبه
۱	ایجاد زمینه کسب اطمینان از فعال بودن سطوح فرمان هشدار نفوذ	Q44	۷/۱۶
۲	استفاده از فضای ابری بومی در راستای حفاظت اطلاعات	Q36	۷/۱۴
۳	پیاده‌سازی زیرساخت‌های مخابراتی برای مدیریت دانش	Q45	۶/۷۷

رتبه	عنوان الزام	کد الزام	میانگین رتبه
۴	استفاده از برنامه نویسی دفاع چند لایه‌ای در رصد نفوذ و مقابله	Q43	۶/۵۶
۵	استفاده از فناوری هوش مصنوعی در تحلیل اطلاعات	Q41	۶/۲۴
۶	ارائه منابع اطلاعاتی و بانک دانش طبقه‌بندی شده به کاربران	Q35	۶/۱۳
۷	بررسی و ارزیابی منطقی و منظم بودن تحلیل‌های هوش مصنوعی در صنعت تحت پوشش	Q42	۵/۸۹
۸	نصب و اجرای دستگاه‌های تولید فرکانسی مناسب (خارج از استاندارد)	Q37	۵/۳۴
۹	توسعه و کاربرد وسایل حمل و نقل خودران	Q39	۵/۲۱
۱۰	استفاده از فناوری‌های نوین ماهواره‌ای بومی در مراکز حیاتی	Q40	۴/۸۹

از آنجا که میزان سطح معنی‌داری آزمون در خصوص اولویت الزامات امنیتی عمومی پیاده‌سازی لجستیک هوشمند (ویژه تمام فناوری‌ها) ۰/۱۳۴ به‌دست آمد و چون این میزان بیشتر از ۰/۰۵است، فرض صفر پذیرفته شد. بر این مبنا، الزامات امنیتی عمومی پیاده‌سازی لجستیک هوشمند (ویژه تمام فناوری‌ها) بر اساس نظرات خبرگان مورد مطالعه که در جدول ۱۲ نمایش داده شده است به لحاظ آماری دارای اولویت یکسان هستند. بر این مبنا می‌توان گفت که تمام الزامات این بعد نیز با میانگین بالایی مورد پذیرش قرار گرفته‌اند.

جدول (۱۲) اولویت الزامات امنیتی عمومی لجستیک هوشمند

ردیف	عنوان الزام	کد الزام	میانگین رتبه
۱	صحت و اعتبارسنجی اطلاعاتی در هوش مصنوعی	Q46	۱/۵۸
۲	استفاده از فناوری بلاک‌چین در ارتقای امنیت تمامی فناوری‌ها	Q47	۱/۴۲

نتیجه‌گیری

در این پژوهش که با هدف شناسایی و اولویت‌بندی الزامات امنیتی لجستیک هوشمند در سامانه آمادی‌بخش دفاع انجام شد. پس از بررسی مبانی نظری و پیشینه پژوهش‌های انجام شده در این حوزه در مجامع بین‌المللی، به طراحی مدلی مفهومی الزامات امنیتی لجستیک هوشمند پرداخته شد و سپس مبتنی بر آن پرسشنامه‌ای برای دریافت نقطه نظرات خبرگان امنیتی و لجستیک و استادان فعال این حوزه تنظیم شد و پس از توزیع در سطح خبرگان تعداد ۳۹ پرسشنامه تکمیل و بازگشت داده شد. در ادامه پاسخ به سؤالات تحقیق براساس تحلیل اطلاعات گردآوری شده، ارائه شده است.

سؤال فرعی اول: عوامل و الزامات امنیتی لجستیک هوشمند در سازمان‌های عمومی و دفاعی، مبتنی بر مبانی نظری و مطالعات کتابخانه‌ای شامل چه مواردی است؟

به‌منظور پاسخ به این سؤال با مرور پژوهش‌های پیشین، عوامل و الزامات امنیتی لجستیک هوشمند، مبتنی بر آخرین دستاوردهای علمی بین‌المللی (با توجه به محدودیت منابع فارسی) شناسایی و به شرح جدول ۱ جمع‌بندی شد. این جدول و الزامات شناسایی شده در آن مبنای طراحی پرسشنامه و پاسخ به سایر سؤالات پژوهش شد.

سؤال فرعی دوم: ابعاد، مؤلفه‌ها و شاخص‌های امنیتی بهره‌برداری از لجستیک هوشمند مبتنی بر نظرات خبرگان آمادی و امنیتی شامل چه مواردی است؟

پس از بررسی و مشاهده یافته‌های پژوهش‌های پیشین، با نظر تعدادی از خبرگان حوزه آماد و لجستیک و امنیت اطلاعات، به شرح عنوان شده دربخش روش و یافته‌های پژوهش و مبتنی بر جدول ۱ ابعاد و فناوری‌های قابل کاربرد در هر یک از ابعاد یادشده مشخص شد و سپس لزوم و ضرورت حضور هر یک از شاخص‌های شناسایی شده برای فناوری‌های یادشده، بر اساس نظرات خبرگان (پرسشنامه) مشخص گردید.

بر اساس نتایج ارائه شده دربخش قبل، تمامی الزامات امنیتی شناسایی شده برای استفاده از فناوری‌های نوین قابل بهره‌برداری در لجستیک هوشمند، مورد پذیرش واقع شدند و بنابراین لازم است شاخص‌های یاد شده برای ارتقاء امنیت استفاده از فناوری‌های هوشمند شناسایی شده و صدور مجوزهای امنیتی لازم مورد توجه نهادهای ذی‌ربط قرار گیرند.

سؤال فرعی سوم: اولویت ابعاد، مؤلفه‌ها و شاخص‌های مرتبط با الزامات امنیتی لجستیک هوشمند مبتنی بر نظرات خبرگان آمادی و امنیتی چگونه است؟

به‌منظور پاسخ این سؤال، از آزمون فریدمن برای هر یک از فناوری‌ها استفاده شد. نتایج در جداول ۴ تا ۱۲ گزارش شده است. بر این اساس به ارزیابان سیستم‌های امنیتی لجستیک هوشمند و افرادی که مجوزهای امنیتی را صادر می‌نمایند پیشنهاد می‌شود ضمن توجه به تمام الزامات شناسایی شده، به الزامات دارای اولویت بالاتر توجه بیشتری داشته باشند.

با توجه به نتایج به‌دست آمده پژوهش پیشنهادات کاربری زیر به سامانه آمادی و به ویژه نهادهای امنیتی مرتبط با حوزه لجستیک دربخش دفاعی ارائه می‌گردد:

۱- الزامات امنیتی شناسایی و تأیید شده به ترتیب اولویت در پیاده‌سازی هر یک از فناوری‌ها مورد استفاده قرارگیرد. لازم به‌ذکر است که اصلی‌ترین اولویت هر یک از فناوری‌ها بر اساس تحلیل نتایج پژوهش عبارت است از:

بلاک‌چین: ایجاد زیر ساخت‌های مناسب در حفظ امنیت اطلاعاتی لجستیک هوشمند

اینترنت اشیاء: ایجاد بستر و سدهای امنیتی مناسب جهت جلوگیری از نفوذ اطلاعاتی در سیستم‌ها

وب ۲: انجام کدینگ و رمزنگاری اطلاعاتی مناسب برای جلوگیری از سرقت و تحریف اطلاعاتی

لجستیک همه‌منظوره: استفاده از شبکه‌های پروتکلی با IP خصوصی نسل جدید (مانند ۱۷۲. ۲۰. ۲۰. ۲۰)

استفاده از پهپادها در لجستیک: انجام کدینگ و رمزنگاری اطلاعاتی مناسب برای جلوگیری از سرقت و تحریف اطلاعاتی

واقعیت افزوده شده در لجستیک: محافظت و مبهم‌سازی اطلاعات کدگذاری برنامه‌های رصد فرآیندهای لجستیک هوشمند

خودروهای خودران یا رباتیک: استفاده از فناوری هوش مصنوعی در تحلیل اطلاعات

لجستیک توزیع: ایجاد زمینه کسب اطمینان از فعال بودن سطوح فرمان هشدار نفوذ

الزامات امنیتی عمومی: صحت و اعتبار سنجی اطلاعاتی در هوش مصنوعی

۲- استفاده از فناوری بومی RFID به منظور ارتقاء امنیت در رصد و پیگیری محموله‌های لجستیکی دارای طبقه‌بندی در راستای نگهداری و کنترل موجودی

۳- توسعه شبکه بیسیم جهت هماهنگی بهتر و بیشتر در طرف‌های لجستیکی در سامانه آمادی

۴- راه‌اندازی پروتکل امن میان طرف‌های لجستیک (بهره‌گیری از الگوی سیستم‌های لجستیکی شرکت‌هایی مانند ایران‌خودرو و ساپکو).

۵- توسعه بسترهای نرم‌افزاری به روز و پویا برای ارتقاء امنیت بر اساس الزامات شناسایی شده

۶- تدوین و پیاده‌سازی فایروال‌های پیشرفته جهت جلوگیری از نفوذ و خرابکاری

۷- افزایش امنیت سطوح دسترسی طرف‌های لجستیکی برای دسترسی به میزان اطلاعات طبقه‌بندی شده.

با توجه به اینکه این پژوهش، اولین پژوهش انجام شده در حوزه مؤلفه‌های امنیتی لجستیک هوشمند دربخش دفاعی است دارای محدودیت‌هایی است. یکی از محدودیت‌های این تحقیق، عدم تمرکز بر یک فناوری خاص می‌باشد. چرا که تمامی ابعاد لجستیک هوشمند را مورد مطالعه قرارداده است. براین مبنا پیشنهاد می‌گردد پژوهشگران آتی به انجام پژوهش‌هایی در حوزه‌های زیر بپردازند:

۱. تمرکز دقیق بر هر یک از فناوری‌ها و آغاز مطالعه برای تعیین و اولویت‌بندی الزامات امنیتی فناوری مربوطه با نگرش به الزامات امنیتی شناسایی و تأییدشده در این پژوهش.

۲. پیاده‌سازی هر یک از فناوری‌ها و الزامات امنیتی شناسایی شده مرتبط با آن در سطح خرد و یک‌بخش محدود (پایلوت) و بازخوردگیری و تعدیل الزامات شناسایی شده.

۳. استفاده از رویکردهای دیگر تحلیل داده به‌ویژه منطق فازی در ارزیابی و توسعه الزامات امنیتی لجستیک هوشمند به منظور پوشش نیازمندی‌های شرایط عدم قطعیت، ریسک و....

قدردانی

از خبرگان توانمندی که در طول پژوهش، دانش خویش را سخاوتمندانه در اختیار محققان این پژوهش قرار دادند و استواری پژوهش حاضر بر مشارکت و دانش این بزرگواران قرارگرفته است بسیار سپاسگزاریم.

منابع

- افشاری، حمیده؛ تاجفر، امیرهوشنگ و قیصری، محمد. (۱۳۹۶). بررسی کاربردهای اینترنتی اشیا در زنجیره تأمین، *نخستین کنفرانس ملی پیشرفت‌ها و فرصت‌های فناوری اطلاعات و ارتباطات*، تهران، دانشگاه فرهنگیان.
- آیرس، جیمز. (۱۳۹۱). *راهنمای مدیریت زنجیره تأمین*، ترجمه تیموری، ابراهیم و حافظ الکتب، اشکا. انتشارات دانشگاه علم و صنعت ایران.
- جعفر نژاد، احمد. ، مروتی شریف‌آبادی، علی. و عطایی، عبدالرضا. (۱۳۹۱). *مدیریت زنجیره تأمین و لجستیک*، انتشارات گسترش علوم، چاپ اول.
- صراف جوشقانی، محمد (۱۳۹۱). *بهینه کاوی در مدیریت زنجیره تأمین نظامی*. تهران: انتشارات دانشگاه امام حسین (علیه السلام).
- طالبی، داوود. و ملاطایفه، فاطمه. (۱۳۹۰). رویکرد ارزیابی و انتخاب عرضه‌کنندگان در طول زنجیره تأمین با استفاده از فن ترکیبی فرآیند تحلیل سلسله مراتبی فازی و برنامه‌ریزی خطی چند هدفی فازی (مطالعه موردی: مرکز بهمن موتور)، *چشم‌انداز مدیریت صنعتی*، ۲، ۲۷-۴۲.
- محققی، جعفر. (۱۳۹۹). *شناسایی الزامات امنیتی توسعه لجستیک هوشمند در یک سازمان دفاعی منتخب*، پایان‌نامه کارشناسی ارشد رشته آماد، دانشگاه علوم و فنون هوایی شهید ستاری.
- Barron, S. Cho, Y. M. Hua, A. Norcross, W. Voigt, J. , and Haimes, Y. (2016, April). Systems-based cyber security in the supply chain. In *IEEE Systems and Information Engineering Design Symposium* (SIEDS) (pp. 20-25). IEEE.
- Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review*, 5(4), 28.
- Chen, C. L. Deng, Y. Y. Weng, W. Zhou, M. and Sun, H. (2021). A blockchain-based intelligent anti-switch package in tracing logistics system. *The Journal of Supercomputing*, *77*(7), 7791-7832.
- Chen, J. Huang, T. Xie, X. Lee, P. T. W. and Hua, C. (2019). Constructing governance framework of a green and smart port. *Journal of Marine Science and Engineering*, 7(4), 83.
- Choi, T. -M. Wallace, S. W. and Wang, Y. (2018), Big Data Analytics in Operations Management. *Prod Oper Manag*, 27: 1868-1883.

- Choi, T-M. , Wen, X. Sun, X. and Chung, S-H. (2019). "The mean-variance approach for global supply chain risk analysis with air logistics in the blockchain technology era," T*ransportation Research Part E: Logistics and Transportation Review*, Elsevier, vol. 127(C), pages 178-191.
- Dauvergne, P. (2020). Is artificial intelligence greening global supply chains? Exposing the political economy of environmental costs. *Review of International Political Economy*, 1-23.
- Ellram, L. Bals, L. and Tate, W. (Eds.). (2018). *Supply Chain Finance: Risk Management, Resilience and Supplier Management*. Kogan Page Publishers.
- Feng, Q. and Shanthikumar, J. G. (2018), How Research in Production and Operations Management May Evolve in the Era of Big Data. *Prod Oper Manag*, 27: 1670-1684.
- Gunawan, T. S. Yaldi, I. R. H. Kartiwi, M. Ismail, N. , and Za'bah, N. F. , Mansor, H. , and Nordin, A. N. (2017). Prototype design of smart home system using internet of things. *Indonesian Journal of Electrical Engineering and Computer Science*, *7*(1), 107-115.
- -Huang, Q. and Yan, X. (2018, July). On the Application of Internet of Things (IOT) in Cold Chain Logistics Management. *In 2018 International Symposium on Communication Engineering & Computer Science* (CECS 2018). Atlantis Press.
- Jian, H. Xu, M. and Zhou, L. (2019). Collaborative collection effort strategies based on the "Internet+ recycling" business model. *Journal of Cleaner Production*, 241, 118120.
- Khoo, L. J. (2019). Design and Develop a Cybersecurity Education Framework Using Capture the Flag (CTF). *In Design, Motivation, and Frameworks in Game-Based Learning* (pp. 123-153). IGI Global.
- Kremer, S. Mé, L. Rémy, D. and Roca, V. (2019). *Cybersecurity.*
- Ku, A. Y. (2017). Anticipating critical materials implications from the Internet of Things (IOT): Potential stress on future supply chains from emerging data storage technologies. *Sustainable Materials and Technologies*.
- Kuo, T. C. , Chen, K. J. , Shiang, W. J. , Huang, P. B. , Otieno, W. , and Chiu, M. C. (2021). A collaborative data-driven analytics of material resource management in smart supply chain by using a hybrid Industry 3. 5 strategy. *Resources, Conservation and Recycling*, 164, 105160.
- Li, X. (2020). Reducing channel costs by investing in smart supply chain technologies. *Transportation Research Part E: Logistics and Transportation Review*, 137, 101927.
- Liu, W. Liang, Y. Wei, S. and Wu, P. (2020a). The organizational collaboration framework of smart logistics ecological chain: a multi-case study in China. *Industrial Management & Data Systems*.

- Liu, W. Shanthikumar, J. G. Lee, P. T. W. , Li, X. , and Zhou, L. (2021). Special issue editorial: Smart supply chains and intelligent logistics services. *Transportation Research Part E: Logistics and Transportation Review*, 147, 102256.
- Liu, W. Shanthikumar, J. G. Lee, P. T. W. , Li, X. , and Zhou, L. (2021). Special issue editorial: Smart supply chains and intelligent logistics services. *Transportation Research Part E: Logistics and Transportation Review*, 147, 102256.
- Liu, W. Wang, S. Lin, Y. Xie, D. and Zhang, J. (2020b). Effect of intelligent logistics policy on shareholder value: evidence from Chinese logistics companies. *Transportation Research Part E: Logistics and Transportation Review*, 137, 101928.
- McFarlane, D. Giannikas, V. Lu, W (2016). Intelligent Logistics: Involving the Customer. *Computers in Industry*. 81, 105-115.
- Nasiri, M. M. and Pourmohammad Zia, N. (2015). A hybrid model for supplier selection and order allocation in supply chain. *Advances in Industrial Engineering*, *49*(1), 117-128.
- Parn, E. A. and Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. *Engineering, Construction and Architectural Management*.
- Petit, J. (2018, July). Automated Vehicles Cybersecurity: Summary AVS'17 and Stakeholder Analysis. *In Automated Vehicles Symposium 2018* (pp. 171-181). Springer, Cham.
- Poster, W. R. (2018). *Cybersecurity needs women*.
- Rasouli, M. R. (2019). An architecture for IoT-enabled intelligent process-aware cloud production platform: a case study in a networked cloud clinical laboratory. *International Journal of Production Research*, 1-16.
- Ricci, J. Breitinger, F. and Baggili, I. (2019). Survey results on adults and cybersecurity education. *Education and Information Technologies*, 24(1), 231-249.
- Ricci, J. Breitinger, F. and Baggili, I. (2019). Survey results on adults and cybersecurity education. *Education and Information Technologies*, 24(1), 231-249.
- Tao, F. Zuo, Y. Da Xu, L. and Zhang, L. (2014). IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing. *IEEE Transactions on Industrial Informatics*, 10(2), 1547-1557.

- Uckelmann, D. (2008, September). A definition approach to smart logistics. *International Conference on Next Generation Wired/Wireless Networking* (pp. 273-284). Springer, Berlin, Heidelberg.
- Wang, J. Lim, M. K. Zhan, Y. and Wang, X. (2020). An intelligent logistics service system for enhancing dispatching operations in an IoT environment. *Transportation Research Part E: Logistics and Transportation Review*, 135, 101886.
- Winkelhaus, S. and Grosse, E. H. (2019). Logistics 4. 0: a systematic review towards a new logistics system. *International Journal of Production Research*, 1-26.
- Xu, B. Wang, W. Hao, Q. Zhang, Z. Du, P. , Xia, T and Wang, X. (2018b). A security design for the detecting of buffer overflow attacks in iot device. *IEEE Access*, *6*, 72862-72869.
- Xu, L. Chen, L. Gao, Z. Chang, Y. , Iakovou, E. , and Shi, W. (2018a, October). Binding the Physical and Cyber Worlds: A Blockchain Approach for Cargo Supply Chain Security Enhancement. *In 2018 IEEE International Symposium on Technologies for Homeland Security* (HST) (pp. 1-5). IEEE.
- Yip, N. S. M. S. (2015). *The Effect of Cyber Supply Chain Security Towards Lean and Agile Supply Chain Performance in Healthcare Industry: The Mediating Effect of Organizational Capabilities* (Doctoral dissertation, Universiti Sains Malaysia).
- Yuen, J. S. , Choy, K. L. , Lam, H. Y. , and Tsang, Y. P. (2018). An Intelligent-Internet of Things (IoT) Outbound Logistics Knowledge Management System for Handling Temperature Sensitive Products. *International Journal of Knowledge and Systems Science* (IJKSS), 9(1), 23-40.
- Zeng, F. Chan, H. K. and Pawar, K. (2020). The adoption of open platform for container bookings in the maritime supply chain. *Transportation Research Part E: Logistics and Transportation Review*, 141, 102019.
- Zhang, N. and Liu, Y. (2019, July). NB-IOT Drives Intelligent Cold Chain for Best Application. *In 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication* (ICEIEC) (pp. 1-4). IEEE.
- Zhang, Y. Guo, Z. , Lv, J. , and Liu, Y. (2018). A framework for smart production-logistics systems based on CPS and industrial IoT. *IEEE Transactions on Industrial Informatics*, 14(9), 4019-4032.
- Zhou, L. Chong, A. Y. , and Ngai, E. W. (2015). Supply chain management in the era of the internet of things. *International Journal of Production Economics*, 159, 1-3.