Providing a risk management framework in smart supply chain processes based on the Internet of Things

Abstract

In addition to being a revolutionary technology for all industries, the Internet of Things; It has also shown its potential in processes such as supply chain. Management, forecasting, and monitoring applications help managers improve their company's distribution operational efficiency and increase transparency in their decisions. The use of the Internet of Things and artificial intelligence, in addition to increasing the analytical power of supply chain data, always has many risks due to the existence and flow of data in the Internet network. Therefore, it is always important to understand the cyber risks that can be faced by businesses in the face of these technologies. In this research, an attempt has been made to identify the most important dimensions, features, and key indicators of cyber risk management in intelligent supply chains based on the Internet of Things by reviewing the literature and opinions of experts active in the field of supply chain and information technology and having relevant work and research records. to be Then a framework to manage risks should be provided. This framework has been evaluated and validated using experts' opinions. Extracting cyber risks and managing them can help improve performance and reduce smart supply chain challenges. Understanding this framework can also be an effective guide to implement safe, intelligent supply chain systems with minimal risk.

Keywords: cause and effect framework, cyber risks smart, supply chain, supply chain risk, supply chain based on the Internet of Things.

ارائه چارچوب مدیریت ریسک‌ها در فرآیند های زنجیره تامین هوشمند مبتنی بر اینترنت اشیا

چکیده

اینترنت اشیاء علاوه بر اینکه یک فناوری انقلابی برای همه صنعت‌هاست؛ توانایی بالقوه خود را در فرآیندهایی مانند زنجیره تأمین نیز نشان داده است. برنامه‌های کاربردی مدیریت، پیش‌بینی و نظارت به مدیران کمک می‌کند تا بهره‌وری عملیاتی توزیع شرکت خود را بهبود بخشیده و شفافیت را در تصمیم‌گیری‌های خود افزایش دهند. استفاده از اینترنت اشیاء و هوش مصنوعی علاوه بر اینکه بر قدرت تحلیلی داده‌های زنجیره تأمین می‌افزاید همواره به دلیل وجود و جریان داده‌ها در شبکه اینترنت دارای ریسک‌های بسیاری نیز می‌باشد. بنابراین درک خطرات سایبری که می‌تواند در مواجه با این فناوری‌ها متوجه کسب‌وکارها باشد همواره قابل ملاحظه است. در این در این پژوهش کوشیده شده است تا با بررسی مرور ادبیات و نظرات خبرگان فعال در حوزه زنجیره تأمین و فناوری اطلاعات و دارای سوابق کاری و پژوهشی مرتبط مهمترین ابعاد، ویژگی‌ها و شاخص‌های کلیدی مدیریت ریسک‌های سابیری در زنجیره‌های تأمین هوشمند مبتنی اینترنت اشیاء شناسایی شده و چارچوبی به منظور مدیریت ریسک‌ها ارائه شود. این چارچوب با استفاده از نظرات خبرگان مورد ارزیابی و اعتبارسنجی قرار گرفته است. استخراج ریسک‌های سایبری و مدیریت آنها می‌توان به بهبود عملکرد و کاهش چالش‌های زنجیره تأمین هوشمند کمک نماید. درک این چارچوب نیز می‌تواند راهنمای موثری به منظور پیاده‌سازی سیستم‌های زنجیره تأمین هوشمند امن با حداقل ریسک باشد.

کلمات کلیدی: چارچوب علی و معلولی، ریسک زنجیره تأمین، ریسک‌های سایبری، زنجیره تأمین مبتنی بر اینترنت اشیاء، زنجیره تأمین هوشمند.

1– مقدمه

امروزه زنجیره‌های تأمین جهانی شرکت‌ها را قادر می‌سازد تا مزایای رقابتی را افزایش داده، انعطاف‌پذیری تولید را افزایش داده و هزینه‌ها را از طریق انتخاب گسترده‌تری از تأمین‌کنندگان کاهش دهند. با وجود این مزایا، درک ناکافی تفاوت‌ها و تغییرات نامشخص منطقه‌ای اغلب خطرات را در عملیات زنجیره تأمین افزایش می‌دهد و حتی منجر به اختلال کامل زنجیره تأمین می‌شود. زنجیره تأمین برای بسیاری از شرکت‌ها تبدیل به یک منبع ریسک فوق‌العاده شده است (Ivanov و همکاران، 2019). روابط زنجیره تأمین، دارایی‌های مهم شرکت در نظر گرفته شده‌اند که می‌تواند اهرمی برای بهبود موقعیت رقابتی شرکت باشد. با تشخیص فرصت‌هایی که زنجیره تأمین شرکت ارائه می‌دهد، ادبیاتی در مورد شکل‌گیری، طراحی و ساختاربندی عملکرد روابط همکاری‌ها در زنجیره تأمین، ایجاد می‌گردد. مدیریت ریسک زنجیره تأمین، مدیریت ریسک‌های موجود در زنجیره تأمین از طریق هماهنگی و همکاری میان اجزاء زنجیره تأمین است به گونه‌ای که سوددهی و پیوستگی زنجیره تأمین را تضمین نماید (Baz و همکاران، 2023).

ارزیابی ریسک یکی از ارکان مدیریت ریسک بوده و هدف آن اندازه‌گیری ریسک‌ها بر اساس شاخص‌های مختلف از قبیل میزان تأثیر و احتمال وقوع می‌باشد و هر چه نتایج این مرحله دقیق‌تر باشد می‌توان گفت که فرایند مدیریت ریسک با درجه اطمینان بالاتری انجام می‌گیرد. رتبه‌بندی ریسک‌ها، قسمت کلیدی این فرایند به شمار می‌رود و امکان تعیین ارجحیت هر ریسک در مقابل سایر ریسک‌ها را فراهم کرده و در نتیجه تصمیم‌گیرندگان می‌تواند در مورد میزان تخصیص منابع موجود برای مقابله با هر ریسک برنامه‌ریزی نماید. مدیریت ریسک زنجیره تأمین سایبری یک ضابطه جدید طراحی شده برای کمک به مجریان فناوری اطلاعات در بیان چالش‌های جهانی سازی سریع و انتشار خارجی سیستم‌های سخت‌افزاری و نرم‌افزاری است (Li و همکاران، 2023).

برخلاف امنیت سایبری، مدیریت ریسک زنجیره تأمین سایبری بر روی به دست آوردن دید و کنترل نه تنها بر سازمان کانونی بلکه بر شرکای سازمانی گسترده آن مانند تأمین‌کنندگان و مشتریان تمرکز دارد. علاوه بر این، در حالی که امنیت سایبری بر ابزارهای کنترل صرفاً فنی تأکید دارد، مدیریت ریسک زنجیره تأمین سایبری به دنبال مهندسی عوامل مدیریتی و انسانی در جلوگیری از خطرات ناشی از اختلال در عملکرد سیستم‌های فناوری اطلاعات است. بر خلاف مدیریت ریسک سازمانی به تنهایی، مدیریت ریسک زنجیره تأمین سایبری بر مکانیزم کنترلی از بالا به پایین برای محیط‌های تجاری نسبتاً ثابت متمرکز نیست، بلکه بیشتر به دنبال پرداختن به پویایی اساسی و در مقیاس جهانی در زمان واقعی شبکه‌های فناوری اطلاعات تطبیقی است. در نهایت، برخلاف مدیریت زنجیره تأمین به تنهایی، مدیریت ریسک زنجیره تأمین سایبری باید با الگوهای تقاضای شبکه دائماً پویا در مقیاس جهانی و اغلب هویت‌های ارائه‌دهنده زنجیره تأمین سروکار داشته باشد (Fernando و همکاران ، 2023).

ساختار مدیریت زنجیره تأمین سایبری در گذشته در پاسخ به نیازهای فوری معماران فناوری اطلاعات برای استراتژی‌ها و مجموعه‌های ابزار برای کنترل مؤثر طراحی، ساخت و استقرار سیستم‌هایی که زیرسیستم‌ها و اجزای سخت‌افزاری و نرم‌افزاری آن‌ها به طور فزاینده‌ای از مناطق دوردست جغرافیایی تأمین می‌شوند، پدید آمده است. تأمین‌کنندگانی که اغلب ناشناخته هستند و قابلیت‌های حیاتی آن‌ها در محیط‌های شبکه با یکپارچگی نامشخص میزبانی، در معرض دید و دسترسی هستند. وجود سیستم‌های مبتنی بر اینترنت، شبکه‌های اجتماعی، سیستم‌های مالی مبتنی بر بلاک‌چین و تحلیل‌های مبتنی بر هوش مصنوعی نیز بر اهمیت روزافزون مدیریت ریسک‌ها در زنجیره‌های تأمین در عصر جدید افزوده است. زیرا حضور شبکه‌ها می‌تواند امنیت را همواره مورد مخاطره قرار دهد (Shakatreh و همکاران، 2023).

زنجیره‌های تأمین دیجیتال انواع جدیدی از ریسک‌های سایبری را در اقتصاد دیجیتال در معرض دید قرار می‌دهند. تأثیر فناوری‌های اینترنت اشیاء بر ریسک سایبری زنجیره تأمین به ندرت در ادبیات دانشگاهی مورد بحث قرار گرفته است و اقتصاد دیجیتال در حال حاضر فاقد شفاف‌سازی در سطوح فردی چالش‌های استراتژیک، کاربردی و عملیاتی از فناوری‌های دیجیتال اینترنت اشیاء و هوش مصنوعی در زنجیره تأمین است. با توجه به اهمیت موضوع در این پژوهش کوشیده شده است تا با استفاده از بررسی مرور ادبیات و نظرات خبرگان فعال در حوزه زنجیره تأمین (در صنایع تند مصرف) که دارای سوابق کاری کافی بوده‌اند و همینطور، خبرگان دانشگاهی دارای سوابق پژوهشی مرتبط، مهمترین ابعاد، مؤلفه‌ها و شاخص‌های کلیدی تاثیرگذار در زنجیره‌های تأمین هوشمند مبتنی بر اینترنت اشیاء استحراج شده و معیارهای امنیت سایبری نیز مورد ارزیابی و واکاوی قرار بگیرد. در نهایت چارچوبی مفهومی برای

این این سیستم امنیتی ارائه می‌شود. درک این چارچوب می‌تواند راهنمای موثری برای پیاده‌سازی سیستم‌های زنجیره تأمین امن مبتنی بر اینترنت اشیاء باشد.

ساختار این مقاله به این صورت می‌باشد. در بخش دوم مرور ادبیات صورت گرفته است. در بخش سوم متدولوژی تحقیق ارائه می‌شود. در بخش چهارم چارچوب مفهومی ارائه می‌گردد و در نهایت در بخش پنجم بحث و نتیجه‌گیری ارائه می‌شود.

2– مرور ادبیات

در این بخش مرور ادبیات در دو بخش ارائه می‌شود. در بخش اول به بررسی ادبیات موضوع در خصوص اینترنت اشیاء و امنیت سایبری پرداخته می‌شود. در بخش دوم زنجیره تأمین مبتنی بر اینترنت اشیاء مورد بررسی قرار می‌گیرد و معیارهای امنیتی در آن واکاوی می‌شود.

2-1 اینترنت اشیاء و امنیت سایبری

اینترنت اشیاء (IoT) شبکه‌ای است. که هر شیء را به اینترنت وصل می‌کند و از ادغام و ترکیب چندین فناوری از جمله شناسایی. خودکار امواج رادیویی، ارتباطات میدان نزدیک ، حسگر سیستم موقعیت‌یاب جهانی و اسکنرهای لیزری تشکیل شده است. که باعث برقراری تبادل اطلاعات و ارتباطات می‌شود و هدف اصلی آن شناسایی هوشمند، ردیابی محل، نظارت و مدیریت است (Ashok و Gopikrishnan، 2023). اینترنت اشیاء مجموعه‌ای از چیزهای تعبیه شده با الکترونیک، نرم افزار، سنسورها و محرک‌ها است و از طریق اینترنت برای جمع‌آوری و مبادله داده به یکدیگر متصل شده‌اند. دستگاه‌های اینترنت اشیاء با سنسورها و قدرت پردازشی مجهز شده‌اند. که آنها را برای توسعه یافتن در بسیاری از محیط‌ها قادر می‌سازند.

کسب و کارها می‌توانند از مزایای اینترنت اشیاء (IoT) بهره ببرند. اما تجهیزات اینترنت اشیاء بیشتر و اکوسیستم پیچیده‌تر اینترنت اشیاء نیز به معنای افزایش آسیب‌پذیری‌های امنیتی است. همه دستگاه‌های اینترنت اشیاء داده‌ها را پردازش کرده و با هم ارتباط برقرار می‌کنند. آن‌ها به برنامه‌ها، سرویس‌ها و پروتکل‌ها برای ارتباط نیاز دارند و بسیاری از آسیب‌پذیری‌های اینترنت اشیاء از رابط‌های ناامن سرچشمه می‌گیرند. بیشترین نگرانی‌ها در امنیت داده‌های برنامه‌های کاربردی Iot ناشی از ارتباطات ناامن و ذخیره‌سازی داده‌ها است. یکی از چالش‌های مهم برای حریم خصوصی و امنیت اینترنت اشیاء این است که می‌توان از دستگاه‌های در معرض خطر برای دسترسی به داده‌های محرمانه استفاده کرد (Vasilescu ،2023).

بنابراین برای حفاظت از استقرار اینترنت اشیاء، در عین حال که از ارزش اقتصادی آن نیز بهره برده می‌شود، لازم است که به صورت سیستماتیک عوامل خطر چندگانه در نظر گرفته شود. زیرا حملات سایبری بارها اتفاق می‌افتند و به طور فزاینده دستگاه‌های اینترنت اشیاء را هدف قرار می‌دهند. با رشد مداوم سطوح و قابلیت‌های حملات سایبری، شدت حملات از طریق فناوری اینترنت اشیاء می‌تواند بسیار بیشتر از آنچه تا به امروز مشاهده شده است، باشد. بنابراین همواره یکی از سؤالات مهم برای سیاست‌های دولت و همچنین استراتژی‌های تجاری بخش خصوصی در رابطه با محصولات، سیستم عامل‌ها و خدمات متصل به اینترنت اشیاء، کفایت اقدامات و روش‌های امنیت سایبری برای به حداقل رساندن ریسک سایبری خواهد بود. پاسخ به این سوال بسیار مهم است و نیازمند بررسی این ریسک‌ها دارد. زیرا قابلیت‌های اینترنت اشیاء، انواع جدیدی از خطرات سایبری را ایجاد می‌کند که در استانداردهای ارزیابی ریسک‌های سایبری موجود پیش‌بینی نشده و درنظر گرفته نمی‌شوند (Sallay، 2023). برای بررسی ریسک‌ها لازم است تا تجزیه و تحلیل کاملی از سازش داده ها، امکانات ارائه دهندگان شبکه ارتباطات یا صاحبان داده با توانایی ایجاد مکانیسم‌های واضح، دقیق و مورد قبول صنعت برای اندازه‌گیری، کنترل، تجزیه وتحلیل، توزیع و مدیریت داده‌های مهم مورد نیاز برای توسعه، استقرار و امنیت سایبری مقرون به صرفه برای زیرساخت‌های مهم انجام شود.

تضمین اینکه اهداف ارکان امنیتی برآورده شوند، مسأله امنیت مناسب با طراحی است. در این حالت شرکت‌ها با اجرای گزینه‌های امنیتی پیشنهادی مانند راه‌حل‌های مدیریت دستگاه و احراز هویت، مبتنی بر تکنیک‌های رمزنگاری، با بسیج دانش تخصصی در اسرع وقت، می‌توانند از دسترسی غیرمجاز به داده‌ها، دستگاه‌ها و نرم‌افزارها جلوگیری کنند. در عوض، این کنترل‌ها به تضمین یکپارچگی داده‌ها و در دسترس بودن خدمات کمک می‌کند. امنیت یک بعد مهم در هر طراحی اینترنت اشیاء است (Vangala و همکاران، 2023).

2-2 زنجیره‌های تأمین مبتنی بر اینترنت اشیاء

تغییر فضای رقابتی بازار و توسعه تجارت الکترونیک باعث شده است تا شرکت‌ها بتوانند محصولات و خدمات خود را بدون محدودیت جغرافیایی، به طیف گسترده‌ای از بازار ارائه کنند. پاسخگویی سریع به نیازهای متنوع مصرف‌کنندگان که از ویژگی‌های ذاتی دنیای تجارت الکترونیک است، اهمیت فرآیندهای لجستیک و زنجیره تأمین را بیش از پیش افزایش داده است. به همین دلیل در دنیای امروز، زنجیره تأمین به یکی از مهم‌ترین عناصر اقتصاد جهانی مبدل شده است (Nozari و همکاران، 2021). همچنین با توجه به حجم تراکنش‌های دنیای تجارت، این زنجیره اکنون بسیار پیچیده‌تر از گذشته و با هزینه‌های بیشتری مواجه است. از این رو کسب‌وکارهای امروزی در بسیاری از صنایع، به دنبال یافتن راهکارهایی برای بهبود وضعیت زنجیره تأمین خود هستند. این تغییرات جدید، صنعت لجستیک را وادار کرده تا هوشمندانه‌تر از پیش عمل کنند (Aliahmadi و همکاران، 2022).

با پیدایش فناوری‌های جدید مانند اینترنت اشیاء، کلان داده‌ها و هوش مصنوعی، زنجیره تأمین سنتی تغییر و تحولات زیادی را تجربه کرده است. به نظر می‌رسد؛ بسیاری از کارکردهای سیستم زنجیره تأمین سنتی با به‌کارگیری این فناوری‌های تازه، بازطراحی شده و شکل تازه‌ای به خود گرفته‌اند. فناوری اینترنت اشیاء به عنوان یکی از عناصر مهم در ارتقای زنجیره تأمین به شمار می‌آید. IoT به کمک ابزارهایی مانند سنسورها، کنترل‌کننده‌ها و دیگر دستگاه‌های مختلف مانند تگ‌های RFID و حتی دستگاه‌های موبایل، ارتباط میان افراد و اشیاء را برقرار می‌کند (Nahr و همکاران، 2021). پیش بینی زمان دقیق تحویل محصول یا خدمت، به عنوان یکی از اساسی‌ترین معضلات زنجیره تأمین؛ به کمک تحلیل کلان داده‌ها، با در نظر گرفتن شرایط آب و هوایی، ویژگی‌های وسایل نقلیه و ... امکان‌پذیر است. پیش‌بینی تقاضا با دقت بیشتر، شناسایی چرخه فرآیند خرید مشتری و مدیریت موجودی انبار، از مهم‌ترین مزایای تحلیل کلان داده‌هاست (Nozari و همکاران، 2022).

تحلیل کلان داده‌ها با شناسایی روندهای بازار، به تولیدکنندگان و شرکت‌های خرده فروشی کمک می‌کند به نوسان‌های تقاضا پاسخ دهند. پیش‌بینی تقاضا، بهبود ارائه خدمات به مشتری، کاهش هزینه‌های انبارداری، بهینه‌سازی انتخاب مسیرهای حمل و نقل و به شکل کلی بهبود وضعیت کسب و کار، برخی از مهم‌ترین نتایج تحلیل کلان داده‌هاست. جمع‌آوری داده‌ها در هر یک از ورودی‌ها در دامنه زنجیره تأمین، با استفاده از کامپیوترها، گوشی‌های هوشمند، تبلت‌ها و انواع حسگرها به عنوان ابزارهای اینترنت اشیاء صورت می‌گیرد (Ghahremani-Nahr و همکاران، 2022). این داده‌ها پس از اخذ با استفاده سیستم‌های پردازش قدرتمند مورد پردازش قرار می‌گیرند و تحلیل‌های کامل به منظور اتخاذ تصمیمات به عنوان خروجی سیستم زنجیره تأمین هوشمند ایجاد می‌شود. هر یک از ابزارهای اینترنت اشیاء با توجه به تعاملات در بخش‌های مختلف زنجیره تأمین می‌توانند عامل ایجاد رخنه و تهدید سایبری برای زنجیره تأمین باشند. با توجه به وجود فضای تعاملی در بسیاری از بخش‌های زنجیره تأمین بخصوص روابط با تأمین‌کنندگان و همچنین مشتریان، همواره بحث حریم خصوصی یکی از مهمتری موضوعات می‌باشد. لذا ایجاد فضای تهدیدآمیز و حملات سایبری در آن بسیار وجود خواهد داشت (Aliahmadi و همکاران، 2022).

در سال‌های اخیر تحقیقات بسیاری در خصوص شاخص‌های امنیتی اینترنت اشیاء و ارتباط این فناوری با زنجیره‌های تأمین صورت گرفته است. به عنوان مثال نوذری و همکاران (2021) تحلیل کمی از معیارهای امنیتی اینترنت اشیاء با متدلوژی تصمیم‌گیری ارائه کردند. آنها نشان دادند که حفظ حریم خصوصی از مهمترین معیارهای امنیتی می‌باشد. Hammi و همکاران (2023) در تحقیقی چالش‌های امنیتی را در زنجیره‌های تأمین مبتنی بر اینترنت اشیاء و بلاک‌چین مورد بررسی و واکاوی قرار دادند. آنها انواع تخدیداتی که به واسطه اینترنت اشیاء در زنجیره تأمین ایجاد می‌شود را استخراج نمودند. نوذری و عدالت‌پناه (2023) چارچوبی تحلیلی را به منظور مدیریت ریسک در سیستم‌های زنجیره تأمین هوشمند ارائه دادند. Vidhateو همکاران (2023) امنیت استفاده از سیستم‌های بلاک‌چین را در زنجیره‌های تأمین صنایع غذایی مورد بررسی قرار دادند. آنها نشان دادند که سیستم‌های هوشمند زنجیره تأمین علاوه بر داشتن مزایای بسیار، چالش‌های امنیتی بسیار را نیز تجربه می‌کند. Antouz و همکاران (2023) تأثیرات و چالش‌های امنیتی استفاده از اینترنت اشیاء را در سیستم‌های لجستیکی مورد بررسی و تحلیل قرار دادند. برخی از تحقیقات انجام شده در این زمینه در جدول (1) نشان داده شده است.

جدول 1: برخی از مطالعات انجام شده در خصوص امنیت زنجیره‌های تأمین هوشمند

نویسنده	رویکرد	تکنیک	صنعت
Abosuliman (2023)	تحلیل امنیت سایبری- فیزیکی	یادگیری عمیق	--
Srivastava(2022)	تحلیل مزایا و چالش‌ها	مرور سیستماتیک	غذایی- کشاورزی
Nozari et al.(2021)	ارزیابی معیارهای امنیتی	تصمیم‌گیری با معیارهای چندگانه	صنایع تند مصرف
Park et al., (2014)	مطالعه میدانی	تحلیل استراتژیک	کارخانجات چند ملیتی
Kieras et al., (2021)	تحلیل ریسک	چارچوب مفهومی	--
Powell (2022)	تحلیل علی و معلولی	سیستم‌های پویا	غذایی
Moudoud (2019)	تحلیل چالش‌ها	شبیه‌سازی	غذایی

مطالعات انجام شده مخصوصاً در سال‌های اخیر نشان از اهمیت بحث امنیت و مدیریت کردن ریسک‌های سایبری در زنجیره‌های تأمین مبتنی بر اینترنت اشیاء دارد. به همین منظور در این پژوهش این مبحث به صورت تحلیلی مورد واکاوی قرار گرفته است.

3- متدولوژی تحقیق

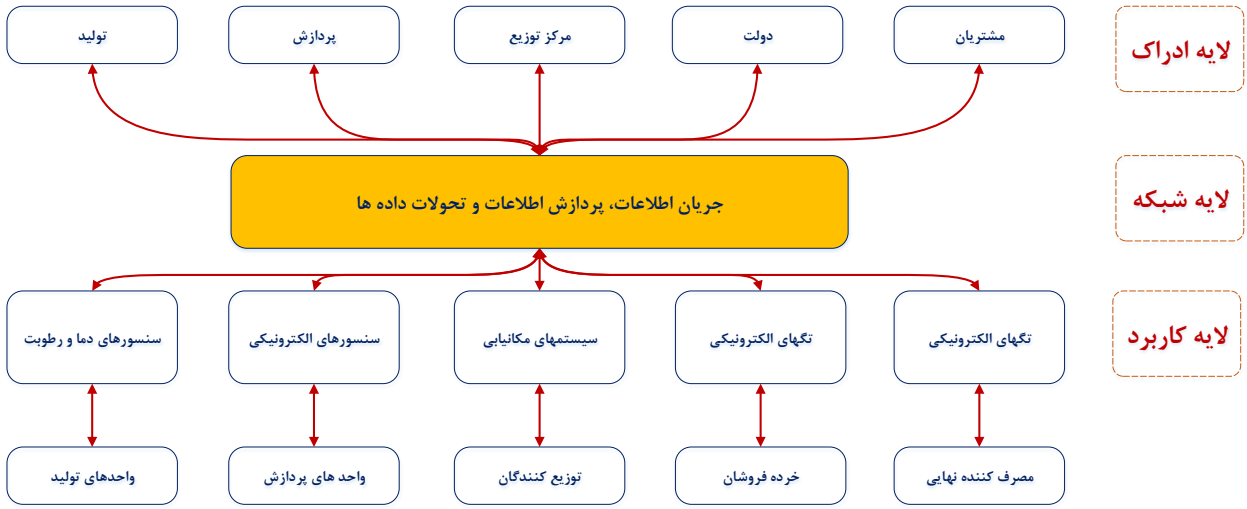
این پژوهش از نظر نتایج پژوهشی کاربردی و از منظر متغیرها کیفی است و در دسته پژوهش‌های توصیفی قرار می‌گیرد. این پژوهش به صورت پیمایشی صورت گرفته است. ابزار مورد استفاده در این پژوهش از نوع پرسشنامه‌های فازی می‌باشد. قلمرو مکانی این پژوهش شرکت‌های تند مصرف می‌باشد.شرکت های تند مصرف از جمله شرکتهایی هستند که دارای نقش پر رنگی در زندگی روزانه مردم داشته و سیستمهای زنجیره تامین آنها به دلیل سیستم توزیع به هنگام، دارای اهمیت بسیار حیاتی میباشد. خبرگان فعال در این پژوهش از میان افراد فعال در حوزه زنجیره تأمین و دارای سوابق کاری مرتبط در نظر گرفته شده‌اند. همچنین خبرگان دانشگاهی از میان اساتید دارای سوابق پژوهشی مرتبط انتخاب شده‌اند. ساختار پژوهش به شرح زیر می‌باشد.

1) بررسی ابعاد و مؤلفه‌های امنیتی در زنجیره تأمین هوشمند مبتنی بر اینترنت اشیاء با استفاده از نظرات خبرگان
2) پالایش داده‌های حاصل از مرور ادبیات با استفاده از نظرات خبرگان و به گزینی داده‌ها
3) اولویت بندی داده‌ها با استفاده از پرسشنامه و نظرات خبرگان
4) تعیین روابط علی و معلولی داده‌ها
5) توسعه چارچوب ارزیابی

چارچوب ارائه شده با تاکید بر روابط علی و معلولی ایجاد شده و با استفاده از نظرات خبرگان فعال اعتبارسنجی می‌شود.

4- چارچوب مدیریت ریسک‌ها زنجیره تأمین مبتنی بر اینترنت اشیاء

در این پژوهش یک سیستم زنجیره تأمین مبتنی بر اینترنت اشیاء در نظر گرفته می‌شود که شامل شبکه‌ای از اجزا و تأمین کنندگان فردی می‌شود. چارچوب ارائه شده، سلسله مراتبی از تأمین‌کنندگان اجزا و شبکه منطقی را در نظر می‌گیرد که وابستگی‌های متقابل اجزا و عملکرد سیستم را مشخص می‌کنند. شکل (1)، زنجیره تأمین مبتنی بر اینترنت اشیاء را در صنعت تند مصرف (صنایع غذایی) نشان می‌دهد.



شکل 1: زنجیره تأمین مبتنی بر اینترنت اشیاء در صنایع تند مصرف

جمع‌آوری و استخراج داده‌ها در هر یک از ورودی‌ها در دامنه زنجیره تأمین، با استفاده از کامپیوترها، گوشی‌های هوشمند، تبلت‌ها و انواع حسگرها به عنوان ابزارهای اینترنت اشیاء صورت می‌گیرد. این داده‌ها پس از اخذ با استفاده سیستم‌های پردازش قدرتمند مورد پردازش قرار می‌گیرند و تحلیل‌های کامل به منظور اتخاذ تصمیمات به عنوان خروجی سیستم زنجیره تأمین هوشمند ایجاد می‌شود. هر یک از ابزارهای اینترنت اشیاء با توجه به تعاملات در بخش‌های مختلف زنجیره تأمین می‌توانند عامل ایجاد رخنه و تهدید سایبری برای زنجیره تأمین باشند. با توجه به وجود فضای تعاملی در بسیاری از بخش‌های زنجیره تأمین بخصوص روابط با تأمین‌کنندگان و همچنین مشتریان، همواره بحث حریم خصوصی یکی از مهمتری موضوعات می‌باشد. لذا ایجاد فضای تهدیدآمیز و حملات سایبری در آن بسیار وجود خواهد داشت. مسائل زمان‌بندی توزیع مخصوصاً برای محصولات فاسدشدنی که زیربنای صنایع تند مصرف را تشکیل میدهند، نیز از جمله مباحث بسیار حیاتی در زنجیره تأمین صنایع تند مصرف می‌باشد. پس از بررسی مرور ادبیات و با استفاده از سیستم پالایش مبتنی بر نظرات خبرگان فعال ریسک‌های سایبری در این سیستم‌های زنجیره تأمین هوشمند استخراج شد. مهمترین ریسک‌های زنجیره تأمین مبتنی بر اینترنت اشیاء در جدول (2)، نشان داده شده است.

جدول 2: مهمترین ریسک‌های سایبری

ریسک‌های سایبری
اختلال در برنامه‌های تشخصی محیط، ترافیک
اختلال در ترابری و تحویل
عدم وجود برنامه امنیتی و حفظ حریم خصوصی در تعامل با تأمین‌کنندگان
عدم نظارت کافی بر دستگاه‌ها و سیستم‌ها برای تشخیص حوادث امنیتی
عدم ورود امنیت در طراحی محصولات و اکوسیستم
اختلال در شناسایی و درمان خطرات محصولات
عدم آگاهی و آموزش کافی امنیتی برای مهندسین
اجرای امنیت و مدیریت ریسک حریم خصوصی در تعامل با مشتریان
اختلال در بررسی موجودی محصولات
تداخل در زمان‌بندی‌ها برای توزیع و فروش

به دلیل پیچیدگی و تنوع ریسک در این زنجیره تأمین، نیاز روش‌های ارزیابی ریسک زنجیره تأمین صنایع تند مصرف تحت اینترنت اشیاء نیز بالا است. استفاده از فناوری‌های جدید در زنجیره تأمین صنایع تند مصرف تحت اینترنت اشیاء خطرات جدیدی را برای این زنجیره به همراه دارد. بنابراین، انتخاب روش ارزیابی ریسک باید بر اساس قابلیت ارزیابی دقیق ریسک‌های ناشناخته و ریسک‌هایی باشد که باعث خسارات قابل توجه یا نوسانات بزرگ می‌شوند. همه خطرات منجر به فروپاشی زنجیره تأمین نمی‌شود. مدیران زنجیره تأمین باید ایده قطعی

در مورد زمان بازسازی و بهینه‌سازی زنجیره تأمین برای به حداقل رساندن هزینه‌های نگهداری زنجیره تأمین و زمان بهبود ارزش آن را داشته باشند.

بر اساس این دو نکته، مدل ارزیابی ریسک زنجیره تأمین با استفاده از اپراتور OWA[1] توسط این مطالعه در مرحله ارزیابی ریسک زنجیره تأمین به کار گرفته شده است. ویژگی‌های اساسی عملگر میانگین وزنی مرتب شده (OWA) منجر به این شد که داده‌ها به ترتیب نزولی باشند و زمانی که هیچ اتصالی برای هر عنصر اتفاق نمی‌افتد، با وزن‌دهی جمع‌آوری می‌شوند. این مدل با مدل همگرایی انتشار ریسک زنجیره تأمین ترکیب می‌شود تا بهترین فرصت برای کنترل ریسک به مدیران زنجیره تأمین ارائه گردد. عملگرهای OWA یک کلاس پارامتری از عملگرهای تجمع نوع متوسط را ارائه می‌دهند.

تابع OWA $A_m \to A(a_1, a_2, ..., a_m)$ مجموعه داده شده‌ای از داده‌ها است که $a_i = (a_{1i}, a_{2i}, ..., a_{ni})^T$ و $W = (w_1, w_2, ..., w_m)^T$ بردارهای وزنی هستند که با تابع OWA مرتبط هستند. مدیران می‌توانند با توجه به وضعیت واقعی و با توجه به سطح تجربه خود، c_{ij} را به عنوان نتایج پردازش وزنی نسبت کوچکترین عناصر ستون j در $(a_1, a_2, ..., a_m)$ به هر عنصر در ستون نسبت دهند. به مقادیر مشخصه مربوطه. این اپراتور قادر است داده‌ها $(a_1, a_2, ..., a_m)$ را با توجه به نوع ارزش دارایی مورد نیاز مانند ویژگی‌های هزینه پردازش کند. پس از بدست آوردن C_{ij}، مقدار وزنی محاسبه شده و نتایج به ترتیب نزولی مرتب می‌شوند. این مدل برای ارزیابی ریسک نوسانات بزرگ در شاخص‌های ریسک و اثرات قابل توجه خطرات قابل استفاده است. این مدل همچنین برای ارزیابی ریسک زنجیره تأمین صنایع تند مصرف مبتنی اینترنت اشیاء مناسب است، که دارای عوامل خطر قابل‌توجه و بی‌ثباتی ریسک بالا است. ما فرض می‌کنیم که یک زنجیره تأمین صنعت تند مصرف با n نوع خطر مواجه می‌شود.

$X = (x_1, ..., x_i, ..., x_n)$ $i = 1,2,...,n$ را تنظیم می‌کنیم و هر ریسک را با توجه به مجموعه شاخص m بیان می‌کنیم. ریسک x_i با ویژگی‌ها اندازه‌گیری می‌شود. پس از آن، مقدار مشخصه a_{ij} از x_i با توجه به وضعیت واقعی برای تشکیل ماتریس تصمیم $A = (a_{ij})n \cdot m$ به دست می آید.

$$A = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & ... & a_{mn} \end{bmatrix} \quad (1)$$

روش‌های محاسبه متفاوتی با توجه به مقادیر مشخصه‌های مختلف موجود است. در این مطالعه، ویژگی‌های هزینه، که می‌توانند به بهترین نحو تأثیر عوامل خطر مختلف را بر کل زنجیره تأمین منعکس کنند، زیرا زنجیره تأمین یک زنجیره ارزش است، برای اندازه‌گیری ارزش ریسک استفاده می‌شود. علاوه بر این، از رابطه (2) برای ارزیابی کمی عوامل خطر مختلف استفاده می‌شود.

$$C_{ij} = \frac{\min_i a_{ij}}{a_{ij}},\ i \in Nor\ C_{ij} = \frac{\max_i a_{ij} - a_{ij}}{\max_i a_{ij} - \min_i a_{ij}},\ i \in N \quad (2)$$

C را می‌توان از A به عنوان استاندارد شده و با معادله (2) بدست آورد.

$$C = \begin{bmatrix} c_{11} & c_{12} & ... & c_{1n} \\ c_{21} & c_{22} & ... & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & ... & c_{mn} \end{bmatrix} \quad (3)$$

عملگر OWA برای جمع‌آوری عوامل خطر مختلف $x_i \ \ i \in N$ برای به دست آوردن مقدار مشخصه جامع $Z_i(w)$ استفاده می‌شود.

$$Z_i(W) = OWA_w(c_{i1}, ..., c_{im}) = \sum_{j=1}^{m} w_j c_{ij} \quad (4)$$

با استفاده از رابطه (4) این خطرات را می‌توان طبقه‌بندی کرد. پس از آن، اثر هر ریسک بر کل زنجیره تأمین را می‌توان تعیین کرد.

[1] ordered weighted averaging

قبل از ارزیابی کمی ریسک ها، دو مشکل، یعنی تخصیص وزن هر ریسک در زنجیره تأمین و تعیین ارزش زیان‌های ناشی از هر ریسک خاص باید مورد توجه قرار گیرد. برای راحتی در محاسبه، تنها یک ریسک در هر سطح از همان نوع انتخاب می‌شود. علاوه بر این، هر وزن تخصیص داده می‌شود و کاهش مربوطه بر اساس گزارش‌های نظرسنجی مربوطه ارزیابی می‌شود. ارزش وزن بر اساس تجربه مدیران تخصیص داده می‌شود و مقادیر تلفات در فاصله زمانی پنج واحد بر اساس اندازه ضرر تنظیم می‌شوند و از 0 تا 100 علامت‌گذاری می‌شوند. داده‌های خاص عمدتاً بر اساس موارد قبلی است ادبیات، مصاحبه و بحث با کارشناسان، و اتخاذ مدل‌های مرتبط از قبل موجود می‌باشد. داده‌های جدول (3) ارزش زیان ریسک و احتمال ریسک را نشان می‌دهد.

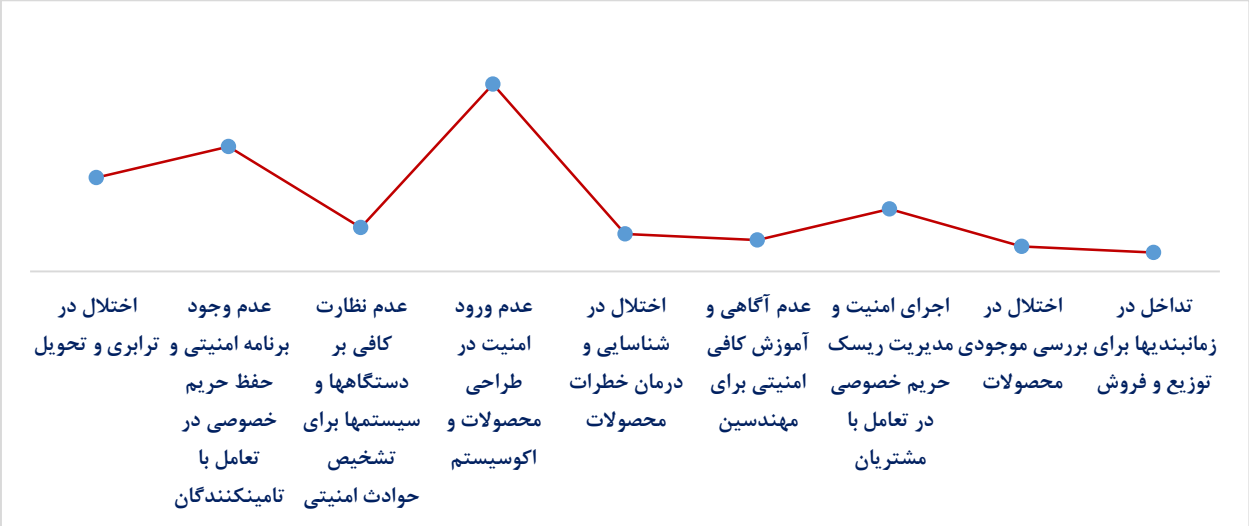
جدول 3: ریسک‌های سایبری زنجیره تأمین مبتنی بر اینترنت اشیاء در صنایع تند مصرف با استفاده از عملگر OWA

ریسک	مقدار زیان	احتمال وقوع
اختلال در برنامه‌های تشخصی محیط، ترافیک	30	15٪
اختلال در ترابری و تحویل	15	20٪
عدم وجود برنامه امنیتی و حفظ حریم خصوصی در تعامل با تأمینکنندگان	10	40٪
عدم نظارت کافی بر دستگاه‌ها و سیستم‌ها برای تشخیص حوادث امنیتی	15	25٪
عدم ورود امنیت در طراحی محصولات و اکوسیستم	25	20٪
اختلال در شناسایی و درمان خطرات محصولات	15	30٪
عدم آگاهی و آموزش کافی امنیتی برای مهندسین	10	25٪
اجرای امنیت و مدیریت ریسک حریم خصوصی در تعامل با مشتریان	5	20٪
اختلال در بررسی موجودی محصولات	20	23٪
تداخل در زمان‌بندی‌ها برای توزیع و فروش	5	11٪

با بدست آوردن مقادیر مشخصه جامع $Z_i(w)$ می‌توانیم اولویت هر داده را درک نماییم.

$$x_4 > x_2 > x_1 > x_8 > x_3 > x_5 > x_7 > x_6 > x_9 > x_{10}$$

خطرات اولیه‌ای که زنجیره تأمین صنایع تند مصرف مبتنی بر اینترنت اشیاء با آن مواجه است امنیت اطلاعات و حفظ حریم خصوصی و ریسک‌های توزیع است. بنابراین، خطرات زنجیره تأمین صنایع تند مصرف مبتنی بر اینترنت اشیاء، نتیجه معرفی فناوری اینترنت اشیاء است. ریسک‌های زنجیره تأمین صنایع تند مصرف سنتی، مانند ریسک‌های همکاری داخلی و خارجی، به طور کلی اجتناب می‌شود. ریسک‌های قدیمی با ظهور ریسک‌های جدید منتقل می‌شوند. مشکل ریسک زنجیره تأمین را می‌توان به طور منطقی حل کرد و بر اساس ریسک‌های ذکر شده می‌توان بر حل تناقض اصلی تمرکز کرد. این رویه نه تنها مشکل ریسک زنجیره تأمین را به طور کارآمد و مؤثر حل می‌کند، بلکه زنجیره تأمین صنایع تند مصرف موجود را نیز بهینه می‌کند. در نتیجه، ارزش کل زنجیره تأمین را می‌توان بهبود بخشید. شکل (2)، میزان اولویت داده‌ها را نشان می‌دهد.



شکل 2: بررسی معیارهای ریسک در زنجیره تأمین مبتنی بر اینترنت اشیاء

همانگونه که مشاهده می‌شود فرآیندهای مربوط به حمل و نقل مواد اولیه و محصولات در صنایع تند مصرف، یکی از مهم‌ترین بخش‌هایی است که به شدت تحت تاثیر فناوری اینترنت اشیا قرار می‌گیرد. حمل و نقل همیشه یک فرآیند غیرقابل پیش‌بینی بوده که مستلزم کنترل است. حالا فناوری اینترنت اشیا فرصتی فراهم کرده است که وسایل نقلیه مجهز به دوربین‌ها و حسگرهایی باشند که می‌تواند وضعیت فیزیکی و حتی روانی راننده را ارزیابی و تجزیه و تحلیل کند. این داده‌ها بی‌درنگ برای افراد مسئول ارسال می‌شود تا بهتر فرآیندهای حمل و نقل را مدیریت کنند. علاوه بر این، امنیت محموله‌ها نیز از این طریق با اطمینان بیشتری تامین می‌شود. به همین دلایل طراحی محصولات و اکوسیستم امن در این فرایندها همواره دارای اهمیت بالایی میباشد که نتایج تحلیل نیز این امر را اثبات میکند.

تأکید بر روی حفظ حریم خصوصی مشتریان و تأمین کنندگان نیز از مهمترین معیارهای امنیتی در زنجیره تأمین هوشمند در صنایع تند مصرف می‌باشد. به لحاظ راهبردی نیز تحقیق حاضر نشان میدهد که سیستمهای هوشمند مبتنی بر اینترنت اشیا اگرچه دارای مزایای بسیاری هستند ولی باید همواره به معیارهای امنیتی در آنها توجه ای ویژه ای داشت.درک درست این معیار ها میتوان راه حل های به هنگامی را در اختیار متولیان و مسئولین سیستمهای زنجیره تامین مخصوصا در صنایع تند مصرف قرار دهد.

نتیجه‌گیری

این پژوهش خطرات زنجیره تأمین صنایع تند مصرف مبتنی بر اینترنت اشیاء را مورد بحث قرار می‌دهد و خطرات زنجیره تأمین صنایع تند مصرف فعلی را از طریق تجزیه و تحلیل کیفی طبقه بندی و خلاصه می‌کند. نویسندگان اندازه عوامل خطر را از دیدگاه کمی بر اساس یک مدل ریاضی اندازه‌گیری می‌کنند. در نهایت، با توجه به محاسبات مدل، چندین معیار مدیریت ریسک و کنترل برای زنجیره تأمین صنایع تند مصرف تحت اینترنت اشیاء پیشنهاد شده است.

زنجیره‌های تأمین هوشمند مبتنی بر اینترنت اشیاء در صنایع تند مصرف در سال‌های اخیر دارای رشد فزاینده بوده است. حضور اینترنت و شبکه همواره بر خطرات موجود در این زنجیره‌های تأمین که دارای اهمیت بالایی در زندگی روزانه مردم هستند می‌افزاید. با این حال، اقدامات خاص می‌تواند به طور قابل توجهی از خطر زنجیره تأمین صنایع تند مصرف مبتنی بر اینترنت اشیاء جلوگیری کند. این اقدامات شامل افزایش به اشتراک گذاری اطلاعات، تضمین امنیت اطلاعات، تسریع ساخت زیرساخت‌ها، بهبود مشارکت دولت و افزایش نظارت است. مدیران زنجیره تأمین نیاز به ارزیابی کمی عوامل خطر در زنجیره تأمین صنایع تند مصرف، تعیین دقیق وضعیت عملکرد زنجیره تأمین صنایع تند مصرف، تنظیم استراتژی مدیریت زنجیره تأمین به موقع، تقویت نظارت بر دستگاه‌ها بر روی اینترنت اشیاء و بهبود تدریجی دارند. توانایی مدیریت ریسک و کنترل زنجیره تأمین صنایع تند مصرف دارای اهمیت بالایی می‌باشد. نتایج ارزیابی می‌تواند مدیران را در پیشنهاد بهبود برای شرکت‌کنندگان زنجیره تأمین راهنمایی کند و در نتیجه کل زنجیره تأمین را در وضعیتی با ارزش کم ریسک قرار دهد. زمانی که شاخص‌های پایش دارای نوسانات قابل‌توجهی هستند یا بالاتر از سطح دوره قبل هستند، مدیران باید فوراً نوسانات داده‌ها را ردیابی کرده و با توجه به محیط فعلی توضیح منطقی ارائه کنند تا احتمال خطر کاهش یابد و توانایی‌های مدیریت اضطراری پس از خطر بهبود یابد. حصول اطمینان از اینکه کل زنجیره تأمین صنایع تند مصرف در حالت ثابت اجرا می‌شود، نیازمند راهنمایی مناسب بخش‌های مدیریت زنجیره تأمین و همچنین همکاری شرکت‌کنندگان مختلف است. همانطور که اینترنت اشیاء به بلوغ می‌رسد و استانداردهای صنعت مربوطه به طور مداوم بهبود می‌یابد، اینترنت اشیاء زنجیره تأمین صنایع تند مصرف به سرعت در آینده توسعه خواهد یافت و به تدریج هدف نوسازی زنجیره تأمین کشاورزی محقق خواهد شد. به همین دلیل در این پژوهش کوشیده شد مهمترین ابعاد و شاخص‌های امنیتی در زنجیره‌های تأمین مبتنی بر اینترنت اشیاء مورد ارزیابی قرار گرفته و چهارچوبی برای کاهش میزان خطرات ارائه شود. درک درست این چاچوب می‌تواند راهنمای ارزشمندی برای پیاده سازی این سیستم‌های هوشمند ارزشمند باشد.

منابع

Nozari, H., Fallah, M., Szmelter-Jarosz, A., & Krzemiński, M. (2021). Analysis of security criteria for IoT-based supply chain: a case study of FMCG industries. *Central European Management Journal*, *29*(4).

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

Nozari, H., & Edalatpanah, S. A. (2023). Smart Systems Risk Management in IoT-Based Supply Chain. In *Advances in Reliability, Failure and Risk Analysis* (pp. 251-268). Singapore: Springer Nature Singapore.

Vidhate, A. V., Saraf, C. R., Wani, M. A., Waghmare, S. S., & Edgar, T. (2023). Applying blockchain security for agricultural supply chain management. In *Research Anthology on Convergence of Blockchain, Internet of Things, and Security* (pp. 1229-1239). IGI Global.

Antouz, Y. A., Akour, I. A., Alshurideh, M. T., Alzoubi, H. M., & Alquqa, E. K. (2023, March). The impact of Internet of Things (IoT) and Logistics Activities on Digital Operations. In *2023 International Conference on Business Analytics for Technology and Security (ICBATS)* (pp. 1-5). IEEE.

Abosuliman, S. S. (2023). Deep learning techniques for securing cyber-physical systems in supply chain 4.0. *Computers and Electrical Engineering*, *107*, 108637.

Srivastava, A., & Dashora, K. (2022). Application of blockchain technology for agrifood supply chain management: A systematic literature review on benefits and challenges. *Benchmarking: An International Journal*.

Nozari, H., Ghahremani-Nahr, J., Fallah, M., & Szmelter-Jarosz, A. (2022). Assessment of cyber risks in an IoT-based supply chain using a fuzzy decision-making method. *International Journal of Innovation in Management, Economics and Social Sciences*, *2*(1).

Park, J., Lee, H., & Kim, C. (2014). Corporate social responsibilities, consumer trust and corporate reputation: South Korean consumers' perspectives. *Journal of business research*, *67*(3), 295-302.

Kieras, T., Farooq, J., & Zhu, Q. (2021). I-SCRAM: A framework for IoT supply chain risk analysis and mitigation decisions. *IEEE Access*, *9*, 29827-29840.

Powell, W., Foth, M., Cao, S., & Natanelov, V. (2022). Garbage in garbage out: The precarious link between IoT and blockchain in food supply chains. *Journal of Industrial Information Integration*, *25*, 100261.

Moudoud, H., Cherkaoui, S., & Khoukhi, L. (2019, September). An IoT blockchain architecture using oracles and smart contracts: the use-case of a food supply chain. In *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)* (pp. 1-6). IEEE.

Ivanov, D., Dolgui, A., & Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *International Journal of Production Research*, *57*(3), 829-846.

El Baz, J., Cherrafi, A., Benabdellah, A. C., Zekhnini, K., Beka Be Nguema, J. N., & Derrouiche, R. (2023). Environmental Supply Chain Risk Management for Industry 4.0: A Data Mining Framework and Research Agenda. *Systems*, *11*(1), 46.

Li, L., Gong, Y., Wang, Z., & Liu, S. (2023). Big data and big disaster: a mechanism of supply chain risk management in global logistics industry. *International Journal of Operations & Production Management*, *43*(2), 274-307.

Fernando, Y., Tseng, M. L., Wahyuni-Td, I. S., de Sousa Jabbour, A. B. L., Chiappetta Jabbour, C. J., & Foropon, C. (2023). Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in Malaysia. *Journal of Industrial and Production Engineering*, *40*(2), 102-116.

Shakatreh, M., Rumman, M. A. A., & Mugableh, M. I. (2023). Reviewing the framework of risk management: policy and hedging. *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.*, *8*(1), 7.

Ashok, K., & Gopikrishnan, S. (2023). Statistical Analysis of Remote Health Monitoring Based IoT Security Models & Deployments From a Pragmatic Perspective. *IEEE Access*, *11*, 2621-2651.

Ashok, K., & Gopikrishnan, S. (2023). Statistical Analysis of Remote Health Monitoring Based IoT Security Models & Deployments From a Pragmatic Perspective. *IEEE Access*, *11*, 2621-2651.

Vasilescu, N. G., Pocatilu, P., & Doinea, M. (2023, January). IoT Security Challenges for Smart Homes. In *Education, Research and Business Technologies: Proceedings of 21st International Conference on Informatics in Economy (IE 2022)* (pp. 41-49). Singapore: Springer Nature Singapore.

Sallay, H. (2023). An Integrated Multilayered Framework for IoT Security Intrusion Decisions. *Intelligent Automation & Soft Computing*, *36*(1).

Vangala, A., Das, A. K., Chamola, V., Korotaev, V., & Rodrigues, J. J. (2023). Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges. *Cluster Computing*, *26*(2), 879-902.

Nozari, H., & Aliahmadi, A. (2022). Lean supply chain based on IoT and blockchain: Quantitative analysis of critical success factors (CSF). *Journal of Industrial and Systems Engineering*, *14*(3), 149-167.

Aliahmadi, A., Nozari, H., Ghahremani-Nahr, J., & Szmelter-Jarosz, A. (2022). Evaluation of key impression of resilient supply chain based on artificial intelligence of things (AIoT). *arXiv preprint arXiv:2207.13174*.

Ghahremani-Nahr, J., Aliahmadi, A., & Nozari, H. (2022). An IoT-based sustainable supply chain framework and blockchain. *International Journal of Innovation in Engineering*, *2*(1), 12-21.

Aliahmadi, A., Nozari, H., & Ghahremani-Nahr, J. (2022). Big Data IoT-based agile-lean logistic in pharmaceutical industries. *International Journal of Innovation in Management, Economics and Social Sciences*, *2*(3), 70-81.

Nahr, J. G., Nozari, H., & Sadeghi, M. E. (2021). Green supply chain based on artificial intelligence of things (AIoT). *International Journal of Innovation in Management, Economics and Social Sciences*, *1*(2), 56-63.

Nozari, H., Fallah, M., Kazemipoor, H., & Najafi, S. E. (2021). Big data analysis of IoT-based supply chain management considering FMCG industries. *Бизнес-информатика*, *15*(1 (eng)), 78-96.