کنگره بین المللی
علوم، مهندسی و تکنولوژی
آمستردام - هلند
۳۰ آبان ۱۳۹۷
SCIENCE, ENGINEERING AND TECHNOLOGY
AMSTERDAM
www.CONGSET.com

مدل تحلیل ریسک امنیت اطلاعات

با استفاده از نظریه‌ی تصمیم‌گیری فازی ETA و FMEA

Information Security Risk Analysis Model
Using FTA ETA and FMEA Fuzzy Decision Making Theory

نام و نام خانوادگی: مریم حاجی عربی

محل کار / شرکت مهندسی قدس نیرو

تحصیل/کارشناسی مهندسی فناوری اطلاعات (IT)

کارشناسی ارشد مهندسی فناوری اطلاعات (IT) - گرایش مهندسی شبکه‌های کامپیوتری

از دانشگاه صنعتی خواجه نصیرالدین طوسی

Email: m.hajiarabi@yahoo.com & mhajiarabi@ghods-niroo.com

چکیده

به دلیل تکامل و گسترش کاربرد اینترنت، آسیب‌پذیری سازمان‌ها در برابر حملات به سیستم‌های فناوری اطلاعات بیشتر می‌شود. این حملات منتج به از بین رفتن و جایگزینی داده‌ها می‌شود و بر خدمات و عملیات کسب‌وکار تاثیرگذار است. بنابراین، برای حداقل‌سازی این شکست‌های بالقوه، این مقاله یک مدل تحلیل ریسک برای ارزیابی و مدیریت امنیت اطلاعات ارائه می‌دهد که دنباله‌ای از رخدادها (که آلترناتیو [1] می‌نامیم) را شناسایی و ارزیابی می‌کند این رخدادها در یک سناریوی تصادفی احتمالی اتفاق می‌افتند که از وقوع یک رویداد آغازکننده‌ی متناظر با سوءاستفاده از سیستم‌های فناوری اطلاعات تبعیت می‌کند. مقاله‌ی پیش‌رو به منظور انجام این ارزیابی، از تحلیل درخت رخداد ترکیب شده با نظریه‌ی تصمیم‌گیری فازی استفاده می‌کند. سهم پژوهشی طرح پیشنهادی شامل این موارد است: ایجاد دسته‌بندی برای سناریوها و رخدادها، رتبه‌بندی آلترناتیوها براساس بحرانی بودن ریسک، لحاظ نمودن زیان مالی، و نهایتاً فراهم نمودن اطلاعاتی در خصوص علل حملات به سیستم‌های اطلاعاتی در بالاترین رده‌ی مدیریتی برای سازمان‌ها. ما مثال مفصلی در خصوص مرکز داده با هدف نشان دادن قابلیت کاربردی مدل پیشنهادی، ارائه دادیم. برای ارزیابی نظام‌مندی آن، دوازده آلترناتیو را با در نظر گرفتن دو روش مختلف تعیین احتمالات وقوع رخدادها، تحلیل نمودیم. نتایج نشان داد که کاوش در حملات سرویس‌های پایگاه داده‌ی خارجی، خطرناک‌ترین آلترناتیو است.این رویکرد شامل تحلیل تاثیرات و حالت شکست (FMEA۲) و نظریه فازی۳ است. این رویکرد به تحلیل پنج وجه امنیت اطلاعات می‌پردازد: دسترسی به اطلاعات و سیستم‌ها، امنیت ارتباطات، زیرساخت، مدیریت امنیت و توسعه سیستم‌های اطلاعاتی ایمن. برای نمایش مدل مفروض، این مدل برای پروژه گروه تحقیقاتی دانشگاه اعمال شده است. نتایج نشان می‌دهند مهمترین ابعاد ریسک امنیت اطلاعات امنیت ارتباطات و سپس زیرساخت هستند.

واژه‌های کلیدی : امنیت اطلاعات؛ تحلیل ریسک؛ نظریه‌ی تصمیم‌گیری فازی.

---

[1] Alternative
[2] Failure modes and effects analysis
[3] Fuzzy logic theory

۱- مقدمه

به گفته‌ی (کیوموتو، فوکوشیما، و میاک (۲۰۱۴)، سیستم‌های فناوری اطلاعات (IT) از شبکه‌ها و منابع محاسباتی تشکیل شده‌اند که از عملکردهای مهم در سازمان‌های پشتیبانی می‌کنند. افزون بر این، سیستم‌های IT نحوه‌ی انجام کسب‌وکارها را ارتقا بخشیده‌اند، و وابستگی سازمان‌ها به سیستم‌های کامپیوتری را بیشتر کرده‌اند (ماگلاراس و فورنل، ۲۰۰۲) با اینحال، با وجود مزایا و معایب سیستم‌های IT، مسائل بسیاری در خصوص وجود برخی نقص‌های امنیتی در زیرساخت‌های IT بیان شده‌اند، این نقص‌ها، سیستم‌ها را در مقابل سوءاستفاده، آسیب‌پذیر می‌کند. به گفته‌ی سوءاستفاده‌های امنیتی به نقص‌های فنی، آسیب‌پذیری سیستم، خطای انسانی، جعل، و رخدادهای خارجی مربوط می‌شوند. زیان مالی اغلب یکی از تبعات سوءاستفاده‌ی امنیتی است عنوان نمود که شرکت‌های بسیاری، دغدغه‌های امنیتی را به عنوان موانع پیش‌رو در استفاده از سرویس‌های رایانش ابری می‌شناسند، برندر و مارکوف اظهار داشتند بایستی این ریسک پیش از ورود به این مبحث به خوبی ارزیابی شوند. در نتیجه، صنعت IT گستره‌ای از ابزارهای امنیتی را فراهم آورده (برای مثال آنتی‌ویروس‌ها و دیواره‌ی آتش) که به کاربران و مدیران سیستم‌ها در پیشگیری، تشخیص، و مقابله با سوءاستفاده از IT کمک می‌کنند. امنیت اطلاعات نقش حیاتی در بقای سازمان‌ها دارد. در نتیجه، چندین راه‌حل امنیتی برای به حداقل رسانیدن ریسک‌هایی که عملکرد سازمان‌ها را به مخاطره می‌اندازند پیشنهاد شده‌اند، اینها محرمانه بودن، یکپارچگی و دسترس‌پذیری اطلاعات را نیز حفظ می‌کنند. این راه‌حل‌ها عمدتاً بر تحلیل تهدیدها و نقاط آسیب‌پذیر در سیستم‌های IT و تصمیم‌گیری در خصوص اقدامات متقابل جهت کاهش ریسک تا یک سطح قابل قبول تمرکز دارند (فنگ، وانگ و لی، ۲۰۱۴در هر صورت، این راه‌حل‌ها، اقداماتی آسان نیستند، چراکه محیط پویا و پیچیده‌ای دارند. ارزیابی مشابهی در فنگ و لی (۲۰۱۱) بیان شده که در آن، تحلیل ریسک امنیت سیستم اطلاعات (ISS)، کاری دشوار بوده و شامل یک سری عدم قطعیت است، که عامل اصلی اثرگذار بر اثربخشی ارزیابی ریسک ISS شناخته می‌شود. با اینحال، این نویسندگان چنین استدلال می‌کنند که چندین روش فعلی برای تحلیل ریسک ISS، کاستی‌هایی در مواجهه با عدم قطعیت دارند. برای غلبه بر این مشکل، مقاله‌ی پیش‌رو با در نظر گرفتن عدم قطعیت ذاتی این مباحث، روشی را ارائه می‌دهد که با گنجاندن دیدگاه رویکرد بیان‌شده. این نه تنها موارد آسیب‌پذیری احتمالی سیستم را شناسایی و رتبه‌بندی می‌کند، بلکه سطوح مختلف تهدید کاوش و حملات مرکز داده‌ی خارجی را نیز شناسایی و پایش می‌کند. در نتیجه، هدف از این مقاله، ارزیابی ریسک است، این گام نخست در روش مدیریت ریسک برای سیستم‌های فناوری اطلاعات است. ارزیابی ریسک به نوبه‌ی خود شامل ۹ گام اصلی است: شناسایی ویژگی‌های سیستم، شناسایی تهدیدات، شناسایی موارد آسیب‌پذیری، تحلیل کنترل، تعیین احتمال، تحلیل اسیب، تعیین ریسک، توصیه‌های کنترلی و مستندسازی نتایج. در این مقاله روش تحلیل درخت رخداد (ETA) از طریق شناسایی نقاط آسیب‌پذیر سازمان و به تبع آن رخدادهای محتمل و سناریوهای احتمالی، از گام شناسایی ویژگی‌های سیستم پشتیبانی می‌کند. گام تعیین ریسک در نظریه‌ی تصمیم و منطق فازی از طریق مشخص‌نمودن احتمال وقوع و قضاوت در خصوص این المان‌ها، پشتیبانی می‌شود. این مقاله، استفاده از روش‌های خاص در مراحل حیاتی ارزیابی ریسک در امنیت اطلاعات را پیشنهاد می‌کند. با توجه به مشخصه‌های ذهنی انواع ارزیابی‌های انجام‌گرفته، دقت بالای ریاضی که برای اطمینان از نظام‌مندی مدل نیاز است، و قضاوت‌های آنهایی که در این فرایند دخیلند، در این مدل لحاظ می‌شوند. به این ترتیب، رویکرد جدید مواجهه با امنیت اطلاعات در سیستم‌های IT به مدیران امکان درک بهتر مسائل با براورد سطح تهدید را می‌دهد، به احتمال زیاد اینها از سناریوی مشخصی در محیط دارای عدم قطعیت نشأت می‌گیرند. بخش نخست این مقاله به بررسی ریسک‌های امنیت اطلاعات در سیستم‌های IT می‌پردازد. سپس، بحث روش‌های موجود در امنیت اطلاعات و اطلاعات زمینه‌ای لازم برای بسط رویکرد پیشنهادی ارائه می‌شود. در ادامه، روش پیشنهادی بیان شده و یک مورد واقعی نحوه‌ی اعتبارسنجی روش پیشنهادی را به تفصیل بیان می‌کند. نهایتاً به محدودیت‌های پژوهشی می‌پردازیم و مطالعات آتی و اظهارات پایانی را بیان می‌کنیم.

۲- تحلیل ریسک امنیت اطلاعات:

مطابق نظر (اوزکان و کاراباکاک (۲۰۱۰) مرحله اولیه مدیریت ریسک تحلیل ریسک است، این مرحله به صورت کاربرد نظام‌مند اطلاعات برای شناسایی منابع و برآورد ریسک تعریف شده است. بنابراین، اگر به خوبی اجرا نشده باشد، انتخاب ضدمعیارها شکست خواهد خورد، و فرایند مدیریت ریسک نمی‌تواند موفق باشد. چند روش تحقیق برای ارزیابی ریسک امنیت اطلاعات وجود دارد. در کل، این روش‌ها براساس دو نوع روش تحلیل ریسک هستند. نوع اول براساس روش‌های تحلیل ریسک کیفی است، که به راحتی موضوع‌های غیرفنی در آن دیده نمی‌شود و مدیران محاسبه‌های ارزیابی-ریسک را ساده تلقی می‌کنند؛ تعیین کمیت تکرار تهدید غیرضروری است نوع دوم، براساس روش‌های تحلیل ریسک کمّی، ابزارهای ریاضیاتی برای ارزیابی ریسک و، در این مورد، روش‌های ریاضیاتی، از جمله منطق فازی، درخت اشتباه و روش‌های چند مقوله‌ای دارد. (بوژانک و ژرمن-بلازیک (۲۰۰۸) چند رویکرد را تحلیل کردند، این رویکردها ارزیابی سرمایه‌گذاری ضروری در فناوری امنیت را از نقطه نظر اقتصادی ممکن ساختند. آنها روش‌هایی برای شناسایی دارایی‌ها، تهدیدها و آسیب‌پذیری‌های سیستم‌های ICT معرفی کردند. آنها روشی برای انتخاب سرمایه‌گذاری مطلوب در فناوری امنیت ضروری، براساس تعیین کمیت ارزش‌های سیستم‌های محافظت شده پیشنهاد کردند. اثر پاتل و همکاران (۲۰۰۸) روشی برای تعیین کمّیت ریسک در قالب ارزش عددی پیشنهاد می‌کنند، این روش شاخص تهدید-تاثیر و شاخص مجازی-آسیب‌پذیری، براساس درختان آسیب‌پذیر، ارائه می‌کند. با تعیین کمیت امنیت اطلاعات به صورت کمی‌و مقایسه شاخص‌ها برای چند ارتقاء امنیت محتمل، مدیران می‌توانند انتخاب‌های ارتقاء امنیت را مطابق با اثربخشی‌شان اولویت‌بندی کنند، بهترین گزینه را انتخاب کنند و به لحاظ آماری ارسال منابع در گزینه منتخب را توجیه کنند.

به گفته‌ی پائولا و ویگنون-داویلیرب (۲۰۰۴)، اکثر روش‌های سنتی مدیریت ریسک امنیت اطلاعات از شناسایی و ارزیابی ریسک‌ها شامل شناسایی دارایی‌های اطلاعاتی هستند، بعد آن هم شناسایی و ارزیابی ریسک‌های مرتبط با آن دارایی‌ها اهمیت می‌یابند. روشی را بیان نمودند که از تحلیل اثرات و حالات خطا (FMEA) و نظریه‌ی فازی تشکیل شده‌اند و پنج بعد از امنیت اطلاعات را تحلیل می‌کنند: دسترسی به اطلاعات و سیستم‌ها، ارتباطات، زیرساخت، مدیریت امنیت و توسعه‌ی سیستم‌های اطلاعات امنیت. ((ماگلاراس و فورنل، ۲۰۰۲) روشی را پیشنهاد نمودند که سطح تهدیدات نشأت‌گرفته از عامل داخلی مشخصی را با معرفی سیستم ارزیابی تهدید مبتنی بر مشخصه‌های خاصی از رفتار کاربر برآورد می‌کند. با توجه به بررسی امنیت و جرائم کامپیوتری مؤسسه‌ی امنیت کامپیوتر که عنوان نمود ۴۹٪ موارد مربوط به رخدادهای امنیت IT در اثر اقدامات خود کاربران قانونی سیستمها روی میدهند، یک رویکرد ابتکاری جدید برای مقابله با خودی‌هایی ارائه نمودند که از سیستم‌های IT سوءاستفاده می‌کنند. با اینحال، تمرکز آنها تنها بر شناسایی تهدیدات داخلی بود. عوامل خارجی و حتی سایر عوامل داخلی که از اقدامات انسانی تفکیک می‌شوند، لحاظ نشده‌اند. یک مدل ارزیابی ریسک امنیت سیستم‌های اطلاعاتی (ISS) مبتنی بر نظریه‌ی ارتقای شواهد را ارائه دادند. مزایای مدل پیشنهاد آنها به شرح زیر است: این مدل بر نظریه‌ی شواهد مبتنی است که می‌تواند بطور مؤثر عدم قطعیت دخیل در روند ارزیابی را مدل کند؛ این مدل راه جدیدی برای تعریف تخصیص باور پایه از طریق سنجش فازی فراهم می‌آورد و امکان رسیدگی به شواهد فازی یافت‌شده در ارزیابی ریسک ISS را مهیا می‌سازد؛ این مدل روشی برای آزمودن یکپارچگی شواهد فراهم می‌کند که می‌تواند عدم قطعیت حاصل از تعارض شواهد ارائه‌شده توسط متخصصان را کاهش دهد. دشواری مرتبط با استفاده از این مدل به قدرت استنباط متخصصان بستگی دارد. در مقابل، شامالا و همکاران (۲۰۱۳) یک چارچوب مفهومی‌در ساختار اطلاعات برای ارزیابی ریسک امنیت اطلاعات (ISRA) پیشنهاد نمودند که از سازمان‌ها در اتخاذ تصمیمات طرح‌ریزی امنیتی پشتیبانی نموده و مدیران را قادر می‌سازد طرح‌های دقیقی برای فرایند ISRA طراحی کنند. این چارچوب، دیدگاه اصلی جریان اطلاعات، انواع اطلاعات گردآوری‌شده، و الزاماتی که قرار است پیش از انجام هرگونه ارزیابی برآورده شوند را تبیین می‌کند. با این وجود، رویکرد پیشنهادی هیچگونه روش

جدید تحلیل ریسک مبتنی بر مقایسات انجام‌گرفته بین ۶ روش ISRA ارائه نمی‌دهد. با شناخت این نقطه ضعف، نویسندگان اطمینان می‌یابند که آنها پژوهش‌های بیشتری مبتنی بر روش‌های کمی‌و کیفی برای تکمیل هرچه بیشتر زیرساخت و جزئیات برای ارزیابی امنیت اطلاعات در انواع سازمان‌ها انجام می‌دهند. یک مدل تحلیل ریسک امنیتی (SRAM) مبتنی بر شبکه‌های بیزی و بهینه‌سازی کلونی مورچگان ارائه دادند. احتمالات وقوع و شدت پیامد ریسک‌های امنیتی را برآورد نموده و سپس مسیرهای انتشار آسیب‌پذیری را با استفاده از بهینه‌سازی کلونی مورچگان محاسبه می‌کند تا راهنمایی برای توسعه‌ی طرح-های اصلاح ریسک امنیتی فراهم آورد. با اینحال، همانگونه که نویسندگان عنوان نمودند، بایستی اصلاح عدم قطعیت توسط SRAM در کارهای آتی لحاظ شود: برای مثال افزودن مجموعه‌های فازی به مدل. این نگرانی بدان خاطر ایجاد می‌شود که تحلیل ریسک امنیتی بسیار پیچیده و مملو از عدم قطعیت است برای ارزیابی سناریوها، استفاده از روش ETA و رویکردی چندوجهی FEMA (جدول ۱) پیشنهاد شده و ارزیابی آلترناتیوها براساس نظریه‌ی تصمیم و منطق فازی انجام می‌گیرد.

جدول ۱. عناصر سیستم FMEA.

عنصر سیستم	شرح
حالت‌های شکست بالقوه و علت‌ها	شکست امنیت اطلاعات باید به وضوح تعریف شود. در اثر فعلی، از کارشناسان امنیت اطلاعات خواسته شد حالت‌های شکست هر سیستم را توضیح دهند
تاثیرات بالقوه شکست	نتیجه‌ی هر حالت شکست باید به دقت بررسی و ثبت شود
تشخیص شکست و جبران خسارت	تمام شکست تشخیص داده شده باید اصلاح شود تا علت از بین برود و پایایی به حداکثر برسد
تعیین شدت، وقوع و تشخیص	درجه‌بندی شدت کارفعلی توسعه یافته است.

۲-۱- بررسی روش تحقیق FMEA

تحلیل تاثیرات و حالت شکست (FMEA) روش‌تحقیق تحلیل مهندسی پیچیده استفاده شده برای شناسایی حالت‌های شکست بالقوه، علت‌های شکست، تاثیرات شکست و حوزه‌های مسئله تاثیرگذار بر موفقیت ماموریت محصول یا سیستم، سخت‌افزار و نرم‌افزار قابل اطمینان، نگهداشت‌پذیری و ایمنی است. این روش فرایندی دارای ساختار برای ارزیابی حالت‌های شکست و کاهش تاثیرات این حالت‌های شکست توسط اقدامات اصلاحی نیز فراهم می‌کند. علاوه بر این، روش FMEA با تحلیل گام به گام تمام سیستم‌ها شروع می‌شود؛ یعنی، با بررسی کارکردهای سیستم و سیستم‌های فرعی. جدول ۱ عناصر سیستم را نشان می‌دهد.

روش FMEA برای بسیاری از حوزه‌های مهندسی اعمال شده است. FMEA با مجموعه‌های فازی ترکیب شده‌اند و روش‌های تصمیم‌گیری چند صفت فازی (FMADM)۴ برای موضوع‌های مهندسی دورکران و دریایی از جمله آب جرم ترازمندی اعمال شده‌اند (Pam, Li, Wall, Yang, andWang, 2013) -(جئوم، چو و پارک رویکردی نظام‌مند برای شناسایی و ارزیابی شکست‌های بالقوه با استفاده از FMEA ویژه خدمات و تحلیل رابطه خاکستری پیشنهاد کردند. ابتدا، FMEA ویژه خدمات فراهم شد تا مشخصات ویژه خدمات را منعکس کند، سه بعد اصلی و نوزده بعد فرعی را یکپارچه کند تا مشخصات خدمات را نشان دهد. به عنوان گام دوم تحت این چارچوب FMEA ویژه خدمات، اولویت ریسک هر حالت شکست با استفاده از تحلیل رابطه‌ای خاکستری محاسبه شد.

[4] Fuzzy Multiple Attribute Decision Making

جدول ۲. مقیاس رتبه بندی شدت.

رتبه بندی	شرح	تعریف
۱۰	کاملاً خطرناک	شکست می تواند باعث مرگ مشتری (بیمار، بازدید کننده، کارمند، عضو پرسنلی، شریک کسب و کار) و/یا شکست کل سیستم، بدون هرگونه هشدار قبلی، شود.
۹	بسیار خطرناک	شکست می‌تواند باعث آسیب عمده یا دائمی و/یا اختلال جدی سیستم با وقفه در خدمات، همراه با هشدار قبلی، شود.
۸		
۷	خطرناک	شکست می تواند باعث آسیب جزئی تا متوسط با نارضایتی زیاد مشتری و/یا مشکلات عمده در سیستم شود که نیازمند تعمیرات اساسی یا دوباره‌کاری قابل توجه است.
۶		
۵	خطر متوسط	شکست می‌تواند باعث آسیب جزئی همراه با نارضایتی برخی از مشتری و/یا مشکلات عمده در سیستم شود.
۴	کم خطر تا خطر متوسط	شکست می‌تواند باعث آسیب بسیار جزئی شود یا آسیبی رخ ندهد اما مشتریان را آزار دهد و/یا منتج به مشکلات جزئی در سیستم شود که می‌توان با تغییرات جزئی در سیستم یا فرایند بر آنها غلبه کرد.
۳		
۲	کم خطر	شکست ممکن است باعث آسیب نشود و مشتری از علت مشکل بی‌اطلاع است؛ با این حال، پتانسیل برای آسیب جزئی وجود دارد. تاثیر بر روی سیستم کم یا هیچ است.
۱	بدون خطر	شکست باعث آسیب نمی‌شود و هیچ تاثیری بر روی سیستم ندارد.

روش VIKOR را اجرا کردند، این روش برای بهینه‌سازی چند مقوله‌ای سیستم‌های پیچیده توسعه یافته بود، توسعه این روش برای مشخص کردن رتبه‌بندی اولویت مصالحه حالت‌های شکست مطابق با عامل‌های ریسک در FMEA بود. در روش‌شناسی، متغیرهای زبانی، اظهار شده با اعداد فازی مثلثی یا ذوزنقه‌ای، برای ارزیابی رتبه‌بندی‌ها و وزن‌ها برای عامل‌های ریسک استفاده شدند. روش گسترده VIKOR برای تعیین اولویت‌های ریسک حالت‌های شکست تعیین شده استفاده شد. مطابق با FMEA، اولویت‌های ریسک حالت‌های شکست در کل توسط عدد اولویت ریسک (RPN)[5] تعیین شدند که سه عامل ریسک را ارزیابی می‌کنند: رخداد (O)[6]، شدت (S)[7] و کشف (D)[8]. در ادامه، RPN در معادله ۱ تعریف شده است.

$$RPN = O_X S_X D \qquad (1)$$

عامل رخداد احتمال رخداد حالت شکست را می‌سنجد. شدت توالی قابل انتظار شرکت است. توانایی شناخت خطا قبل از تاثیرگذاری نتایجش بر مشتریان توسط عامل کشف سنجیده شده است. با ملاحظه وجه عینی این عامل‌های ریسک، تصمیم‌گیرنده (DM)[9] ارزیابی فازی از این ارزش‌ها با استفاده از مقیاس ویژه برای هر عامل فراهم می‌کند. رهنمون‌های امتیازدهی متفاوت وجود دارد، و در این مقاله، مدل پیشنهادی از مقیاس زبانی ۱۰ امتیازی برای ارزیابی عامل‌های O، S و D استفاده می‌کند، همانطور که گودمن (۱۹۹۶) پیشنهاد کرد و در کاربردهای فراوان FMEA استفاده شده است این مقیاس‌ها در جدول‌های ۲ تا ۴ شرح داده شده‌اند.

[5] Risk Priority Number
[6] Occurrence
[7] Severity
[8] Discovery
[9] Dissection maker

جدول ۳- مقیاس رتبه‌بندی رخداد.

رتبه بندی	شرح	میزان شکست بالقوه
۱۰	احتمال خاص وقوع	شکست حداقل یک بار در روز رخ می‌دهد، یا شکست تقریبا هر دفعه رخ می‌دهد.
۹	شکست تقریبا اجتناب ناپذیر است	شکست به صورت قابل پیش‌بینی رخ می‌دهد، یا شکست هر ۳-۴ روز رخ می‌دهد
۸	احتمال بسیار بالای رخداد	شکست اغلب اتفاق می‌افتد، یا شکست یک بار در هفته رخ می‌دهد.
۷	احتمال نسبتاً بالای رخداد	شکست تقریباً ماهی یک بار رخ می‌دهد
۶	احتمال متوسط رخداد	شکست گاهی اوقات رخ می‌دهد، یا شکست ۳ ماه یک بار رخ می‌دهد.
۵	احتمال پایین رخداد	شکست به ندرت رخ می‌دهد، یا شکست یک بار در سال رخ می‌دهد.
۴	احتمال ضعیف رخداد	شکست به ندرت رخ می‌دهد، یا شکست سالی یک بار رخ می‌دهد. شکست اغلب هرگز رخ نمی‌دهد؛ هیچ‌کس آخرین شکست را به یاد نمی‌آورد.

جدول ۴- مقیاس رتبه‌بندی کشف

رتبه‌بندی	شرح	تعریف
۱۰	بدون شانس کشف	مکانیزم مشخص برای کشف شکست وجود ندارد.
۹	شانس بسیار ضعیف /غیرقابل اعتماد کشف	توسط بازرسی، و این کار عملی نیست یا به آسانی قابل اجرا نیست
۸	شانس ضعیف کشف	خطا را می‌توان با بازرسی دستی کشف کرد، اما فرایندی در جریان نیست، بنابراین این کشف به شانس محول می‌شود.
۷	شانس متوسط کشف	فرایندی برای کنترل دوگانه یا بازرسی دوگانه وجود دارد، اما خودکار نیست و/یا تنها برای نمونه اعمال شده است و/یا متکی بر چالاکی است.
۶	شانس بالای کشف	۱۰۰٪ بازرسی یا بررسی فرایند وجود دارد، اما خودکار نیست.
۵	شانس بسیار بالا برای کشف	۱۰۰ بازرسی فرایند انجام می‌شود و خودکار است.
۴	شانس کشف قریب به یقین است	«خاموشی‌ها»ی خودکار یا محدودیت‌هایی برای جلوگیری از شکست وجود دارد.

۲-۲-نظریه‌ی تصمیم‌گیری فازی

مطابق نظر (پدریکز، ایکل و پاریرس (۲۰۱۱) نظریه مجموعه فازی، طراحی شده توسط زاده (۱۹۶۵)، یکی از اساسی‌ترین مفاهیم علوم و مهندسی است، چرا که می‌تواند اطلاعات نادرست را با دستکاری شرایط ریاضی مدیریت کند. مفهوم مجموعه‌های فازی کاملاً شهودی و شفاف هستند چرا که لزوم نحوه ادراک و شرح کارها در زندگی روزمره را می‌شناسد. مفهوم مجموعه فازی نمایش گروه‌ها/دسته‌هایی را مدیریت می‌کند که مرزهایی با تعریف ناقص یا انعطاف‌پذیر به وسیله کارکردهای مشخصه دارای ارزش در مجموعه منظم مقادیر عضویت دارند بنابراین، مجموعه فازی A، طبق تعریف، تابع عضویتی است که عناصر جامعه X را برای وقفه واحد [۰،۱]، به شرح ذیل، ترسیم می‌کند.

$$A : X \rightarrow [0, 1] \qquad (2)$$

بنابراین مجموعه فازی A در X توسط تابع عضویت $f_A(x)$ توصیف شده است، این مجموعه هر نقطه X را با عدد واقعی در فاصله [۰،۱] با مقدار $f_A(x)$ نمایش‌دهنده سطح تداعی x با مجموعه A مرتبط می‌کند. بنابراین، هرچقدر مقدار $f_A(x)$ به یک نزدیکتر فرض شود، عضویت عنصر x برای مجموعه A بیشتر خواهد بود (زاده، ۱۹۶۵). این فرض که A اولویت برای مقادیر متغیر x در X را نشان می‌دهد و از آنجایی که x متغیر تصمیم‌گیری و مجموعه فازی A محدودیت منعطف برای توصیف مقادیر شدنی و اولویت‌های تصمیم‌گیرنده است، $f_A(v)$ نشان دهنده درجه اولویت به نفع v به اندازه x است. این تفسیر در بهینه‌سازی فازی و تحلیل تصمیم‌گیری شایع است (پدریکز و همکاران، ۲۰۱۱). مدل‌های ارزیابی و کمّی‌سازی ریسک عمدتاً از مدل‌های احتمالاتی استفاده می‌کنند که رکن اساسی تصمیم‌گیری آگاهانه در ارتباط با ریسک در بسیاری حوزه‌ها هستند. با اینحال، ممکن است مدل احتمالاتی ساخته‌شده براساس نظریه‌ی مجموعه‌ی فازی قابلیت تعریف برخی ریسک‌ها به شیوه‌ی عملی و معنادار را نداشته باشد از این منظر، پژوهشگران بسیاری بکارگیری منطق فازی و نظریه‌ی مجموعه‌ی فازی بیان‌شده توسط ریاضیدان لطفی زاده در سال ۱۹۶۵ را برای مدیریت ریسک پیشنهاد کرده‌اند. نیز چنین استدلال نمود که پذیرش مدل‌های تصمیم‌گیری را می‌توان با استفاده از ابزارهای فازی و احتمالات فازی ارتقا بخشید، چراکه نظریه‌ی تصمیم گیری هنجاری به ندرت در عمل برای حل مسائل دنیای واقعی استفاده می‌شود. با انتشار مقاله‌ی مجموعه‌های فازی توسط زاده در سال ۱۹۶۵، نظریه‌ی مجموعه‌های فازی به عنوان راهی جدید برای مدلسازی مدل‌های تصمیم‌گیری واقع‌گرایانه‌تر مطرح شد و مدلسازی داده‌های مبهم با بیشترین دقت ممکن را عملی ساخت. پس از آن، برخی المان‌های فازی برای استفاده در مدلهای تصمیم‌گیری مطرح شدند: اعمال فازی، رخدادهای فازی، احتمالات فازی، مقادیر سودمندی فازی، و مواردی از این قبیل. با اینحال، بسیاری از این المان‌های فازی در عمل استفاده نمی‌شوند، یا به این خاطر که اکثر افراد با آنها آشنایی ندارند یا به این دلیل که کاربرد محدودی برای مسائل واقعی دارند. در این مقاله، برای تحلیل درخت رویداد (ETA) از مقادیر مورد انتظار فازی (FEV)[۱۰] که در (رومل‌فانگر (۲۰۰۳) بحث شده، برای تعریف ریسک مورد انتظار هر یک از اقدامات-رخدادهای مرتبط با مدیریت امنیت اطلاعات پیشنهاد می‌شود. از این منظر، قابلیت کاربردی دو المان فازی بررسی می‌شود.

احتمالات فازی:

$$\tilde{P}_j = \tilde{P}(s_j) = \{(p, \mu_{P_j}(p)) | p \in [0, 1]\},$$

مقادیر سودمندی فازی (پیامدها):

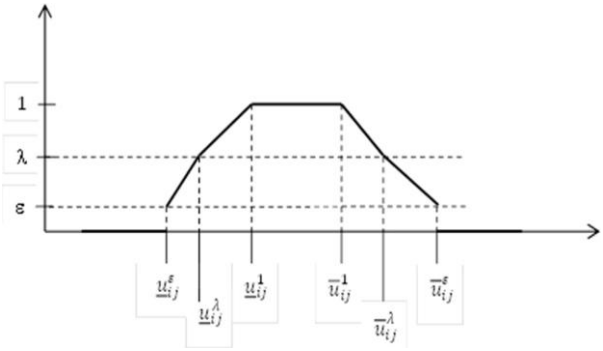
$$\tilde{U}_{ij} = \tilde{U}(a_i, s_j) = \{u, \mu_{U_{ij}}(u) | u \in U\}$$

در این رابطه a_i بیانگر اقدامات و s_i معرف حالات طبیعی احتمالی (سناریوهای احتمالی) است. همچون مقاله‌ی نحوه‌ی دستیابی به توابع سودمندی (فازی) در اینجا نیز بررسی نمی‌شود. چنین فرض می‌شود که تصمیم‌گیرنده یا متخصص، تابع سودمندی $u = u(g_{ij})$ را می‌شناسد. آنگاه، نتایج فازی در سودمندی‌های فازی $\tilde{U}_{ij} = \{u(g), \mu_{\tilde{G}_{ij}}(g) | g \in G\}$ نگاشته می‌شوند یا در عوض متخصصان مستقیماً مقادیر سودمندی $\tilde{U}_{ij} = \{u, \mu_{\tilde{U}_{ij}}(u) | u \in U\}$ را تعیین می‌کنند، U مجموعه‌ی احتمالی مقادیر سودمندی قطعی است.

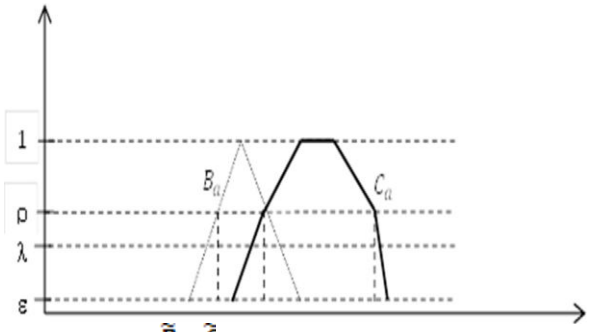
[۱۰] Fuzzy expected values

جدول ۱- مراحل توسعه‌ی تحلیل درخت تصمیم‌گیری

فعالیت‌ها	تعریف
گام ۱ – شناسایی سناریوهای تصادفی	انجام تحلیل خطر بر روی مرکز داده برای شناسایی خطرات سیستم موجود و سناریوهای اتفاقات.
گام ۲ – شناسایی رخدادهای آغازکننده	اصلاح تحلیل خطر برای شناسایی رخدادهای آغازکننده‌ی مهم در اتفاقات مرکز داده. رخدادهای آغازکننده عبارتند از تهاجم از طریق دسترسی داخلی و خارجی.
گام ۳ – شناسایی رخدادهای اساسی	شناسایی منبع وقوع خطا در تهاجم به مرکز داده.
گام ۴ – ایجاد دیاگرام درخت رخدادها	ایجاد دیاگرام‌های درخت رخدادهای منطقی، که با رخدادهای اولیه آغاز می‌شود و با رخدادهای اساسی ادامه می‌یابد و نهایتاً با نتایج هر مسیر پایان می‌پذیرد.
گام ۵ – شناسایی ریسک نتایج	ارزیابی ریسک برای هر یک از مسیرهای حاصله در دیاگرام درختی رخدادها



تصویر ۱. تابع عضویت $\tilde{U}_{ij}$.



تصویر ۲. تابع عضویت مجموعه‌های $\tilde{B}$ e $\tilde{C}$؛ اولویت-ρ

۲-۲-۱-مقادیر مورد انتظار فازی (FEV)

همانگونه که در (رومل‌فانگر (۲۰۰۳) شد، فرض کنید یک عدد حقیقی a را بتوان به شکل یک عدد فازی همانند زیر مدل کرد:

$$\hat{A} = \left\{ \left(x, \mu_{\hat{A}}(x)\right) | x \in R \right\} \text{ with} \mu_{\hat{A}}(x) = \begin{cases} 1 \text{if} x = a \\ 0 \text{else} \end{cases} \qquad (1)$$

هر یک از ترکیبات عمل-رخداد (a_i, s_j) توسط یک بازه‌ی فازی، مقداردهی می‌شود:

$$\tilde{U}_{ij} = \left(\underline{u}_{ij}^{\varepsilon}; \underline{u}_{ij}^{\lambda}; \underline{u}_{ij}^{1}; \overline{u}_{ij}^{1}; \overline{u}_{ij}^{\lambda}; \overline{u}_{ij}^{\varepsilon}\right)^{\lambda,\varepsilon}, \; i = 1, \ldots, m; \; j = 1, \ldots, n. \qquad (2)$$

تابع عضویت $\tilde{U}_{ij}$ چندضلعی نشان داده شده در تصویر ۱ است. این تابع عضویت با توجه به این موضوع پیشنهاد شده که تقریبی از مجموعه‌ی فازی را می‌توان با استفاده از تعداد کمی برش-α ایجاد نمود. و در نتیجه، برای:

$\alpha = 1: \mu_{\tilde{v}_{ij}}(u) = 1$ ، u بالاترین احتمال تعلق داشتن به مجموعه‌ی مقادیر سودمندی مرتبط با ترکیب عمل-رخداد (a_i, s_j) را دارد. $\alpha = \lambda: \mu_{\tilde{v}_{ij}}(u) \geq \lambda$ ، تصمیم‌گیرنده یا متخصص تمایل دارد u را به عنوان مقدار در دسترس برای زمان حال بپذیرد. یک مقدار u با $\mu_{\tilde{v}_{ij}}(u) \geq \lambda$ شانس خوبی برای تعلق گرفتن به مجموعه‌ی مقادیر سودمندی مرتبط با ترکیب عمل-رخداد (a_i, s_j) دارد. مقادیر متناظر u برای تصمیم‌گیری مناسبند. $\alpha = \epsilon: \mu_{\tilde{v}_{ij}}(u) < \epsilon$ ، u شانس بسیار کمی برای تعلق گرفتن به مجموعه‌ی مقادیر سودمندی متناظر با ترکیب عمل-رخداد (a_i, s_j) دارد. متخصص میل دارد از مقادیر u با $\mu_{\tilde{v}_{ij}}(u) < \epsilon$ صرف‌نظر کند. حال این را در نظر بگیرید که متخصص احتمالات پیشین $p(s_j), j = 1, 2, \dots, n$ را شناسایی کند، مقادیر مورد انتظار برای هر آلترناتیو را می‌توان اینگونه محاسبه نمود:

$$\tilde{E}(a_i) = \tilde{U}_{il} \otimes p(s_1) \oplus \quad \dots \oplus \quad \tilde{U}_{in} \otimes p(s_n) = \left(\underline{E}_i^{\varepsilon}; \underline{E}_i^{\lambda}; \underline{E}_i^{1}; \overline{E}_i^{1}; \overline{E}_i^{\lambda}; \overline{E}_i^{\varepsilon}\right)^{\varepsilon,\lambda} \quad (3)$$

که در آن داریم:

$$\underline{E}_i^{\alpha} = \sum_{j=1}^{n} \underline{u}_{ij}^{\alpha} \times p\left(s_j\right), \alpha = \epsilon, \lambda, 1 \quad (4)$$

$$\bar{E}_i^{\alpha} = \sum_{j=1}^{n} \bar{u}_{ij}^{\alpha} \times p\left(s_j\right), \alpha = 1, \lambda, \epsilon \quad (5)$$

۲-۲-۲- مرتب‌سازی اولویت‌های فازی

بایستی متخصص تمامی ترکیبات عمل-رخداد را که بهترین نتیجه را حاصل می‌کنند شناسایی کند. پس از محاسبه‌ی مقادیر مورد انتظار، بایستی متخصص مجموعه‌های فازی را مقایسه نموده و مرتب‌سازی اولویت‌های فازی را انجام دهد. این گام شناسایی زمانیکه مجموعه‌های فازی در مدل کلاسیک استفاده شوند، اهمیت دارد. اکثر مفاهیم بر غیرفازی‌سازی مبتنی است، به این معنا که هر مجموعه‌ی فازی در یک عدد حقیقی قطعی واحد فشرده‌سازی می‌شود. به عبارت دیگر، (اکل و شافتر نتو (۲۰۰۶)) عنوان نمودند که مرتب‌سازی مقادیر فازی به معنای تبدیل یک کمیت فازی به یک عدد حقیقی و سپس پایه‌ریزی مقایسه‌ی مقادیر فازی بر روی آن اعداد حقیقی است. می‌توان برخی کاستی‌ها را در ارتباط با این روش‌ها ذکر کرد: گسترش مجموعه‌های فازی در روند غیرفازی‌سازی نادیده گرفته شده است (رامل‌فانگر، ۲۰۰۳)؛ هر رویکرد تبدیلی به یک جنبه‌ی منحصر بفرد از مقادیر فازی توجه دارد (اکل و شافتر نتو (۲۰۰۶)) ممکن است روش‌های غیرفازی‌سازی رتبه‌بندی‌های مختلفی برای یک مسأله یکسان داشته باشند)، و گاهاً انتخاب‌هایی حاصل شوند که با شهود سازگاری ندارند، نهایتاً اکثر روش‌ها یک تمایز الزامی را بین آلترناتیوها فرض می‌کنند، که طبیعی نیست، چراکه عدم قطعیت اطلاعات به نواحی عدم قطعیت تصمیم‌گیری منجر می‌شود (اکل و شافنر نتو، ۲۰۰۶). به منظور اجتناب از این کاستی‌ها، استفاده از الویت-ρ و اولویت-ϵ به عنوان آلترناتیو برای انجام مرتب‌سازی اولویت‌ها مفاهیم زیر را پیشنهاد کرد. مجموعه‌ی فازی $\tilde{B}$ بر مجموعه‌ی فازی $\tilde{C}$ در سطح $\rho, \rho \in [0, 1]$ اولویت دارد و می‌نویسیم $\tilde{B}\ \rho\ \tilde{C}$، اگر :

ρ کوچک‌ترین عدد حقیقی باشد، بطوریکه: $Inf\ B_{\alpha} \geq Sup\ C_{\alpha}$ برای تمامی $\alpha \in [\rho, 1]$ (۶)

و برای حداقل یک $\alpha \in [\rho, 1]$، نامساوی (۶) بطور اکید برقرار باشد.

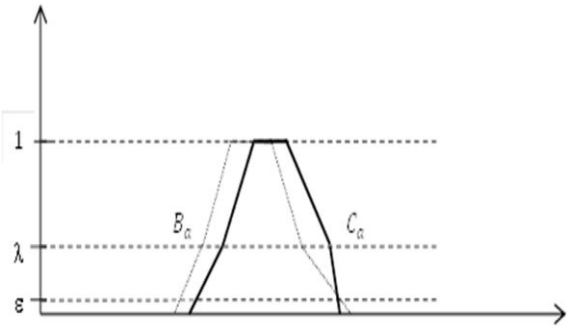
در اینجا مجموعه سطوح ρ از $\tilde{B}$ و $\tilde{C}$ به شکل زیر تعریف می‌شوند:

$$B_{\alpha} = \left\{x \in X : \mu_{\tilde{B}}(x) \geq a\right\}$$

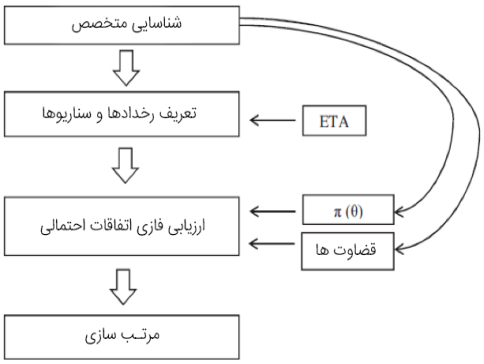
$$C_{\alpha} = \left\{x \in X : \mu_{\tilde{C}}(x) \geq a\right\}$$

تصویر ۲ نمونه‌ای را نشان می‌دهد که در آن داریم: $\tilde{B}\ \rho\ \tilde{C}$.

در مواردی که رابطه‌ی اولویت-ρ به مرتب‌سازی اولویت‌های آلترناتیوهای مشخص ختم نمی‌شود، رابطه‌ی اولویت - ϵ مناسب‌تر است، زیرا رابطه‌ی اولویت - ϵ در مقایسه با اولویت-ρ ضعیف‌تر است. برای جزئیات بیشتر، رامل‌فانگر (۲۰۰۳) را ببینید. در سطح - $\epsilon \in [0,1]$ ϵ، مجموعه‌ی فازی $\tilde{B}$ بر مجموعه‌ی فازی $\tilde{C}$ اولویت دارید، و می‌نویسیم $\tilde{B}\ \epsilon\ \tilde{C}$، اگر: ϵ کوچک-ترین عدد حقیقی باشد، بطوریکه: $Sup\ B_\alpha \geq Sup\ C_\alpha$ و $Inf\ B_\alpha \geq Inf\ C_\alpha$ برای تمامی $\alpha \in [\epsilon,1]$ (۷) و برای حداقل یک $\alpha \in [\epsilon,1]$، یک از نامساوی (۷) بطور اکید برقرار باشد. تصویر ۳ نمونه‌ای را نشان می‌دهد که در آن داریم: $\tilde{B}\ \epsilon\ \tilde{C}$.



تصویر ۳- تابع عضویت مجموعه‌های $\tilde{B}\ \epsilon\ \tilde{C}$؛ اولویت-$\rho$



تصویر ۴- مراحل مدل پیشنهادی ETA

۳- مدل پیشنهادی ETA برای ارزیابی ریسک امنیت اطلاعات:

مدل پیشنهادی برای امنیت اطلاعات، چهار مرحله دارد (تصویر ۴): شناسایی متخصص، تعیین سناریوها و رخدادها، ارزیابی فازی و مرتب‌سازی. هدف از مدل پیشنهادی، ارزیابی نتایج هر آلترناتیو در قالب زیان مالی (متغیری که به سادگی درک می‌شود) با در نظر گرفتن سناریوهای احتمالی مختلف (حالات طبیعی احتمالی) است.

۳-۱- شناسایی متخصص

گام اول، شناسایی متخصص است. متخصص فرد یا گروهی از افراد است که براساس تجربه، توانایی شناسایی اینها را دارند: نقاط آسیب‌پذیر سازمان، و به تبع آن، اتفاقات احتمالی؛ سناریوهای احتمالی؛ احتمال وقوع و قضاوت‌ها در خصوص هر یک از المان‌ها. سه شاخص توصیه شده است: تعداد مقالات علمی‌چاپ‌شده، توصیه‌های شمار زیادی از متخصصان، و تجارب مطالعات مشابه پیشین، این را می‌توان برای انتخاب مناسب متخصصانی که تخصص آنها بیشترین ارتباط را با سیستم مورد ارزیابی دارد، مورد استفاده قرار داد.

۳-۲- مشخص نمودن رخدادها و سناریوها

روش ETA برای بیان مسائل مرتبط با ارزیابی ریسک امنیت اطلاعات، نقاط آسیب‌پذیری آنها و تبعات آن ایجاد شده است **(تصویر ۵ را ببینید)**. در سیستم‌های اطلاعاتی، ریسک‌های امنیتی توسط عوامل مختلف داخلی و خارجی مرتبط به هم بسیاری ایجاد شده و ممکن است از ویروس‌ها، کرم‌ها، هکرها، و کراکرها ناشی شوند (گرانت، ادگار، سوکومار و مایر، ۲۰۱۴) تهدیدات داخلی شامل این موارد است: استفاده‌ی نامناسب از دستگاه‌ها، وجود نقض در داده‌های شبکه، گم شدن / دزدیده شدن لپ‌تاپ، عدم آموزش، عدم تجربه، آسیب عمدی، هرزنامه ، فریب، تهدیدات امنیتی خارجی به شکل آسیب‌های تصادفی نمود پیدا می‌کنند. پس از آنکه ETA امنیت اطلاعت ایجاد شد، به عنوان ابزاری برای ارزیابی ریسک مبتنی بر نظریه‌ی تصمیم و منطق فازی عمل می‌کند.

۳-۳- ارزیابی فازی اتفاقات احتمالی و مرتب‌سازی

نقطه‌ی شروع استفاده از رویکرد نظریه‌ی تصمیم برای ارزیابی اتفاقات احتمالی، تشکیل ماتریسی ایت (8) که سطرهای آن، آلترناتیوها (برای نمونه، اتفاقات احتمالی مرتبط با امنیت اطلاعات در سرویس‌های مرکز داده) و ستون‌های آن، سناریوهای احتمالی را نشان دهند. متخصص برای هر درایه‌ی ماتریس، از منطق فازی برای تعریف زیانهای مالی حاصل از ترکیبات این متغیرها (آلنرناتیوها، سناریوها) استفاده می‌کند. متخصص، احتمال هر سناریو را با در نظر گرفتن ابزارهای مختلف وقوع سناریو ارائه می‌دهد. اینها احتمالات پیشین $(p(s_j))$ هستند که در حالت کاربردی آنها را با $\pi(q)$ نمایش می‌دهیم.

۴- مدل پیشنهادی FMEA برای مدیریت بهینه سازی اطلاعات

ارزیابی نوع مجموعه فازی از نقطه نظر پایداری‌اش برای مدیریت رویه‌های بهینه‌سازی ضروری است رایج‌ترین دسته‌های تابع‌های عضویت – همگی تعریف شده در جهان اعداد واقعی- عبارتند از: تابع‌های عضویت مثلثی، ذوزنقه‌ای، گاسیان و شبه-نمایی. عدد فازی ذوزنقه‌ای A، که در این مقاله استفاده شده است، قابل شرح مطابق با تابع عضویتش به شرح ذیل است:

$$\mu_A(x)=\begin{cases}0 & \text{if } x<a_1,\\ \dfrac{x-a_1}{b_1-a_1} & \text{if } a_1\le x\le b_1,\\ 1 & \text{if } b_1\le x\le b_2,\\ \dfrac{x-a_2}{b_2-a_2} & \text{if } b_2\le x\le a_2,\\ 0 & \text{if } x>a_2,\end{cases} \qquad (3)$$

در آن A نیز قابل نمایش توسط $A=(a_1,b_1,b_2,a_2)$ است **(شکل ۱)**.

اگر $b_1=b_2=a_M$، A عدد فازی مثلثی است: $A=(a_1,\ a_M,\ a_M,\ \ a_2)=(a_1,a_m,a_2)$

عملیات اصلی نظریه مجموعه فازی را می‌توان در اینجا مرور کرد. آنها گستره‌هایی از اعداد تعریف شده متناظر هستند که از تعیین عدد فازی حمایت می‌کنند. فرض کنید $A_1=(a_1,\ b_1,\ b_2,\ a_2)$ و $A_2=(a_3,\ b_3,\ b_4,\ a_4)$ دو عدد فازی ذوزنقه‌ای غیرمنفی باشند آنگاه:

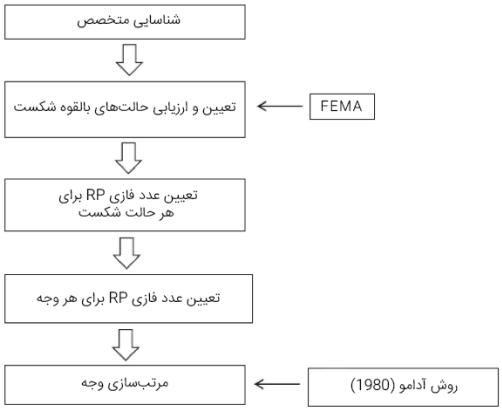
$$A_1 + A_2 = (a_1, b_1, b_2, a_2) + (a_3, b_3, b_4, a_4) = (a_1 + a_3, b_1 + b_3, b_2 + b_4, a_2 + a_4)$$

$$A_1 - A_2 = (a_1, b_1, b_2, a_2) - (a_3, b_3, b_4, a_4) = (a_1 - a_3, b_1 - b_3, b_2 - b_4, a_2 - a_4)$$

$$-A_1 = -(a_1, b_1, b_2, a_2) = (-a_2, -b_2, -b_1, -a_1)$$

$$A_1 \otimes A_2 = (a_1, b_1, b_2, a_2) \otimes (a_3, b_3, b_4, a_4) \cong (a_1 a_3, b_1 b_3, b_2 b_4, a_2 a_4)$$

با ملاحظه ارزیابی دقیق سه عامل ریسک، متخصصین آنها را با استفاده از متغیرهای زبان‌شناسی ارزیابی کرده‌اند.



شکل ۲- مراحل رویکرد پیشنهادی.

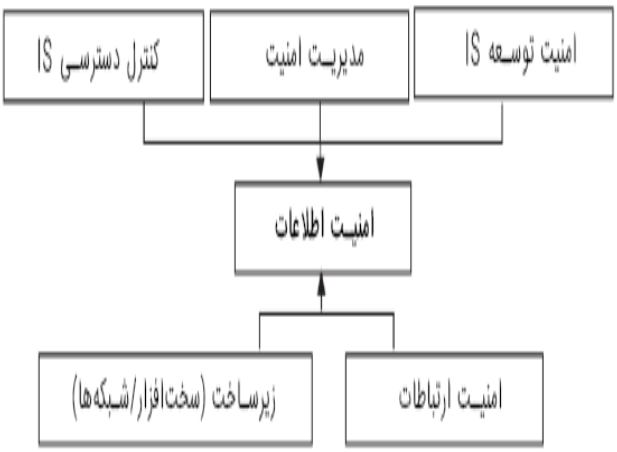
مفهوم متغیرهای زبانی را می‌توان متغیرهایی با مقادیری در نقش مجموعه‌های فازی تصور کرد و مقادیری متشکل از کلمات یا جملات اظهار شده در زبانی اختصاصی فرض می‌شوند، نقش اصلی منطق فازی روش تحقیق برای محاسبه با کلمات است و هنگامی لازم است که اطلاعات در دسترس خیلی دقیق نیستند تا کاربرد اعداد را توجیه کنند و هنگامی مفید هستند که تحمل بی‌دقتی وجود داشته باشد و قابل بهره‌برداری برای رسیدن به نرمی، قدرت، راه‌حل هزینه کم و ارتباط بهتر با واقعیت است.

۴-۱- شناسایی متخصص

اولین گام رویکرد این مدل نیز مطابق مدل ETA متشکل از شناسایی متخصص است. متخصص فردی است که سیستم‌های شرکت و آسیب‌پذیری‌های‌شان را می‌شناسد و قادر است ریسک امنیت اطلاعات را برای سازمان با توجه به پنج وجه ارزیابی کند. این گام می‌تواند گروهی از متخصصان را نیز شناسایی کند و تحلیل را با ملاحظه قضاوت‌شان اجرا کند.

۴-۲- تعیین و ارزیابی حالت‌های شکست بالقوه

این گام حالت‌های شکست را تعیین می‌کند که با پنج وجه ناظر بر امنیت اطلاعات ارتباط دارند. این پنج وجه براساس (چن و ژائو (۲۰۱۳) هستند، آنها عامل‌های تاثیرگذار در ارزیابی ریسک‌های امنیت اطلاعات را بررسی کردند، و لی و تانگ (۲۰۱۳) چارچوب مهندسی امنیت اطلاعات (ISE) را، براساس چهار موضوع اصلی امنیت اطلاعات، پیشنهاد کردند: تعریف، نظریه اساسی، روش‌شناسی و کاربرد.



شکل ۳- ابعاد امنیت اطلاعات

جدول ۵- توضیحات وجهی

عنصر وجهی	شرح
کنترل دسترسی IS	مربوط به معیارهایی است که دسترسی مردم به اطلاعات و سیستم‌ها را کنترل می‌کند
امنیت توسعه IS	مربوط به روش‌ها، سیاست‌ها و رویه‌هایی است که منجر به توسعه سیستم اطلاعات ایمن می‌شود
زیرساخت (سخت‌افزار/شبکه‌ها)	اشاره به زیرساخت امنیت اطلاعات دارد که از منابع سخت‌افزاری و شبکه‌ای تشکیل شده است
مدیریت امنیت	مربوط به برنامه‌ریزی و ارزیابی سیستم‌های اطلاعاتی و ایمن نگه داشتن سیستم‌های اطلاعات سازمان براساس اصول ذیل است: محرمانه بودن، ادغام و در دسترس بودن (پشتیبانی، بازیابی و وابستگی در میان مردم)
امنیت ارتباطات	اشاره به معیارهای اتخاذ شده برای اطمینان از ارتباطات ایمن حاصله بین مردم دارد

در سطح روش تحقیق، آنها تکنیک‌های متفاوت برای تحلیل و ارزیابی پیشنهاد کردند. در این مقاله، FMEA و منطق فازی را ترکیب کردیم تا مدیریت ریسک امنیت اطلاعات بهبود یابد. حالت‌های شکست در ارتباط با هر وجه آسیب‌پذیری شرکت را نشان می‌دهد. نتایج شکست می‌تواند ویران‌کننده باشد. براساس چهار موضوع اصلی در ارتباط با امنیت اطلاعات بررسی شده توسط لی و تانگ (۲۰۱۳)، و چن و ژائو (۲۰۱۳)، این مقاله ساختاری ارائه می‌کند که شامل پنج وجه در ارتباط با شکست‌های بالقوه امنیت اطلاعات است.هر وجه در شکل ۳ به تفصیل در جدول ۵ شرح داده شده است. اقدامات مختلف می‌توانند به این ابعاد آسیب بزنند، این آسیب منتج به حالت‌های شکست فوری یا نهایی در IS می‌شود (جدول ۶). این حالت‌های شکست مطابق با سه عامل ریسک ارزیابی شده‌اند، این سه عامل توسط FMEA پیشنهاد شده‌اند: رخداد، شدت و کشف. در نمایش ما، پنج عبارت زبانی ناملموس مطابق با اعداد فازی ذوزنقه‌ای متناظر ذیل، از مقیاس زبانی ۱۰ امتیازی، تعریف شده‌اند. علاوه بر این، زبان‌شناسی فازی با پنج مقیاس نیز برای تعیین تاثیرگذاری هر حالت شکست در هر وجه استفاده شده‌اند. جدول ۷ هر دو مقیاس زبان‌شناسی و اعداد فازی ذوزنقه‌ای را برای ارزیابی عملکرد و تاثیرگذار شرح می‌دهد. شکل‌های ۴ و ۵ به تفصیل مقادیر عضویت عامل‌های ریسک (عملکرد) و تاثیر هر حالت شکست را در هر وجه، به ترتیب، "نشان می‌دهند.

۴-۳- تعیین عدد فازی RP

این گام عدد فازی RP را برای هر حالت شکست با استفاده از اعداد فازی ذوزنقه‌ای تعیین می‌کند که برای ارزیابی حالت‌های شکست در ارتباط با عامل‌های ریسک استفاده شده بودند: رخداد، شدت و کشف. فرض کنید O_{ij}، S_{ij} و D_{ij} اعداد فازی ذوزنقه‌ای باشند که نشان دهنده ارزیابی‌های رخداد، شدت و کشف برای وجه i و حالت شکست j هستند. در ادامه، عدد فازی RP محصول این عامل‌های ریسک است:

$$RP \ \ fuzzy \ \ number_{ij} \cong O_{ij} \otimes S_{ij} \otimes D_{ij} \qquad (4)$$

جدول ۶- حالت‌های شکست در ارتباط با هر وجه IS.

D1- دسترسی به اطلاعات و سیستم‌ها	D1.1: فقدان مدیریت رسانه‌های کامپیوتری برداشتنی D1.2: فقدان کنترل کلمه عبور کاربر (سیستم اطلاعاتی و کلمه‌های عبور شبکه‌ای) D1.3: فقدان ثبت کاربر D1.4: فقدان تشخیص ترمینال خودکار D1.5: فقدان تصدیق شماره شناسایی کاربر D1.6: فقدان مدیریت دسترسی بیرونی
D2- امنیت ارتباطات	D2.1: فقدان ایمنی پست الکترونیک D2.2: فقدان ایمنی سیستم‌های دفتری الکترونیک D2.3: فقدان مدیریت کنترل رمزنگاری D2.4: فقدان دسترسی محتوای محدود به اینترنت D2.5: فقدان آموزش و پرورش ایمنی اطلاعات
D3- زیرساخت	D3.1: فقدان پشتیبانی از اطلاعات D3.2: فقدان گواهی گره شبکه‌ای D3.3: فقدان ابتکار نرم‌افزاری D3.4: فقدان دفاع ایمن نرم‌افزاری D3.5: فقدان سرور خوشه‌ای D3.6: فقدان تولیدکننده الکتریکی پشتیبان
D4- مدیریت امنیت	D4.1: فقدان بررسی امنیت اطلاعات D4.2: فقدان سیاست برای ایمنی اطلاعات D4.3: فقدان مسئولیت برای ایمنی اطلاعات D4.4: فقدان نگهداری از نرم‌افزار و سخت‌افزار D4.5: فقدان بررسی سیاست‌های اجرا شده امنیت اطلاعات
D5- توسعه سیستم‌های اطلاعات ایمن	D5.1: فقدان استانداردسازی و مستندسازی فرایند توسعه نرم‌افزار D5.2: شکست در آزمایش در برابر آسیب‌پذیری‌ها و تعارض‌های نرم‌افزاری D5.3: فقدان واقعه‌نگاری نظارت بر تغییر

جدول ۷- مقیاس زبان‌شناسی و اعداد فازی ذوزنقه‌ای برای ارزیابی عملکرد و تاثیرگذاری.

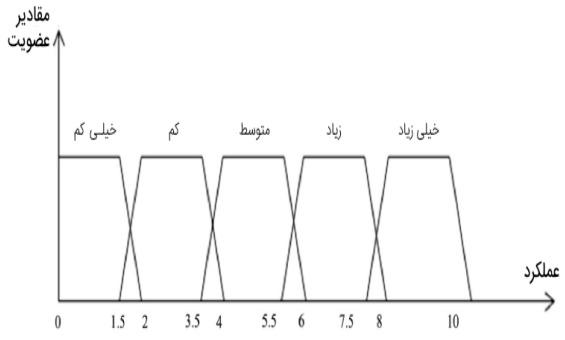
+	تاثیرگذاری
خیلی کم (VL): (0; 0; 1.5; 2)	مطلقاً با تاثیرگذاری کم (LI): (0; 0; 0.15; 0.2)
کم (L): (1.5; 2; 3.5; 4)	تاثیرگذاری کم (LI): (0.15; 0.2; 0.35; 0.4)
متوسط (M): (3.5; 4; 5.5; 6)	تاثیرگذاری متوسط (MI): (0.35; 0.4; 0.55; 0.6)
زیاد (H): (5.5; 6; 7.5; 8)	تاثیرگذار (I): (0.55; 0.6; 0.75; 0.8)
خیلی زیاد (VH): (7.5; 8; 9.5; 10)	خیلی تاثیرگذار (VI): (0.75; 0.8; 0.9; 1)

۴-۴- ارزیابی وجه

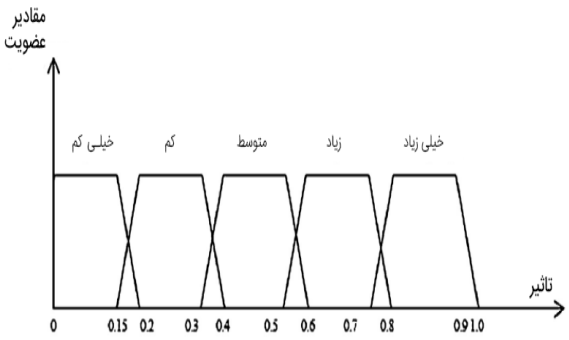
اکنون می‌توانیم کل اعداد فازی RP را برای ابعاد محاسبه کنیم تا آنها را با توجه به ریسک مقایسه و رتبه‌بندی کنیم. آنها توسط متخصص برای وجه i و حالت شکست j، با توجه به پیامدهای اقتصادی و عملیاتی ارزیابی شده‌اند. در نهایت، فرض کنید I_{ij} تاثیرگذاری (یا تاثیر) هر حالت شکست j بر هر وجه i باشد.

$$RP\ \ fuzzy\ \ number_i = \sum_{j=1}^{m} RP\ \ fuzzy\ \ number_{ij} \quad j = 1, 2, \ldots, m. \quad (5)$$

در آن عدد فازی RP کل امتیاز فازی RP وجه mام است و امتیاز فازی RP حالت شکست jام در وجه iام را نشان می‌دهد، و j تعداد حالت‌های شکست در هر وجه است.



شکل ۴- تابع عضویت عملکرد.



شکل ۵- تابع عضویت تاثیر

جدول ۸- ارزیابی‌های حالت‌های شکست بالقوه

وجه	حالت‌های شکست بالقوه	رخداد (O)	شدت (S)	کشف (D)
D1- دسترسی به اطلاعات و سیستم‌ها	D1.1: فقدان مدیریت رسانه‌های کامپیوتری برداشتنی	(VL)	(VH)	(H)
	D1.2: فقدان کنترل کلمه عبور کاربر (سیستم اطلاعاتی و کلمه‌های عبور شبکه‌ای)	(M)	(H)	(M)
	D1.3: فقدان ثبت کاربر	(L)	(M)	(L)
	D1.4: فقدان تشخیص ترمینال خودکار	(M)	(H)	(M)
	D1.5: فقدان تصدیق شماره شناسایی کاربر	(L)	(M)	(M)
	D1.6: فقدان مدیریت دسترسی بیرونی	(H)	(VH)	(L)
D2- امنیت ارتباطات	D2.1: فقدان ایمنی پست الکترونیک	(VH)	(H)	(H)
	D2.2: فقدان ایمنی سیستم‌های دفتری الکترونیک	(L)	(H)	(M)
	D2.3: فقدان مدیریت کنترل رمزنگاری	(L)	(M)	(L)
	D2.4: فقدان دسترسی محتوای محدود به اینترنت	(VH)	(M)	(H)
	D2.5: فقدان آموزش و پرورش ایمنی اطلاعات	(M)	(H)	(L)
D3- زیرساخت	D3.1: فقدان پشتیبانی از اطلاعات	(L)	(VH)	(L)
	D3.2: فقدان گواهی گره شبکه‌ای	(H)	(M)	(M)
	D3.3: فقدان ابتکار نرم‌افزاری	(M)	(H)	(H)
	D3.4: فقدان دفاع ایمن نرم‌افزاری	(H)	(H)	(M)
	D3.5: فقدان سرور خوشه‌ای	(M)	(H)	(L)
	D3.6: فقدان تولیدکننده الکتریکی پشتیبان	(VL)	(VH)	(M)
D4- مدیریت امنیت	D4.1: فقدان بررسی امنیت اطلاعات	(L)	(M)	(M)
	D4.2: فقدان سیاست برای ایمنی اطلاعات	(L)	(L)	(L)
	D4.3: فقدان مسئولیت برای ایمنی اطلاعات	(M)	(M)	(M)
	D4.4: فقدان نگهداری از نرم‌افزار و سخت‌افزار	(H)	(VH)	(M)
	D4.5: فقدان بررسی سیاست‌های اجرا شده امنیت اطلاعات	(M)	(H)	(L)
D5- توسعه سیستم‌های اطلاعات ایمن	D5.1: فقدان استانداردسازی و مستندسازی فرایند توسعه نرم‌افزار	(H)	(L)	(M)
	D5.2: شکست در آزمایش در برابر آسیب‌پذیری‌ها و تعارض‌های نرم‌افزاری	(VH)	(M)	(H)
	D5.3: فقدان واقعه‌نگاری نظارت بر تغییر	(H)	(H)	(M)

۴-۵- مرتب‌سازی بُعد

مفاهیم متفاوت برای مقایسه مجموعه‌های فازی و برای ساخت ترتیب‌بندی‌های اولویت پیشنهاد شده‌اند اغلب مفاهیم براساس غیرفازی‌سازی هستند، یعنی هر مجموعه فازی در عدد واقعی تعریف شده فشرده‌سازی شده است. گسترش مجموعه‌های فازی در فرایند غیرفازی سازی نادیده گرفته شده‌اند. در این اثر، از روش پیشنهادی آدامو (۱۹۸۰) استفاده خواهیم کرد، این روش تمام ویژگی‌های پیشنهادی توسط وانگ و کری (۲۰۰۱) را توجیه می‌کند و صرفاً عدد فازی در نقطه سمت راست برش آلفا برای آلفای مربوطه را ارزیابی می‌کند:

$$AD_{\alpha}(A) = a_{\alpha}^{+} \qquad (6)$$

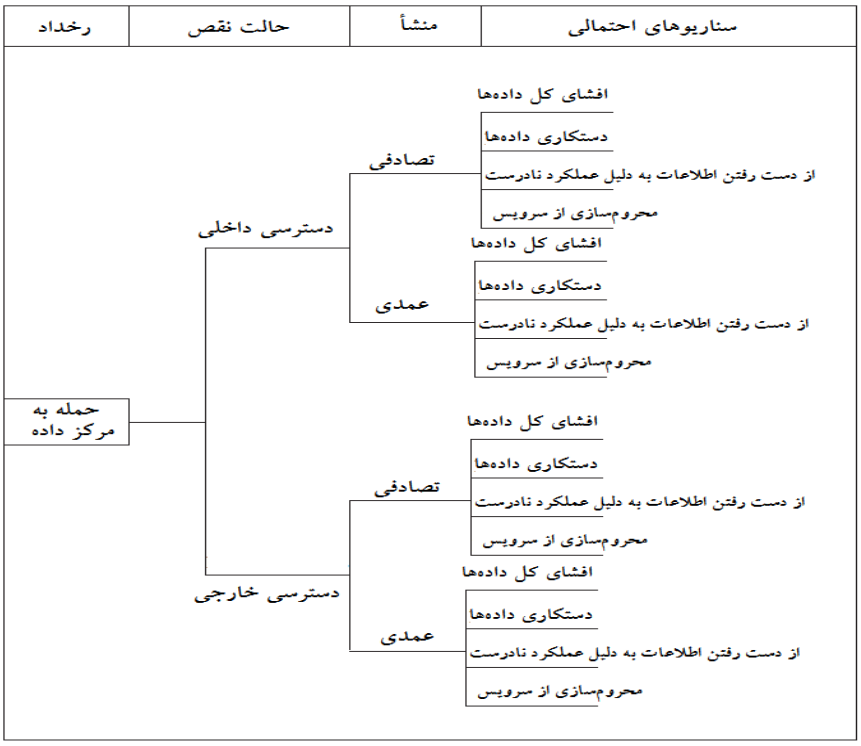
جدول ۹- عدد فازی RP برای هر حالت شکست

وجه	حالت‌های بالقوه شکست	عدد فازی RP
D1- دسترسی به اطلاعات و سیستم‌ها	D1.1: فقدان مدیریت رسانه‌های کامپیوتری برداشتنی D1.2: فقدان کنترل کلمه عبور کاربر (سیستم اطلاعاتی و کلمه‌های عبور شبکه‌ای) D1.3: فقدان ثبت کاربر D1.4: فقدان تشخیص ترمینال خودکار D1.5: فقدان تصدیق شماره شناسایی کاربر D1.6: فقدان مدیریت دسترسی بیرونی	(0; 0; 85.5; 160) (67.375; 96; 165; 288) (7.875; 16; 38.5; 96) (67.375; 96; 165; 288) (18.375; 32; 77; 144) (61.875; 96; 142.5; 320)
D2- امنیت ارتباطات	D2.1: فقدان ایمنی پست الکترونیک D2.2: فقدان ایمنی سیستم‌های دفتری الکترونیک D2.3: فقدان مدیریت کنترل رمزنگاری D2.4: فقدان دسترسی محتوای محدود به اینترنت D2.5: فقدان آموزش و پرورش ایمنی اطلاعات	(226.875; 288; 427.5; 640) (28.875; 48; 105; 192) (7.875; 16; 38.5; 96) (144.375; 192; 313.5; 480) (28.875; 48; 82.5; 192)
D3- زیرساخت	D3.1: فقدان پشتیبانی از اطلاعات D3.2: فقدان گواهی گره شبکه‌ای D3.3: فقدان ابتکار نرم‌افزاری D3.4: فقدان دفاع ایمن نرم‌افزاری D3.5: فقدان سرور خوشه‌ای D3.6: فقدان تولیدکننده الکتریکی پشتیبان	(16.875; 32; 66.5; 160) (67.375; 96; 165; 288) (105.875; 144; 247.5; 384) (105.875; 144; 225; 384) (28.875; 48; 82.5; 192) (0; 0; 57; 120)
D4- مدیریت امنیت	D4.1: فقدان بررسی امنیت اطلاعات D4.2: فقدان سیاست برای ایمنی اطلاعات D4.3: فقدان مسئولیت برای ایمنی اطلاعات D4.4: فقدان نگهداری از نرم‌افزار و سخت‌افزار D4.5: فقدان بررسی سیاست‌های اجرا شده امنیت اطلاعات	(18.375; 32; 77; 144) (3.375; 8; 24.5; 64) (42.875; 64; 121; 216) (144.375; 192; 285; 480) (28.875; 48; 82.5; 192)
D5- توسعه سیستم‌های اطلاعات ایمن	D5.1: فقدان استانداردسازی و مستندسازی فرایند توسعه نرم‌افزار D5.2: شکست در آزمایش در برابر آسیب‌پذیری‌ها و تعارض‌های نرم‌افزاری D5.3: فقدان واقعه‌نگاری نظارت بر تغییر	(28.875; 48; 105; 192) (144.375; 192; 313.5; 480) (105.875; 144; 225; 384)

۵- مثال گویا برای ETA

این بخش مثالی را بیان می‌کند که قابلیت کاربردی مدل پیشنهادی ETA را به تصویر می‌کشد. این کاربرد بر محتوای واقعی استوار است. هرچندکه داده های واقعی، با توجه به اطلاعات مورد نیاز، استفاده نشده‌اند، اما داده ها که برای داشتن دیدی از مدل استفاده شده‌اند، واقع گرایانه هستند. با دنبال کردن مراحل مدل پیشنهادی (**تصویر ۴**) که در بخش ۳ شرح داده شد، اطلاعات مورد نیاز (داده‌های واقعی) توسط یک متخصص ریسک امنیت برای حوزه‌ی اطلاعات، مبتنی بر قضاوت و

تخصص ارائه شد. او بر ریسک‌های استفاده از مرکز داده به عنوان در تقابل با برداشت خود از نقاط آسیب‌پذیر سرویس‌های آن استفاده کرد. این شامل تعداد فزاینده‌ای از گره‌های مدیریت‌شده در محیط‌های ناهمگون پخش‌شده بر روی موقعیت‌های بسیار زیاد است. در این روند، متخصص خلاصه‌ی اولیه‌ای از مشخصه‌های اصلی سرویس‌های مرکز داده نیز ارائه می‌دهد، **جدول ۲** را ببینید. در گام بعدی مدل پیشنهادی، تحلیل ETA براساس دانش متخصص انجام شد (**تصویر ۵**) تا تعاریف رخدادها و سناریوها در حمله به مرکز داده فراهم شود. با در نظر گرفتن دشواری تخصیص یک مقدار عددی به اتفاقات تصادفی، و عدم قطعیت موجود، استفاده از اعضای فازی، و بطور خاص اعضای فازی مثلثی را پیشنهاد می‌کنیم. اعضای فازی مثلثی که در جدول ۳ آمده است، براساس یک مقیاس کلامی ۵ نقطه‌ای (خیلی کم، کم، متوسط، زیاد، خیلی زیاد) برای نمایش تبعات مالی هر آلترناتیو مرتبط با یکی از سناریوها تعیین شدند.



تصویر ۵-تحلیل درخت رخدادها برای حمله به مرکز داده

جدول ۲- سرویس‌های مرکز داده

سرویس‌ها	تعریف
وبسایت	سرویس میزبانی که برای افراد یا شرکت‌ها امکان ذخیره‌سازی اطلاعات، تصاویر، ویدئوها، یا هرگونه محتوای سیستم-های آنلاین قابل دسترس از طریق وب را فراهم می‌آورد.
تجارت الکترونیک	سرویسی که پلتفرم فنی دارای روش‌های پرداخت امن، خرید و backend پایگاه داده‌ی بزرگ، پشتیبانی از فروش محصولات و خدمات از طریق اینترنت.
پایگاه داده به عنوان سرویس	سرویسی که میزبان پایگاه‌های داده در یک ابر است و انتخاب مناسبی برای کسب‌وکارهایی است که برنامه‌های سفارشی تحت وب را توسعه می‌دهند

جدول ۳- مقیاس کلامی مرتبط با گستره‌ی پولی

عبارات زبانی	عدد فازی	مقادیر	واحد
بسیار کم	مثلثی	(۲۰۰؛ ۱۵۰؛ ۱۰۰)	هزار دلار آمریکا
کم	مثلثی	(۴۵۰؛ ۳۵۰؛ ۲۵۰)	هزار دلار آمریکا
متوسط	مثلثی	(۸۰۰؛ ۶۰۰؛ ۳۵۰)	هزار دلار آمریکا
زیاد	مثلثی	(۱۳۰۰؛ ۱۰۰۰؛ ۶۵۰)	هزار دلار آمریکا
بسیار زیاد	مثلثی	(۲۰۰۰؛ ۱۶۰۰؛ ۱۰۰۰)	هزار دلار آمریکا

جدول ۴- ارزیابی استنباط متخصص

آلترناتیوها (A_i)	θ_1	θ_2	θ_3	θ_4
W/I/A(A_1)	H	VH	M	L
W/I/D (A_2)	L	M	M	H
W/E/A(A_3)	L	VL	VL	VL
W/E/D(A_4)	M	M	VH	VH
EC/I/A(A_5)	M	L	VL	L
EC/I/D(A_6)	VL	VL	L	L
EC/E/A(A_7)	M	L	M	M
EC/E/D(A_8)	L	H	M	VH
DB/I/A(A_9)	H	VH	VH	M
DB/I/D(A_{10})	VH	M	H	VH
DB/E/A(A_{11})	L	M	M	L
DB/E/D(A_{12})	H	VH	H	VH

استفاده از توابع عضویت مثلثی در این مقاله، به خاطر سادگی و کاربردی بودن در بیان محتوا، قابل توجیه است (پدریز، ۱۹۹۴). در متون و مقالات، اعضای فازی مثلثی با یک سه‌گانه نمایش داده می‌شوند (a; m; b)، a و b به معنای حدهای پایینی و بالایی مجموعه‌ی فازی و پارامتر m به معنای مقدار مُدال این مجموعه است. (کافمن و گوپتا، ۱۹۸۸). براساس اطلاعات به دست آمده از متخصص، زیان مالی حاصل از حمله به مرکز داده می‌تواند در گستره‌ی ۱۰۰۰۰۰,۰۰ دلار آمریکا تا ۲۰۰۰۰۰۰,۰۰ دلار آمریکا باشد. در نتیجه، مقیاس کلامی، این بازه را پوشش می‌دهد. با اینحال، بایستی به خاطر داشت که مدل پیشنهادی امکان تغییر دامنه‌ی مقادیر همراستا با محتوای مورد بررسی را فراهم می‌آورد. برای انجام ارزیابی فازی اتفاقات احتمالی، لازم است که مقدار مورد انتظار هر یک از آلترناتیوها بر حسب ریسک را محاسبه کنیم. بدین منظور، بایستی نخست حالات طبیعی و آلترناتیوها (ترکیبات عمل-رخداد) را محاسبه کنیم. سپس بایستی ارزیابی آلترناتیوها بیان‌شده توسط متخصص با استفاده از منطق فازی و احتمالات پیشین $p(s_j)$ انجام شود، در این مثال آن را با $\pi(\theta)$ نمایش می‌دهیم چراکه در نظریه‌ی تصمیم، حالات طبیعی با θ و احتمال پیشین با π مشخص می‌شوند.

در نتیجه، حالات طبیعی (θ) که سناریوهای حاصله‌ی احتمالی (حالت طبیعی) حمله به مرکز داده هستند (تصویر ۵)، اینگونه تعریف شدند: پراکنده ساختن داده‌ها (θ_1)، اصلاح داده‌ها (θ_2)، از دست رفتن یا تخریب داده‌ها (θ_3) و اختلال در سرویس (θ_4). آلترناتیوها (ترکیبات عمل-رخداد) با گروه‌بندی هر یک از سرویس‌های مرکز داده (وبسایت (W)، تجارت الکترونیک (EC)، و پایگاه داده (DB) با دو حالت نقص (دسترسی داخلی (I) و خارجی (E)) و دو منشأ احتمالی (تصادفی (A) و عمدی (D)) ایجاد شدند، این ۱۲ آلترناتیو را نتیجه داد (جدول ۵).

جدول ۵- ارزیابی استنباط متخصص

آلترناتیوها (A_i)	θ_1	θ_2	θ_3	θ_4
W/I/A(A_1)	(650;1000;1300)	(1000;1600;2000)	(350;600;800)	(250;350;450)
W/I/D (A_2)	(250;350;450)	(350;600;800)	(350;600;800)	(650;1000;1300)
W/E/A(A_3)	(250;350;450)	(100;150;200)	(100;150;200)	(100;150;200)
W/E/D(A_4)	(350;600;800)	(350;600;800)	(1000;1600;2000)	(1000;1600;2000)
EC/I/A(A_5)	(350;600;800)	(250;350;450)	(100;150;200)	(250;350;450)
EC/I/D(A_6)	(100;150;200)	(100;150;200)	(250;350;450)	(250;350;450)
EC/E/A(A_7)	(350;600;800)	(250;350;450)	(350;600;800)	(350;600;800)
EC/E/D(A_8)	(250;350;450)	(650;1000;1300)	(350;600;800)	(1000;1600;2000)
DB/I/A(A_9)	(650;1000;1300)	(1000;1600;2000)	(1000;1600;2000)	(350;600;800)
DB/I/D(A_{10})	(1000;1600;2000)	(350;600;800)	(650;1000;1300)	(1000;1600;2000)
DB/E/A(A_{11})	(250;350;450)	(350;600;800)	(350;600;800)	(250;350;450)
DB/E/D(A_{12})	(650;1000;1300)	(1000;1600;2000)	(650;1000;1300)	(1000;1600;2000)

جدول ۶- مقدار مورد انتظار فازی (**FEV**)

آلترناتیوها (A_i)	رتبه‌بندی (معیار لاپلاس)	رتبه‌بندی (استنباط متخصص)
W/I/A(A_1)	4th	6th
W/I/D (A_2)	5th	7th
W/E/A(A_3)	10th	12th
W/E/D(A_4)	3rd	3rd
EC/I/A(A_5)	8th	10th
EC/I/D(A_6)	9th	11th
EC/E/A(A_7)	6th	8th
EC/E/D(A_8)	4th	5th
DB/I/A(A_9)	2nd	4th
DB/I/D(A_{10})	2nd	2nd
DB/E/A(A_{11})	7th	9th
DB/E/D(A_{12})	1st	1st

جدول ۷- رتبه‌بندی آلترناتیوها

آلترناتیوها (A_i)	FEV (معیار لاپلاس)	FEV (استنباط متخصص)
W/I/A(A_1)	(562.5; 887.5; 1137.5)	(541; 842; 1078)
W/I/D (A_2)	(400; 637.5; 837.5)	(430; 674; 882)
W/E/A(A_3)	(137.5; 200; 262.5)	(142; 206; 270)
W/E/D(A_4)	(674; 1100; 1400)	(675; 1100; 1400)
EC/I/A(A_5)	(237.5; 362.5; 475)	(257; 392; 513)
EC/I/D(A_6)	(175; 250; 325)	(175; 250; 325)
EC/E/A(A_7)	(325; 537.5; 712.5)	(328; 545; 723)
EC/E/D(A_8)	(562.5; 887.5; 1137.5)	(622; 978; 1244)
DB/I/A(A_9)	(750; 1200; 1525)	(668; 1072; 1372)
DB/I/D(A_{10})	(750; 1200; 1525)	(808; 1296; 1638)
DB/E/A(A_{11})	(300; 475; 625)	(286; 440; 576)
DB/E/D(A_{12})	(825; 1300; 1650)	(853; 1348; 1706)

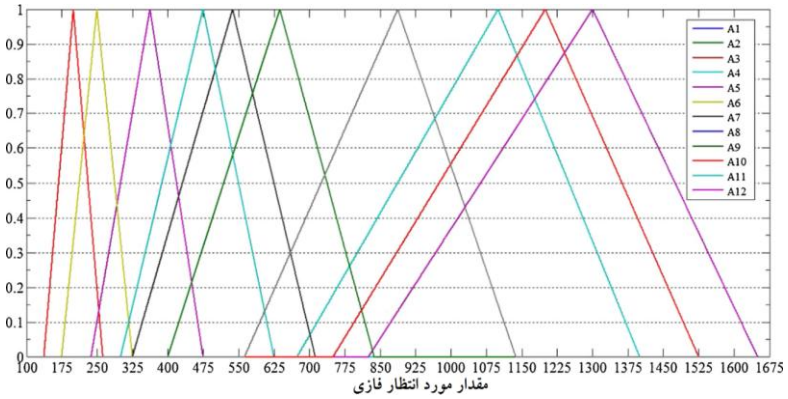
جدول ۴ ارزیابی متخصص از هر جفت آلترناتیو و سناریو را نشان می‌دهد. این ارزیابی با استفاده از مقیاس زبانی ۵ نقطه‌ای از خیلی کم (VL) تا خیلی زیاد (VH) انجام شد.

قضاوت‌های متخصص راجع به زیان‌های مالی آلترناتیوها (اتفاقات احتمالی: ترکیبات عمل-رخداد) برای هر حالت طبیعی (سناریوهای احتمالی) در جدول ۵ آمده است.

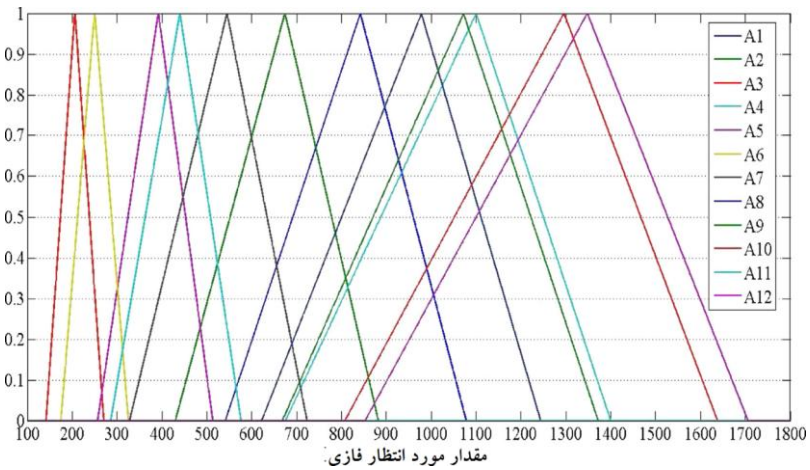
تعریف احتمال پیشین، $\pi(\theta)$، تجربه‌ی متخصص یا داده‌های قبلی مرتبط با حملات مرکز داده را لحاظ می‌کند. چنین فرض شد که متخصص هیچ نفع یا زیانی از جنبه‌های مالی نمی‌برد. برای ارزیابی نظام‌مند بودن مدل پیشنهادی، دو روش برای تعیین $\pi(\theta)$ تحلیل می‌شوند:

روش اول از معیار لاپلاس و روش دوم از تجربه‌ی متخصص استفاده می‌کند. براساس رابطه‌ی (۳)، مقدار مورد انتظار فازی (FEV) (جدول ۶) با استفاده از این روش‌های متفاوت محاسبه شد. در ستون اول، احتمالات با استفاده از معیار لاپلاس با در نظر گرفتن $\pi(\theta_1) = \pi(\theta_2) = \pi(\theta_3) = \pi(\theta_4) = 0.25$ تعریف شدند و در ستون دوم، احتمالات توسط متخصص بیان شدند $\pi(\theta_1) = 0.28,\ \pi(\theta_2) = 0.22, \pi(\theta_3) = 0.14,\ \pi(\theta_4) = 0.36$. اعداد فازی مثلثی متناظر در تصاویر ۶ و ۷ آمده است. تصویر ۷ رتبه‌بندی ارائه‌شده توسط دو روش را نشان می‌دهد. این رتبه‌بندی‌ها براساس رویکرد بیان‌شده توسط (رومل‌فانگر ۲۰۰۳) تعریف شدند.

بنابراین، در نتیجه‌ی بکارگیری این مدل، آلترناتیو A12 (حمله‌ی خارجی عمدی به پایگاه داده) نیاز به افزایش سطح هشیاری برای هر دو سناریو را نشان می‌دهد. با استفاده از معیار لاپلاس، آلترناتیوهای A9 و A10، ریسک یکسانی دارند. از سوی دیگر، بیان اینکه آلترناتیو A10 با استفاده از استنباط متخصص و نیر معیار لاپلاس، دومین مورد پرخطر است، اهمیت دارد. یک نتیجه‌ی مهم دیگر این است که آلترناتیو A3 حمله‌ی خارجی تصادفی به سایت، کم‌خطرترین آلترناتیو برای هر دو روش است.



تصویر ۶- اعداد فازی مثلثی آلترناتیوها – معیار لاپلاسی.



تصویر ۷. اعداد فازی مثلثی – استنباط متخصصین.

۶- کاربرد عددی FMEA

روش پیشنهادی در آزمایشگاه دانشگاه اجرا شد. متخصصی هم مشارکت داشت. مراحل اجرایی مشابه با مراحل نمایش داده شده در شکل ۲ هستند و در زیر ارائه شده‌اند :

مرحله ۱: شناسایی متخصص

ارزیابی‌ها از متخصصان با تجربه در زمینه امنیت اطلاعات با استفاده از قضاوت‌های‌شان حاصل شد، این قضاوت‌ها براساس دانش و تخصص‌شان درباره هر عامل ریسک بود. متخصص می‌تواند مقدار عددی دقیق، بازه مقادیر عددی، عبارت زبان‌شناسی یا عدد فازی فراهم کند. در بسیاری از شرایط، اگر اطلاعات صحیح به دست آید و عامل ریسک به لحاظ کمّی قابل سنجش باشد، احتمالاً متخصص مقدار عددی دقیق یا بازه مقادیر عددی ممکن را فراهم می‌کند. با این حال، گاهی اوقات متخصصان متوجه می‌شوند دادن مقادیر عددی به خاطر عدم‌حتمیت‌های موجود یا بدان خاطر که عامل ریسک به لحاظ کمّی غیرقابل سنجش هستند دشوار است. تحت این شرایط، در ادامه عبارت زبان‌شناسی یا عدد فازی در مدل پیشنهادی استفاده خواهد شد.

مرحله ۲: ارزیابی و تعیین حالت‌های بالقوه شکست

جدول ۸ ارزیابی‌های حالت بالقوه شکست را برای رخداد، شدت و کشف نشان می‌دهد.

مرحله ۳: تعیین عدد فازی RP

جدول ۹ عدد فازی RP را برای هر حالت شکست نشان می‌دهد. در مرحله بعدی، هر بعد را ارزیابی خواهیم کرد.

مرحله ۴: ارزیابی بعد۲

براساس عدد فازی RP برای هر حالت شکست، اکنون می‌توانیم کل عدد فازی RP را برای هر بعد برای مقایسه و رتبه‌بندی آنها با توجه به ریسک‌ها، مطابق با معادله (۵)، محاسبه کنیم. اعداد فازی RP در جدول ۱۰ ارائه شده‌اند.

جدول ۱۰- عدد فازی RP برای هر وجه.

وجه	عدد فازی RP
D1- دسترسی به اطلاعات و سیستم‌ها	(222.875; 336; 673.5; 1296)
D2- امنیت ارتباطات	(436.875; 592; 967; 1600)
D3- زیرساخت	(324.875; 464; 777.5; 1528)
D4- مدیریت امنیت	(237.875; 344; 590; 1096)
D5- توسعه سیستم‌های اطلاعات ایمن	(279.125; 384; 643.5; 1056)

جدول ۱۱- رتبه‌بندی ابعاد.

مرتب‌سازی واسطه	وجه	مقدار
۱	D2- امنیت ارتباطات	۱۲۸۳,۵
۲	D3- زیرساخت	۱۱۵۲,۵
۳	D1- دسترسی به اطلاعات و سیستم‌ها	۹۸۴,۷۵
۴	D5- توسعه سیستم‌های اطلاعات ایمن	۸۴۹,۷۵
۵	D4- مدیریت امنیت	۸۴۳

مرحله ۵: مرتب‌سازی بعد

در نهایت، برای آلفا= ۰,۵، ابعاد مرتب در جدول ۱۱، مطابق مقدار آدامو، ارائه می‌کنیم.

۷- بحث تخصصی این مقاله

در این مقاله، مدلی برای مدیریت ریسک امنیت اطلاعات فرمول‌بندی شده و با استفاده از یک مثال گویای مبتنی بر مرکز داده، به تصویر کشیده شد. این مدل با پرداختن به برخی جنبه‌های حیاتی، در شیوه‌های امنیت اطلاعات، ارزیابی و تحلیل سناریوهای احتمالی، حالت احتمالی نقص و منشأ آنها نقش مهمی دارد. روش ETA برای شناسایی آلترناتیوهای مورد نظر که براساس دسته‌بندی رخدادها و سناریوها تعریف شده بودند، مورد استفاده قرار گرفت و در نتیجه تحلیل ارزیابی ریسک انجام شد. به خوبی می‌دانیم که دانش یک متخصص اغلب زمانی مورد استفاده قرار می‌گیرد که روش ETA استفاده شود، چراکه در اکثر موارد، گردآوری داده، دشوار و یا بسیار هزینه‌بر است. هرچندکه دانش چندین متخصص می‌تواند در مقایسه با دانش یک متخصص واحد، اطلاعاتی با قابلیت اطمینان بالاتر برای مشاهدات فراهم آورد (برای نمونه احتمال یک رخداد)، اما قضاوت‌های متخصص، ماهیت کیفی / زبانی داشته و ممکن است چنانچه اجماعی بین متخصصین صورت نگیرد، ناسازگاری پیش بیاید. افزون بر این، که چارچوب احتمالاتی کلاسیک در پرداختن به مفاهیم مبهم یا ناقص / متناقض، چندان کارآمد نیست. مقالات مشابه از دانش تنها یک متخصص برای فراهم آوردن قضاوت‌های ارزشمند که بیانگر درک و / یا اولویت‌های آن فرد است، استفاده کرده‌اند. براین اساس، شایان ذکر است که احتمالات رخدادهای ETA در این مقاله تعریف نشده است. در نتیجه، اطلاعات کمی از متخصص دریافت می‌شود. در مقابل، متخصص ارزیابی‌هایی در ارتباط با هر جفت آلترناتیو (اتفاقات احتمالی: ترکیبات عمل-رخداد) برای هر حالت طبیعی (سناریوی احتمالی) فراهم خواهد آورد. این ارزیابی توسط متخصصی انجام شد که از مقیاس زبانی ۵ نقطه‌ای از بسیار کم (VL) تا بسیار زیاد (VH) برای دامنه‌ی پولی استفاده می‌کند. متخصص با استفاده از رویکردهای استنباطی، احتمال پیشین $\pi(\theta)$ برای هر یک از حالات طبیعی (و نه احتمال یک رخداد) را بیان می‌کند. لازم به ذکر است این احتمالات پیشین، که توسط متخصص تعریف می‌شوند و آنهایی که از معیار لاپلاس به دست می‌آیند، با نگاهی به ایجاد مدل و ارتقای دقت آن مورد استفاده قرار گرفتند. مثال گویا، که از جنبه‌های مالی تشکیل شده نشان می‌دهد اگرچه تفاوت‌هایی بین احتمالات برای هر دو روش تحلیل وجود دارد، اهمیت آلترناتیوها اساساً یکسان باقی خواهد ماند، این نظام‌مندی طرح پیشنهادی و محتوای آن را نشان می‌دهد. با اینحال یکی از دلایل این اختلاف می‌تواند این باشد که چهار حالت طبیعی به عنوان مسائل امنیت اطلاعات، بسیار متداولند. به علاوه، دو مسئله‌ی احتمالی اصلی از اقدامات عمدی، و نه اقدامات تصادفی ناشی می‌شوند، اینها افزایش تلاش‌ها در پایش داخلی فعالیت‌های سازمان را توجیه می‌کنند، چراکه تبعات ناشی از این اقدامات عمدی معمولاً آسیب‌زایی بالاتری دارند.

۸- نتیجه گیری

در این مقاله با استفاده ۲ روش FMEA و ETA در کنار نظریه‌ی تصمیم‌گیری فازی، یک مدل ریسک امنیت اطلاعات پیشنهاد نمود، در روش تحلیل درخت رویداد که متشکل از چهار گام شناسایی متخصص، مشخص نمودن سناریوها و رخدادها، ارزیابی فازی و مرتب‌سازی است و رویکرد چندوجهی که FMEA و امنیت اطلاعات را با هم ترکیب و به بررسی پنج وجه امنیت اطلاعات می‌پردازد. در روش تحلیل درخت رویداد ، هدف ارزیابی تبعات هر یک از آلترناتیوها در قالب متغیری با درک ساده‌تر (زیان مالی) با در نظر گرفتن حالات طبیعی مختلف (سناریوها) است. برای دستیابی به این هدف، یک طبقه بندی از رخدادها و سناریوها با استفاده از روش ETA تعریف کردیم که به عنوان شالوده‌ای برای تحلیل ریسک عمل نموده و هوشیاری نسبت به سطح تهدیدات حمله به مرکز داده‌ی خارجی را به دنبال دارد. در ادامه هر یک از آلترناتیوها را براساس سطح اهمیت ریسک‌ها، مرتب‌سازی کردیم. با وجود ماهیت مفهومی این مقاله، سهم پژوهشی آن قابلیت فراهم آوردن اطلاعات مرتبط با علل حملات به سیستم‌های اطلاعاتی در بالاترین سطح مدیریتی برای سازمان است. اگرچه این مقاله بر کاربرد مدل برای ارزیابی ریسک امنیت اطلاعات در مرکز داده تمرکز دارد، اما محدود به تنها این حوزه نیست. این مدل را می‌توان در سایر حوزه‌ها که بایستی سیاست‌های امنیت اطلاعات در اولویت قرار گیرند مورد استفاده قرار داد، و نیز در سازمان‌های خصوصی و دولتی قابل اجراست. برای کارهای آتی، کاربرد مدل در سازمان‌های خصوصی / دولتی و استفاده از رویکرد چندمعیاره به منظور گنجاندن سایر معیارها همچون دسترس‌پذیری سرویس‌ها، توصیه می‌شود که می‌توان با استفاده از روش پیشنهادی درخت رویداد انجام داد، این روش بر ایجاد و تحلیل ماتریس‌های غرامت استوار است که اثرات حاصل از ترکیبات مختلف آلترناتیو پاسخ و حالات طبیعی یا سناریوها را نشان می‌دهند و امکان اظهار نظر در خصوص ارزیابی ریسک‌های خاص تک-معیاره و نیز ریسک‌های تجمعی چندمعیاره را فراهم می‌آورند. یک موضوع دیگر برای پژوهش‌های آتی، ارائه‌ی راه‌حل برای به حداقل رسانیدن زیان‌های احتمالی است. برای پژوهش آتی در حوزه تحلیل درخت رویدا ، استفاده از تحلیل ریسک چندبعدی (دی‌المدیا و همکاران، ۲۰۱۵) به منظور گنجاندن سایر معیارها و دستیابی به دیدی وسیع‌تر، توصیه می‌شود. نهایتاً یک دیدگاه دیگر، تحلیل ریسک از منظر متخصصان متعدد است. بستر امنیت اطلاعات، بسیار پیچیده است. در نتیجه برای اینکه بتوانیم دانشی ترکیبی از متخصص‌های متعدد بیرون بکشیم بایستی تا حد امکان تخصصی بیشتری به دست آوریم و نظام‌مندی نحوه‌ی انجام برآوردها را ارتقا بخشیم. رویکرد چندوجهی FMEA پنج وجه پیشنهاد می‌کند که بخش بزرگی از ریسک‌های امنیت اطلاعات موجود است. در ادامه هر حوزه براساس حساسیت ریسک اولویت‌بندی می‌شود، هرچند در این مقاله به دلائل حملات سیستمی می‌پردازد، اما بایستی توجه کرد که تاثیرات/پیامدهای مهم نیز ممکن است در دیدگاه‌های مختلف ظاهر شود، از جمله: تنزل عملکرد در سرورها، ایستگاه‌های کاری یا شبکه‌ها؛ آسیب به سیستم و شبکه؛ نشت اطلاعات یا از بین رفتن اطلاعات (نقض محرمانه بودن تجارت)؛ زیان مالی (هزینه بازیابی اطلاعات)؛ از بین رفتن اعتبار (نقص عملکرد تجاری)؛ و وقفه خدماتی (اختلال در اقدامات تجاری). در نهایت، نقش اصلی این مقاله توانایی برای فراهم کردن اطلاعات در ارتباط با ابعاد حیاتی و شکست‌های برنامه‌های امنیت اطلاعات‌شان برای سازمان است که آسیب‌پذیری را در سیستم‌های‌شان ایجاد می‌کند. علاوه بر این، این مدل ابعاد حساس برنامه‌های امنیت اطلاعات را می‌سنجد.

فهرست منابع مآخذ

References 1:

Information security risk analysis model using fuzzy decision theory

jou rnal h om epage: www.elsevier.com/locate/ijinfomgt

1- Adamo, J. M. (1980). Fuzzy decision trees. Fuzzy Sets and Systems, 4(3), 207–219.

2- Alter, S., & Sherer, S. (2004). A general, but readily adaptable model of informationsystem risk. Communications of the AIS, 14(1), 1–28.

3- Anderson, R. (2001). Why information security is hard: An economic perspective.ACSAC '01: Proceedings of the seventeenth annual computer security applicationsconference (vol. 358) Los Alamitos, CA: IEEE Computer Society, (p. 2001).

4- Anderson, R., & Schneier, B. (2005). Economics of information security. IEEE Securityand Privacy.

5- Andrews, J. D., & Dunnet, S. J. (2000). Event-tree analysis using binary decisiondiagrams. IEEE Transactions on Relialability, 49(2).

6- Bidder, O. R., Arandjelovi´c, O., Almutairi, F., Shepard, E. L. C., Lambertucci, S. A.,Qasem, L. A., et al. (2014). A risky business or a safe BET? A fuzzy set event treefor estimating hazard in biotelemetry studies. Animal Behavior, 93, 143–150.

7- Bojanc, R., & Jerman-Blazic, B. (2008). An economic modelling approach toinformation security risk management. International Journal of InformationManagement, 28, 413–422.

8- Bortolan, S. G., & Degani, R. (1985). A review of some methods for ranking fuzzynumbers. Fuzzy Sets Systems, 15, 1–19.

9- Brender, N., & Markov, I. (2013). Risk perception and risk management in cloudcomputing: results from a case study of Swiss companies. International Journalof Information Management, 33, 726–733.

10- Brito, A. J., & de Almeida, A. T. (2009). Multi-attribute risk assessment for riskranking of natural gas pipelines. Reliability Engineering and Systems Safety, 94,187–198.

11- Chen, S. M., & Sanguansat, K. (2011). Analyzing fuzzy risk based on a new fuzzyranking method between generalized fuzzy numbers. Expert Systems withApplications, 38, 2163–2171.

12- Chen, G., & Zhao, D. (2013). Model of information security risk assessment basedon improved wavelet neural network. Journal of Networks, 8(9).

13- Cheng, C. H. (1998). A new approach for ranking fuzzy numbers by distancemethod. Fuzzy Sets Systems, 95, 307–317.

14- Lo, C.-C., & Chen, W.-J. (2012). A hybrid information security risk assessmentprocedure considering interdependences between controls. Expert Systemswith Applications, 39, 247–257.

15- Clifton, A., & Ericson, I. I. (2005). Hazard analysis techniques for system safety. NewYork: John Wiley & Sons.

16- Cooke, R. M., ElSaadany, S., & Huang, X. (2008). On the performance of socialnetwork and likelihood-based expert weighting schemes. ReliabilityEngineering & System Safety, 93(5), 745–756.

17- Destercke, S., & Couso, I. (2014). Ranking of fuzzy intervals seen through theimprecise probabilistic lens. Fuzzy Sets and Systems (accessed 24.12.14.).

18- Dubois, D., & Prade, H. (1980). Fuzzy sets systems: theory and applications. NewYork: Academic Press.

19- Dzazali, S., Sulaiman, A., & Zolait, A. H. (2009). Information security landscape andmaturity level: case study of Malaysian public service (MPS) organizations.Government Information Quarterly, 26, 584–593.

20- Ekel, P. Ya., & Schuffner Neto, F. H. (2006). Algorithms of discrete optimization andtheir application to problems with fuzzy coefficients. Information Sciences, 176,2846–2868.

21- Ekel, P. Ya., Pedrycz, W., & Schinzinger, R. (1998). A general approach to solving awide class of fuzzy optimization problems. Fuzzy Sets and Systems, 97, 49–66.

22- Ekel, P. Ya., Martini, J. S. C., & Palhares, R. M. (2008). Multicriteria analysis indecision making under information uncertainty. Applied Mathematics andComputation, 200, 501–516.

23- Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for informationsystems: causal relationships of risk factors and vulnerability propagationanalysis. Information Sciences, 256, 57–73.

24- Feng, N., & Li, V. (2011). An information systems security risk assessment modelunder uncertain environment. Applied Software in Computetrs, 11(7),4332–4340.

25- Ferdous, R., Khan, F., Sadiq, R., Amyotte, P., & Veitch, B. (2009). Handling datauncertainties in event tree analysis. Process Safety and EnvironmentalProtection, 87(5), 283–292.

26- Grant, K., Edgar, D., Sukumar, A., & Meyer, M. (2014). Risky business: perceptionsof e-business risk by UK small and medium sized enterprises (SMEs).International Journal of Information Management, 34, 99–122.

27- Hong, E.-S., Lee, I.-M., Shin, H.-S., Nam, S.-W., & Kong, J.-S. (2009). Quantitative riskevaluation based on event-tree analysis technique: application to the design ofshield TBM. Tunnelling and Underground Space Technology, 24(3), 269–277.

28- Jain, R. (1976). Decision making in the presence of variables. IEEE Transactions onSystems Man and Cybernetics, 6, 698–703.

References 2:

A multidimensional approach to information security riskmanagement using FMEA and fuzzy theoryMaisa

jou rnal h om epage: www.elsevier.com/locate/ijinfomgt

1- Abbasbandy, S. (2009). Ranking of fuzzy numbers, some recent and new formulas.In Proceedings of IFSA-EUSFLAT 2009 (pp. 642–646).

2- Adamo, J. M. (1980). Fuzzy decision trees. Fuzzy Sets and Systems, 4(3), 207–219.

3- Bang, Y., Lee, D.-Y., Bae, Y.-S., & Ahnc, J.-H. (2012). Improving information securitymanagement: An analysis of ID–password usage and a new login vulnerabilitymeasure. International Journal of Information Management, 32, 409–418.

4- Bellman, R. E., & Zadeh, L. A. (1970). Decision making in a fuzzy environment. Man-agement Science, 17, 4.

5- Belohlavek, R., & Klir, G. J. (2011). Concepts and fuzzy logic. Cambridge MA: The MITPress.

6- Belton, V., & Stewart, T. J. (2002). Multiple criteria decision analysis: An integratedapproach. Dordrecht, Netherlands: Kluwer Academic Publishers.

7- Bojadziev, G., & Bojadziev, M. (2007). Fuzzy logic for business, finance and management(2nd ed.). Inc. River Edge, NJ, USA: World Scientific Publishing Company.

8- Bojanc, R., & Blazic, B. J. (2008). An economic modelling approach to informationsecurity risk management. International Journal of Information Management, 28,413–422.

9- Brunelli, M., & Mezei, J. (2013). How different are ranking methods for fuzzy num-bers? A numerical study. International Journal of Approximate Reasoning, 54,627–639.

10- Chen, G., & Zhao, D. (2013). Model of information security risk assessment based onimproved wavelet neural network. Journal of Networks, 8.

11- Deursen, N. V., Buchanan, W. J., & Duff, A. (2013). Monitoring information securityrisks within health care. Computers & Security, 37, 31–45.

12- Dubois, D., & Prade, H. (1998). An introduction to fuzzy sets. Clinica Chimica Acta,70(1), 3–29.

13- Geum, Y., Cho, Y., & Park, Y. (2011). A systematic approach for diagnosing service fail-ure: Service-specific FMEA and grey relational analysis approach. Mathematicaland Computer Modelling, 54, 3126–3142.

14- Goodman, S.L. (1996). Design for Manufacturability at Midwest Industries, HarvardBusiness School, February 2, Lecture.Hoo, K. S. (2000). How much is enough? A risk-management approach to computersecurity (Working Paper).

Palo Alto, CA: Consortium for Research on InformationSecurity and Policy (CRISP), Stanford University.

15- Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study ofinformation systems security effectiveness. International Journal of InformationManagement, 23, 139–154.

16- Li, M., & Tang, M. (2013). Information security engineering: A framework for researchand practices. International Journal of Computers Communications, 8, 578–587.

17- Lin, Q.-L., Wand, D.-J., Lin, W.-G., & Liu, H.-C. (2014). Human reliability assessment formedical devices based on failure mode and effects analysis and fuzzy linguistictheory. Safety Science, 62, 248–256.

18- Liu, H. C., Liu, L., Liu, N., & Mao, L. X. (2012). Risk evaluation in failure mode andeffects analysis with extended VIKOR method under fuzzy environment. ExpertSystems with Applications, 39, 12926–12934.

19- Ozkan, S., & Karabacak, B. (2010). Collaborative risk method for information securitymanagement practices: A case context within Turkey. International Journal ofInformation Management, 30, 567–572.

20- Pam, E. D., Li, K. X., Wall, A., Yang, Z., & Wang, J. (2013). A subjective approach forballast water risk estimation. Ocean Engineering, 61, 66–76.

21- Patel, S. C., Graham, J. H., & Ralston, P. A. S. (2008). Quantitatively assessing the vul-nerability of critical information systems: A new method for evaluating securityenhancements. International Journal of Information Management, 28, 483–491.

22- Pedrycz, W., Ekel, P., & Parreiras, R. (2011). Fuzzy multicriteria decision-making: Mod-els methods and applications. John Wiley and Sons.

23- McDemortt, R. E., Mikulak, R. J., & Beauregard, M. R. (2008). The basics of FMEA (2nded.). New York: Taylor & Francis Group.

24- Rommelfanger, H. J. (2003). Fuzzy decision theory intelligent ways for solving real-world decision problems and for solving information costs. In G. Della Riccia, R.Kruse, D. Dubois, & H.-J. Lenz (Eds.), Planning based on decision theory (Vol. 472).CISM International Centre for Mechanical Sciences.

25- Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abusein organizations: A field study. MIS Quarterly, 14(1), 45–60.

چکیده انگلیسی

ENGLISH ABSTRACT

In this paper, using an FMEA and ETA method, along with the fuzzy decision-making theory, we proposed an information security risk model. In an event tree method, which consists of four steps of expert identification, identifying scenarios and events, fuzzy evaluation, and Sorting is a multi-faceted approach that combines FMEA and information security to examine five aspects of information security. In Event tree analysis, the objective of evaluating the consequences of each alternate is in the form of a variable with a simpler understanding (financial loss) with different natural scenarios (scenarios). To achieve this, we have defined a classification of events and scenarios using the ETA method, which serves as a basis for risk analysis and leads to an awareness of the threat level of the attack on the external data center.

We then sorted each of the alternatives based on the importance of the risks. Despite the conceptual nature of this article, its research contribution is the ability to provide information related to the causes of attacks on information systems at the highest level of management for the organization. Although this article focuses on the application of the model for assessing data security risk in the data center, it is not limited to this area alone. This model can be used in other areas where information security policies should be prioritized, as well as in private and public organizations. For future work, the application of the model in private / public organizations and the use of multi-criteria approach to include other criteria such as availability of services is recommended, which can be done using the proposed tree-event method, this The method is based on the creation and analysis of compensation matrices, which shows the effects of different alternatives, responses, and scenarios, and the possibility of commenting on the assessment of individual single-risk specific risks as well as multi-criteria cumulative risk Provide. Another issue for future research is to provide a solution to minimize potential losses. For future research in the field tree analysis, the use of multidimensional risk analysis (Dialalia et al., 2015) is recommended in order to include other criteria and achieve a broader view. Finally, a different perspective is the risk analysis from the perspective of many specialists. The information security platform is very complicated. As a result, in order to be able to extract a combination of different experts, we should get as much specialized expertise as possible and improve the systematic way of performing the estimates. The FMEA Multidisciplinary approach suggests that a large part of the information security risk is available. Each domain is prioritized on the basis of risk sensitivity, although in this article the reasons for systemic attacks are addressed, but it should be noted that important influences may also appear in different perspectives, including degrading performance on servers, workstations, or networks. ; Damage to the system and network; information leakage or loss of information (breach of trade secrecy); financial loss (information retrieval); loss of credit (business failure); and service interruption (disturbance in business practices). Finally, the main role of this article is the ability to provide information about critical dimensions and failures of their information security programs for the organization, which creates vulnerabilities in their systems. In addition, this model measures the sensitive dimensions of information security programs.