Journal of Decisions and Operational Research

Journal of Decisions & Operations Research

Volume 5, Issue 4, Winter 2020

Quantitative Analysis of Cyber Risks in IoT-Based Supply Chain (FMCG Industries)

Mohammad Fallah[1,*], Hamed Nozari[2]

[1]Associate Professor of Industrial Engineering, Faculty of Engineering, Central Tehran Branch, Islamic Azad University, Tehran, Iran.
[2]Assistant Professor of Department of Industrial Engineering, Central Tehran Branch, University of Tehran Markaz, Tehran, Iran.

Abstract

The Internet of Things (IoT) is a system of computers, computing machines, digital and mechanical devices, humans and animals, each with an independent code and as a distinct device, in the network and a significant share of information exchange and behavior and the relationship between them is done without direct human intervention and supervision. Businesses are no exception and try to use the IoT to make business smarter. The supply chain is one of the most vital parts of the business cycle and its smartening creates a dramatic change in the optimization of business processes. However, since this technology is based on the Internet and the use of the Internet can always be associated with different risks, so recognizing the cyber risks that can be faced by businesses in the face of these technologies is always significant IoT-based supply chain cyber to be identified and analyzed. In order to rank these risks, nonlinear mathematical modeling method has been used. The results show that privacy in interaction with suppliers as well as customers is the most important and effective measures should be taken to address these risks.

Keywords: IoT, Cyber risks, Smart supply chain, IoT security, FMCG industry supply chain.

Original Paper

Receive: 09/06/2020 Review: 14/07/2020 Revise: 14/09/2020 Accept: 08/11/2020

Citation:

Fallah, M., & Nozari, H. (2020). Quantitative analysis of cyber risks in iot-based supply chain (FMCG Industries). *Decisions & operations research, 5*(4), 510-521.

*** Corresponding Author**

Email Address: mohammad.fallah43@yahoo.com

DOI: 10.22105/dmor.2020.261431.1281

www.journal-dmor.ir

Journal of Decisions & Operations Research, Volume 5, Issue 4, Winter 2020, Page: 510-521

نشریه علمی
تصمیم‌گیری و تحقیق در عملیات
Journal of Decisions and Operational Research
دوره ۵، شماره ۴، زمستان ۱۳۹۹

بررسی کمی ریسک‌های سایبری در زنجیره تامین مبتنی بر اینترنت اشیا صنایع (صنایع FMCG)

محمد فلاح[۱،*]، حامد نوذری[۲]

[۱]دانشیار گروه مهندسی صنایع، دانشکده مهندسی، واحد تهران مرکز، دانشگاه آزاد اسلامی، تهران، ایران.

[۲]استادیار گروه مهندسی صنایع، واحد تهران مرکز، دانشگاه آزاد اسلامی، تهران، ایران.

چکیده

اینترنت اشیاء یک الگوی نوظهور است که بر اتصال دستگاه‌ها و اشیاء به یکدیگر برمبنای اینترنت و کاربران متمرکز می‌باشد. این فناوری پایه‌ای برای هوشمند سازی زندگی امروزه انسان‌ها است. در این میان کسب‌وکارها نیز از این امر مستثنی نیستند و می‌کوشند تا با استفاده از این فناوری اینترنت اشیا در راستای هوشمند کردن کسب‌وکار استفاده نمایند. زنجیره تامین یکی از حیاتی‌ترین بخش‌های چرخه کسب‌وکار می‌باشد و هوشمندسازی آن تحول شگرفی در بهینه‌سازی فرایندهای کسب‌وکار ایجاد می‌نماید. اما از آن‌جایی که این فناوری با اینترنت همراه بوده و همواره استفاده از اینترنت می‌تواند با خطراتی همراه باشد بنابراین درک خطرات سایبری که می‌تواند در مواجه با این فناوری‌ها متوجه کسب‌وکارها باشد همواره قابل ملاحظه است.در این پژوهش سعی شده است تا خطرات سایبری زنجیره تامین مبتنی بر اینترنت اشیا شناسایی و بررسی شود. به‌منظور رتبه‌بندی این خطرات، از روش مدل‌سازی ریاضی غیرخطی استفاده شده است. نتایج نشان می‌دهد که حفظ حریم خصوصی در تعامل با تامین کنندگان و همچنین مشتریان دارای بیشترین اهمیت می‌باشد و باید برای مواجهه با این خطرات تمهیدات موثری در نظر گرفته شود.

واژه‌های کلیدی: اینترنت اشیا، ریسک‌های سایبری، زنجیره تامین هوشمند، امنیت اینترنت اشیا، زنجیره تامین صنایع *FMCG*.

مقاله پژوهشی

دریافت: ۱۳۹۹/۰۳/۲۰ داوری: ۱۳۹۹/۰۴/۱۴ اصلاح: ۱۳۹۹/۰۶/۲۴ پذیرش: ۱۳۹۹/۰۹/۱۸

۱- مقدمه

اخیرا، مفهوم کسب‌وکارها هوشمند و ابزارهای آن ، به‌عنوان شکلی جدید از توسعه پایدار گسترش یافته‌اند و بیانگر مدل کسب‌وکاری می باشند که ارائه‌دهنده راهکارهایی برای بهبود کیفیت و عملکرد فعالیت‌ها و بهینه‌سازی فرایندها، به‌منظور تعامل بهتر بین بازیگران اصلی سیستم‌های تولیدی و خدماتی می‌باشند (دیماس و همکاران[۱]، ۲۰۱۸). فضای هوشمند کسب‌وکارها، همواره با بخش عظیمی از داده‌ها سروکار دارد و همین امر چالش‌ها و فرصت‌های بسیاری در این زمینه ایجاد کرده است. منابع اطلاعاتی جدید فرصت‌هایی را برای برنامه‌های

[۱]DiMase et al.

* نویسنده مسئول
آدرس رایانامه: mohammad.fallah43@yahoo.com
شناسه دیجیتال: 10.22105/dmor.2020.261431.1281

جدید فراهم می‌کنند تا کیفیت فعالیت‌ها را بهبود بخشند. بررسی داده‌های حاصل از فعالیت‌ها در بخش‌های مختلف کسب کار، علاقهٔ جوامع تحقیقاتی حوزه‌های گوناگون ازجمله داده‌کاوی و یادگیری ماشین، علوم انرژی و محیط‌زیست، علوم اجتماعی،بهینه‌سازی، برنامه‌ریزی و حمل‌ونقل را به خود جلب کرده است (سعادتی و مهرشاد[۱]، ۲۰۱۷). فناوری اینترنت اشیا به‌عنوان یکی از بزرگ‌ترین منابع تولید داده‌های عظیم نقش بسیار پررنگی در هوشمندسازی کسب‌وکارها دارد. اما تولید، ذخیره‌سازی، نگهداری و پردازش این داده‌ها همواره چالش‌های بسیاری را با خود همراه خواهد داشت.حفظ حریم خصوصی و امنیت داده‌ها یک نگرانی بزرگ برای آن‌هاست. تعاملات در شبکه‌های اجتماعی و به اشتراک‌گذاری داده‌ها، استفاده از تلفن‌ها هوشمند که به خصوصی‌ترین بخش‌های زندگی امروزی تسلط دارند و بسیاری از چالش‌های دیگر همواره نگرانی‌هایی را برای صاحبان کسب‌وکارها فراهم آورده است (بویس و همکاران[۲]، ۲۰۱۸). چالش‌هایی که باید به‌شدت مورد واکاوی قرار بگیرند زیرا بی‌توجهی به آن‌ها می‌توان خسارت‌های جبران‌ناپذیری را به همراه داشته باشد.

زنجیره تامین چرخه اساسی کسب‌وکارها است و بنابراین بهینه‌سازی فرایندهای آن می‌توان تاثیر مستقیمی روی رشد کسب‌وکار داشته باشد. هر چه میزان داده‌های موجود در فرایندهای کسب‌وکار بیشتر باشد، این امر می‌تواند تصمیم‌گیری در بخش‌های مختلف را آسان‌تر کند، به‌شرط آن‌که راهکارهای اساسی برای استفاده درست از داده‌ها و عملیات مناسب برای تحلیل صحیح داده‌ها وجود داشته باشد. ادغام فن‌آوری دیجیتال اینترنت اشیا[۳] (*IoT*) در زنجیره‌های تأمین نیاز به معماری استانداردسازی مراجع به‌منظور مدیریت کارآمد پیچیدگی‌ها و منابع دارد (گوبی و همکاران[۴]، ۲۰۱۳).زنجیره‌های تامین دیجیتال انواع جدیدی از ریسک‌های سایبری را در اقتصاد دیجیتال در معرض دید قرار می‌دهند. تأثیر فن‌آوری‌های اینترنت اشیا بر ریسک سایبری زنجیره تأمین به‌ندرت در ادبیات دانشگاهی موردبحث قرار گرفته است و اقتصاد دیجیتال درحال حاضر فاقد شفاف‌سازی در سطوح فردی چالش‌های استراتژیک، کاربردی و عملیاتی از فناوری‌های دیجیتال اینترنت اشیا در زنجیره تأمین است. به همین دلیل در این پژوهش سعی شده است تا با بررسی ادبیات موضوع و همچنین بررسی زنجیره تامین صنایع تند مصرف[۵] (*FMCG*) (به‌طور خاص صنایع غذایی و صنایع دارویی) و استفاده از نظرات خبرگان ریسک‌های سایبری که به‌واسطه استفاده از اینترنت اشیا در زنجیره تامین رخ خواهد داد، بررسی شود. پس از آن با استفاده از روش رتبه‌بندی فازی با استفاده از متد مدل‌سازی غیرخطی میخایلوف[۶] (۲۰۰۳) که مبتنی بر روش تحلیل سلسه مراتبی است، به بررسی میزان اهمیت هر یک از ریسک‌های سایبری پرداخته می‌شود.در بخش اول مرور ادبیات موضوع در دو شاخه بررسی اینترنت اشیا و زنجیره تامین مبتنی بر اینترنت اشیا بررسی می‌شود. در بخش دوم ریسک‌های سایبری زنجیره تامین هوشمند با تاکید بر زنجیره تامین شرکت‌های *FMCG* مورد واکاوی قرار می‌گیرند و سپس با معرفی روش رتبه‌بندی فازی غیرخطی، وزن و رتبه هر یک از ریسک‌های سایبری حاصل خواهد شد. در انتها نیز نتایج موردبررسی قرار خواهد گرفت.

۲- مرور ادبیات

در این بخش به بررسی ادبیات موضوع در زمینه بررسی اینترنت اشیا و کاربردهای آن و پژوهش‌های صورت‌گرفته در این زمینه می پردازیم، و در بخش دوم نیز به بررسی ادبیات مرتبط با زنجیره تامین مبتنی بر اینترنت اشیا که اساس این تحقیق را تشکل می‌دهد خواهیم پرداخت.

---

[۱] Saadati & Mehrshad
[۲] Boyes et al.
[۳] Internet of Things
[۴] Gubbi et al.
[۵] Fast-Moving Consumer Goods
[۶] Mikhailov

۱-۲- اینترنت اشیا

اینترنت اشیا درواقع شبکه‌ای است که در آن هر شیء فیزیکی به‌وسیله برچسبی هویت می‌یابد و با اشیاء دیگر رابطه پیدا می‌کند. این ارتباط را می‌توان با استفاده از فناوری‌های موجود در تلفن‌های هوشمند و تبلت‌ها کنترل نمود و مدیریت کرد (اشتون[۱]، ۲۰۰۹). با استفاده از فناوری اینترنت اشیا، کالاها می‌توانند نسبت به شناسه‌های الکترونیکی مزایایی بیشتری را همراه داشته باشند (https://www.itu.int/en/ITU-T/ssc/resources/Pages/topic-001.aspx).

استفاده از اینترنت اشیا، به‌عنوان یکی از بزرگ‌ترین منابع تولید داده‌های عظیم یا کلان داده‌ها[۲] (کاتاکیس[۳]، ۲۰۱۵)، دارای مزایای بسیاری برای زندگی هوشمند و همچنین کسب‌وکارهای هوشمند است. این منافع شامل بهبود فرآیندهای عملیاتی، خلق ارزش، کاهش هزینه و حداقل‌کردن ریسك می‌باشند که درنتیجه‌ی شفافیت، قابلیت رهگیری، سازگاری، مقیاس‌پذیری و انعطاف‌پذیری ایجادشده توسط اینترنت اشیا است (چای و همکاران[۴]، ۲۰۱۰). در الگوی اینترنت اشیاء، بسیاری از اشیاء موجود در اطراف ما به یک شکل یا شکل دیگر در شبکه قرار می‌گیرند. شناسایی مبتنی بر فرکانس رادیویی[۵] (RFID) و فن‌آوری‌های شبکه حسگر برای برطرف‌کردن این چالش جدید افزایش می‌یابند و سیستم‌های اطلاعاتی و ارتباطی به‌طور ناخواسته در محیط اطراف ما تعبیه می‌شوند. این امر خود منجر به تولید مقادیر عظیمی از داده‌هایی می‌شود که باید به‌صورت یکپارچه، کارآمد و قابل تفسیر، ذخیره و پردازش و ارائه شوند (اتزوری و همکاران[۶]،۲۰۱۰). محاسبات ابری می‌تواند زیرساخت‌های مجازی برای چنین محاسباتی را ارائه دهد به‌طوری که توانایی یکپارچه‌سازی دستگاه‌های مانیتورینگ ، ابزارهای تحلیلی ذخیره‌سازی ، قالب‌بندی‌ها و تحویل مشتری را در یکجا و به‌صورت هم‌زمان داشته باشند (ورمسان و فریز[۷]، ۲۰۱۴).

مدل مبتنی بر هزینه که محاسبات ابری ارائه می‌دهند امکان ارائه خدمات کامل نرم‌افزاری و سخت‌افزاری را برای مشاغل و کاربران به‌منظور دسترسی به برنامه‌های درخواستی از هرجایی فراهم می‌کند. اتصال هوشمند با شبکه‌های موجود و محاسبه جامع با استفاده از منابع شبکه ، یک بخش ضروری از اینترنت اشیا است. با این وجود، برای ظهور موفقیت‌آمیز چشم‌اندازهای اینترنت اشیا، نیاز به محاسباتی فراتر از سناریوهای رایانه‌ای و تلفن همراه است که از تلفن‌های هوشمند و قابل‌حمل استفاده می‌کنند و در اتصال اشیاء موجود روزمره و هوشمندسازی‌های متداول در محیط ما تکامل می‌یابد (ال-ترجمان[۸]، ۲۰۱۹). با توجه به اهمیت موضوع و رشد روزافزون استفاده از این فناوری و قابلیت‌های آن تحقیقات بسیاری در این زمینه تاکنون صورت گرفته است. برای نمونه اکیلیدیز[۹] و همکاران (۲۰۰۲) در تحقیقی به بررسی استفاده از اینترنت اشیا در سیستم‌های حمل‌ونقل اتوبوس پرداختند.کلی[۱۰] و همکاران (۲۰۱۳) نیز در تحقیقی اجرای مؤثر اینترنت اشیاء به‌منظور نظارت بر شرایط منظم داخلی از طریق سیستم سنجش همه‌کاره کم‌هزینه را موردبررسی قرار دادند. هو[۱۱] و همکاران (۲۰۱۷) نیز مدیریت ابزارهای اینترنت اشیا با استفاده از فناوری بلاک‌چین[۱۲] را ارزیابی کردند.

نشریه تصمیم‌گیری و تحقیق در عملیات، دوره ۵، شماره ۴، زمستان ۱۳۹۹، صفحه: ۵۲۱-۵۱۰

---

۱ Ashton
۲ Big Data
۳ Katakis
۴ Chui et al.
۵ Radio-Frequency Identification
۶ Atzori et al.
۷ Vermesan & Friess
۸ Al-Turjman
۹ Akyildiz
۱۰ Kelly
۱۱ Huh
۱۲ Blockchain

در تحقیقات بسیاری نیز به ارتباط بین اینترنت اشیا و ایجاد شهرهای هوشمند پرداخته شده است. کاربردهای اینترنت اشیا و همچنین فناوری‌های مورد استفاده به‌منظور هوشمند سازی شهرها از کاربردهای متداول اینترنت اشیا می‌باشد (سانچز و همکاران[۱]، ۲۰۱۴؛ پررا و همکاران[۲]، ۲۰۱۴؛ لیو و همکاران[۳]، ۲۰۱۹؛ ساین و همکاران[۴]، ۲۰۱۹). از دیگر کاربردهای اینترنت اشیا که بسیار موردتوجه پژوهشگران قرار دارد می‌تواند به بررسی این فناوری در صنایع خدمات درمانی اشاره نمود (مطلق و همکاران[۵]، ۲۰۱۹؛ پائول و همکاران[۶]، ۲۰۱۹؛ ادهیکاری و همکاران[۷]، ۲۰۱۹). تحقیقات بسیاری نیز به توسعه اینترنت اشیا و کاربردهای بسیار آن در توسعه کسب‌وکارها و هوشمندسازی کسب‌وکار پرداخته‌اند (ریگینس و فوسووامبا[۸]، ۲۰۱۹؛ ویری یاسیتاوات و همکاران[۹]، ۲۰۱۹). در ادامه به بررسی بیشتر استفاده از اینترنت اشیا در توسعه و هوشمند سازی زنجیره تامین صنایع می‌پردازیم.

۲-۲- زنجیره تامین مبتنی بر اینترنت اشیا

ظهور اینترنت اشیا و فناوری اطلاعات مفاهیم بسیاری را تغییر داده است که کسب‌وکار هوشمند و درنتیجه آن زنجیره تامین هوشمند یکی از آن‌ها است. درنتیجه، بسیاری از شرکت‌ها و سازمان‌ها از فناوری اطلاعات و ارتباطات برای افزایش کارایی، کاهش هزینه‌ها و افزایش کیفیت محصولات استفاده می‌کنند (استوک و سلیگر[۱۰]، ۲۰۱۶). زنجیره تامین هوشمند مبتنی بر زیرساخت اطلاعات توزیع‌شده و مستقل شامل هزاران منبع اطلاعاتی است و در آن ابزارها و امکانات مختلف ، با استفاده از اینترنت اشیا یا سایر فناوری‌های مشابه، به یکدیگر متصل هستند (ساین و گوپتا[۱۱]، ۲۰۱۵). اینترنت اشیا با تجزیه‌وتحلیل داده‌های عظیم ارتباط تنگاتنگی دارد و به‌شدت درحال نفوذ در بسیاری از حوزه‌ها برای بهینه‌سازی بهره‌وری انرژی و کاهش آثار مخرب زیست‌محیطی است. این امر عمدتاً به استفادهٔ مؤثر از منابع طبیعی، مدیریت هوشمند زیرساخت‌ها و تسهیلات و ارتقای خدمات ارائه‌شده برای حمایت از محیط‌زیست مربوط می‌شود. به همین ترتیب، برنامه‌های مرتبط با داده‌های عظیم و اینترنت اشیا در تسهیل و بهبود روند توسعه پایدار محیط‌زیست تأثیر بسزایی دارند (بیبری[۱۲]، ۲۰۱۸). امروزه بوجود آمدن عناوینی مانند کسب‌وکارهای هوشمند و یا هوشمندسازی کسب‌وکار با استفاده فناوری تولید داده‌های عظیم و جمع‌آوری، ذخیره، پردازش و نگهداری از این داده‌ها باعث بوجود آمدن مفاهیم جدیدی هم‌چون زنجیره تامین هوشمند شده است. درزمینه زنجیره تامین هوشمند و پایدار، حجم تولید داده‌ها به‌شدت در حال افزایش می‌باشد و حجم وسیعی از اطلاعاتی که از حوزه‌های گوناگون زنجیره تامین مانند بخش‌های تامین مواد اولیه و ارتباط با تامین‌کنندگان و حمل مواد به سایت‌های تولیدی، تولید و ساخت و امکانات مرتبط با برنامه‌ریزی تولید و درنهایت توزیع منظم و در زمان‌بندی دقیق و ارتباطات با خرده‌فروشان و مشتریان نهایی در دسترس‌اند، به‌اندازه‌ای ارزشمند است که می‌توان با همکاری برنامه‌ریزان و تصمیم‌گیرندگان در زمینه زنجیره‌تامین و متخصصان فناوری اطلاعات و ارتباطات برای پیشرفت پایداری محیطی از آن‌ها بهره برد. فناوری‌های مطرح در اینترنت اشیا شامل انواع حس‌گرها، سیستم‌های پردازش داده، شبکه‌های ارتباطی بیسیم و فعال‌سازهای سیستم‌ها در محیط فیزیکی می‌باشند (ا دونووان و همکاران[۱۳]، ۲۰۱۵). بنابراین اصلاح زنجیره تامین هوشمند پایدار برای توصیف زنجیره تامینی است که توسعه فراگیر فناوری اطلاعات و ارتباطات پیشرفته و استفاده گسترده از آن در سیستم‌های مختلف زنجیره را چنان تجهیز می‌کند که با استفاده از ابزارهای ایمن، پایدار و کارآمد کنترل، نتایج اقتصادی و اجتماعی منابع موجود را کنترل کند (لی[۱۴]، ۲۰۲۰). در زمینه ارتباط میان زنجیره تامین و هوشمندسازی آن با

---

۱ Sanchez et al.
۲ Perera et al.
۳ Liu et al.
۴ Singh et al.
۵ Mutlag et al.
۶ Paul et al.
۷ Adhikary et al.
۸ Riggins & Fosso Wamba
۹ Viriyasitavat et al.
۱۰ Stock & Seliger
۱۱ Singh & Gupta
۱۲ Bibri
۱۳ O'Donovan et al.
۱۴ Lee

استفاده از اینترنت اشیا تحقیقات مختلفی تاکنون انجام شده است. در تحقیقات بسیاری به بررسی سیستم‌های شناسایی مبتنی بر فرکانس رادیویی و ارتباط آن‌ها با سیستم‌های تامین و توزیع پرداخته شده است (موسا و دابو[۱]، ۲۰۱۶؛ ناتیوی و لی[۲]، ۲۰۱۲؛ انگای و همکاران[۳]، ۲۰۱۴). در تحقیقات دیگری نیز به بررسی موضوع تولید و ایجاد کارخانه‌های هوشمند با امکان ذخیره‌سازی انرژی و کنترل فرایندها به‌منظور ایجاد پایداری برای موضوع محیط‌زیست سالم پرداخته شده است (استروزی و همکاران[۴]، ۲۰۱۷؛ تائو و همکاران[۵]، ۲۰۱۴).

۳- ریسک‌های سایبری زنجیره تامین مبتنی بر اینترنت اشیا

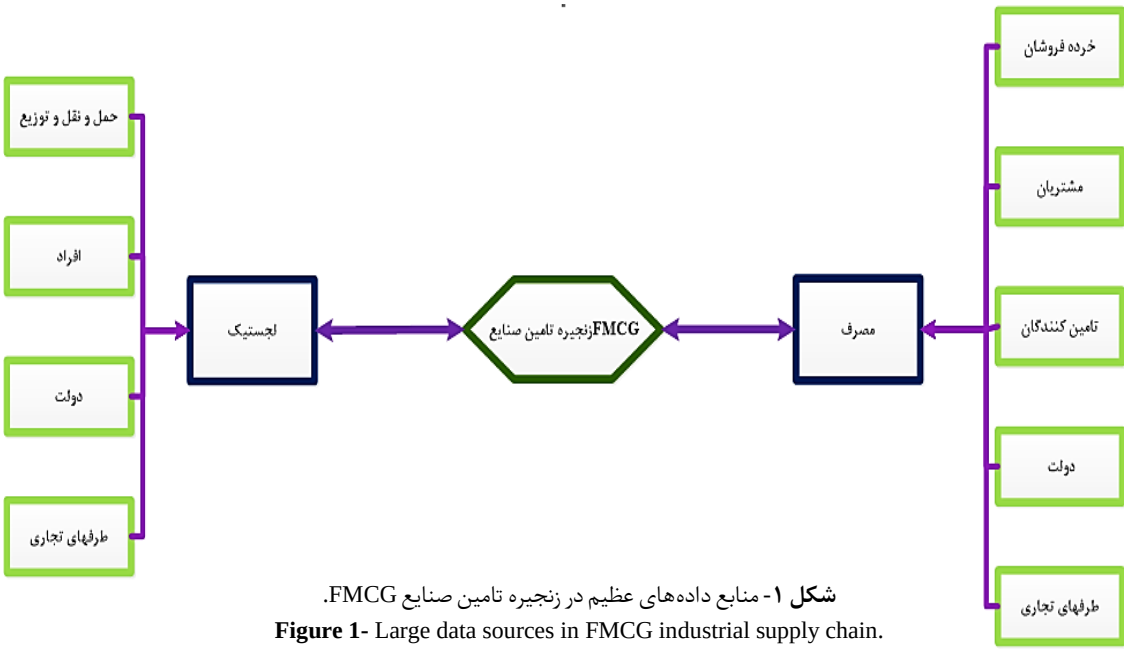
ریسک‌ها همیشه در اطراف ما هستند و دولت‌ها، مشاغل و افراد هر روز بارها و بارها در تصمیم‌گیری‌های مبتنی بر ریسک شرکت می کنند. سیستم‌های مبتنی بر اینترنت اشیا، شامل قابلیت همکاری در چند دسته سیستم‌های سایبری- فیزیکی، ادغام فناوری‌های مرتبط با شبکه‌های هوشمند کسب‌وکار، حمل‌ونقل هوشمند، زنجیره تأمین و تولید هوشمند است. چنین فناوری‌های جدیدی با انواع جدیدی از ریسک‌ها همراه هستند به‌طوری که روش‌های پیش‌بینی و مدیریت این ریسک‌ها دارای طراحی خاص هست (عروج لو و آزگومی[۶]، ۲۰۱۷). بنابراین برای حفاظت از استقرار اینترنت اشیا، در عین‌حال که از ارزش اقتصادی آن نیز بهره برده می‌شود، لازم است که به‌صورت سیستماتیک عوامل خطر چندگانه درنظر گرفته شود. زیرا حملات سایبری بارها اتفاق می‌افتند و به‌طور فزاینده دستگاه‌های *IoT* را هدف قرار می‌دهند. با رشد مداوم سطوح و قابلیت‌های حملات سایبری، شدت حملات از طریق فناوری اینترنت اشیا 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، سیستم‌عامل‌ها و خدمات متصل به اینترنت اشیا ، کفایت اقدامات و روش‌های امنیت سایبری برای به‌حداقل رساندن ریسک سایبری خواهد بود (رادانلیو و همکاران[۷]، ۲۰۱۸). پاسخ به این سوال بسیار مهم است و نیازمند بررسی این ریسک‌ها دارد. زیرا قابلیت‌های اینترنت اشیا، انواع جدیدی از خطرات سایبری را ایجاد می‌کند که در استانداردهای ارزیابی ریسک‌های سایبری موجود پیش‌بینی نشده و درنظر گرفته نمی‌شوند (یان و همکاران[۸]، ۲۰۱۴). برای بررسی ریسک‌ها لازم است تا تجزیه‌وتحلیل کاملی از سازش داده‌ها، امکانات ارائه‌دهندگان شبکه ارتباطات یا صاحبان داده را با توانایی ایجاد مکانیسم‌های واضح، دقیق و موردقبول صنعت برای اندازه‌گیری، کنترل، تجزیه‌وتحلیل، توزیع و مدیریت داده‌های مهم موردنیاز برای توسعه، استقرار و امنیت سایبری مقرون به‌صرفه برای زیرساخت‌های مهم را انجام دهید. در این پژوهش به‌منظور بررسی ریسک‌های سایبری زنجیره تامین مبتنی بر اینترنت اشیا، زنجیره تامین شرکت‌های *FMCG* به‌عنوان مطالعه موردی انتخاب گردید. این شرکت‌ها دارای محصولاتی هستند که بخش اعظمی از نیازهای روزانه مردم را تشکیل می‌دهند. بخش بسیار زیادی از هزینه خانوارها صرف خرید محصولات این شرکت‌ها می‌شود. با توجه به اهمیت و کاربردی‌بودن این صنایع، ما در این مطالعه از نظرات خبرگان فعال در بخش زنجیره تامین و همچنین بخش فناوری اطلاعات این شرکت‌ها استفاده نموده‌ایم. از آن‌جایی که اینترنت اشیا به‌عنوان یکی از مهم‌ترین منابع داده‌های عظیم می‌باشند، لذا برای بررسی ریسک‌های سایبری لازم است تا مبادی تولید داده‌ها در این زنجیره مشخص شود.

شکل ۱، مهم‌ترین منابع تامین داده عظیم برای زنجیره تامین شرکت‌های *FMCG* را نشان می‌دهد (جی و همکاران[۹]، ۲۰۱۷). دامنه فعالیت اینترنت اشیا در بخش‌های تامین، تولید و توزیع محصولات می‌باشد. اطلاعات از طریق سیستمهای مبتنی بر اینترنت اشیا،

نشریه تصمیم‌گیری و تحقیق در عملیات، دوره ۵، شماره ۴، زمستان ۱۳۹۹، صفحه: ۵۲۱-۵۱۰

[۱] Musa & Dabo
[۲] Nativi & Lee
[۳] Ngai et al.
[۴] Strozzi et al.
[۵] Tao et al.
[۶] Orojloo & Azgomi
[۷] Radanliev et al.
[۸] Yan et al.
[۹] Ji et al.

جمع‌آوری و نگهداری می‌شوند و بر اساس سیستمهای محاسبات ابری مورد پردازش قرار میگرند تا به‌منظور هوشمند سازی زنجیره تامین استفاده گردند.



شکل ۱- منابع داده‌های عظیم در زنجیره تامین صنایع FMCG.

Figure 1- Large data sources in FMCG industrial supply chain.

جمع‌آوری داده‌ها در هر یک از ورودی‌ها در دامنه زنجیره تامین، با استفاده از کامپیوترها، گوشی‌های هوشمند، تبلت ها و انواع حسگرها به‌عنوان ابزارهای اینترنت اشیا صورت می‌گیرد. این داده‌ها پس از اخذ با استفاده سیستم‌های پردازش قدرتمند مورد پردازش قرار می گیرند و تحلیل‌های کامل به‌منظور اتخاذ تصمیمات به‌عنوان خروجی سیستم زنجیره تامین هوشمند ایجاد می‌شود. هر یک از ابزارهای اینترنت اشیا با توجه به تعاملات در بخش‌های مختلف زنجیره تامین می‌توانند عامل ایجاد رخنه و تهدید سایبری برای زنجیره تامین باشند. با توجه به وجود فضای تعاملی در بسیاری از بخش‌های زنجیره تامین بخصوص روابط با تامین کنندگان 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 نیز ازجمله مباحث بسیار حیاتی در زنجیره تامین محصولات *FMCG* می‌باشد، زیرا اختلال در زمان‌بندی‌ها و عدم توزیع مناسب، اشکال در مسیریابی بهینه و انتخاب مسیرهای پرترافیک برای توزیع محصولات خود می‌توانند خطر جدی برای تامین و توزیع و همچنین بهینه بودن فعالیت‌های زنجیره تامین باشد. با توجه به زنجیره تامین شرکت‌های *FMCG*، و همچنین راه‌های ورود داده‌های عظیم و بررسی ادبیات موضوع و نظرات خبرگان فعال ریسک‌های سایبری زنجیره تامین در سه حوزه تامین، تولید و توزیع بدست آمد (**جدول ۱**).

جدول ۱- ریسک‌های سایبری برای زنجیره تامین مبتنی بر اینترنت اشیا.

Table 1- Cyber risks for IoT-based supply chain.

حوزه	ریسک‌های سایبری	نماد
تامین	عدم وجود برنامه امنیتی و حفظ حریم خصوصی در تعامل با تامین‌کنندگان.	W1
	اختلال در ترابری و تحویل.	W2
تولید	عدم نظارت کافی بر دستگاه‌ها و سیستم‌ها برای تشخیص حوادث امنیتی.	W3
	عدم ورود امنیت در طراحی محصولات و اکوسیستم.	W4
	اختلال در شناسایی و درمان خطرات محصولات.	W5
	عدم آگاهی و آموزش کافی امنیتی برای مهندسین.	W6
توزیع و فروش	اجرای امنیت و مدیریت ریسک حریم خصوصی در تعامل با مشتریان.	W7
	اختلال در بررسی موجودی محصولات.	W8
	اختلال در برنامه‌های تشخصی محیط، ترافیک.	W9
	تداخل در زمان‌بندی‌ها برای توزیع و فروش.	W10

بر اساس اطلاعات **جدول ۱** می‌توان دریافت، یکی از مهم‌ترین دغدغه‌ها برای تعامل با تامین کنندگان کالا و خدمات و همچنین مشتریان، حفظ حریم خصوصی است. بواسته استفاده از ابزارهای الکترونیک و دریافت اطلاعات از تامین کنندگان و ارتباطات گسترده کاری از طریق تلفن‌های هوشمند و تبلت‌ها، حجم عظیمی از اطلاعات شخصی و مالی می‌تواند به اشتراک گذاشته شود که فراهم‌کردن امنیت برای این بخش‌ها می‌تواند یکی از مهم‌ترین چالش‌ها و نگرانی‌ها باشد. عدم وجود برنامه‌های امنیتی برای برنامه‌های تعاملی همواره یکی از مهم‌ترین تهدیداتی است که می‌تواند کسب‌وکار را با خطر مواجه نماید. برای صنایعی که دارای مواد اولیه فاسدشدنی هستند تحویل به هنگام مواد اولیه و عدم اختلال در این بخش می‌تواند بسیار پراهمیت باشد. دریافت اطلاعات ترافیکی و وضعیت توزیع منظم، تداخل در زمان‌بندی‌ها، اطلاعات دقیق و درست در زمین موجودی مواد اولیه و همچنین محصولات آماده تحویل همگی اطلاعاتی هستند که در صورت وجود حملات سایبری می‌توانند لطمات جبران‌ناپذیری را به سیستم‌های کسب‌وکار وارد آورند. بنابراین درک درست از خطرات سایبری در کسب‌وکارهایی که به‌واسطه اینترنت اشیا هوشمند شده‌اند، می‌تواند عامل بوجود آورنده آرامش سازمانی بوده و درنتیجه افزایش راندمان را به همراه داشته باشد.

۴- متدولوژی

روش تحقیق استفاده‌شده در این تحقیق از نوع پیمایشی است و ازنظر نوع هدف کاربردی است زیرا درصدد به‌کارگیری از یک روش تصمیم‌گیری به‌منظور رتبه‌بندی ریسک‌های سایبری زنجیره تامین مبتنی بر اینترنت اشیا می‌باشد. قسمت بسیاری از اطلاعات این پژوهش از طریق ارسال و تکمیل پرسشنامه توسط متخصصان و خبرگان حوزه موردمطالعه جمع‌آوری شده است. دامنه تحقیق برخی صنایع *FMCG* (به‌طور خاص شرکت‌های مواد غذایی و دارویی) می‌باشد. برای این پژوهش ازنظر ۳۵ متخصص فعال در زنجیره تامین شرکت‌های *FMCG* بهره گرفته شده است. ساختار شبکه‌ای مسئله با استفاده از بررسی کتابخانه‌ای و مرور ادبیات و همچنین مصاحبه با خبرگان حاصل شده است و سپس با استفاده ازنظر خبرگان این ساختار صحت‌سنجی شده است. به‌منظور هم‌راستایی پاسخنامه‌ها سعی شده است تا پاسخ‌های خبرگان به‌صورت مشاهده‌ای کنترل شود. به‌صورت خلاصه چارچوب ارزیابی این پژوهش به‌صورت خلاصه شامل مراحل زیر می‌باشد.

- *شناسایی ریسک‌های سایبری در زنجیره تامین مبتنی بر اینترنت اشیا. برای دستیابی به این هدف با استفاده از مطالعات کتابخانه‌ای و ادبیات موضوع، به بررسی ریسک‌ها و تهدیدات سایبری حاصل از به‌کارگیری اینترنت اشیا در زنجیره تامین به‌منظور هوشمند سازی آن پرداخته شد. این ریسک‌ها با استفاده ازنظر خبرگان مورد پالایش قرار گرفت و صحت سنجی گردید.*
- *ایجاد ساختار سلسله مراتبی. ساختار سلسله مراتبی ریسک‌های سایبری برای زنجیره تامین مبتنی بر اینترنت اشیا با استفاده از سطوح هدف و معیار و گزینه ایجاد شد. این ساختار در **جدول ۱** ، نشان داده شده است. در این ساختار هدف بررسی ریسک‌های سایبری برای زنجیره تامین بوده و در محدوده تامین، تولید و توزیع موردبررسی قرار گرفته است.*
- *ایجاد ماتریس‌های قضاوت فازی. برای تحلیل و رتبه ریسک‌های سایبری در زنجیره تامین هوشمند، از ماتریس‌های توافقی قضاوت فازی بر اساس نظریات خبرگان و بر مبنای روش تحلیل سلسله مراتبی[1] (AHP) استفاده می‌شود. بنابراین به‌منظور تبیین ترجیحات افراد و تحلیل نظرات آن‌ها از معیارهای زبانی استفاده می‌شود. معیارهای زبانی برای مقایسات زوجی فازی مورداستفاده در این پژوهش، در جدول ۲ نشان داده شده است. این مقیاس‌ها بر اساس اعداد مثلثی فازی می‌باشند.*
- *طراحی و حل مدل ریاضی غیرخطی فازی . به‌منظور رتبه‌بندی ریسک‌های سایبری در زنجیره تامین مبتنی بر اینترنت اشیا، از یک روش رتبه‌بندی ریاضی غیرخطی و فازی استفاده می‌شود. این روش بر مبنای روش تحلیل سلسله مراتبی فازی می‌باشد.*

[1] Analytic Hierarchy Process

جدول ۲- معیارهای زبانی برای مقایسات زوجی فازی.
Table 2- Linguistic criteria for fuzzy pairwise comparisons.

مقادیر زبانی	معادل فازی
خیلی کم	(1,2,3)
کم	(4,2,3)
متوسط	(5,4,3)
زیاد	(6,5,4)
خیلی زیاد	(7,6,5)

۱-۴- روش برنامه‌ریزی ترجیحی فازی گروهی

در این پژوهش از یک روش رتبه‌بندی فازی بر مبنای تحلیل سلسله مراتبی استفاده شده است.این روش برای اولین بار در سال ۲۰۰۳ توسط میخایلوف ارائه شد (میخایلوف، ۲۰۰۳). در این روش ابتدا ماتریس ادغامی مقایسات زوجی فازی بر مبنای اعداد مثلثی و معیارهای زبانی (**جدول ۲**) حاصل می‌شود. سپس این مقادیر حاصل‌شده، با استفاده از روش مدل‌سازی ریاضی غیرخطی فازی **رابطه (۱)** به‌منظور رتبه‌بندی معیارها مورد استفاده قرار می‌گیرند.

$$
\begin{aligned}
&\max \ \lambda \\
&s.t. \\
&\quad (m_{ij} - l_{ij})\lambda w_j - w_i + l_{ij} w_j \le 0 \\
&\quad (u_{ij} - m_{ij})\lambda w_j + w_i - u_{ij} w_j \le 0 \\
&\quad \sum_{k=1}^{n} w_k = 1 \\
&\quad w_k > 0, k = 1,2,...,n; \quad i = 1,2,...,n-1; \ j = 2,3,...,n, \\
&\quad j > i.
\end{aligned}
\qquad (۱)
$$

در **رابطه (۱)** ، مقادیر حاصل از اعداد مثلی فازی که از ماتریس مقایسات زوجی حاصل شده‌اند($\tilde{a}_{ij} = (l_{ij}, m_{ij}, u_{ij})$)، در رابطه قرار گرفته و پس از آن باید مدل ایجادشده حل شود.از آنجایی که مدل ایجادشده، غیرخطی است، لذا با استفاده از روش‌های ساده برنامه‌ریزی ریاضی نمی‌توان آن‌ها را حل نمود. بنابراین برای حل مدل ایجادشده از نرم‌افزارهایی مانند *GAMS* یا *LINGO* استفاده می‌شود. در پژوهش حاضر برای حل مدل‌هایی که بر اساس ماتریس مقایسات زوجی ایجاد شده‌اند از نرم‌افزار *LINGO*، استفاده شده است.

پس از حل مدل، مقدار مثبت بدست آمده، نشان‌دهنده این است که تمام وزن‌ها کاملا در قضاوت‌های اولیه صدق می‌کنند، ولی در صورتی که شاخص منفی باشد، می‌توان درک کرد که قضاوت‌های فازی سازگاری کامل را ندارند و یا به عبارتی ناسازگار هستند.

۵- یافته‌ها پژوهش

مراحل اصلی بررسی و رتبه‌بندی ریسک‌های سایبری در زنجیره تامین هوشمند، به دو بخش کلی تقسیم می‌شوند. در مرحله اول با استفاده از تولید پرسشنامه‌های فازی، نظرات خبرگان استخراج و ادغام می‌شود (**جداول ۳ تا ۶**). سپس با استفاده از مدل ریاضی غیرخطی که در پژوهش ارائه شده است به رتبه‌بندی ریسک‌ها پرداخته می‌شود (**جداول ۷ تا ۹**).

جدول ۳- مقایسات زوجی فازی بر اساس ادغام نظرات کارشناسان برای حوزه‌های کلی زنجیره تامین.

Table 3- Fuzzy pairwise comparisons based on the integration of expert opinions for general areas of the supply chain.

	تامین A1			**تولید A2**			**توزیع A3**		
A1	-	-	-	-	-	-	-	-	-
A2	3.1	3	7	-	-	-	-	-	-
A3	3	3.1	5.6	2	2.5	2.5	-	-	-

جدول ۴- مقایسات زوجی فازی بر اساس ادغام نظرات کارشناسان برای بخش تامین.

Table 4- Fuzzy pair comparisons based on the integration of expert opinions for the supply sector.

	W1			**W2**	
W1	-	-	-	-	-
W2	3.1	4.3	6.1	-	-

جدول ۵- مقایسات زوجی فازی بر اساس ادغام نظرات کارشناسان برای بخش تولید.

Table 5- Fuzzy pair comparisons based on the integration of expert opinions for the production sector.

	W3			**W4**			**W5**			**W6**		
W3	-	-	-	-	-	-	-	-	-	-	-	-
W4	4.5	3.3	6.1	-	-	-	-	-	-	-	-	-
W5	4.5	3	4.1	4.5	3	4	-	-	-	-	-	-
W6	3.1	3.25	6	3	4.1	4.1	2	2.3	2.6	-	-	-

جدول ۶- مقایسات زوجی فازی بر اساس ادغام نظرات کارشناسان برای بخش توزیع.

Table 6- Fuzzy pair comparisons based on the integration of expert opinions for the distribution sector.

	W7			**W8**			**W9**			**W10**		
W7	-	-	-	-	-	-	-	-	-	-	-	-
W8	5.1	4.2	6	-	-	-	-	-	-	-	-	-
W9	2.25	3.1	4.3	2.1	2.1	3.2	-	-	-	-	-	-
W10	2.5	4	4.4	3	6.1	3	2	2.1	3.2	-	-	-

با قرار دادن داده‌های حاصل از جداول مقایسات زوجی که از ادغام نظرات خبرگان بدست آمده است، مدل‌های ریاضی غیرخطی فازی را تشکیل داده و مدل‌های حاصله را با استفاده از نرم‌افزار *LINGO* حل کرده‌ایم. وزن و رتبه هر یک از ریسک‌های سایبری در حوزه‌های تامین، تولید و توزیع حاصل شد. نتایج در **جداول ۷** تا **۹** نشان داده شده است.

جدول ۷- وزن و رتبه هر یک از ریسک‌های سایبری برای بخش تامین.

Table 7- Weight and rating of each cyber risk for the supply sector.

رتبه	**وزن**	**نماد**	**ریسک سایبری**
1	0.612734	W1	عدم وجود برنامه امنیتی و حفظ حریم خصوصی در تعامل با تامین کنندگان.
2	0.387266	W2	اختلال در ترابری و تحویل.

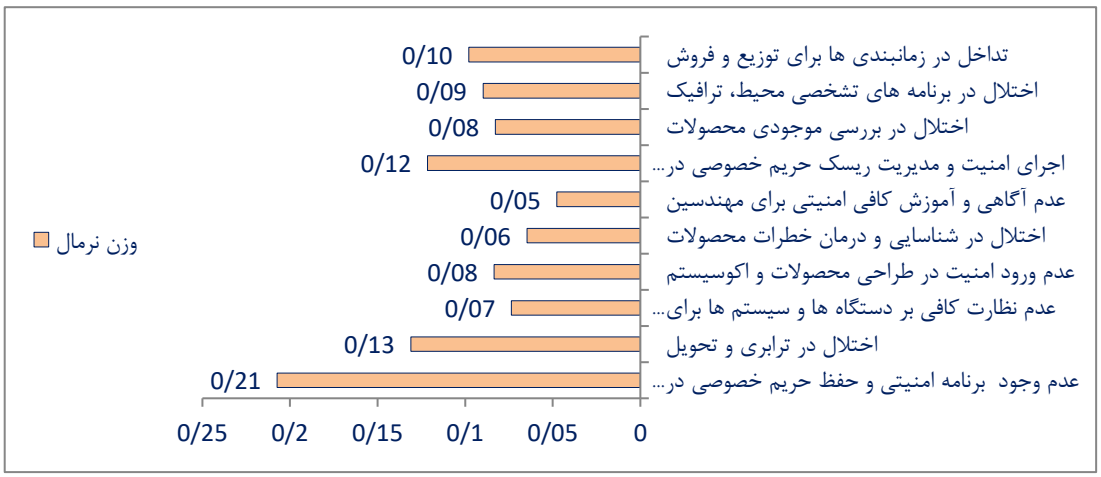
جدول ۸- وزن و رتبه هر یک از ریسک‌های سایبری برای بخش تولید.
Table 8- Weight and rating of each cyber risk for the production sector.

رتبه	وزن	نماد	ریسک سایبری
2	0.273004	W3	عدم نظارت کافی بر دستگاه‌ها و سیستم‌ها برای تشخیص حوادث امنیتی.
1	0.309915	W4	عدم ورود امنیت در طراحی محصولات و اکوسیستم.
3	0.240076	W5	اختلال در شناسایی و درمان خطرات محصولات.
4	0.177004	W6	عدم آگاهی و آموزش کافی امنیتی برای مهندسین.

جدول ۹- وزن و رتبه هر یک از ریسک‌های سایبری برای بخش توزیع.
Table 9- Weight and rating of each cyber risk for the distribution sector.

رتبه	وزن	نماد	ریسک سایبری
1	0.309915	W7	اجرای امنیت و مدیریت ریسک حریم خصوصی در تعامل با مشتریان.
4	0.211259	W8	اختلال در بررسی موجودی محصولات.
3	0.228911	W9	اختلال در برنامه‌های تشخصی محیط، ترافیک.
2	0.249915	W10	تداخل در زمان‌بندی‌ها برای توزیع و فروش.

با بررسی وزن‌های حاصل‌شده از حل مدل‌سازی ریاضی می‌توان به درک میزان خطرات سایبری در زنجیره تامین مبتنی بر اینترنت اشیا پی برد. با نرمال‌سازی وزن‌های بدست آمده رتبه‌بندی کلی ریسک‌های سایبری در زنجیره تامین هوشمند حاصل خواهد شد. این رتبه‌بندی در **شکل ۲** نشان داده شده است که بیانگر این امر است که حفظ حریم خصوصی در تعامل با تامین کنندگان و همچنین مشتریان، بیشترین اهمیت را در میان ریسک‌های سایبری زنجیره تامین هوشمند دارند.



شکل ۲- نمودار وزن نرمال ریسک‌های سایبری در زنجیره تامین هوشمند.
Figure 2- Normal weight chart of cyber risks in the smart supply chain.

۶- نتیجه‌گیری

امروزه با ظهور فناوری اینترنت اشیا و مزایای بسیاری که برای استفاده از این فناوری وجود دارد، کسب‌وکارها نیز به دنبال استفاده بهینه از این فناوری هستند. در این میان ادغام مفهوم اینترنت اشیا با زنجیره تامین به‌عنوان چرخه حیاتی کسب‌وکارها، باعث شده تا محققان بسیاری به بررسی ابعاد مختلف این ادغام بپردازند. با توجه به این‌که زنجیره تامین بخش بزرگی از فعالیت‌ها در سازمان‌ها از تامین مواد اولیه تا توزیع را در بر می‌گیرند، بنابراین درک درست از کاربردهای این فناوری می‌توان تسهیل‌کننده بهینه‌شدن انواع فرایندها در سازمان باشد. اینترنت اشیا یکی از مهم‌ترین بزرگ‌ترین تولیدکننده داده می‌تواند باشد که این داده‌ها در صورت تحلیل و پردازش درست می‌توانند کمک شایانی به تصمیم‌گیری‌های بهنگام در سازمان داشته باشند. در عین‌حال از آن‌جایی که این فناوری با اینترنت آمیخته است بنابراین همواره استفاده از آن می‌تواند چالش‌ها و نگرانی‌هایی را به همراه داشته باشد. در پژوهش حاضر سعی شده است تا با شناسایی مبادی

تولید ده‌های کلان در زنجیره تامین صنایع *FMCG* (صنایع غذایی و دارویی) به‌عنوان موضوع موردمطالعه، به شناسایی و درک ریسک‌های سایبری که یک زنجیره تامین مبتنی بر اینترنت اشیا می‌تواند با آن‌ها سروکار داشته باشد پرداخته شود. برای بررسی میزان اهمیت هر یک از این ریسک‌ها از یک روش رتبه‌بندی فازی با استفاده از مدل‌سازی ریاضی غیرخطی استفاده شده است. نتایج پژوهش مشان می‌دهد که حفظ حریم خصوصی در تعامل با تامین کنندگان و مشتریان از مهم‌ترین ریسک‌های سایبری زنجیره تامین هوشمند در این شرکت‌ها می‌باشد.

منابع

Adhikary, T., Jana, A. D., Chakrabarty, A., & Jana, S. K. (2019, January). The internet of things (IoT) augmentation in healthcare: An application analytics. *International conference on intelligent computing and communication technologies* (pp. 576-583). Singapore: Springer. https://doi.org/10.1007/

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer networks*, *38*(4), 393-422.

Al-Turjman, F. (2019). 5G-enabled devices and smart-spaces in social-IoT: an overview. *Future generation computer systems*, *92*, 732-744. https://doi.org/10.1016/j.future.2017.11.035

Ashton, K. (2009). That 'internet of things' thing. *RFID journal*, *22*(7), 97-114.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

Bibri, S. E. (2018). The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability. *Sustainable cities and society*, *38*, 230-253. https://doi.org/10.1016/j.scs.2017.12.034

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in industry*, *101*, 1-12.

Chui, M., Loffler, M., & Roberts, R. (n.d.). *The internet of things*. Retrieved September 15, 2020, from https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-internet-of-things#

DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment systems and decisions*, *35*(2), 291-300.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.

https://www.itu.int/en/ITU-T/ssc/resources/Pages/topic-001.aspx

Huh, S., Cho, S., & Kim, S. (2017, February). Managing IoT devices using blockchain platform. *2017 19th international conference on advanced communication technology (ICACT)* (pp. 464-467). Bongpyeong, South Korea: IEEE.

Ji, G., Hu, L., & Tan, K. H. (2017). A study on decision-making of food supply chain based on big data. *Journal of systems science and systems engineering*, *26*(2), 183-198.

Katakis, I. (2015). Mining urban data (part A). *Journal of information Systems*, *54*, 113-114. https://doi.org/10.1016/j.is.2015.08.002

Kelly, S. D. T., Suryadevara, N. K., & Mukhopadhyay, S. C. (2013). Towards the implementation of IoT for environmental condition monitoring in homes. *IEEE sensors journal*, *13*(10), 3846-3853. DOI: 10.1109/JSEN.2013.2263379

Lee, I. (2020). Internet of things (IoT) cybersecurity: literature review and iot cyber risk management. *Future internet*, *12*(9), 157.

Liu, Y., Yang, C., Jiang, L., Xie, S., & Zhang, Y. (2019). Intelligent edge computing for IoT-based energy management in smart cities. *IEEE network*, *33*(2), 111-117.

Mikhailov, L. (2003). Deriving priorities from fuzzy pairwise comparison judgements. *Fuzzy sets and systems*, *134*(3), 365-385.

Musa, A., & Dabo, A. A. A. (2016). A review of RFID in supply chain management: 2000–2015. *Global journal of flexible systems management*, *17*(2), 189-228. https://doi.org/10.1007/s40171-016-0136-2

Mutlag, A. A., Abd Ghani, M. K., Arunkumar, N. A., Mohammed, M. A., & Mohd, O. (2019). Enabling technologies for fog computing in healthcare IoT systems. *Future generation computer systems*, *90*, 62-78.

Nativi, J. J., & Lee, S. (2012). Impact of RFID information-sharing strategies on a decentralized supply chain with reverse logistics operations. *International journal of production economics*, *136*(2), 366-377.

Ngai, E. W., Cheung, B. K., Lam, S. S., & Ng, C. T. (2014). RFID value in aircraft parts supply chains: A case study. *International journal of production economics*, *147*, 330-339. https://doi.org/10.1016/j.ijpe.2012.09.017

O'Donovan, P., Leahy, K., Bruton, K., & O'Sullivan, D. T. (2015). An industrial big data pipeline for data-driven analytics maintenance applications in large-scale smart manufacturing facilities. *Journal of big data*, *2*(1), 1-26.

Orojloo, H., & Azgomi, M. A. (2017). A game-theoretic approach to model and quantify the security of cyber-physical systems. *Computers in industry*, *88*, 44-57. https://doi.org/10.1016/j.compind.2017.03.007

Paul, M. A. V., Sagar, T. A., Venkatesan, S., & Gupta, A. K. (2019). Impact of mobility in IoT devices for healthcare. In *Digital business* (pp. 243-261). Cham: Springer. https://doi.org/10.1007/978-3-319-93940-7_11

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Sensing as a service model for smart cities supported by internet of things. *Transactions on emerging telecommunications technologies*, *25*(1), 81-93.

Radanliev, P., De Roure, D., Cannady, S., Montalvo, R. M., Nicolescu, R., & Huth, M. (2018). Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. *Living in the internet of things: cybersecurity of the IoT - 2018* (9 pp.). DOI: 10.1049/cp.2018.0003

نشریه تصمیم‌گیری و تحقیق در عملیات، دوره ۵، شماره ۴، زمستان ۱۳۹۹، صفحه: ۵۲۱-۵۱۰

Riggins, F., & Fosso Wamba, S. (2019, January). Introduction to the minitrack on business value of smart devices on the internet of things. *Proceedings of the 52nd Hawaii international conference on system sciences*. DOI: 10.24251/HICSS.2019.712

Saadati, Z., & Mehrshad, B. (2017). The internet of things and big data applications in sustainable smart cities. *Journal of science and technology policy lettersis*, 7(3), 17-30. (**In Persian**). http://stpl.ristip.sharif.ir/article_20442.html?lang=en

Sanchez, L., Muñoz, L., Galache, J. A., Sotres, P., Santana, J. R., Gutierrez, V., ... & Pfisterer, D. (2014). SmartSantander: IoT experimentation over a smart city testbed. *Computer networks*, *61*, 217-238. https://doi.org/10.1016/j.bjp.2013.12.020

Singh, A. K., Kumar, D., & Prakash, V. (2019, March). Importance and Needs of IoT in Developing Smart Cities. *Proceedings of 2nd international conference on advanced computing and software engineering (ICACSE)*. http://dx.doi.org/10.2139/ssrn.3350286

Singh, B., & Gupta, A. (2015). Recent trends in intelligent transportation systems: a review. *Journal of transport literature*, *9*(2), 30-34.

Stock, T., & Seliger, G. (2016). Opportunities of sustainable manufacturing in industry 4.0. *Procedia cirp*, *40*, 536-541. https://doi.org/10.1016/j.procir.2016.01.129

Strozzi, F., Colicchia, C., Creazza, A., & Noè, C. (2017). Literature review on the 'Smart Factory'concept using bibliometric tools. *International journal of production research*, *55*(22), 6572-6591. https://doi.org/10.1080/00207543.2017.1326643

Tao, F., Zuo, Y., Da Xu, L., & Zhang, L. (2014). IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing. *IEEE transactions on industrial informatics*, *10*(2), 1547-1557. DOI: 10.1109/TII.2014.2306397

Vermesan, O., & Friess, P. (Eds.). (2014). *Internet of things-from research and innovation to market deployment* (Vol. 29). Aalborg: River publishers.

Viriyasitavat, W., Da Xu, L., Bi, Z., & Pungpapong, V. (2019). Blockchain and internet of things for modern business process in digital economy—the state of the art. *IEEE transactions on computational social systems*, *6*(6), 1420-1432.

Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of network and computer applications*, *42*, 120-134.