University of Qom
Engineering Management and Soft Computing
JEMSC.QOM
Online ISSN: 2538-2675

# A hybrid model of extended FMEA model based on F-PIPRECIA and Z-EDAS methods with Bow Tie to evaluate cybersecurity risks in Industry 4.0

**Ali Memarpour Ghiaci**[1] **and Jafar Gheidar-Kheljani** ✉[2]

1. Ph.D Student, Industrial Engineering Department, Malek Ashtar University of Technology, Tehran 1774-15875, Iran. Email: ali.memarpour@mut.ac.ir
2. Corresponding author, Associate Professor, Industrial Engineering Department, Malek Ashtar University of Technology, Tehran 1774-15875, Iran. Email: kheljani@mut.ac.ir

**Article Info**

**Article type:**
Research Article

**Article history:**
Received 2023 October 26
Received in revised form 2023 December 11
Accepted 2024 February 19
Published online 2024 March 15

**Keywords:**
customer churn,
machine learning,
random forest algorithm,
site optimization.

**ABSTRACT**

Cybersecurity issues have become a complex challenge for companies obligating to the Industry 4.0 paradigm. On the other hand, the concept of cybersecurity in the context of Industry 4.0 proved to be an emerging topic in recent literature. Therefore, in the present study, for the first time, a hybrid FMEA model developed based on multi-criteria decision-making methods in uncertain environments with the Bowtie method in four phases has been used to evaluate cyber security in Industry 4.0: First, based on the literature, 16 cybersecurity risks in the fourth industrial revolution are identified based on the FMEA model, and the determinants of RPN are quantified. Then, the PIPRECIA fuzzy method was used to weigh the factors, and the Z-EDAS method was used to prioritize and critically identify. Finally, Bow Tie analysis has been used to analyze these analyses. The result of the proposed implementation has shown its capability and superiority compared to other methods of traditional effects, such as FMEA and Fuzzy EDAS.

**Cite this article:** Memarpour Ghiaci, A. & Gheidar-Kheljani, J. (2023). A hybrid model of extended FMEA model based on F-PIPRECIA and Z-EDAS methods with Bow Tie to evaluate cybersecurity risks in Industry 4.0. *Enginiiring Management and Soft Computing, 9 (2)*. 149-176. **DOI**: https://doi.org/


DOI: https://doi.org/

**Publisher**: University of Qom

JEMSC.QOM
شاپا الکترونیکی: ۲۶۷۵-۲۵۳۸

مدیریت مهندسی و رایانش نرم

دانشگاه قم

# یک مدل ترکیبی FMEA توسعه‌یافته مبتنی بر روش‌های F-PIPRECIA و Z-EDAS باروش Bow Tie جهت ارزیابی خطر امنیت سایبری در انقلاب صنعتی چهارم

**علی معمارپور غیاثی[۱] و جعفر قیدر خلجانی[۲]✉**

۱. دانشجوی دکتری، گروه مهندسی صنایع، دانشکده مدیریت و مهندسی صنایع، دانشگاه صنعتی مالک اشتر، تهران، ایران. رایانامه: ali.memarpour@mut.ac.ir

۲. نویسنده مسئول، دانشیار، گروه مهندسی صنایع، دانشکده مدیریت و مهندسی صنایع، دانشگاه صنعتی مالک اشتر، تهران، ایران. رایانامه: kheljani@mut.ac.ir

**اطلاعات مقاله**

**نوع مقاله:** مقاله پژوهشی

**تاریخ دریافت:** ۱۴۰۲/۰۸/۰۴

**تاریخ بازنگری:** ۱۴۰۲/۰۹/۲۰

**تاریخ پذیرش:** ۱۴۰۲/۱۱/۳۰

**تاریخ انتشار:** ۱۴۰۲/۱۲/۲۵

**کلیدواژه‌ها:**
EDAS،
PIPRECIA،
امنیت سایبری،
انقلاب صنعتی چهارم،
تئوری اعداد Z.

**چکیده**

مسائل امنیت سایبری به چالشی پیچیده برای شرکت‌هایی که به پارادایم انقلاب صنعتی چهارم پایبند هستند، تبدیل شده‌است. از سوی دیگر، مفهوم امنیت سایبری در زمینه انقلاب صنعتی چهارم موضوعی نوظهور در ادبیات اخیر است. لذا در مطالعه حاضر، برای اولین‌بار جهت ارزیابی خطرهای امنیت سایبری در انقلاب صنعتی چهارم از یک مدل ترکیبی FMEA توسعه‌یافته مبتنی بر روش‌های تصمیم‌گیری چندمعیاره در شرایط عدم قطعیت با روش Bow Tie و در چهار فاز استفاده شده‌است. ابتدا ۱۶ خطر امنیت سایبری در انقلاب صنعتی چهارم طبق مدل FMEA شناسایی شده و عوامل تعیین‌کننده RPN مقداردهی می‌شوند. سپس از روش PIPRECIA Fuzzy برای وزن‌دهی به عوامل و روش Z-EDAS جهت اولویت‌بندی و شناسایی خطرهای بحرانی استفاده شده‌است. در آخر، از تحلیل Bow Tie برای تحلیل این خطرها استفاده شده‌است. نتایج حاصل از پیاده‌سازی رویکرد پیشنهادی نشانگر قابلیت و برتری آن در مقایسه با سایر روش‌های سنتی نظیر FMEA و Fuzzy EDAS بوده‌است.

**استناد:** معمارپور غیاثی، علی و قیدر خلخالی، جعفر. (۱۴۰۲). «یک مدل ترکیبی FMEA توسعه‌یافته مبتنی بر روش‌های F-PIPRECIA و Z-EDAS باروش Bow Tie جهت ارزیابی خطر امنیت سایبری در انقلاب صنعتی چهارم». *مدیریت مهندسی و رایانش نرم، دوره ۹ (۲)*. صص: ۱۷۶-۱۴۹.
https://doi.org/

ناشر: دانشگاه قم

## ۱) مقدمه

امنیت سایبری جهت جلوگیری از فقدان رقابت‌پذیری شرکت‌ها در زمینه انقلاب صنعتی چهارم، نقشی اساسی ایفا می‌کند. درواقع امروزه تجهیزات صنعتی در برابر حملات سایبری آسیب‌پذیر هستند که این امر می‌تواند کل مدل کسب‌وکار را تحت تاثیر قرار دهد. طبق گزارش‌های سالانه امنیت سایبری سیسکو در سال ۲۰۱۸ (سیسکو، ۲۰۱۸) ۳۱ درصد از سازمان‌ها، حملات سایبری به فناوری عملیاتی را تجربه کرده‌اند. درحالیکه ۳۸ درصد انتظار دارند حملات از فناوری اطلاعات به فناوری عملیاتی گسترش یابد. اگرچه امنیت سایبری از سوی ۷۵ درصد کارشناسان به‌عنوان یک اولویت تلقی می‌شود، تنها ۱۶ درصد تایید می‌کنند که شرکت آنها به‌خوبی برای رویارویی با چالش‌های امنیت سایبری آماده است (لتزی، لازوی و کرالو، ۲۰۱۸). از طرفی تعداد فزاینده‌ای از شرکت‌ها با تجهیز به اینترنت، در جهت بهبود کارآیی و اثربخشی به پارادایم انقلاب صنعتی چهارم که به‌عنوان اینترنت صنعتی اشیا یا اینترنت صنعتی نیز شناخته می‌شود، گام برمی‌دارند. درنتیجه در صنایع مجهز به اینترنت، مسائل امنیت سایبری ازجمله خطرهای آن، یکی از مهمترین چالش‌هایی است که باید مورد ارزیابی قرار گیرد.

روش FMEA یکی از معروف‌ترین روش‌های شناسایی و ارزیابی حالات خرابی و خطرهاست. FMEA یک رویکرد سیستماتیک بر پایه تیمی از خبرگان و پیشگیری قبل از وقوع است (جعفرزاده قوشچی، معمارپور غیاثی، رهنمای بناب و رنجبرزاده، ۲۰۲۲). در اغلب تحقیقاتی که از روش FMEA استفاده شده‌است، شناسایی موانع و خطرها براساس شاخص سنتی RPN انجام شده‌است. این در حالی است که این شاخص دارای کاستی‌هایی است. به‌عنوان مثال: عدم درنظرگرفتن اهمیت نسبی میان فاکتورها از مهمترین کاستی‌های این روش است (گول و آک، ۲۰۲۱). همچنین به دلیل کنشی‌بودن و تیمی‌بودن روش FMEA، میزان عوامل تعیین‌کننده RPN را اغلب نمی‌توان به‌صورت قطعی درنظر گرفت (قوشچی، یوسفی و خزائیلی، ۲۰۱۹؛ جعفرزاده قوشچی، شفیعی حق‌شناس، معمارپور غیاثی، گویدو و ویتاله، ۲۰۲۲). بنابراین جهت دستیابی به نتایج قابل‌اطمینان در برابر نظرات خبرگان، نیاز است تا اولویت‌بندی خطرها با درنظرگرفتن اهمیت نسبی میان فاکتورهای ارزیابی و با توجه به عدم قطعیت موجود در این فاکتورها انجام شود. علاوه بر استفاده از مدل FMEA، ارزیابی خطرهای بحرانی با استفاده از روش Bow Tie برای توصیف علل، اقدامات پیشگیرانه، پیامدها و اقدامات کاهش‌دهنده انجام می‌شود (آمبراواتی، یولیاستری و سولیستیواتی، ۲۰۲۲؛ مولکاهی، بویلان، سیگمن و استوارت، ۲۰۱۷؛ ویکو، پانایتسکو، پانایتسکو، دومیترسکو و تورف، ۲۰۱۸).

هدف اصلی این پژوهش شناسایی و اولویت‌بندی خطرهای امنیت سایبری در انقلاب صنعتی چهارم با ارائه یک رویکرد جدید جهت پوشش برخی از کاستی‌های مدل FMEA سنتی می‌باشد. این رویکرد برای اولین‌بار، براساس ترکیب روش توسعه‌یافته FMEA مبتنی بر روش Fuzzy PIPIRECIA (F-PIPRECIA) جهت وزن‌دهی به معیارها و روش Z-number EDAS (Z-EDAS) جهت اولویت‌بندی خطرها با روش Bow Tie جهت شناسایی و تحلیل خطرهای بحرانی ارائه می‌گردد. در این رویکرد با بکارگیری تئوری اعداد Z، سعی بر آن است عدم قطعیت و قابلیت‌اطمینان در عوامل تعیین‌کننده RPN درنظر گرفته شود. لازم به ذکر است اولویت‌بندی خطرها براساس امتیاز حاصل از رویکرد پیشنهادی به‌صورتی است که خطر با امتیاز بالاتر، در اولویت اول رسیدگی قرار خواهد گرفت. سپس علل، اقدامات پیشگیرانه، پیامدها و اقدامات

کاهش‌دهنده برای خطرهای دارای اولویت (بحرانی) با استفاده از تحلیل Bow Tie، شناسایی می‌شوند. جهت ارزیابی قابلیت رویکرد پیشنهادی، اولویت‌بندی خطرهای امنیت سایبری در انقلاب صنعتی چهارم توسط نتایج پیاده‌سازی رویکرد پیشنهادی حاصل از مدل توسعه‌یافته FMEA مبتنی بر روش‌های F-PIPRECIA و Z-EDAS در مقایسه با برخی از روش‌های مرسوم ارائه شده‌است.

## ۲) ادبیات پیشین

### ۲-۱) انقلاب صنعتی چهارم

طرفداران انقلاب صنعتی چهارم در حال ایجاد یک محیط تولید هوشمند هستند (غیاثی و قوشچی، ۲۰۲۳؛ واکانما، اسلام، محارانی، لی و کیم، ۲۰۲۱) و اینترنت اشیا را می‌توان یک پارادایم در این زمینه با پتانسیل تکنولوژیکی بسیار بالا درنظر گرفت. وجود اشیا مختلف که به‌صورت هوشمند با یکدیگر ارتباط برقرار می‌کنند و حجم زیادی از اطلاعات را انتقال می‌دهند، باعث ایجاد خطرات امنیتی می‌شوند و امنیت سایبری را به موضوع بسیار مرتبط با انقلاب صنعتی چهارم تبدیل می‌کنند (کرالو، لازوی و لتزی، ۲۰۲۰). با درنظرگرفتن این که پیاده‌سازی تکنولوژی اینترنت اشیا در تولید هوشمند، حجم زیادی از اطلاعات را تولید و به اشتراک می‌گذارد، اگر این سیستم آسیب ببیند، می‌تواند منجر به توقف تولید شود. با رشد استفاده از اینترنت اشیا، تخمین‌زده می‌شود که ترافیک اینترنت تا سال ۲۰۲۲ حدود ۴۵ درصد خواهد بود (الفقها، گویزانی، محمدی، الادهاری و ایاش، ۲۰۱۵؛ بلدا، منتوث، بلوم و تنتی، ۲۰۱۷). در فرآیندهای ساخت‌وتولید که توسط سیستم‌های هوشمند انجام می‌شود، مراحل از طراحی تا تولید را می‌توان از هر جایی کنترل و مدیریت کرد (بهرین، عثمان، عزلی و طالب، ۲۰۱۶). فلات، شرینگل، جسپرنیت، رسک و آدامزیک (۲۰۱۶) نمونه‌هایی از عملیات در انقلاب صنعتی چهارم مانند نظارت بر تولید هوشمند، تجزیه‌وتحلیل تولید و بهینه‌سازی تولید را معرفی می‌کنند. تغییرات برجسته‌ای که توسط انقلاب صنعتی چهارم تعریف شده‌است، پارادایم‌های مدیریتی جدیدی را ایجاد کرده‌است که جنبه‌های مختلف یک سازمان مانند پایداری (آردانزا، مورنو، سگورا، دلاکروز و آگویناگا، ۲۰۱۹)، منابع‌انسانی (جیمز، ۲۰۲۲) و مدیریت زنجیره تامین قگه، ارکارا، مرادلو و گسوامی، ۲۰۲۰) را شامل می‌شود.

### ۲-۲) خطرهای امنیت سایبری

توصیف خطرهای امنیت سایبری در سازمان‌ها می‌تواند راه‌حلی کلیدی برای کمک به آنها برای درک مفهوم اصلی امنیت سایبری باشد. طبق (رناد و ویر، ۲۰۱۶)، دارایی‌های سازمان‌ها معمولا در معرض تهدید حملات سایبری مانند دستکاری داده‌ها، جعل داده‌ها و امتناع از دسترسی به داده‌ها هستند که ممکن است بر چندین مورد از فعالیت‌های کسب‌وکار تاثیر منفی بگذارد. با این حال، بسیاری از نشانه‌ها حاکی از این است که سازمان‌ها تهدیدات سایبری را دست کم می‌گیرند و از استفاده اقدامات امنیتی کارآمد، امتناع می‌کنند (رناد و ویر، ۲۰۱۶). اکثر کارشناسان اعتراف کرده‌اند که جرایم سایبری بزرگترین تهدید برای هر شرکتی خواهد بود درحالیکه شرکت‌های کوچک و متوسط معتقدند که به دلیل اندازه خود، آسیب‌پذیر نیستند (بارلت، گاندولف و جاون، ۲۰۱۷). علاوه بر این، برآورد هزینه جرایم سایبری به دلیل برخی از حوادث سایبری که هنوز اعلام نشده‌اند یا هنوز نامرئی هستند، یک چالش مهم درنظر گرفته می‌شود (بری و بری، ۲۰۱۸). اخیرا

گزارش‌های رسمی نشان می‌دهند که شرکت‌های کوچک و متوسط به ارزشمندترین هدف برای حملات سایبری تبدیل شده‌اند. دلیل اصلی در بیشتر موارد، تکنیک‌های دفاعی ضعیفی است که توسط این سازمان‌ها در مقایسه با شرکت‌های بزرگ استفاده می‌شود. این تکنیک‌های ضعیف شامل تخصص کمتر، برون‌سپاری ناشناخته و روش‌های امنیتی قدیمی می‌شود (بارلت و همکاران، ۲۰۱۷). حبیبور رحمان، سون و شفائی (۲۰۲۳) یک رویکرد تئوری‌گراف را برای مدل‌سازی و ارزیابی خطر امنیت سایبری برای سیستم‌های تولید هوشمند پیشنهاد کرده‌اند. بیتون (۲۰۲۳) چارچوبی جهت تجزیه‌وتحلیل تهدیدات امنیت سایبری در سیستم‌های مبتنی بر یادگیری ماشین معرفی کرده‌اند. همچنین در این پژوهش، از روش AHP برای رتبه‌بندی ویژگی‌های مختلف حملات سایبری استفاده شده‌است. سونر، کیسگلو، بلات و تام (۲۰۲۳) در پژوهش خود، از روش FMEA برای ارزیابی خطر امنیت سایبری در یک سیستم ضبط‌کننده داده‌های سفر دریایی به‌منظور شناسایی آسیب‌پذیری‌ها و حملات سایبری خاصی که ممکن است علیه این سیستم انجام شود، استفاده کرده‌اند. سوکومار، مهدیرایی و جعفری-صادقی (۲۰۲۳) به‌منظور ارزیابی خطرات سایبری در خرده‌فروشی‌های آنلاین، از یک رویکرد یکپارچه براساس روش‌های SWARA و BWM استفاده کرده‌اند.

## ۳) روش‌های تصمیم‌گیری چند معیاره FMEA و Bowtie

به‌عنوان یک حوزه شناخته‌شده از تحقیقات، روش‌های تصمیم‌گیری چندمعیاره (MCDM) به‌طور گسترده توسط محققان برای بهبود عملکرد FMEA مورد استفاده قرار گرفته‌اند و به‌عنوان ابزاری ارزشمند در بهبود کاستی‌های مربوط به روش RPN مرسوم درنظر گرفته شده‌اند (قوشچی و همکاران، ۲۰۲۲؛ قوشچی و همکاران، ۲۰۱۹). آگویرا، پرز-دمینگز، لوویانو-کروز و کردرو-دیاز (۲۰۲۳) یک روش FMEA اصلاح‌شده مبتنی بر روش AHP و تحلیل بعدی (DA) جهت ارزیابی خطرهای توسعه محصول جدید ارائه کردند. کوماری، احمد، خان و احمد (۲۰۲۳) از یک مدل FMEA توسعه‌یافته استفاده از روش‌های تصمیم‌گیری چندمعیاره استفاده کرد. این رویکرد براساس روش‌های Fuzzy AHP و Fuzzy TOPSIS جهت ارزیابی حالات خرابی تصفیه‌خانه‌های پساب در مناطق نیمه‌گرمسیری ارائه شده‌است. جعفرزاده قوشچی، شفیعی حق‌شناس و همکاران (۲۰۲۲) یک رویکرد یکپارچه ارزیابی خطر براساس مدل FMEA مبتنی بر روش‌های SWARA و MARCOS در شرایط عدم قطعیت ارائه کردند. این رویکرد در ارزیابی خطرهای ایمنی جاده‌های روستایی در کشور ایتالیا پیاده‌سازی شده‌است. جین، منگ و فنگ (۲۰۲۲) از روش AHP Fuzzy براساس روش FMEA برای تجزیه‌وتحلیل حالات شکست سیستم لجستیک در همه‌گیری COVID-19 استفاده کرد. در این مقاله دوازده حالت خرابی شناسایی شده‌است و اقدامات پیشگیرانه و اصلاحی مربوطه جهت کاهش تاثیر خرابی‌ها توصیه شده‌است. غیاثی و قوشچی (۲۰۲۳) یک مدل FMEA توسعه‌یافته مبتنی بر روش‌های تصمیم‌گیری چندمعیاره جهت ارزیابی موانع پیاده‌سازی سیستم‌های اقتصاد چرخشی مبتنی بر اینترنت اشیا ارائه کردند. در این رویکرد از روش‌های SWARA و MOORA در شرایط عدم قطعیت جهت پوشش برخی کاستی‌های مدل FMEA سنتی استفاده شده‌است. بیازیت و کپتن (۲۰۲۳) جهت ارزیابی خطرهای آلودگی دریایی از روش شبکه بیزین فازی مبتنی بر تحلیل Bow Tie استفاده کردند. کاظمی، عباسی، کاظمی، جمشیدزاده و رشیدی

(۲۰۲۱) از رویکرد تلفیقی Bow Tie و FMEA جهت بررسی خطرهای موجود در ۱۸ واحد مختلف پالایشگاه گاز ایلام استفاده کردند.

## ۴) شکاف تحقیقاتی

در بخش مرور ادبیات، مفاهیم مربوط به انقلاب صنعتی چهارم، خطرهای امنیت سایبری، و همچنین مقالات مربوط به توسعه مدل FMEA براساس روش‌های تصمیم‌گیری چند معیاره و روش Bow Tie مورد بررسی قرار گرفته‌است. اگرچه مقالاتی در حوزه امنیت سایبری در انقلاب صنعتی چهارم منتشر شده‌است اما تعداد کمی از آنها بر روی خطرهای امنیت سایبری متمرکز است. از این رو، فقدان تحقیق برای ارائه راهکارهایی جهت شناسایی و اولویت‌بندی این خطرها احساس می‌شود. همچنین با بررسی مقالات موجود مبتنی بر روش FMEA، کمبود مدل FMEA توسعه‌یافته که علاوه بر عدم قطعیت، قابلیت‌اطمینان را نیز مورد بررسی قرار دهد، احساس می‌شود. درنتیجه مطالعه حاضر برای اولین‌بار به ارائه یک مدل ترکیبی FMEA توسعه‌یافته براساس روش‌های تصمیم‌گیری چندمعیاره PIPRECIA Fuzzy و Z-EDAS با روش Bow Tie جهت شناسایی و اولویت‌بندی خطرهای امنیت سایبری در انقلاب صنعتی چهارم می‌پردازد. برخی از نوآوری‌های مطالعه حاضر عبارتنداز:

- ارائه یک مدل ترکیبی از روش توسعه‌یافته FMEA بر پایه روش‌هایFuzzy PIPRECIA و Z-EDAS با روش Bow Tie.
- درنظرگرفتن قابلیت‌اطمینان در کنار عدم قطعیت به واسطه تئوری اعداد Z در مدل یکپارچه پیشنهادی.
- درنظرگرفتن هزینه به‌عنوان یک شاخص مهم مدیریتی در کنار معیارهای روش FMEA (شدت، وقوع و احتمال کشف).
- استفاده از رویکرد Fuzzy PIPRECIA جهت ارزیابی اهمیت نسبی معیارها.
- مقایسه رویکرد پیشنهادی با برخی رویکردهای موجود در ادبیات جهت اعتبارسنجی مدل.

## ۵) روش‌ها

### ۵–۱) روش Fuzzy PIPRECIA

روش PIPRECIA برای اولین‌بار در سال ۲۰۱۷ ارائه شده‌است (ستانوجیک، زاوادسکاس، کاراباسویچ، ماراندا‌چ و تورسکیس، ۲۰۱۷). در ادامه گام‌های مربوط به روش توسعه‌یافته PIPRECIA در محیط فازی ارائه شده‌است.

گام ۱) تشکیل مجموعه معیارها جهت ارزیابی و تشکیل یک تیم تصمیم‌گیری

گام ۲) برای تعیین اهمیت نسبی معیارها، هر تصمیم‌گیرنده به‌طور جداگانه معیارهای از پیش مرتب‌شده را با شروع از معیار دوم ارزیابی می‌کند مانند رابطه (۱).

رابطه ۱)

$$\overline{S_j^r} = \begin{cases} > \overline{1} & if \quad C_j > C_{j-1} \\ = \overline{1} & if \quad C_j = C_{j-1} \\ < \overline{1} & if \quad C_j < C_{j-1} \end{cases}$$

که در اینجا $\overline{S_j^r}$ نشان‌دهنده ارزیابی انجام‌شده توسط تصمیم‌گیرنده r است.

برای به‌دست‌آوردن یک ماتریس $\overline{S_j}$، لازم است میانگین‌گیری انجام شود.

ماتریس $\overline{S_j^r}$ با استفاده از میانگین هندسی به یک ماتریس تبدیل می‌شود. تصمیم‌گیرندگان با اعمال مقیاس‌های تعریف‌شده در جداول ۱ و ۲ معیارها را ارزیابی می‌کنند.

**جدول ۱. ارزیابی معیارها براساس مقیاس ۱-۲**

| | | DFV | u | m | l |
|---|---|---|---|---|---|
| تقریبا برابر | 1 | 1.008 | 1.050 | 1.000 | 1.000 |
| کمی با اهمیت‌تر | 2 | 1.150 | 1.200 | 1.150 | 1.100 |
| نسبتا با اهمیت‌تر | 3 | 1.292 | 1.350 | 1.300 | 1.200 |
| با اهمیت‌تر | 4 | 1.433 | 1.500 | 1.450 | 1.300 |
| بسیار با اهمیت‌تر | 5 | 1.575 | 1.650 | 1.600 | 1.400 |
| به‌طور غالب با اهمیت‌تر | 6 | 1.717 | 1.800 | 1.750 | 1.500 |
| کاملا با اهمیت‌تر | 7 | 1.858 | 1.950 | 1.900 | 1.600 |

مقیاس ۱-۲

**جدول ۲. ارزیابی معیارها براساس مقیاس ۰-۱**

| | | | DFV | u | m | l |
|---|---|---|---|---|---|---|
| کمی کم اهمیت‌تر | SLS | 0.944 | 1.000 | 1.000 | 0.667 | |
| نسبتا کمتر با اهمیت | MLS | 0.694 | 1.000 | 0.667 | 0.500 | |
| کم اهمیت‌تر | LS | 0.511 | 0.667 | 0.500 | 0.400 | |
| واقعا کم اهمیت‌تر | RLS | 0.406 | 0.500 | 0.400 | 0.333 | |
| بسیار کم اهمیت‌تر | MULS | 0.337 | 0.400 | 0.333 | 0.286 | |
| به‌طور غالب کم اهمیت‌تر | DLS | 0.288 | 0.333 | 0.286 | 0.250 | |
| کاملا کم اهمیت‌تر | ALS | 0.251 | 0.286 | 0.250 | 0.222 | |

مقیاس ۰-۱

گام ۳) تعیین ضریب $\overline{k_j}$

رابطه ۲)

$$\overline{k_j} = \begin{cases} = \overline{1} & if \quad j = 1 \\ 2 - \overline{s_j} & if \quad j > 1 \end{cases}$$

گام ۴) تعیین وزن فازی

رابطه ۳)

$$\overline{q_j} = \begin{cases} = \overline{1} & if \quad j = 1 \\ \dfrac{\overline{q_{j-1}}}{\overline{k_j}} & if \quad j > 1 \end{cases}$$

گام ۵) تعیین وزن نسبی معیار

رابطه ٤)
$$\overline{w_j} = \frac{\overline{q}_j}{\sum_{j=1}^{n} \overline{q}_j}$$

در مراحل زیر معکوس روش PIPRECIA فازی پیاده‌سازی می‌شود:

گام ۶) برای تعیین اهمیت نسبی معیارها، هر تصمیم‌گیرنده به‌طور جداگانه معیارهای از پیش مرتب‌شده را با شروع از معیار ماقبل‌آخر ارزیابی می‌کند.

رابطه ٥)
$$\overline{S_j^r}' = \begin{cases} > \bar{1} & if \quad C_j > C_{j+1} \\ = \bar{1} & if \quad C_j = C_{j+1} \\ < \bar{1} & if \quad C_j < C_{j+1} \end{cases}$$

مجددا ماتریس $\overline{S_j^r}'$ با استفاده از میانگین هندسی به‌دست می‌آید.

گام ۷) تعیین ضریب $\overline{k_j}'$

رابطه ٦)
$$\overline{k_j}' = \begin{cases} = \bar{1} & if \quad j = n \\ 2 - \overline{s_j} & if \quad j > n \end{cases}$$

که در اینجا n تعداد کل معیارها می‌باشد.

گام ۸) تعیین وزن فازی $\overline{q_j}'$

رابطه ۷)
$$\overline{q_j}' = \begin{cases} = \bar{1} & if \quad j = n \\ \dfrac{\overline{q_{j+1}}'}{\overline{k_j}} & if \quad j > n \end{cases}$$

گام ۹) تعیین وزن نسبی معیار

رابطه ۸)
$$\overline{w_j}' = \frac{\overline{q}_j'}{\sum_{j=1}^{n} \overline{q}_j'}$$

گام ۱۰) تعیین وزن نهایی

رابطه ۹)
$$\overline{w_j}'' = \frac{1}{2}(\overline{w_j} + \overline{w_j}')$$

### ۵-۲) روش Z-number EDAS

روش EDAS در سال ۲۰۱۵ ارائه شده‌است (کشاورز قرابائی، زاوادسکاس، الفت و تورسکیس، ۲۰۱۵). در ادامه گام‌های مربوط به روش توسعه‌یافته EDAS براساس تئوری اعداد Z ارائه شده‌است.

گام ۱) تشکیل ماتریس تصمیم با استفاده از متغیرهای زبانی Z

با توجه به متغیرهای زبانی ارائه‌شده در جدول ۳ هر یک از گزینه‌ها با توجه به معیارهای مورد بررسی، مقداردهی می‌شوند.

**جدول ۳. تبدیل متغیرهای زبانی مربوط به اعداد Z به اعداد فازی مثلثی**

| متغیرهای زبانی | تابع عضویت | | | متغیرهای زبانی | تابع عضویت | | |
|---|---|---|---|---|---|---|---|
| | l | m | u | | l | m | u |
| VH,VH | 8.54 | 9.49 | 9.49 | VH,H | 7.53 | 8.37 | 8.37 |
| VH,M | 6.36 | 7.07 | 7.07 | VH,L | 4.93 | 5.48 | 5.48 |
| VH,VL | 2.85 | 3.16 | 3.16 | H,VH | 6.64 | 8.54 | 9.49 |
| H,H | 5.86 | 7.53 | 8.37 | H,M | 4.95 | 6.36 | 7.07 |
| H,L | 3.84 | 4.93 | 5.48 | H,VL | 2.21 | 2.85 | 3.16 |
| MH,VH | 4.74 | 6.64 | 8.54 | MH,H | 4.18 | 5.86 | 7.53 |
| MH,M | 3.54 | 4.95 | 6.36 | MH,L | 2.74 | 3.84 | 4.93 |
| MH,VL | 1.58 | 2.21 | 2.85 | M,VH | 2.85 | 4.74 | 6.64 |
| M,H | 2.51 | 4.28 | 5.86 | M,M | 2.12 | 3.54 | 4.95 |
| M,L | 1.64 | 2.74 | 3.83 | M,VL | 0.95 | 1.58 | 2.21 |
| ML,VH | 0.95 | 2.85 | 4.74 | ML,H | 0.84 | 2.51 | 4.18 |
| ML,M | 0.71 | 2.12 | 3.54 | ML,L | 0.55 | 1.64 | 2.74 |
| ML,VL | 0.32 | 0.95 | 1.58 | L,VH | 0 | 0.95 | 2.85 |
| L,H | 0 | 0.84 | 2.51 | L,M | 0 | 0.71 | 2.12 |
| L,L | 0 | 0.55 | 1.64 | L,VL | 0 | 0.32 | 0.95 |
| VL,VH | 0 | 0 | 0.95 | VL,H | 0 | 0 | 0.84 |
| VL,M | 0 | 0 | 0.71 | VL,L | 0 | 0 | 0.55 |
| VL,VL | 0 | 0 | 0.32 | | | | |

گام ۲) تشکیل ماتریس تصمیم‌گیری

متغیرهای زبانی ارائه‌شده در گام قبل با استفاده از جدول ۳ به اعداد فازی مثلثی تبدیل می‌شوند. ماتریس تصمیم مجموع β به‌صورت رابطه (۱۰) نمایش داده می‌شود.

$$\begin{bmatrix} (x_{11}^l, x_{11}^m, x_{11}^u) & \cdots & (x_{12}^l, x_{12}^m, x_{12}^u) & \cdots & (x_{1n}^l, x_{1n}^m, x_{1n}^u) \\ \cdots & & \cdots & & \cdots \\ \cdots & & \cdots & & \cdots \\ (x_{m1}^l, x_{m1}^m, x_{m1}^u) & \cdots & (x_{m2}^l, x_{m2}^m, x_{m2}^u) & \cdots & (x_{mn}^l, x_{mn}^m, x_{mn}^u) \end{bmatrix} \beta = \quad \text{رابطه ۱۰)}$$

که در آن m تعداد گزینه‌ها، n تعداد معیار ها، و $x_{mn}$ نشان‌دهنده ترجیح گزینه iام در معیار jام است.

گام ۳) تشکیل ماتریس تصمیم‌گیری متوسط

متغیرهای زبانی ارائه‌شده در گام قبل با استفاده از جدول ۳ به اعداد فازی مثلثی تبدیل می‌شوند. ماتریس تصمیم مجموع β به‌صورت رابطه (۱۰) نمایش داده می‌شود.

$$\tilde{x}_{ij} = \frac{1}{k} \oplus_{p=1}^{k} \tilde{x}_{ij}^{p} \quad \text{رابطه ۱۱)}$$

که در آن $\tilde{x}_{ij}^{p}$ نشانگر عملکرد گزینه iام با توجه به معیار jام از دیدگاه تصمیم‌گیرنده pام از میان k تصمیم‌گیرنده می‌باشد.

گام ۴) نرمال‌کردن ماتریس تصمیم‌گیری

جهت بی‌مقیاس‌سازی ماتریس تصمیم از روابط زیر استفاده می‌شود.

رابطه ۱۲) $$AV = [\widetilde{av_{ij}}]_{1\times m}$$

رابطه ۱۳) $$\widetilde{av}_j = \frac{1}{n}\oplus_{i=1}^{n}\tilde{x}_{ij}$$

که در آن عناصر $\widetilde{av}_j$ نشانگر مقادیر متوسط با توجه به هر معیار است.

گام ۵) محاسبه ماتریس‌های PDA و NDA

در این مرحله ماتریس‌های فاصله مثبت از میانگین (PDA) و فاصله منفی از میانگین (NDA) با توجه به نوع معیار (سود (B) و هزینه (N)) با استفاده از روابط زیر محاسبه می‌شوند.

رابطه ١٤) $$PDA = [\widetilde{pda_{ij}}]_{n\times m}$$

رابطه ١٥) $$NDA = [\widetilde{nda_{ij}}]_{n\times m}$$

رابطه ١٦) $$\widetilde{pda_{ij}} = \begin{cases} \frac{\psi(\tilde{x}_{ij} \ominus \widetilde{av}_j)}{k(\widetilde{av}_j)} \; if\; j \in B \\ \frac{\psi(\widetilde{av}_j \ominus \tilde{x}_{ij})}{k(\widetilde{av}_j)} \; if\; j \in N \end{cases}$$

رابطه ١٧) $$\widetilde{nda_{ij}} = \begin{cases} \frac{\psi(\widetilde{av}_j \ominus \tilde{x}_{ij})}{k(\widetilde{av}_j)} \; if\; j \in B \\ \frac{\psi(\tilde{x}_{ij} \ominus \widetilde{av}_j}{k(\widetilde{av}_j)} \; if\; j \in N \end{cases}$$

گام ۶) محاسبه فواصل مثبت و منفی موزون برای همه گزینه‌ها

رابطه ١٨) $$\tilde{sp}_i = \oplus_{j=1}^{m}(\tilde{w}_j \otimes \widetilde{pda_{ij}})$$

رابطه ١٩) $$\tilde{sn}_i = \oplus_{j=1}^{m}(\tilde{w}_j \otimes \widetilde{nda_{ij}})$$

گام ۷) نرمال‌سازی مقادیر (sp)˜_i و (sn)˜_i برای همه گزینه‌ها

رابطه ٢٠) $$\widetilde{nsp}_i = \frac{\tilde{sp}_i}{\max_i(k(\tilde{sp}_i)}$$

رابطه ٢١) $$\widetilde{nsn}_i = 1 - \frac{\tilde{sn}_i}{\max_i(k(\tilde{sn}_i)}$$

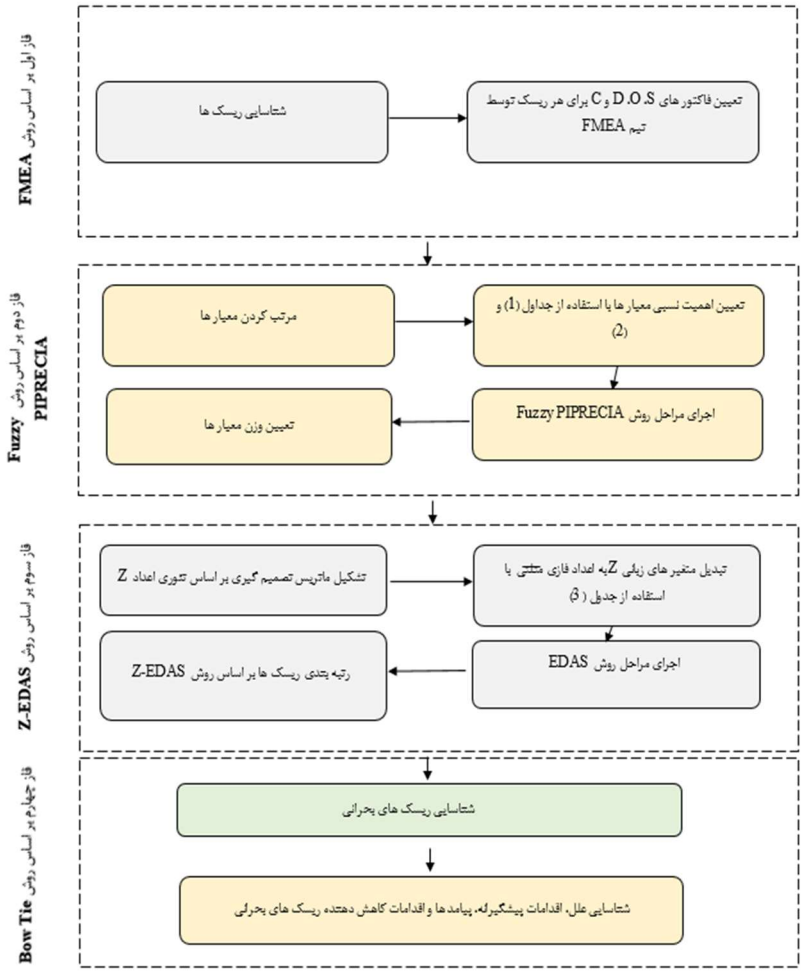
گام ۸) محاسبه امتیاز ارزیابی((as)˜_i) برای همه گزینه‌ها

رابطه ٢٢) $$\tilde{as}_i = \frac{1}{2}(\widetilde{nsp}_i \oplus \widetilde{nsn}_i)$$

گام ۹) رتبه‌بندی گزینه‌ها به‌صورت نزولی براساس مقدار $\widetilde{as}_i$

## ۶) رویکرد پیشنهادی

در این بخش، رویکرد پیشنهادی این تحقیق با بهره‌گیری از روش‌های FMEA، PIPRECIA Fuzzy، Z-EDAS و Bow Tie برای ارزیابی و اولویت‌بندی خطرها ارائه می‌گردد. رویکرد پیشنهادی در چهار فاز ارائه می‌گردد. در فاز اول این رویکرد ضمن شناسایی خطرها توسط تیم FMEA، مقادیر معیارهای چهارگانه نیز امتیازدهی می‌شوند. در این فاز قابلیت‌اطمینان هر کدام از خطرهای شناسایی‌شده، توسط تیم خبره تعیین می‌گردد. در فاز دوم، در راستای درنظرگرفتن اهمیت متفاوت به ازای معیارها از روش PIPRECIAFuzzy استفاده می‌گردد به نحوی که پس از مرتب‌کردن معیارها با استفاده از متغیرهای کلامی، این متغیرها با استفاده از جداول ۱ و ۲ به اعداد فازی مثلثی تبدیل می‌گردد. در ادامه مراحل روش PIPRECIA با توجه به این مقادیر پیاده‌سازی‌شده و وزن هر معیار تعیین می‌گردد. در فاز سوم براساس خروجی‌های فاز اول و دوم سعی شده‌است اولویت‌بندی خطرهای شناسایی‌شده با توجه به وزن معیارها، با استفاده از روش Z-EDAS انجام گیرد. این روش برخلاف روش EDAS مرسوم، علاوه بر درنظرگرفتن مقادیر فازی، توانایی درنظرگرفتن قابلیت‌اطمینان برای هر معیار به ازای گزینه را دارد. در این روش پس از تعیین ماتریس تصمیم که درایه‌های آن متشکل از اعداد فازی و مقادیر قابلیت اطمینان (اعداد–Z) هستند، این مقادیر با استفاده از جدول ۳ به اعداد فازی مثلثی تبدیل می‌شوند سپس مراحل روش EDAS در محیط فازی اجرا می‌گردند. در فاز چهارم این رویکرد؛ علل، اقدامات پیشگیرانه، پیامدها و اقدامات کاهش‌دهنده برای خطرهای دارای اولویت‌های اول تا سوم براساس نتایج روش Z-EDAS به‌عنوان خطرهای بحرانی با استفاده از روش Bow Tie شناسایی می‌گردد. روند اجرایی رویکرد پیشنهادی در شکل ۱ نیز نمایش داده شده‌است.




**شکل ۱. رویکرد پیشنهادی**

## ۷) مطالعه موردی و تحلیل نتایج

در راستای بررسی قابلیت رویکرد پیشنهادی در این تحقیق، سعی بر آن است که اولویت‌بندی خطرها، خطرهای امنیت سایبری در انقلاب صنعتی چهارم با استفاده از این رویکرد صورت پذیرد. فهرست ۱۶ خطر شناسایی‌شده ناشی از روش FMEA در جدول ۴ ارائه شده‌است.

**جدول ٤. خطرها پیاده‌سازی لجستیک هوشمند**

| نشان | عنوان خطر | منبع |
|---|---|---|
| R1 | دستکاری و یا جعل داده‌ها | Khalid et al., 2018; Preuveneers, Joosen, & Ilie-Zudor, ) (2017b; Xu, He, Wang, Susilo, & Jin, 2017 |
| R2 | حمله عدم پذیرش سرویس (DoS) با استفاده از ترافیک حجیم | Cheminod et al., 2017; Corbò, Foglietta, Palazzo, & ) Panzieri, 2018; Hassanzadeh, Modi, & Mulchandani, 2015; Kobara, 2016; Lee, Lee, Yoo, Kwon, & Shon, 2018; Preuveneers, Joosen, & Ilie-Zudor, 2017a; Preuveneers et Liu, 2017; & ,al., 2017b; Ren, Wu, Zhang, Terpenny (Urquhart & McAuley, 2018 |
| R3 | استراق سمع شبکه | (Sukumar et al., 2023) |
| R4 | اعطای امتیاز خاص | (Kobara, 2016; Preuveneers et al., 2017a, 2017b) |

| نشان | عنوان خطر | منبع |
|---|---|---|
| R5 | انتقال داده‌ها از/به دستگاه‌های غیرمجاز | Dieber et al., 2017; Januário, Carvalho, Cardoso, & Gil, ) (2016; Lee et al., 2018; Preuveneers et al., 2017b |
| R6 | آلودگی به بدافزارها و ویروس‌ها (به‌صورت تصادفی یا عمدی) | Benias & Markopoulos, 2017; Hassanzadeh et al., 2015; ) (Khalid et al., 2018; Urquhart & McAuley, 2018 |
| R7 | القای عملیات غیرعادی با استفاده از کد عملکرد غیرعادی پروتکل شبکه توزیع‌شده(DNP3) | (Lee et al., 2018) |
| R8 | حملات روز صفر | (Kobara, 2016; Ren et al., 2017) |
| R9 | پارازیت، تکرار گره و مسیریابی نادرست اطلاعات | (Januário et al., 2016) |
| R10 | آلودگی دادگان هوش مصنوعی | (Sukumar et al., 2023) |
| R11 | حملات مهندسی اجتماعی | (Urquhart & McAuley, 2018) |
| R12 | حملات انکار | (Preuveneers et al., 2017a, 2017b) |
| R13 | تخریب‌های فیزیکی | (Khalid et al., 2018; Xu et al., 2017) |
| R14 | حملات خودی و رفتارهای ناخواسته | (Khalid et al., 2018; Urquhart & McAuley, 2018) |
| R15 | تهدید پایدار پیشرفته(APT) | (Hassanzadeh et al., 2015; Urquhart & McAuley, 2018) |
| R16 | حملات فیشینگ | Hassanzadeh et al., 2015; Ren et al., 2017; Urquhart & ) (McAuley, 2018; van Lier, 2017 |

در این بخش نتایج حاصل از پیاده‌سازی رویکرد پیشنهادی در ارزیابی خطرهای امنیت سایبری در انقلاب صنعتی چهارم بررسی می‌شود. ابتدا خطرهای موجود توسط تیم FMEA متشکل از خبرگان شناسایی شده و مقادیر شاخص‌های چهارگانه (شدت (S)، وقوع (O)، احتمال کشف (D) و هزینه (C) به ازای هر خطر توسط تیم FMEA تعیین می‌گردد (جدول ۵ مشاهده شود). سپس با توجه به عدم قطعیت و همچنین عدم اطمینان در این فاکتورها از تئوری اعداد Z بهره گرفته‌می‌شود. تئوری اعداد Z علاوه بر درنظرگرفتن عدم قطعیت در معیارها، عدم قطعیت نظرات خبرگان را نیز مورد توجه قرار می‌دهد. مقادیر متغیرهای زبانی معیارهای چهارگانه به ازای خطرها با توجه به نظرات تیم FMEA در جدول ۵ ارائه شده‌است. سپس این مقادیر متغیرهای زبانی با استفاده از جدول ۳ به اعداد فازی مثلثی تبدیل می‌شوند.

**جدول ۵. مقادیر شاخص‌ها به ازای استراتژی‌ها در قالب متغیرهای زبانی Z**

| | S | | | O | | | D | | | C | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Risk | **DM1** | **DM2** | **DM3** | **DM1** | **DM2** | **DM3** | **DM1** | **DM2** | **DM3** | **DM1** | **DM2** | **DM3** |
| R1 | VH,VL | MH,VL | MH,H | ML,VL | H,L | M,H | VH,M | MH,VL | H,L | M,H | M,M | VH,VL |
| R2 | MH,H | VH,VL | ML,H | ML,H | ML,VL | MH,H | VH,VH | H,VL | MH,VL | MH,L | M,H | MH,H |
| R3 | MH,H | VH,VL | L,H | VH,H | H,L | MH,VL | ML,H | ML,VL | L,VL | VH,H | ML,M | VH,H |
| R4 | VL,H | VL,VL | M,H | ML,VL | MH,H | H,L | MH,VL | VH,H | VH,H | M,H | MH,L | MH,H |
| R5 | MH,VH | VH,H | VH,H | H,H | VH,M | H,VH | ML,VL | L,VH | M,M | VH,H | H,H | MH,VL |
| R6 | VH,M | VH,H | H,VL | H,VH | H,M | M,M | M,M | L,VL | H,L | MH,VL | H,H | ML,VL |
| R7 | MH,VH | M,H | ML,VL | VH,VL | VH,H | M,M | MH,VL | ML,H | H,L | H,H | MH,H | ML,VL |
| R8 | M,VH | L,VL | ML,H | VH,VL | M,VH | MH,H | MH,VL | MH,L | L,VL | M,VL | ML,VL | ML,VH |
| R9 | ML,VL | MH,L | L,L | H,M | H,M | M,M | MH,H | H,M | MH,L | L,VL | ML,M | L,VL |
| R10 | ML,H | L,H | VL,VH | VH,H | VH,VH | ML,VL | VH,H | MH,VL | MH,VL | MH,L | MH,VH | M,M |
| R11 | VH,M | VH,VH | H,L | VH,VH | H,VH | ML,VL | VL,VL | VL,VH | L,M | MH,VL | VH,VH | ML,M |
| R12 | VL,H | M,H | MH,H | MH,H | VH,H | MH,VL | VL,VH | ML,H | ML,VL | MH,H | MH,H | MH,L |
| R13 | MH,M | ML,VL | MH,H | L,M | MH,VL | MH,VL | L,H | VL,VL | ML,VL | MH,VL | VH,H | MH,L |
| R14 | VL,M | VL,H | L,H | ML,M | VH,VL | MH,VL | L,H | M,L | L,VL | MH,VL | H,VL | VH,H |
| R15 | VL,VL | ML,VL | VL,M | H,H | MH,M | H,VH | VH,VL | VL,VL | M,M | ML,VL | MH,VL | MH,VL |
| R16 | ML,VH | VL,VH | MH,H | VH,VL | H,L | VH,M | ML,VL | ML,VL | MH,H | M,H | ML,VL | ML,M |

در ادامه و براساس فاز دوم رویکرد پیشنهادی، وزن فاکتورها با استفاده از روش F-PIPRECIA تعیین می گردد.

**جدول ٦. نگرش تیم خبرگان با استفاده از مقیاس زبانی برای PIPRECIA Fuzzy**

| PIPR. | S | O | D | C |
|---|---|---|---|---|
| DM1 | | واقعا کم اهمیت‌تر | کم اهمیت‌تر | نسبتا با اهمیت‌تر |
| DM2 | | کم اهمیت‌تر | کمی کم اهمیت تر | بسیار با اهمیت‌تر |
| DM3 | | نسبتا کمتر با اهمیت | واقعا کم اهمیت‌تر | با اهمیت‌تر |

**جدول ۷. نگرش تیم خبرگان با استفاده از مقیاس زبانی برای PIPRECIA Fuzzy معکوس**

| PIPR-I | C | D | O | S |
|---|---|---|---|---|
| DM1 | | کم اهمیت‌تر | تقریبا برابر | کمی با اهمیت‌تر |
| DM2 | | بسیار کم اهمیت‌تر | نسبتا با اهمیت تر | با اهمیت‌تر |
| DM3 | | واقعا کم اهمیت‌تر | به‌طور غالب با اهمیت‌تر | با اهمیت‌تر |

در این مرحله، متغیرهای زبانی ارائه‌شده در جداول ۶ و ۷ با استفاده از جداول ۱ و ۲ به اعداد مثلثی تبدیل می‌شوند. در ادامه اعداد فازی مثلثی حاصل از نظر خبرگان در تعیین میزان اهمیت معیارهای چهارگانه در جداول ۸ و ۹ ارائه شده‌است.

**جدول ۸. نگرش تیم خبرگان براساس اعداد فازی مثلثی برای PIPRECIA Fuzzy**

| PIPR. | S | | | O | | | D | | | C | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | l | m | u | l | m | u | l | m | u | l | m | u |
| DM1 | | | | 0.333 | 0.400 | 0.500 | 0.400 | 0.500 | 0.667 | 1.200 | 1.300 | 1.350 |
| DM2 | | | | 0.400 | 0.500 | 0.667 | 0.667 | 1.000 | 1.000 | 1.400 | 1.600 | 1.650 |
| DM3 | | | | 0.500 | 0.667 | 1.000 | 0.333 | 0.400 | 0.500 | 1.300 | 1.450 | 1.500 |

**جدول ۹. نگرش تیم خبرگان با استفاده از مقیاس زبانی برای PIPRECIA Fuzzy معکوس**

| PIPR-I | C | | | D | | | O | | | S | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | l | m | u | l | m | u | l | m | u | l | m | u |
| DM1 | | | | 0.400 | 0.500 | 0.667 | 1.000 | 1.000 | 1.050 | 1.100 | 1.150 | 1.200 |
| DM2 | | | | 0.286 | 0.333 | 0.400 | 1.200 | 1.300 | 1.350 | 1.300 | 1.450 | 1.500 |
| DM3 | | | | 0.333 | 0.400 | 0.500 | 1.500 | 1.750 | 1.800 | 1.300 | 1.450 | 1.500 |

جزئیات محاسبات روش PIPRECIA فازی در جدول ۱۰ آمده‌است.

**جدول ۱۰. جزئیات محاسبات روش PIPRECIA Fuzzy**

| PIPRECIA | $s_j$ | | | $k_j$ | | | $q_j$ | | | $w_j$ | | | DF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | l | m | u | l | m | u | l | m | u | l | m | u | |
| S | | | | 1.000 | 1.000 | 1.000 | 1.000 | 1.000 | 1.000 | 0.276 | 0.325 | 0.381 | 0.326 |
| O | 0.411 | 0.522 | 0.722 | 1.278 | 1.478 | 1.589 | 0.629 | 0.677 | 0.783 | 0.174 | 0.220 | 0.298 | 0.225 |
| D | 0.467 | 0.633 | 0.722 | 1.278 | 1.367 | 1.533 | 0.410 | 0.495 | 0.613 | 0.113 | 0.161 | 0.233 | 0.165 |
| C | 1.300 | 1.450 | 1.500 | 0.500 | 0.550 | 0.700 | 0.586 | 0.900 | 1.225 | 0.162 | 0.293 | 0.467 | 0.300 |
| Σ | | | | | | | 2.626 | 3.072 | 3.620 | | | | |

نتایج حاصل از پیاده‌سازی روش PIPRECIA Fuzzy معکوس در جدول ۱۱ آمده‌است.

**جدول ۱۱. جزئیات محاسبات روش PIPRECIA Fuzzy معکوس**

| PIPRECIA-I | $s'_j$ | | | $k'_j$ | | | $q'_j$ | | | $w'_j$ | | | DF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | l | m | u | l | m | u | l | m | u | l | m | u | |
| **S** | 1.233 | 1.350 | 1.400 | 0.600 | 0.650 | 0.767 | 1.025 | 1.490 | 1.880 | 0.283 | 0.485 | 0.716 | 0.490 |
| **O** | 1.233 | 1.350 | 1.400 | 0.600 | 0.650 | 0.767 | 0.786 | 0.968 | 1.128 | 0.217 | 0.315 | 0.430 | 0.318 |
| **D** | 0.340 | 0.411 | 0.522 | 1.478 | 1.589 | 1.660 | 0.602 | 0.629 | 0.677 | 0.166 | 0.205 | 0.258 | 0.207 |
| **C** | | | | 1.000 | 1.000 | 1.000 | 1.000 | 1.000 | 1.000 | 0.276 | 0.325 | 0.381 | 0.326 |
| **Σ** | | | | | | | 3.413 | 4.087 | 4.684 | | | | |

با توجه به جداول ۱۰ و ۱۱، وزن نهایی معیارهای شدت (S)، وقوع (O)، احتمال کشف (D) و هزینه (C) با استفاده از رابطه (۹) به ترتیب ۰.۴۰۸، ۰.۲۷۲، ۰.۱۸۶ و ۰.۳۱۳ آمده‌است. در فاز سوم رویکرد پیشنهادی و براساس نتایج فازهای اول و دوم، اولویت‌بندی خطرها با استفاده از روش توسعه‌یافته Z-EDAS انجام می‌پذیرد. در ابتدا ماتریس تصمیم‌گیری روش Z-EDAS در قالب درایه‌های اعداد Z تشکیل می‌شود به نحوی که سطرها نشانگر گزینه‌های مورد ارزیابی یا همان خطرها و ستون‌های این ماتریس نشانگر معیارهای ارزیابی یا همان فاکتورهای چهارگانه می‌باشد. بدین ترتیب متغیرهای زبانی ارائه‌شده در جدول ۵ با استفاده از جدول ۳ به مقادیر فازی مثلثی تبدیل می‌شوند. سپس نظرات خبرگان با استفاده از رابطه (۱۱) تجمیع می‌شود. جدول ۱۲ ماتریس تصمیم تجمیع‌شده را نشان می‌دهد.

**جدول ۱۲. ماتریس تصمیم تجمیع شده**

| | S | | | O | | | D | | | C | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | l | m | u | l | m | u | l | m | u | l | m | u |
| R1 | 2.870 | 3.743 | 4.513 | 2.223 | 3.387 | 4.307 | 3.927 | 4.737 | 5.133 | 2.493 | 3.660 | 4.657 |
| R2 | 2.623 | 3.843 | 4.957 | 1.780 | 3.107 | 4.430 | 4.110 | 4.850 | 5.167 | 3.143 | 4.660 | 6.107 |
| R3 | 2.343 | 3.287 | 4.400 | 4.317 | 5.170 | 5.567 | 0.387 | 1.260 | 2.237 | 5.257 | 6.287 | 6.760 |
| R4 | 0.837 | 1.427 | 2.340 | 2.780 | 3.913 | 4.863 | 5.547 | 6.317 | 6.530 | 3.143 | 4.660 | 6.107 |
| R5 | 6.600 | 7.793 | 8.427 | 6.287 | 7.713 | 8.310 | 0.813 | 1.813 | 3.127 | 4.990 | 6.037 | 6.530 |
| R6 | 5.367 | 6.097 | 6.200 | 4.570 | 6.147 | 7.170 | 1.987 | 2.930 | 3.793 | 2.587 | 3.563 | 4.267 |
| R7 | 2.523 | 3.957 | 5.327 | 4.167 | 5.023 | 5.493 | 2.087 | 3.217 | 4.170 | 3.453 | 4.780 | 5.827 |

| | S | | | O | | | D | | | C | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R8 | 1.230 | 2.523 | 3.923 | 3.293 | 4.587 | 5.777 | 1.440 | 2.123 | 2.910 | 0.740 | 1.793 | 2.843 |
| R9 | 1.020 | 1.780 | 2.717 | 4.007 | 5.420 | 6.363 | 3.957 | 5.353 | 6.510 | 0.237 | 0.920 | 1.813 |
| R10 | 0.280 | 1.117 | 2.547 | 5.463 | 6.270 | 6.480 | 3.563 | 4.263 | 4.690 | 3.200 | 4.673 | 6.140 |
| R11 | 6.247 | 7.163 | 7.347 | 5.167 | 6.327 | 6.853 | 0.000 | 0.237 | 1.130 | 3.610 | 4.607 | 5.293 |
| R12 | 2.230 | 3.380 | 4.743 | 4.430 | 5.480 | 6.250 | 0.387 | 1.153 | 2.237 | 3.700 | 5.187 | 6.663 |
| R13 | 2.680 | 3.920 | 5.157 | 1.053 | 1.710 | 2.607 | 0.107 | 0.597 | 1.470 | 3.950 | 4.807 | 5.383 |
| R14 | 0.000 | 0.280 | 1.353 | 1.713 | 2.497 | 3.183 | 0.547 | 1.300 | 2.430 | 3.773 | 4.477 | 4.793 |
| R15 | 0.107 | 0.317 | 0.870 | 5.347 | 7.007 | 8.073 | 1.657 | 2.233 | 2.810 | 1.160 | 1.790 | 2.427 |
| R16 | 1.710 | 2.903 | 4.407 | 4.350 | 5.053 | 5.237 | 1.607 | 2.587 | 3.563 | 1.180 | 2.450 | 3.660 |
| AV | 2.417 | 3.346 | 4.327 | 3.809 | 4.926 | 5.685 | 2.008 | 2.811 | 3.619 | 2.914 | 4.022 | 4.954 |

سپس بسته به نوع معیار، فاصله‌های مثبت (PDA) و فاصله‌های منفی (NDA) از میانگین محاسبه می‌شوند. مقادیر فاصله مثبت (PDA) با استفاده از رابطه (۱۶) جدول ۱۳ و مقادیر فاصله منفی (NDA) از میانگین با استفاده از رابطه (۱۷) به‌دست می‌آید (جدول ۱۴).

**جدول ۱۳. مقادیر PDA**

| | S | | | O | | | D | | | C | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | l | m | u | l | m | u | l | m | u | l | m | u |
| R1 | -0.433 | 0.118 | 0.623 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 |
| R2 | -0.506 | 0.148 | 0.755 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | -0.457 | 0.161 | 0.806 |
| R3 | 0.000 | 0.000 | 0.000 | -0.285 | 0.051 | 0.366 | -0.081 | 0.551 | 1.149 | 0.076 | 0.571 | 0.971 |
| R4 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | -0.457 | 0.161 | 0.806 |
| R5 | 0.676 | 1.323 | 1.787 | 0.125 | 0.580 | 0.936 | -0.398 | 0.355 | 0.998 | 0.009 | 0.508 | 0.912 |
| R6 | 0.309 | 0.818 | 1.125 | -0.232 | 0.254 | 0.699 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 |
| R7 | -0.536 | 0.182 | 0.865 | -0.316 | 0.020 | 0.350 | 0.000 | 0.000 | 0.000 | -0.379 | 0.191 | 0.735 |
| R8 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | -0.321 | 0.244 | 0.775 | 0.000 | 0.000 | 0.000 |
| R9 | 0.000 | 0.000 | 0.000 | -0.349 | 0.103 | 0.531 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 |
| R10 | 0.000 | 0.000 | 0.000 | -0.046 | 0.280 | 0.556 | 0.000 | 0.000 | 0.000 | -0.443 | 0.164 | 0.814 |
| R11 | 0.571 | 1.135 | 1.466 | -0.108 | 0.291 | 0.633 | 0.312 | 0.915 | 1.287 | -0.339 | 0.148 | 0.600 |
| R12 | -0.623 | 0.010 | 0.692 | -0.261 | 0.115 | 0.508 | -0.081 | 0.589 | 1.149 | -0.317 | 0.294 | 0.946 |
| R13 | -0.490 | 0.171 | 0.815 | 0.000 | 0.000 | 0.000 | 0.191 | 0.787 | 1.249 | -0.253 | 0.198 | 0.623 |
| R14 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | -0.150 | 0.537 | 1.092 | -0.298 | 0.115 | 0.474 |
| R15 | 0.000 | 0.000 | 0.000 | -0.070 | 0.433 | 0.887 | -0.285 | 0.205 | 0.698 | 0.000 | 0.000 | 0.000 |
| R16 | 0.000 | 0.000 | 0.000 | -0.278 | 0.027 | 0.297 | -0.553 | 0.080 | 0.716 | 0.000 | 0.000 | 0.000 |

**جدول ۱٤. مقادیر NDA**

| | S | | | O | | | D | | | C | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | l | m | u | l | m | u | l | m | u | l | m | u |
| R1 | 0.000 | 0.000 | 0.000 | -0.104 | 0.320 | 0.720 | 0.109 | 0.685 | 1.111 | -0.440 | 0.091 | 0.621 |
| R2 | 0.000 | 0.000 | 0.000 | -0.129 | 0.378 | 0.812 | 0.175 | 0.725 | 1.123 | 0.000 | 0.000 | 0.000 |
| R3 | -0.590 | 0.018 | 0.590 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 |
| R4 | 0.023 | 0.571 | 1.038 | -0.219 | 0.211 | 0.604 | 0.685 | 1.247 | 1.608 | 0.000 | 0.000 | 0.000 |
| R5 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 |
| R6 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | -0.580 | 0.042 | 0.635 | -0.341 | 0.116 | 0.597 |

| | S | | | O | | | D | | | C | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R7 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | -0.545 | 0.144 | 0.769 | 0.000 | 0.000 | 0.000 |
| R8 | -0.448 | 0.245 | 0.921 | -0.409 | 0.071 | 0.498 | 0.000 | 0.000 | 0.000 | 0.018 | 0.562 | 1.063 |
| R9 | -0.089 | 0.466 | 0.983 | 0.000 | 0.000 | 0.000 | 0.120 | 0.904 | 1.601 | 0.278 | 0.783 | 1.190 |
| R10 | -0.039 | 0.663 | 1.203 | 0.000 | 0.000 | 0.000 | -0.020 | 0.517 | 0.954 | 0.000 | 0.000 | 0.000 |
| R11 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 |
| R12 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 |
| R13 | 0.000 | 0.000 | 0.000 | 0.250 | 0.669 | 0.964 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 |
| R14 | 0.316 | 0.912 | 1.287 | 0.130 | 0.505 | 0.826 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 |
| R15 | 0.460 | 0.901 | 1.255 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.123 | 0.563 | 0.957 |
| R16 | 0.91 | 0.99 | 1.09 | 0.59 | 0.69 | 0.80 | 0.14 | 0.37 | 0.71 | 0.62 | 0.67 | 0.72 |

در ادامه گام‌های روش Z-EDAS پیاده‌سازی می‌شود سپس امتیاز ارزیابی هر گزینه با استفاده از رابطه (۲۲) محاسبه و پس از فازی‌زدایی، در آخر رتبه‌بندی خطرها انجام می‌پذیرد (جدول ۱۵).

**جدول ۱۵. مجموع فواصل وزن‌دارشده، مقادیر نرمال‌شده آنها و امتیازات گزینه‌ها**

| Risk | $\widetilde{sp}_i$ | | | $\widetilde{sn}_i$ | | | $\widetilde{nsp}_i$ | | |
|---|---|---|---|---|---|---|---|---|---|
| | l | m | u | l | m | u | l | m | u |
| R1 | -0.177 | 0.048 | 0.254 | -0.146 | 0.243 | 0.597 | -0.203 | 0.055 | 0.292 |
| R2 | -0.350 | 0.111 | 0.561 | -0.003 | 0.238 | 0.430 | -0.401 | 0.127 | 0.643 |
| R3 | -0.069 | 0.296 | 0.617 | -0.241 | 0.007 | 0.241 | -0.079 | 0.339 | 0.708 |
| R4 | -0.143 | 0.050 | 0.252 | 0.077 | 0.522 | 0.887 | -0.164 | 0.058 | 0.289 |
| R5 | 0.239 | 0.923 | 1.455 | 0.000 | 0.000 | 0.000 | 0.274 | 1.058 | 1.669 |
| R6 | 0.063 | 0.403 | 0.649 | -0.215 | 0.044 | 0.305 | 0.072 | 0.462 | 0.744 |
| R7 | -0.423 | 0.140 | 0.679 | -0.101 | 0.027 | 0.143 | -0.485 | 0.160 | 0.778 |
| R8 | -0.060 | 0.046 | 0.144 | -0.288 | 0.295 | 0.844 | -0.069 | 0.052 | 0.165 |
| R9 | -0.095 | 0.028 | 0.144 | 0.073 | 0.604 | 1.072 | -0.109 | 0.032 | 0.166 |
| R10 | -0.151 | 0.127 | 0.406 | -0.019 | 0.367 | 0.669 | -0.173 | 0.146 | 0.466 |
| R11 | 0.156 | 0.759 | 1.198 | 0.000 | 0.000 | 0.000 | 0.178 | 0.870 | 1.374 |
| R12 | -0.440 | 0.237 | 0.931 | 0.000 | 0.000 | 0.000 | -0.504 | 0.272 | 1.067 |
| R13 | -0.244 | 0.278 | 0.760 | 0.068 | 0.182 | 0.262 | -0.279 | 0.319 | 0.872 |
| R14 | -0.121 | 0.136 | 0.352 | 0.164 | 0.509 | 0.750 | -0.139 | 0.156 | 0.404 |
| R15 | -0.072 | 0.156 | 0.371 | 0.226 | 0.544 | 0.812 | -0.083 | 0.179 | 0.425 |
| R16 | -0.178 | 0.022 | 0.214 | -0.300 | 0.178 | 0.616 | -0.205 | 0.025 | 0.245 |
| R1 | 1.250 | 0.583 | -0.024 | 0.524 | 0.319 | 0.134 | 0.325 | 10 | |
| R2 | 1.004 | 0.592 | 0.263 | 0.302 | 0.360 | 0.453 | 0.371 | 8 | |
| R3 | 1.413 | 0.988 | 0.587 | 0.667 | 0.663 | 0.648 | 0.659 | 4 | |
| R4 | 0.867 | 0.104 | -0.522 | 0.352 | 0.081 | -0.116 | 0.105 | 15 | |
| R5 | 1.000 | 1.000 | 1.000 | 0.637 | 1.029 | 1.334 | 1.000 | 1 | |
| R6 | 1.369 | 0.924 | 0.476 | 0.721 | 0.693 | 0.610 | 0.675 | 3 | |
| R7 | 1.174 | 0.954 | 0.754 | 0.344 | 0.557 | 0.766 | 0.556 | 6 | |
| R8 | 1.495 | 0.494 | -0.448 | 0.713 | 0.273 | -0.141 | 0.282 | 12 | |
| R9 | 0.875 | -0.035 | -0.840 | 0.383 | -0.002 | -0.337 | 0.015 | 16 | |
| R10 | 1.033 | 0.371 | -0.147 | 0.430 | 0.259 | 0.159 | 0.283 | 11 | |
| R11 | 1.000 | 1.000 | 1.000 | 0.589 | 0.935 | 1.187 | 0.904 | 2 | |
| R12 | 1.000 | 1.000 | 1.000 | 0.248 | 0.636 | 1.034 | 0.639 | 5 | |
| R13 | 0.883 | 0.688 | 0.551 | 0.302 | 0.504 | 0.711 | 0.506 | 7 | |
| R14 | 0.718 | 0.126 | -0.286 | 0.289 | 0.141 | 0.059 | 0.163 | 13 | |
| R15 | 0.612 | 0.067 | -0.393 | 0.265 | 0.123 | 0.016 | 0.134 | 14 | |
| R16 | 1.515 | 0.695 | -0.057 | 0.655 | 0.360 | 0.094 | 0.370 | 9 | |

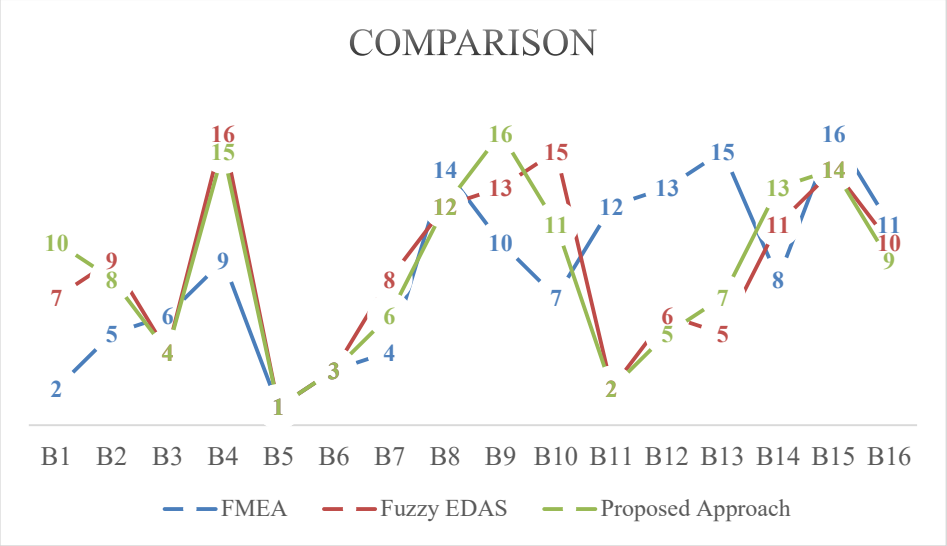
با توجه به جدول ۱۵ مشاهده می‌شود که براساس رویکرد پیشنهادی (FPIPRECIA-ZEDAS) خطرهای R5، R11 و R6 به ترتیب در اولویت‌های اول الی سوم قرار گرفته‌اند. به بیانی دیگر این خطرها به‌عنوان خطرهای بحرانی درنظر گرفته‌شده و نیازمند برنامه‌ریزی جهت اقدامات اصلاحی/پیشگیرانه می‌باشند. همچنین می‌توان نتیجه گرفت که خطر R9 در اولویت آخر قرار گرفته و در حال حاضر نیازی به اقدامات اصلاحی نمی‌باشد.

در ادامه جهت اعتبا سنجی و ارزیابی اثربخشی و قابلیت‌های رویکرد پیشنهادی، نتایج حاصل از این رویکرد با برخی روش‌های مرسوم ازجمله Fuzzy EDAS و FMEA سنتی مقایسه می‌شود. با توجه به جدول ۱۶ مشاهده می‌شود که براساس نتایج به‌دست‌آمده از هر سه روش، خطر R5 در اولویت اول رسیدگی قرار گرفته‌است. اما در اولویت دوم، اختلافاتی وجود دارد و براساس روش FMEA، خطر R1 در اولویت دوم قرار گرفته‌است. درحالیکه براساس نتایج رویکرد پیشنهادی و همچنین روش Fuzzy EDAS، خطر R11 در اولویت دوم قرار دارد. علاوه بر این، براساس نتایج روش FMEA، خطرهای R9 و R13 به‌طور به‌طور مشترک در جایگاه چهارم و R2 و R7 به‌طور مشترک در جایگاه ششم قرار گرفته‌اند. بنابراین رویکرد FMEA سنتی خطرها را در ۱۴ دسته به جای ۱۶ دسته رتبه‌بندی کرده‌است. این ضعف در رویکرد Fuzzy EDAS به جهت درنظرگرفتن شرایط عدم قطعیت و وزن‌دهی به فاکتورها برطرف شده‌است. نتایج نشان می‌دهد نتایج حاصل از پیاده‌سازی رویکرد پیشنهادی، با روش Fuzzy EDAS به‌عنوان یک روش قابل‌اطمینان (پلات و بایهان، ۲۰۲۲) در شناسایی خطرهای بحرانی تقریبا مشابه عمل کرده و نتایج ضریب همبستگی ۹۳ درصد را نشان می‌دهد و فقط در چند مورد اولویت‌بندی خطرها متفاوت است که این تفاوت به علت درنظرگرفتن قابلیت‌اطمینان در کنار عدم قطعیت در مقادیر عوامل می‌باشد که این برتری رویکرد پیشنهادی نسبت به روش‌های موجود در ادبیات را نشان می‌دهد.

**جدول ۱۶. مقایسه اولویت‌بندی حاصل از رویکرد پیشنهادی و روش‌های مرسوم**

| | FMEA | | Fuzzy EDAS | | Proposed Approach | |
|---|---|---|---|---|---|---|
| | RPN | Rank | $K_i$ | Rank | $K_i$ | Rank |
| R1 | 1406.667 | 2 | 0.۵۱۶ | 7 | 0.325 | 10 |
| R2 | 1045.333 | 6 | 0.358 | 9 | 0.371 | 8 |
| R3 | 954.66۷ | 8 | 0.773 | 4 | 0.659 | 4 |
| R4 | 832 | 11 | ۰.۰۳۷ | 16 | 0.105 | 15 |
| R5 | 1456 | 1 | 1.000 | 1 | 1.000 | 1 |
| R6 | 1278.667 | 3 | 0.۸۱۸ | 3 | 0.675 | 3 |
| R7 | 1045.333 | 6 | 0.۴۹۸ | 8 | 0.556 | 6 |
| R8 | 616 | 15 | 0.۲۲۵ | 12 | 0.282 | 12 |
| R9 | 1176 | 4 | 0.152 | 13 | 0.015 | 16 |
| R10 | 880 | 9 | 0.116 | 15 | 0.283 | 11 |
| R11 | 666.66۷ | 13 | 0.۹۸۹ | 2 | 0.904 | 2 |
| R12 | 656 | 14 | 0.542 | 6 | 0.639 | 5 |
| R13 | 1176 | 4 | 0.۶۲۶ | 5 | 0.506 | 7 |
| R14 | 848 | 10 | 0.261 | 11 | 0.163 | 13 |
| R15 | 385.333 | 16 | 0.۱۴۶ | 14 | 0.134 | 14 |
| R16 | 672 | 12 | 0.325 | 10 | 0.370 | 9 |

شکل ۲ نتایج روش‌های مرسوم Fuzzy EDAS و امتیاز RPN سنتی در ارائه رتبه‌بندی کامل در مقایسه با رویکرد پیشنهادی این پژوهش را نشان می‌دهد.




**شکل ۲. مقایسه اولویت‌بندی خطرها براساس رویکرد های FPIPRECIA-ZEDAS، Fuzzy EDAS و امتیاز RPN**

سه خطر با اولویت‌های اول تا سوم براساس روش Z-EDAS، با استفاده از روش Bow Tie، مورد تجزیه‌وتحلیل قرار می‌گیرند. خطر "انتقال داده‌ها از/به دستگاه‌های غیرمجاز" در اولویت اول قرار گرفته‌است. نتایج تحلیل روش Bow Tie، در "انتقال داده‌ها از/به دستگاه‌های غیرمجاز" شکل ۳، شش دلیل بروز خطر را نشان داد. با این حال مدیران سازمان می‌توانند هفده اقدام پیشگیرانه را انجام دهند. سپس پنج پیامد درصورت بروز خطر و چهارده اقدام کاهش‌دهنده پیامدها وجود دارد. نتایج روش Bow Tie از روش طوفان فکری و مصاحبه با خبرگان به‌دست می‌آید. در ادامه برخی از دلایل بروز این خطر آورده شده‌است:

خطای انسانی: خطر انتقال داده از و به دستگاه‌های غیرمجاز می‌تواند ناشی از خطای انسانی باشد. کارمندان ممکن است به‌طور تصادفی داده‌ها را به یک دستگاه غیرمجاز انتقال دهند یا ناآگاهانه به یک شبکه ناامن متصل شوند. اقدامات پیشگیرانه برای این علت می‌تواند شامل آموزش کارکنان، کمپین‌های آگاهی و اجرای سیاست‌ها و رویه‌های امنیتی باشد که خطرات مربوط به انتقال داده‌ها به دستگاه‌های غیرمجاز را برطرف می‌کند. سازمان‌ها همچنین می‌توانند کنترل‌های دسترسی و رمزگذاری را برای جلوگیری از انتقال تصادفی داده‌ها پیاده‌سازی کنند.

بدافزار: بدافزارهایی مانند ویروس‌ها، تروجان‌ها و غیره می‌توانند دستگاه‌ها را آلوده کرده و اجازه دسترسی غیرمجاز به داده‌ها را صادر کند. بدافزار می‌تواند از طریق پیوست‌های ایمیل، وب‌سایت‌های آلوده و شبکه‌های ناامن منتشر شود. کنترل‌های پیشگیرانه برای این علت می‌تواند شامل پیاده‌سازی راه‌حل‌های ضدبدافزار، به‌روزرسانی نرم‌افزار و سیستم عامل‌ها و اجرای سیاست‌های امنیتی باشد که مانع از دانلود یا نصب نرم‌افزار بر روی دستگاه‌های خود بدون مجوز می‌شود. سازمان‌ها همچنین می‌توانند از فایروال‌ها و سیستم‌های جلوگیری از نفوذ برای شناسایی و مسدودکردن بدافزارها استفاده کنند.

استفاده از دستگاه شخصی: استفاده از دستگاه‌های شخصی مانند تلفن‌های هوشمند، لپ‌تاپ و تبلت در محل کار می‌تواند خطر انتقال غیرمجاز داده‌ها را افزایش دهد. کارمندان ممکن است دستگاه‌های شخصی خود را به شبکه شرکت متصل کنند که می‌تواند منجر به نقض داده‌ها شود. اقدامات پیشگیرانه برای این دلیل می‌تواند شامل اجرای یک خط‌مشی جهت استفاده قابل‌قبول از دستگاه‌های شخصی را تعریف می‌کند مانند الزام کارکنان به نصب نرم‌افزار ضد بدافزار و رمزگذاری داده‌های حساس. همچنین سازمان‌ها می‌توانند دستگاه‌های شخصی که به شبکه متصل می‌شوند را نظارت و کنترل کنند.

اقدامات امنیتی ضعیف: اقدامات امنیتی ضعیف مانند رمزهای عبور ضعیف، شبکه‌های ناامن و عدم رمزگذاری می‌تواند خطر انتقال غیرمجاز داده را افزایش دهد. زمانیکه اقدامات امنیتی ضعیف باشد، هکرها به‌راحتی می‌توانند به داده‌ها دسترسی پیدا کنند. کنترل‌های پیشگیرانه برای این علت می‌تواند شامل اجرای سیاست‌های رمز عبور قوی، استفاده از رمزگذاری برای محافظت از داده‌های حساس، اجرای کنترل‌های دسترسی برای محدودکردن دسترسی به داده‌ها و استفاده از سیستم‌های تشخیص/جلوگیری از نفوذ برای محافظت از شبکه باشد.

تهدیدات داخلی: کارمندان با نیت مخرب می‌توانند عمدا داده‌ها را به دستگاه‌های غیرمجاز منتقل کنند. این می‌تواند برای منافع شخصی یا آسیب‌رساندن به سازمان باشد. اقدامات پیشگیرانه برای این علت می‌تواند شامل اجرای بررسی پیشینه برای کارمندان جدید، نظارت بر فعالیت کارکنان و اجرای کنترل‌های دسترسی با محدودکردن دسترسی به داده‌های حساس باشد. سازمان‌ها همچنین می‌توانند سیاست‌هایی را اجرا کنند که کارکنان را ملزم به گزارش هرگونه فعالیت مشکوک کند.

مهندسی اجتماعی: مجرمان سایبری می‌توانند از تاکتیک‌های مهندسی اجتماعی برای فریب کارمندان برای انتقال داده‌ها به دستگاه‌های غیرمجاز استفاده کنند. آنها ممکن است به‌عنوان یک موجودیت قانونی ظاهر شوند یا از ایمیل‌های فیشینگ برای دسترسی به داده‌های حساس استفاده کنند. اقدامات پیشگیرانه برای این علت می‌تواند شامل آموزش کارکنان باشد که به آنها درمورد خطرات حملات مهندسی اجتماعی و نحوه شناسایی و پیشگیری از آنها آموزش می‌دهد. سازمان‌ها می‌توانند سیاست‌هایی را اجرا کنند که کارمندان را ملزم کند هویت شخصی که درخواست دسترسی به داده‌ها را قبل از انتقال آنها می‌خواهد، تأیید کنند.

پیامدهای "انتقال داده‌ها از/به دستگاه‌های غیرمجاز" شامل موارد زیر می‌باشد:

از دست دادن داده‌ها: انتقال داده‌ها به دستگاه‌های غیرمجاز می‌تواند منجر به از دست رفتن داده‌ها شود که می‌تواند منجر به خسارات مالی، از دست دادن مالکیت معنوی و آسیب به اعتبار شود. اقدامات کاهش‌دهنده می‌تواند شامل پشتیبان‌گیری از داده‌ها، برنامه‌های بازیابی و رمزگذاری داده‌ها باشد.

دسترسی غیرمجاز: انتقال غیرمجاز داده می‌تواند منجر به دسترسی غیرمجاز به داده‌های حساس شود که می‌تواند منجر به نقض داده‌ها و سایر حملات سایبری شود. کنترل‌های کاهش‌دهنده می‌تواند شامل کنترل‌های دسترسی، تقسیم‌بندی شبکه و رمزگذاری داده‌ها باشد.

آسیب اعتبار: نقض داده‌ها می‌تواند به اعتبار سازمان آسیب برساند و اعتماد مشتری را از بین ببرد. کنترل‌های کاهش‌دهنده می‌تواند شامل افشای به موقع نقض داده‌ها و شفافیت با مشتریان باشد.

زیان‌های مالی: انتقال داده‌ها به دستگاه‌های غیرمجاز می‌تواند منجر به خسارات مالی ناشی از سرقت یا از دست دادن داده‌های حساس شود. کنترل‌های کاهش‌دهنده می‌تواند شامل پشتیبان‌گیری از داده‌ها، سیاست‌های بیمه و اجرای کنترل‌های امنیتی باشد که از سرقت داده‌ها جلوگیری می‌کند.


**شکل ۳. تجزیه‌وتحلیل Bow Tie برای "انتقال داده‌ها از/به دستگاه‌های غیر مجاز"**

خطر "حملات مهندسی اجتماعی" در اولویت اول قرار گرفته‌است. نتایج تحلیل روش Bow Tie در "حملات مهندسی اجتماعی" (شکل )۴، پنج دلیل بروز خطر را نشان داد. با این حال مدیران سازمان می‌توانند هفت اقدام پیشگیرانه را انجام دهند. سپس پنج پیامد درصورت بروز خطر و یازده اقدام کاهش‌دهنده پیامدها وجود دارد. در ادامه برخی از دلایل بروز این خطر آورده شده‌است:

خطای انسانی: مجرمان سایبری می‌توانند از خطای انسانی برای فریب افراد برای افشای اطلاعات حساس یا انجام اقداماتی که امنیت را به خطر می‌اندازد، استفاده کنند. به‌عنوان مثال: کارمندان ممکن است روی یک پیوند کلیک کنند یا یک پیوست را از منبعی ناشناس دانلود کنند یا رمز عبور یا اطلاعات حساب را ارائه دهند. سازمان‌ها می‌توانند خطر حملات مهندسی اجتماعی ناشی از خطای انسانی را با ارائه آموزش‌های منظم آگاهی امنیتی برای کارکنان کاهش دهند. آموزش باید موضوعاتی مانند نحوه تشخیص تاکتیک‌های مهندسی اجتماعی، نحوه ایجاد رمزهای عبور قوی، نحوه مدیریت امن اطلاعات حساس و نحوه گزارش حوادث امنیتی را پوشش دهد.

عدم آگاهی امنیتی: اگر افراد از خطرات مرتبط با حملات مهندسی اجتماعی آگاه نباشند، ممکن است تشخیص ندهند که چه زمانی مورد هدف قرار می‌گیرند. آنها ممکن است ندانند به دنبال چه چیزی باشند یا چه اقدامات احتیاطی را برای محافظت از خود و سازمانشان انجام دهند. آموزش منظم آگاهی امنیتی می‌تواند به افزایش آگاهی امنیتی در بین کارکنان و کاهش خطر حملات مهندسی اجتماعی کمک کند. همچنین سازمان‌ها می‌توانند از حملات مهندسی اجتماعی شبیه‌سازی‌شده برای آزمایش آگاهی کارکنان و شناسایی زمینه‌های بهبود استفاده کنند.

اشتراک‌گذاری بیش از حد اطلاعات در شبکه‌های اجتماعی: مجرمان سایبری می‌توانند اطلاعات افراد را از طریق شبکه‌های اجتماعی جمع‌آوری کنند و از آن اطلاعات برای ایجاد ایمیل یا پیام‌های فیشینگ قانع‌کننده، استفاده کنند.

سازمان‌ها می‌توانند کارکنان را درمورد خطرات مرتبط با اشتراک‌گذاری بیش از حد اطلاعات شخصی در شبکه‌های اجتماعی آموزش دهند و آنها را تشویق کنند که میزان اطلاعات شخصی را که به‌صورت آنلاین به اشتراک می‌گذارند، محدود کنند. آنها همچنین می‌توانند سیاست‌های شبکه‌های اجتماعی را با هدف ممنوعیت اشتراک‌گذاری اطلاعات حساس در شبکه‌های اجتماعی، اجرا کنند.

رمزهای عبور ضعیف: رمزهای عبور ضعیف اهداف آسانی برای مجرمان سایبری هستند. آنها می‌توانند از تاکتیک‌های مهندسی اجتماعی برای فریب افراد برای افشای رمزهای عبور استفاده کنند یا می‌توانند از ابزارهای خودکار برای شکستن رمزهای عبور ضعیف استفاده کنند. سازمان‌ها می‌توانند از کارمندان بخواهند از رمزهای عبور قوی استفاده کنند که شامل ترکیبی از حروف بزرگ و کوچک، اعداد و کاراکترهای خاص است. آنها همچنین می‌توانند احراز هویت دو مرحله ای را برای ارائه یک لایه امنیتی اضافی پیاده‌سازی کنند.

نرم‌افزار قدیمی: نرم‌افزارهای قدیمی می‌توانند دارای آسیب‌پذیری هایی باشند که می‌توانند توسط مجرمان سایبری برای دسترسی به سیستم‌ها و داده‌ها مورد سوء استفاده قرار گیرند. آنها می‌توانند از تاکتیک های مهندسی اجتماعی برای متقاعد کردن افراد برای دانلود نرم‌افزارهای مخرب یا باز کردن پیوست هایی که از این آسیب‌پذیری ها سوء استفاده می‌کنند استفاده کنند. سازمان‌ها می‌توانند با اجرای یک برنامه مدیریت به‌روزرسانی نرم‌افزارها، خطر حملات مهندسی اجتماعی را که از آسیب‌پذیری‌های نرم‌افزارهای قدیمی سوء استفاده می‌کنند، کاهش دهند. این برنامه باید شامل به‌روزرسانی‌های منظم نرم‌افزارها برای رفع آسیب‌پذیری‌های شناخته‌شده باشد.

پیامدهای "حملات مهندسی اجتماعی" شامل موارد زیر می‌باشد:

نقض داده‌ها: حملات مهندسی اجتماعی می‌تواند منجر به نقض داده‌ها شود که در آن اطلاعات حساس مورد دسترسی، سرقت یا به خطر افتادن قرار می‌گیرد. سازمان‌ها می‌توانند این خطر را با اجرای کنترل‌های دسترسی قوی، رمزگذاری و ابزارهای نظارتی برای شناسایی و واکنش سریع به نقض داده‌ها کاهش دهند.

زیان مالی: حملات مهندسی اجتماعی می‌تواند منجر به زیان مالی برای افراد و سازمان‌ها شود. برای مثال: کلاهبرداران ممکن است از تاکتیک‌های مهندسی اجتماعی برای فریب‌دادن افراد برای ارائه اطلاعات بانکی خود یا انتقال وجوه به حساب‌های جعلی استفاده کنند. سازمان‌ها می‌توانند با اجرای کنترل‌های احراز هویت قوی و نظارت بر تراکنش‌های مالی برای فعالیت‌های مشکوک، این خطر را کاهش دهند.

آسیب به اعتبار: حملات مهندسی اجتماعی می‌تواند به اعتبار یک سازمان آسیب برساند. اگر اطلاعات حساس افشا شود یا اگر کارکنان فریب داده شوند، اظهارات عمومی به وجهه سازمان آسیب می‌زند. سازمان‌ها می‌توانند با اجرای سیاست‌های سختگیرانه برای ارتباطات عمومی و آموزش کارکنان درمورد نحوه برقراری ارتباط موثر و ایمن، این خطر را کاهش دهند.

پیامدهای قانونی: حملات مهندسی اجتماعی درصورت دسترسی به اطلاعات حساس یا نقض مقررات می‌توانند منجر به عواقب قانونی شود. سازمان‌ها می‌توانند با استفاده از ابزارهای نظارتی برای اطمینان از رعایت مقررات، این خطر را کاهش دهند.

اختلالات عملیاتی: حملات مهندسی اجتماعی می‌تواند عملیات سازمان را مختل کند. اگر سیستم‌ها به خطر بیافتند یا اگر کارکنان فریب داده شوند، اطلاعات حساسی را که برای عملیات تجاری موردنیاز است، ارائه می‌دهند. سازمان‌ها می‌توانند این خطر را با اجرای کنترل‌های دسترسی قوی، سیستم‌های نظارت بر فعالیت‌های مشکوک و ارائه آموزش‌های آگاهی امنیتی منظم برای کارکنان کاهش دهند.


**شکل ٤. تجزیه‌وتحلیل Bow Tie برای "حملات مهندسی اجتماعی"**

خطر "آلودگی به بدافزارها و ویروس‌ها (به‌صورت تصادفی یا عمدی)" در اولویت سوم قرار گرفته‌است. نتایج تحلیل روش Bow Tie، در "آلودگی به بدافزارها و ویروس‌ها (به‌صورت تصادفی یا عمدی)" (شکل ۵)، پنج دلیل بروز خطر را نشان داد. با این حال، مدیران سازمان می‌توانند هفت اقدام پیشگیرانه را انجام دهند. سپس پنج پیامد درصورت بروز خطر و دوازده اقدام کاهش‌دهنده پیامدها وجود دارد. در ادامه برخی از دلایل بروز این خطر آورده شده‌است:

حملات فیشینگ: یکی از رایج‌ترین راه‌های انتشار بدافزارها و ویروس‌ها از طریق حملات فیشینگ است. برای جلوگیری از این حملات، سازمان‌ها می‌توانند از فیلترهای ایمیل برای شناسایی و مسدودکردن ایمیل‌های مشکوک استفاده کنند. آنها همچنین می‌توانند برنامه‌های آموزشی کارکنان را برای کمک به کارکنان در شناسایی ایمیل‌های فیشینگ و جلوگیری از قربانی‌شدن این حملات انجام دهند.

نرم‌افزار قدیمی: نرم‌افزار قدیمی می‌تواند دارای آسیب‌پذیری‌هایی باشد که مهاجمان می‌توانند از آنها برای انتشار بدافزارها و ویروس‌ها سوء استفاده کنند. برای جلوگیری از این امر، سازمان‌ها می‌توانند با یک برنامه مدیریت به‌روزرسانی نرم‌افزارها، خطر حملات مهندسی فیشینگ را کاهش دهند.

وب‌سایت‌های مخرب: بازدید از وب‌سایت‌های مخرب می‌تواند منجر به آلوده‌شدن بدافزارها و ویروس‌ها شود. برای جلوگیری از این امر، سازمان‌ها می‌توانند فیلترهای وب را پیاده‌سازی کنند که دسترسی به وب‌سایت‌های مخرب شناخته‌شده را مسدود می‌کند.

شبکه‌های ناامن: شبکه‌های ناامن می‌توانند توسط مهاجمان برای راه‌اندازی حملات و انتشار بدافزارها و ویروس‌ها استفاده شوند. برای جلوگیری از این امر، سازمان‌ها می‌توانند کنترل‌های امنیتی شبکه مانند فایروال‌ها و سیستم‌های جلوگیری از نفوذ را اجرا کنند.

دانلودهای ناامن: دانلود نرم‌افزار یا فایل‌ها از منابع نامعتبر می‌تواند منجر به آلودگی بدافزارها و ویروس‌ها شود. برای جلوگیری از این امر، سازمان‌ها می‌توانند دسترسی کارمندان را به منابع نامعتبر محدود کنند و از نرم‌افزارهای حفاظت استفاده کنند که همه فایل‌های دانلودشده را برای شناسایی بدافزار اسکن می‌کند.

رمزهای عبور ضعیف: رمزهای عبور ضعیف می‌توانند به‌راحتی توسط مهاجمان شکسته شوند و دسترسی آنها به سیستم‌ها و داده‌ها را فراهم می‌کند. برای جلوگیری از این امر، سازمان‌ها می‌توانند سیاست‌های رمز عبور قوی را اجرا کنند که کارکنان را ملزم به استفاده از رمزهای عبور پیچیده و اجرای احراز هویت چند عاملی می‌کند.

پیامدهای "آلودگی به بدافزارها و ویروس‌ها (به‌صورت تصادفی یا عمدی)" شامل موارد زیر می‌باشد:

سرقت یا از دست دادن داده‌ها: بدافزار می‌توانند برای سرقت داده‌های حساس یا از بین بردن آنها استفاده شوند. برای کاهش این موضوع، سازمان‌ها می‌توانند رویه‌های پشتیبان‌گیری و بازیابی داده‌ها را پیاده‌سازی کنند. دسترسی کارکنان به داده‌های حساس را محدود کنند و از رمزگذاری برای محافظت از داده‌های حساس استفاده کنند.

از کار افتادن سیستم: بدافزارها و ویروس‌ها می‌توانند سیستم‌ها را مختل کرده و باعث خرابی شوند. برای کاهش این امر، سازمان‌ها می‌توانند از سیستم‌های پشتیبان استفاده کنند.

زیان‌های مالی: بدافزارها و ویروس‌ها می‌توانند برای سرقت وجوه یا انجام تراکنش‌های غیرمجاز استفاده شوند. برای کاهش این امر، سازمان‌ها می‌توانند کنترل‌های مالی مانند احراز هویت چندمرحله‌ای برای تراکنش‌های مالی و حسابرسی منظم تراکنش‌های مالی را اجرا کنند.

آسیب اعتبار: حمله بدافزار می‌تواند به اعتبار سازمان آسیب برساند و منجر به از دست دادن اعتماد و درآمد مشتری شود. برای کاهش این امر، سازمان‌ها می‌توانند درمورد حوادث امنیتی شفاف باشند، به‌طور منظم با مشتریان و ذینفعان ارتباط برقرار کنند و در ایجاد یک فرهنگ امنیتی قوی سرمایه‌گذاری کنند.

نقض انطباق: حملات بدافزار می‌تواند منجر به نقض انطباق، مانند نقض قوانین حفاظت از داده‌ها شود. برای کاهش این امر، سازمان‌ها می‌توانند ابزارهای نظارت و گزارش انطباق را پیاده‌سازی کنند، ممیزی‌های انطباق منظم را انجام دهند و کارکنان را درمورد الزامات انطباق آموزش دهند.


**شکل ۵. تجزیه‌وتحلیل Bow Tie برای "آلودگی به بدافزارها و ویروس‌ها (به‌صورت تصادفی یا عمدی)"**

## ۸) نتیجه‌گیری و پیشنهادها

هر جا که داده‌های دیجیتال در دسترس باشد، حملات و مسائل سایبری، امنیت سایبری اکوسیستم دیجیتالی را تهدید می کند. بنابراین ارزیابی خطرهای امنیت سایبری، از اهمیت بالایی برخوردار است. FMEA یکی از مدل‌های شناسایی و رتبه‌بندی خطرهاست که به دلیل تحلیل‌پذیری مناسب، جزء پرکاربردترین روش‌ها است. با وجود گستردگی کاربرد این مدل، کاستی‌ها و نقاط ضعف این روش منجر شده‌است که برخی از محققان به دنبال بهبود این روش سنتی باشند. بنابراین در این پژوهش، یک رویکرد ترکیبی از روش توسعه‌یافته FMEA با استفاده از روش F-PIPRECIA جهت وزن‌دهی به معیارها و Z-EDAS و روش تحلیل خطر Bow Tie جهت اولویت‌بندی و تحلیل خطرهای امنیت سایبری در انقلاب صنعتی چهارم ارائه شده‌است. براساس نتایج به‌دست آمده، به ترتیب "انتقال داده‌ها از/به دستگاه‌های غیر مجاز"، "حملات مهندسی اجتماعی"و " آلودگی به بدافزارها و ویروس‌ها (به‌صورت تصادفی یا عمدی)" به‌عنوان خطرهای بحرانی انتخاب شده و در اولویت رسیدگی هستند. از طرفی، "پارازیت، تکرار گره و مسیریابی نادرست اطلاعات" به‌عنوان اولویت آخر انتخاب شده و در حال حاضر نیازمند اقدام اصلاحی نمی‌باشد. همچنین نتایج تحلیل خطر با استفاده از روش Bow Tie، منجر به استخراج ۳۷ فعالیت کاهش‌دهنده پیامدهای خطرهای امنیت سایبری شده‌است. استفاده از رویکرد توسعه‌یافته منجر به رفع برخی نواقص روش FMEA سنتی مانند عدم ارائه رتبه‌بندی کامل گزینه‌ها و عدم درنظرگرفتن اهمیت نسبی شاخص‌ها شده‌است. تعداد محدود خبرگان در این حوزه و همچنین عدم تخصیص وزن به هر یک از خبرگان براساس سطح دانش و میزان تجربه آنها، ازجمله محدودیت‌های این پژوهش می‌باشد. در آینده ما تحقیقات خود را در راستای رفع محدودیت‌های پژوهش حاضر و توسعه روش FMEA با استفاده از روش‌های تصمیم‌گیری چندمعیاره در محیط‌های عدم قطعیت نظیر فازی فیثاغورثی، q-rung و فازی کروی و همچنین ترکیب این روش با روش‌های دیگر ارزیابی خطر، گسترش خواهیم داد. فارغ از مسئله استفاده‌شده جهت پیاده‌سازی رویکرد پیشنهادی این پژوهش، این رویکرد در سناریوهای مختلف شناسایی و تحلیل خطر و حالات خرابی قابل اجرا خواهد بود.

## منابع


Aguirre, P. A. G., Pérez-Domínguez, L., Luviano-Cruz, D., Solano-Noriega, J., & Cordero-Díaz, M. C. (2023). AHP-FMEA-DA multi-criteria method for NPD project launch analysis. *International Journal of Innovation and Sustainable Development, 17*(1-2), 138-15 .۱- doi.org/10.1016/j.ejor.2369.05.967

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials, 17*(4), 2347-2376 . doi.org/10.1016/j.ejor.4157.05.638

Ambarwati, R., Yuliastri, D ,. & Sulistiyowati, W. (2022). Human resource risk control through COVID-19 risk assessment in Indonesian manufacturing. *Journal of Loss Prevention in the Process Industries, 74*, 104665 . doi.org/10.1016/j.ejor.6375.05.967

Ardanza, A., Moreno, A., Segura, Á., de la Cruz, M., & Aguinaga, D .(۲۰۱۹) .Sustainable and flexible industrial human machine interfaces to support adaptable applications in the Industry 4.0 paradigm. *International Journal of Production Research, 57*(12), 4045-4059 . doi.org/10.1016/j.ejor.1389.05.967

Bahrin, M. A. K., Othman, M. F., Azli, N. H. N., & Talib ,M. F. (2016). Industry 4.0: A review on industrial automation and robotic. *Jurnal teknologi, 78* .(۶-۱۳) doi.org/10.1016/j.ejor.3178.05.635

Balda, J. C., Mantooth, A., Blum, R., & Tenti, P. (2017). Cybersecurity and power electronics: Addressing the security vulnerabilities of the internet of things. *IEEE Power Electronics Magazine, 4*(4), 37-43 . doi.org/10.1016/j.ejor.6359.05.617

Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEOs' information security behavior in SMEs: Does ownership matter? *Systèmes d'information et management, 22*(3), 7-45 . doi.org/10.1016/j.ejor.2369.05.319

Bayazit, O., & Kaptan, M. (2 .(۰۲۳Evaluation of the risk of pollution caused by ship operations through bow-tie-based fuzzy Bayesian network. *Journal of cleaner production, 382*, 135386 . doi.org/10.1016/j.ejor.2169.05.007

Benias, N., & Markopoulos, A. P. (2017). *A review on the readiness level and cyber-security challenges in Industry 4.0.* Paper presented at the 2017 South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). doi.org/10.1016/j.ejor.2008.05.027

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management, 8*(1), 1-10 . doi.org/10.1016/j.ejor.2008.05.027

Bitton, R., Maman, N., Singh, I., Momiyama, S., Elovici, Y., & Shabtai, A. (2023). Evaluating the Cybersecurity Risk of Real-world, Machine Learning Production Systems. *ACM Computing Surveys, 55*(9), 1-36 . doi.org/10.1016/j.ejor.2008.05.027

Cheminod, M., Durante, L., Seno, L., Valenza, F., Valenzano, A., & Zunino, C. (2017). *Leveraging SDN to improve security in industrial networks.* Paper presented at the 20 ۱۷IEEE 13th International Workshop on Factory Communication Systems (WFCS). doi.org/10.1016/j.ejor.2008.05.027

Cisco. (2018). Cisco 2018 Annual Cybersecurity Report. In: Cisco Technology News Site San Jose, CA, USA. doi.org/10.1016/j.ejor.2008.05.027

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry, 114*, 103165 . doi.org/10.1016/j.ejor.2008.05.027

Corbò, G., Foglietta, C., Palazzo, C., & Panzieri, S. (2018). Smart behavioural filter for industrial internet of things: A security extension for plc. *Mobile Networks and Applications, 23*, 809-816 . doi.org/10.1016/j.ejor.2008.05.027

Dieber, B., Breiling, B., Taurer, S., Kacianka, S., Rass, S., & Schartner, P. (2017). Security for the robot operating system. *Robotics and Autonomous Systems, 98*, 192-203 . doi.org/10.1016/j.ejor.2008.05.027

Flatt, H., Schriegel, S., Jasperneite, J., Trsek, H., & Adamczyk, H. (2016). *Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements.* Paper presented at the 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA). doi.org/10.1016/j.ejor.2008.05.027

Ghadge, A., Er Kara, M., Moradlou, H., & Goswami, M. (2020). The impact of Industry 4.0 implementation on supply chains. *Journal of Manufacturing Technology Management, 31*(4), 669-686 . doi.org/10.1016/j.ejor.2008.05.027

Ghiaci, A. M., & Ghoushchi ,S. J. (2023). Assessment of barriers to IoT-enabled circular economy using an extended decision-making-based FMEA model under uncertain environment. *Internet of Things*, 100719 . doi.org/10.1016/j.ejor.2008.05.027

Ghoushchi, S. J., Jalalat, S. M., Bonab, S. R., Ghiaci, A. M., Haseli, G ,. & Tomaskova, H. (2022). Evaluation of wind turbine failure modes using the developed SWARA-CoCoSo methods based on the spherical fuzzy environment. *IEEE Access, 10*, 86750-86764 . doi.org/10.1016/j.ejor.2008.05.027

Ghoushchi, S. J., Yousefi, S., & Khazaeili, M. (2019). An extended FMEA approach based on the Z-MOORA and fuzzy BWM for prioritization of failures. *Applied Soft Computing, 81*, 105505 . doi.org/10.1016/j.ejor.2008.05.027

Gul, M., & Ak, M. F. (2021). A modified failure modes and effects analysis using interval-valued spherical fuzzy extension of TOPSIS method: case study in a marble manufacturing facility. *Soft Computing, 25*(8), 6157-6178 . doi.org/10.1016/j.ejor.2008.05.027

Habibor Rahman, M., Son, Y.-J., & Shafae, M. (2023). Graph-Theoretic Approach for Manufacturing Cybersecurity Risk Modeling and Assessment. *arXiv e-prints*, arXiv: 2301.07305 . doi.org/10.1016/j.ejor.2008.05.027

Hassanzadeh, A., Modi, S., & Mulchandani, S. (2015). *Towards effective security control assignment in the Industrial Internet of Things.* Paper presented at the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). doi.org/10.1016/j.ejor.2008.05.027

Jafarzadeh Ghoushchi, S., Memarpour Ghiaci, A., Rahnamay Bonab, S., & Ranjbarzadeh, R. (2022). Barriers to circular economy implementation in designing of sustainable medical waste management systems using a new extended decision-making and FMEA models. *Environmental Science and Pollution Research*, 1-19 . doi.org/10.1016/j.ejor.137.05.975

Jafarzadeh Ghoushchi, S., Shaffiee Haghshenas, S., Memarpour Ghiaci, A., Guido, G., & Vitale, A. (2022). Road safety assessment and risks prioritization using an integrated SWARA and MARCOS approach under spherical fuzzy environment. *Neural Computing and Applications*, 1-19 . doi.org/10.1016/j.ejor.2369.05.627

James, A. T., Kumar, G., Tayal, P., Chauhan, A., Wadhawa, C., & Panchal, J. (2022). Analysis of human resource management challenges in implementation of industry 4.0 in Indian automobile industry. *Technological Forecasting and Social Change, 176*, 121483 . vdoi.org/10.1016/j.ejor.2084.05.317

Januário, F., Carvalho, C., Cardoso, A., & Gil, P. (2016). *Security challenges in SCADA systems over Wireless Sensor and Actuator Networks.* Paper presented at the 2016 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). doi.org/10.1016/j.ejor.2008.05.4196

Jin, G., Meng, Q., & Feng, W. (2022). Optimization of Logistics System with Fuzzy FMEA-AHP Methodology. *Processes, 10*(10), 1973 . doi.org/10.1016/j.ejor.2008.05.1962

Kazemi, M., Abbasi, A., Kazemi, M., Jamshidzadeh, N., & Rashidi, M. A .(۲۰۲۱) .Identification of Hazards and Risk Assessment among Various Units of Ilam Gas Refinery using the Integrated Approach of Bow-tie and FMEA Methods. *Journal of Ilam University of Medical Sciences, 29*(2), 1-12 . doi.org/10.1016/j.ejor.2008.05.927

Keshavarz Ghorabaee, M., Zavadskas, E. K ,.Olfat, L., & Turskis, Z. (2015). Multi-criteria inventory classification using a new method of evaluation based on distance from average solution (EDAS). *Informatica, 26*(3), 435-451 . doi.org/10.1016/j.ejor.2015.05.418

Khalid, A., Kirisci, P., Khan, Z. H., Ghrairi, Z., Thoben, K.-D ,. & Pannek, J. (2018). Security framework for industrial collaborative robotic cyber-physical systems. *Computers in Industry, 97*, 132-145 .

Kobara, K. (2016). Cyber physical security for industrial control systems and IoT. *IEICE TRANSACTIONS on Information and Systems, 99*(4), 787-795 . doi.org/10.1016/j.ejor.2016.05.418

Kumari, S., Ahmad, K., Khan, Z. A., & Ahmad, S. (2023). Failure mode and effects analysis of common effluent treatment plants of humid sub-tropical regions using fuzzy based MCDM methods. *Engineering Failure Analysis, 145*, 1070 .۱۰ doi.org/10.1016/j.ejor.2023.05.964

Lee, S., Lee, S., Yoo, H., Kwon, S., & Shon, T. (2018). Design and implementation of cybersecurity testbed for industrial IoT systems. *The Journal of Supercomputing, 74*, 4506-4520 . doi.org/10.1016/j.ejor.2018.05.630

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry, 103*, 97-110 . doi.org/10.1016/j.ejor.2018.05.361

Mulcahy, M. B., Boylan, C., Sigmann, S., & Stuart, R. (2017). Using bowtie methodology to support laboratory hazard identification, risk management, and incident analysis. *Journal of Chemical Health & Safety, 24*(3), 14-20 . doi.org/10.1016/j.ejor.2017.05.369

Nwakanma, C. I., Islam, F. B., Maharani, M. P., Lee, J.-M., & Kim, D.-S. (2021). Detection and classification of human activity for emergency response in smart factory shop floor. *Applied Sciences, 11*(8), 3662 . doi.org/10.1016/j.ejor.2021.05.084

Polat, G., & Bayhan, H. G. (2022). Selection of HVAC-AHU system supplier with environmental considerations using Fuzzy EDAS method. *International journal of construction management, 22*(10), 1863-1871 . doi.org/10.1016/j.ejor.2022.05.362

Preuveneers, D., Joosen, W., & Ilie-Zudor, E. (2017a). *Identity management for cyber-physical production workflows and individualized manufacturing in industry 4.0.* Paper presented at the Proceedings of the Symposium on Applied Computing. doi.org/10.1016/j.ejor.2008.05.382

Preuveneers, D., Joosen, W., & Ilie-Zudor, E. (20۱۷b). Trustworthy data-driven networked production for customer-centric plants. *Industrial Management & Data Systems* .

Ren, A., Wu, D., Zhang, W., Terpenny, J., & Liu, P. (2017). *Cyber security in smart manufacturing: Survey and challenges.* Paper presented at the IIE Annual Conference. Proceedings. doi.org/10.1016/j.ejor.2008.05.418

Renaud, K., & Weir, G. R. (2016). *Cybersecurity and the unbearability of uncertainty.* Paper presented at the 2016 Cybersecurity and Cyberforensics Conference (CCC). doi.org/10.1016/j.ejor.2008.05.047

Söner, Ö., Kayisoglu, G., Bolat, P., & Tam, K .(۲۰۲۳) .Cybersecurity risk assessment of VDR. *The Journal of Navigation*, 1-18 . vdoi.org/10.1016/j.ejor.2008.05.086

Stanujkic, D., Zavadskas, E. K., Karabasevic, D., Smarandache, F., & Turskis, Z. (2017). *The use of the pivot pairwise relative criteria importance assessment method for determining the weights of criteria*: Infinite Study. doi.org/10.1016/j.ejor.2008.05.087

Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis* . doi.org/10.1016/j.ejor.2008.05.415

Urquhart ,L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. *Computer law & security review, 34*(3), 450-466 . doi.org/10.1016/j.ejor.2008.05.369

van Lier, B. (2017). The industrial internet of things and cyber security: An ecological and systemic perspective on security in digital industrial ecosystems. Paper presented at the 2017 21st International Conference on System Theory, Control and Computing (ICSTCC). doi.org/10.1016/j.ejor.1998.05.301

Voicu, I., Panaitescu, F., Panaitescu, M., Dumitrescu, L., & Turof, M. (2018). *Risk management with Bowtie diagrams.* Paper presented at the IOP Conference Series: Materials Science and Engineering. doi.org/10.1016/j.ejor.2012.05.065

Xu, P., He, S., Wang, W., Susilo, W., & Jin, H. (2017). Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks. *IEEE Transactions on industrial informatics, 14*(8), 3712-3723. doi.org/10.1016/j.ejor.2009.05.036