نشریه علمی مطالعات مدیریت کسب و کار هوشمند- سال هشتم ـ شماره ۳۱ ـ بهار ۱۳۹۹
صفحات ۹۴- ۶۱
10.22054/IMS.2020.43633.1531

مدل ریاضی انتخاب راهکارهای امنیتی در فرآیندهای کسب‌وکار

سید احسان ملیحی*
سمانه صدیقی**

چکیده

فرآیندهای کسب‌وکار نقشی کلیدی در کسب مزیت رقابتی سازمان‌ها دارند. اجرای بدون توقف عملیات روزمره فرآیندها که ناشی از افزایش امنیت فرایندهای کسب‌وکار است، به‌عنوان یکی از شاخص‌های مهم کیفیت فرآیندهای کسب‌وکار در نظر گرفته می‌شود. هرچند افزایش سطح امنیت در سازمان‌ها، هزینه‌های ناشی از نقص امنیت را کاهش می‌دهد اما در مقابل هزینه‌های مستقیم و غیرمستقیم استقرار ویژگی‌های امنیتی را به سازمان تحمیل می‌کند. در این پژوهش برای حل این مسئله مدیریتی، مدلی ریاضی ارائه شده است تا با هدف بیشینه‌سازی سطح امنیت و کمینه‌سازی هزینه‌های استقرار، تصمیم بهینه برای انتخاب راهکارهای امنیتی از بین گزینه‌های موجود برای هر فعالیت در فرآیند کسب‌وکار را مشخص کند. بخش‌های مختلف مدل با استفاده از مطالعه ادبیات نظری و مطالعه موردی فرآیند خرید الکترونیکی شناسایی شد. سپس مثالی عددی در چهارچوب مدل ارائه شده با استفاده از الگوریتم ژنتیک حل شد و نتایج حل مدل با نتایج راهکارهای انتخاب‌شده توسط گروهی از متخصصین مورد مقایسه قرار گرفت. نتایج این مقایسه بیانگر برتری جواب مدل نسبت به جواب خبرگان بود.

کلیدواژگان: فرآیندهای کسب‌وکار، ویژگی‌های امنیتی، کیفیت فرآیندهای کسب‌وکار، مدیریت فرآیندهای کسب‌وکار امن.

---

*عضو هیئت‌علمی، گروه مهندسی صنایع، دانشکده فنی و مهندسی، دانشگاه خوارزمی، تهران.(نویسنده مسئول)؛ Malihi@khu.ac.ir
** کارشناسی ارشد، مهندسی صنایع، دانشکده فنی و مهندسی، دانشگاه آزاد اسلامی- تهران شمال، تهران.

تاریخ دریافت: ۱۳۹۸/۰۳/۱۵ **تاریخ پذیرش:** ۱۳۹۸/۱۰/۳۰

مقدمه

نیاز روزافزون سازمان‌ها در پاسخ سریع به تغییرات محیطی و تداوم بهبود کیفیت، باعث توجه روزافزون آن‌ها به رویکرد فرآیند گرایی شده است (هروی‌زاده[1]، ۲۰۰۹؛ حیدری و لوکپلس[2]، ۲۰۱۴). نگاه به موضوعات و مسائل سازمان با رویکرد فرآیندی باعث می‌شود تا به‌جای نگاه‌های بخشی، تصمیم‌ها در نگاهی کلان اتخاذ شوند. در این رویکرد، عملکرد هر تصمیم در سازمان با در نظر گرفتن تأثیر آن بر نتیجه مورد انتظار مشتری فرآیند، مدیریت می‌شود (هارویکوزا[3]، ۲۰۱۲). تصمیم‌گیری در مورد کیفیت فعالیت‌های سازمان، یکی از موضوعاتی است که در سال‌های اخیر با رویکرد فرآیندی تحت عنوان مدیریت کیفیت فرآیندهای کسب‌وکار مورد توجه سازمان‌ها و محققین قرار گرفته است (هروی‌زاده، ۲۰۰۹). مدیریت کیفیت فرآیندهای کسب‌وکار، یک رویکرد ساختاریافته با هدف بهبود کیفیت محصول و خدمات است که فرآیندهای سازمان را با استراتژی سازمان همسو کرده و به‌موازات آن رضایت مشتری را با افزایش کیفیت، بهبود می‌دهد (هارویکوزا، ۲۰۱۲). کیفیت در فرآیندهای کسب‌وکار را می‌توان از چهار منظر عملکرد، ورودی/خروجی، منابع انسانی و منابع غیرانسانی مورد بررسی قرار داد (هروی‌زاده و همکاران، ۲۰۰۹). در هر یک از چهار منظر موضوعات مختلفی مانند قابلیت اطمینان، اثربخشی، بهره‌وری، به‌روز بودن و ... به‌عنوان ابعاد کیفیت فرآیند در نظر گرفته می‌شوند.

یکی از موضوعات در حوزه کیفیت فرآیند، امنیت است که با توجه به توسعه تبادلات الکترونیکی و کسب‌وکارهای اینترنتی و همچنین تهدیدات تروریستی، اهمیتی بیش‌ازپیش پیدا کرده است و تحت عنوان امنیت در فرآیندهای کسب‌وکار مورد بررسی قرار گرفته است (پیکام و سلیمی فر، ۱۳۹۵؛ هروی‌زاده و همکاران، ۲۰۰۹ ؛ نور و روهریگ[4]، ۲۰۰۱). افزایش سطح امنیت فرآیندهای کسب‌وکار به‌خصوص در کسب‌وکارهای الکترونیکی، می‌تواند از خسارت‌های قابل‌توجهی که انتظار می‌رود تا سال ۲۰۲۱ به ۶ تریلیون دلار برسد، بکاهد

1. Heravizadeh
2. Loucopoulos
3. Hajkova
4. Knorr and Rohrig

(گارتنر[1]، ۲۰۱۶). افزایش سطح امنیت فرآیندهای کسب‌وکار ازآنجاکه امکان دسترسی غیرمجاز به منابع، داده‌ها و اطلاعات و کنترل اجرای فعالیت‌ها را کاهش می‌دهد (هروی‌زاده و همکاران، ۲۰۰۹)، امکان بروز فعالیت‌های خرابکارانه و تروریستی را نیز کاهش می‌دهد (کدرسکی[2]، ۲۰۰۰).

از دیدگاه امنیت، فرآیندهای کسب‌وکار در سه وضعیت امن، ناامن یا در حالت بازیابی بین این دو موقعیت قرار می‌گیرند. در وضعیت امن، فرآیند به‌صورت معمول در حال فعالیت است. حالت ناامن زمانی به وجود می‌آید که یک حادثه امنیتی رخ دهد و حالت بازیابی، اقدامات لازم و ضروری را قبل از اینکه فرآیند دوباره در حالت امن قرار گیرد را نشان می‌دهد. سازمان‌ها تلاش می‌کنند تا با به‌کارگیری مکانیسم‌های امنیتی در طول فرآیند، امنیت فرآیند را حفظ نموده یا مدت‌زمان بازیابی فرآیندهای خود از حالت ناامن به امن را کوتاه کنند (ولتر و رینکل[3]، ۲۰۱۰). هر مکانیسم امنیتی که از بین گزینه‌های مختلف برای هر یک از فعالیت‌های فرآیند انتخاب می‌شود، باعث می‌شود تا ویژگی‌های امنیتی کل فرآیند مانند محرمانگی، یکپارچگی، کنترل دسترسی و ... دستخوش تغییر قرار گیرند و در نهایت سطح امنیت کل فرآیند ارتقا یابد (الشافی و بوتویچ[4]، ۲۰۱۲)؛ اما استقرار هر مکانیسم امنیتی در کنار ارتقا سطح امنیت کل فرآیند باعث می‌شود تا هزینه‌های اجرای فرآیند، به دلایل مختلف مانند هزینه‌های ایجاد مکانیسم امنیتی و هزینه‌های نگهداری و تعمیرات آن‌ها و همچنین تأثیرگذاری مکانیسم‌های امنیتی در افزایش پیچیدگی‌های اجرای فرآیند، افزایش پیدا کند. ازاین‌رو لازم است با در نظر گرفتن محدودیت‌های اجرایی در استقرار مکانیسم‌های امنیتی در فرآیندهای کسب‌وکار مانند محدودیت هزینه و سطح امنیتی مورد انتظار، توازنی بین هزینه‌های ناشی از افزایش امنیت و هزینه‌های بالقوه ناشی از نقض امنیتی که به فرآیند وارد می‌شود، برقرار گردد تا ضمن رسیدن به یک سطح قابل‌قبول از امنیت، میزان هزینه‌ها نیز کاهش یابد (اولوفسون[5]،۱۹۹۲). هدف از این

1. www.gartner.com
2. Kedrosky
3. Wolter and Reinecke
4. Elshaafi and Botvich
5. Olovsson

مقاله پاسخ به این سؤال است که مکانیسم‌های امنیتی در کدام‌یک از فعالیت‌های فرآیند مستقر شود تا ضمن افزایش امنیت در بالاترین سطح مورد انتظار، هزینه‌های ایجاد امنیت و خسارات ناشی از نبود امنیت نیز حداقل گردد.

نوآوری و مشارکت علمی این مقاله در ادبیات موضوع در مقایسه با تحقیقات پیشین، ارائه مدل کمی برای "ایجاد توازن بهینه میان سطح امنیت و میزان هزینه در چهارچوب فرآیندهای کسب‌وکار" است. هرچند طبق نظر اولوفسون (۱۹۹۲)، به ازای افزایش سطح امنیت در سازمان‌ها، هزینه‌های ناشی از نقض امنیت کاهش و هزینه‌های ایجاد مکانیسم‌های امنیتی افزایش می‌یابد و بایستی به سطح بهینه از امنیت و هزینه رسید که ضمن دست یافتن به سطح امنیت قابل‌قبول، میزان هزینه‌ها نیز کاهش یابد؛ اما در تمام تحقیقات بررسی‌شده در سال‌های بعد، مدلی که به‌صورت کاربردی رسیدن به سطح بهینه از امنیت و هزینه را با انتخاب راهکارهای امنیتی مدل‌سازی کند، ارائه نشده است. در پیشینه ادبیات عموم تحقیقات به چگونگی در نظر گرفتن امنیت در متدولوژی‌های مدیریت فرآیند کسب‌وکار یا چگونگی به‌کارگیری الزامات امنیتی در سیستم‌های مدیریت گردش کار و تجزیه‌وتحلیل ریسک فرآیند کسب‌وکار از منظر اقتصادی در صورت نبود مکانیسم‌های امنیتی در فرآیند پرداخته شده است.

در بخش دوم، پیشینه ادبیات مرتبط با امنیت در فرآیندهای کسب‌وکار مورد بررسی قرار گرفته است. در بخش سوم مدل مفهومی تعیین نقاط بهینه برای استقرار مکانیسم‌های امنیتی در طول فرآیند ارائه شده است و بر اساس آن در بخش چهارم مدل ریاضی تصمیم‌گیری تعیین مکان این نقاط در فرآیند کسب‌وکار با توجه به تأثیرگذاری در ایجاد هزینه و ارتقا سطح امنیت در کل فرآیند، ضمن در نظر گرفتن محدودیت‌های موجود، ارائه شده است. در بخش پنجم، مدل ریاضی ارائه شده، بر اساس داده‌های واقعی از فرآیند خرید الکترونیکی یک فروشگاه اینترنتی به کار گرفته شده و نتایج به‌دست‌آمده از طریق مقایسه خروجی‌های مدل ریاضی با نظر خبرگان اعتبارسنجی شده است. در بخش پنج، نتیجه‌گیری و تحقیقات پیش رو ارائه شده است.

پیشینه پژوهش

اگرچه با افزایش نفوذ اینترنت و تجارت الکترونیک در کسب‌وکارها و الکترونیکی شدن فرآیندهای کسب‌وکار، تهدیدات امنیتی بالقوه افزایش یافته است، اما ارزش اجرای حفاظت‌های امنیتی هنوز به‌صورت شایسته مورد توجه قرار نگرفته است. لذا در نظر گرفتن حفاظت‌های امنیتی در متدولوژی‌های مدیریت فرآیند کسب‌وکار به‌عنوان یک موضوع مهم، برای کاهش شکاف بین امنیت فناوری اطلاعات و مدیریت فرآیندهای کسب‌وکار، مورد توجه محققین قرار گرفته است (کمبل و همکاران[1]، ۲۰۰۳). محققینی مانند هرمن و پرنول[2] (۱۹۹۸)، هرمن و پرنول (۱۹۹۹) و رایم[3] و همکاران (۱۹۹۹) بر مدل‌سازی معانی امنیت[4] فرآیندهای کسب‌وکار تمرکز کرده‌اند. در هرمن و پرنول (۱۹۹۸) بررسی میزان الزامات امنیتی در جریان مدیریت گردش‌کار و اجزای یک گردش‌کار توسط اقدامات امنیتی مورد بررسی قرار گرفته است. در تحقیق هرمن و پرنول(۱۹۹۹) با توجه به اهمیت امنیت و یکپارچگی به‌عنوان عامل اصلی موفقیت در تجارت الکترونیک، چارچوبی برای در نظر گرفتن یکپارچه الزامات امنیتی از پنج دیدگاه مختلف در فرآیندهای کسب‌وکار ارائه شده است. در تحقیق رایم و همکاران(۱۹۹۹) برای مدل‌سازی معاملات امن کسب‌وکار، چهارچوبی با یک زبان خاص به‌عنوان ALMOST[5] ارائه کرده‌اند. در تحقیقی دیگر، نور و روهریگ (۲۰۰۱) با ارائه چهارچوبی به تحلیل نیازهای امنیتی در فرآیندهای کسب‌وکار در تجارت الکترونیک پرداخته‌اند. ماهیت این چارچوب به‌منظور در نظر گرفتن نیازهای ناهمگون امنیتی، بازطراحی شده است. مهم‌ترین ابعاد این چارچوب، اجزا تحت تأثیر در فرآیند و اهداف امنیتی مشتمل بر محرمانه بودن، یکپارچگی، دسترسی و پاسخگویی است. آن‌ها سپس چارچوب POSeM[6] را به‌منظور توصیف مناسب حفاظت‌های امنیتی در فرآیندهای کسب‌وکار معرفی کردند که به اختصاص سطوح امنیتی به اجزای مختلف فرآیند کسب‌وکار مانند بازیگران، خروجی‌ها و

1. Campbell et al.
2. Herrmann and Pernul
3. Rohm
4. Modeling Security Semantics
5. A Language for Modelling Secure Business Transactions
6. Process-Oriented Security Model

فعالیت‌ها با یک زبان توصیفی می‌پردازد (نور و روهریگ ، ۲۰۰۴). بکس و همکاران[1] (۲۰۰۳) یک روش برای ادغام نیازهای امنیتی دلخواه در توسعه فرآیندهای کسب و کار ارائه کرده‌اند که بر ترکیب رمزنگاری در فرآیندهای کسب‌وکار تأکید دارد

برخی از تحقیقات از نمودارهای uml[2] به‌منظور تسهیل اجرای الزامات امنیتی در فرآیندهای کسب‌وکار استفاده نموده‌اند. جورجنس[3] (۲۰۰۲) در همین زمینه گسترش UMLsec[4] را برای پشتیبانی از توسعه سیستم‌های امن معرفی کرده است. در ادامه رودریگز[5] و همکاران (۲۰۰۶) یک نمودار UML 2.0 برای مدل‌سازی فرآیندهای کسب و کار ایمن ارائه کرده‌اند. بیسن و همکاران[6] (۲۰۰۶) نیز یک رویکرد جدید برای ایجاد سیستم‌های امنیتی ارائه داده‌اند که آن را "مدل مبتنی بر امنیت[7] " می‌نامند. مک‌دمرت و فاکس[8] (۱۹۹۹) از نمودارهای UML به‌عنوان پایه‌ای برای الگوهای مرتبط با امنیت بهره برده‌اند و از آن‌ها برای نمایش و تجزیه‌وتحلیل نیازهای امنیتی استفاده کرده‌اند. در این تحقیق نمودارهای موارد کاربری[9]، تعامل بین بازیگران و فرآیند برای اصلاح موارد سوءاستفاده[10] و بازگشت فرآیند به حالت استاندارد نشان داده شده است. سیندر[11] (۲۰۰۰) رویکرد مشابهی را برای شناسایی نیازهای امنیتی مبتنی بر "نمودار موارد کاربری " ارائه داده‌اند. هرمن و هرمن[12] (۲۰۰۶) یک چارچوب جامع برای تحلیل نیازهای امنیتی فرآیندهای کسب و کار به نام چارچوب مدل‌سازی معناشناسی امنیت فرآیندهای کسب و کار[13] (MoSSBP) را مطرح کردند که در آن چهار لایه

1. Backes
2. Unified Modeling Language
3. Jurjens
4. Unified Modeling Language Security
5. Rodriguez
6. Basin
7. Model Driven Security
8. McDermott and Fox
9. Use Cases
10. Abuse Cases
11. Sindre
12. Herrmann and Herrmann
13. Modeling Security Semantics of Business Processes

مخزن را که حاوی مفاهیم گرافیکی از الزامات امنیتی و مدل‌های مرجع هستند را مشخص می‌کنند.

گروهی از تحقیقات با برداشتن یک گام فراتر، با هدف کاربردی نمودن الزامات امنیتی در فرآیندهای کسب‌وکار، در چگونگی به‌کارگیری الزامات امنیتی در سیستم‌های مدیریت گردش‌کار پرداخته‌اند. در این زمینه الوری [1](۲۰۰۱) به خلأ تحقیقاتی در این حوزه اشاره کرده و بیان می‌کند که اکثر سیستم‌های گردش کار تجاری، ویژگی‌های امنیتی مانند احراز هویت را نادیده می‌گیرند و نیازهای امنیتی که باید برای ساخت سیستم‌های گردش کار ایمن مورد توجه قرار گیرد را توصیف می‌نماید. کیندلر و سویی[2] (۱۹۹۶) نیز ویژگی کنترل دسترسی در سیستم‌های مدیریت گردش کار را توصیف می‌کند و بر تکمیل محافظت‌های امنیتی در سیستم‌های جریان کاری موجود تمرکز کرده است. ریبریو و گودس[3] (۱۹۹۹) یک تحلیل‌گر[4] را برای بررسی خودکار انسجام بین مشخصات گردش کاری و سیاست‌های امنیتی سازمان ارائه می‌دهد. این تحلیل‌گر فرآیندهای گردش کار را با استفاده از زبان توصیف فرآیند گردش کار[5] (WPDL) و سیاست‌های امنیتی را از طریق یک زبان سیاست امنیتی خاص[6] (SPL) و همچنین اجازه، ممنوعیت یا شکل خاصی از تعهد را توصیف می‌نماید. این رویکرد بر تعریف رسمی یک سیاست کنترل دسترسی تمرکز دارد.

ازآنجاکه اجرای الزامات امنیتی در فرآیندهای کسب و کار به‌عنوان یک سرمایه‌گذاری در نظر گرفته می‌شود (وظیفه و همکاران،۱۳۹۷)، تحقیقاتی در این زمینه نیز در ادبیات موضوع دیده می‌شود. لگزیان و موسوی (۱۳۹۷) رویکردهای سرمایه‌گذاری در امنیت اطلاعات را مورد بررسی قرار داده‌اند. یکی از اولین روش‌ها، انجام تجزیه‌وتحلیل ریسک توسط ضرر سالیانه مورد انتظار[7] (ALE) بود (موسسه ملی استانداردها و تکنولوژی[8]، ۱۹۹۲). "نبود داده‌های تجربی

1. Atluri
2. Kindler and Soyez
3. Ribeiro and Guedes
4. Analyzer
5. Workflow Process Description Language
6. Security Policy Language
7. Annual Loss Expectancy
8. NIST(National Institute of Standards and Technology)

درباره تکرار وقوع حملات و پیامدهای مرتبط با آن " و "فرض برابر بودن هزینه تمام نقض‌های امنیتی "، دو محدودیت اصلی در این روش است. تجزیه‌وتحلیل هزینه و منفعت[1] (CBA) روش دیگری است که برای اندازه‌گیری ارزش اجتماعی خالص[2] اجرای برنامه‌های امنیتی ارائه شده است (تامپسن[3]، ۱۹۸۰). در تحقیق ماکری[4] (۲۰۰۳) روش‌های متداول مانند، پروژه مدل‌سازی تجزیه‌وتحلیل هزینه‌های حادثه[5] (ICAMP)، نرخ بازده داخلی[6] (IRR) و حداکثر ارزش فعلی خالص[7] (NPV) ارزیابی شده است. هرچند این تحقیقات روش‌هایی برای ارزیابی ارزش سرمایه‌گذاری در امنیت فرآیندهای کسب و کار ارائه می‌دهند، اما رسیدن به سطح مشخصی از امنیت به‌عنوان یک متغیر تصمیم، مدنظر قرار نمی‌گیرد. به‌عبارت‌دیگر این تحقیقات با فرض یک سطح مشخص از امنیت، روش‌هایی برای ارزش سرمایه‌گذاری در امنیت به سازمان‌ها ارائه می‌کنند و تأثیر متقابل هزینه و سطح امنیت مورد بررسی قرار نمی‌گیرد (مرسلی و همکاران[8]، ۲۰۰۷).

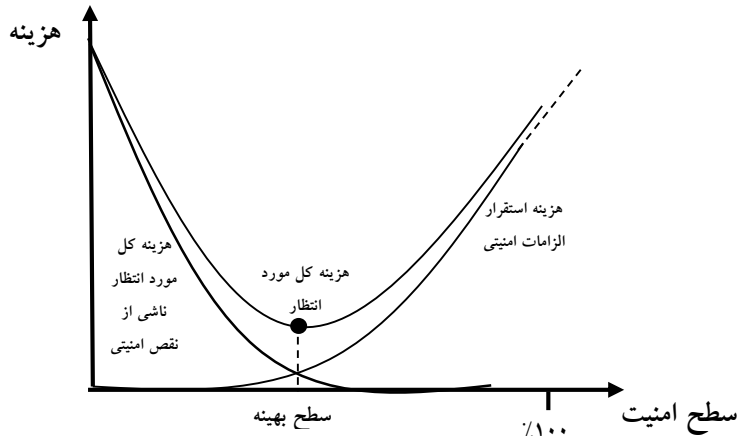
هروی‌زاده و همکاران (۲۰۰۹) و حیدری و لوکپلس (۲۰۱۴) چهارچوب‌هایی برای تبیین ابعاد کیفیت در فرآیندهای کسب و کار ارائه کرده‌اند که امنیت و هزینه را به‌عنوان بخشی از ابعاد کیفیت فرآیندهای کسب و کار معرفی کرده‌اند. هرچند تحقیقات متعددی مانند تحقیقات گوان و همکاران[9] (۲۰۱۴)، مرسلی و همکاران (۲۰۰۷) و ولتر و رینکل (۲۰۱۰) در زمینه تبیین رابطه امنیت با ابعاد دیگر کیفیت فرآیندهای کسب‌وکار صورت گرفته است، اما در زمینه رابطه امنیت و هزینه به‌عنوان دو بعد مهم کیفیت فرآیندهای کسب‌وکار، تحقیقات معدودی مانند تحقیق اولوفسون(۱۹۹۲) انجام شده است. اولوفسون بیان می‌کند به ازای افزایش سطح امنیت در سازمان‌ها، هزینه‌های ناشی از نقض امنیت کاهش و هزینه‌های ایجاد مکانیسم‌های امنیتی افزایش می‌یابد، بنابراین بایستی به سطح بهینه از امنیت و هزینه رسید که

1. Cost-Benefit analysis
2. Net Social Value
3. Thompson
4. Mercuri
5. Incident Cost Analysis Modeling Project
6. Internal Rate of Return
7. Net Present Value
8. Morselli et al.
9. Guan

ضمن دست یافتن به سطح امنیت قابل‌قبول، میزان هزینه‌ها نیز کاهش یابد. بررسی ادبیات موضوع در محدوده مشاهدات نویسندگان این مقاله، نشان می‌دهد موضوع "ایجاد توازن بهینه میان سطح امنیت و میزان هزینه در چهارچوب فرآیندهای کسب و کار" یکی از زمینه‌هایی است که می‌تواند به‌عنوان خلأ تحقیقاتی مورد توجه قرار گیرد. لذا در این مقاله مدلی ریاضی ارائه شده است تا با هدف بیشینه‌سازی سطح امنیت و کمینه‌سازی هزینه‌های استقرار مکانیسم‌های امنیتی، تصمیم بهینه برای انتخاب مکانیسم‌های امنیتی از بین گزینه‌های موجود برای هر فعالیت در فرآیند را اتخاذ کند.

مبانی نظری

الزامات امنیتی در فرآیندها، متناسب با نوع و کارکرد فعالیت‌های فرآیند تعیین می‌شوند. به‌عنوان نمونه الزامات امنیتی نقل‌وانتقال الکترونیکی وجوه، متناسب با نوع و مقدار پرداخت می‌تواند متفاوت باشد. متناسب با سطح به‌کارگیری الزامات امنیتی در فعالیت‌های مختلف فرآیندها، سطح امنیت فرآیند می‌تواند از مقیاس صفر یعنی کاملاً ناامن تا یک یعنی امنیت کامل تغییر کند. نفوذ اخلال‌گران به فرآیندهای امن و تحت تأثیر قرار دادن عملکرد فعالیت مستلزم صرف زمان و هزینه زیادی است که باعث می‌شود تا از نفوذ آن‌ها پیش‌گیری شود. هرچند افزایش سطح امنیت باعث می‌شود تا از بروز هزینه‌های بالقوه ناشی از نفوذ و اخلال فرآیند جلوگیری شود، اما از طرف دیگر باعث می‌شود تا هزینه‌های ایجاد الزامات امنیتی در فرآیند افزایش یابد. هزینه کسب و استقرار الزامات امنیتی، هزینه‌های مورد نیاز برای تعمیر و نگهداری نرم‌افزارها و سخت-افزارهای الزامات امنیتی، هزینه‌های ناشی از افزایش پیچیدگی و یا هزینه‌های احتمالی ناشی از کند شدن فرآیند به دلیل رعایت الزامات امنیتی، نمونه‌هایی از هزینه‌های ناشی از ایجاد الزامات امنیتی در فرآیند هستند. برخی از این هزینه‌ها به طریقی پیچیده با یکدیگر در ارتباط هستند. ممکن است رسیدن به یک سطح بالا از امنیت، منجر به از بین رفتن برخی از قابلیت‌های سازمانی یا مزیت‌های رقابتی گردد که این امر نیز منجر به افزایش هزینه می‌شود (اولوفسون، ۱۹۹۲).



شکل ۱: سطح بهینه امنیت و هزینه (اولوفسون، ۱۹۹۲)

هنگامی‌که دست‌یابی به سطح امنیت نزدیک به ۱۰۰ درصد موردنظر باشد، هزینه‌های ایجاد امنیت به‌صورت نمایی افزایش می‌یابد؛ بنابراین لازم است تا با توجه به محدودیت منابع سازمان و حفظ سطح مشخصی از قابلیت‌های سازمانی، برای شناسایی سطح بهینه امنیت، میان هزینه ناشی از افزایش امنیت و هزینه‌های بالقوه ناشی از نقص امنیتی که به سیستم وارد می‌گردد، تعادل برقرار شود (شکل ۱). در این مقاله با ایجاد یک مدل کمی بر اساس مفهوم اشاره شده در شکل ۱، مدل انتخاب الزامات امنیتی با در نظر گرفتن سطح امنیت مورد انتظار و هزینه‌های ناشی از نقض امنیت و هزینه‌های ایجاد امنیت ارائه شده است.

مدل ریاضی مسئله

برای ایجاد امنیت در فرآیند می‌توان ویژگی‌های امنیتی متعددی مانند رمزنگاری، محرمانگی، کنترل دسترسی، کنترل اصالت اطلاعات و ... را در نظر گرفت. متناظر با هر ویژگی امنیتی یک مکانیسم وجود دارد که می‌تواند توسط راهکارهای مختلف اجرا و عملی شود. طراح فرآیند برای یک فعالیت مشخص از فرآیند می‌تواند یک ویژگی امنیتی را انتخاب کرده یا از آن صرف‌نظر کند. در مرحله بعد در صورت انتخاب یک ویژگی امنیتی، برای پیاده‌سازی مکانیسم

آن ویژگی امنیتی لازم است تا از بین راهکارهای مختلف یکی را انتخاب و از بقیه راهکارها صرف‌نظر کند. متناسب با ویژگی‌ها و راهکارهای امنیتی انتخاب‌شده، سطح امنیت فرآیند تعیین می‌شود. سطح امنیت در بازه‌ای میان صفر تا یک قرار می‌گیرد. نبود هیچ‌کدام از ویژگی‌های امنیتی نشان‌دهنده عدد صفر است که باعث می‌شود تا فرآیند در برابر اخلال‌ها بسیار آسیب‌پذیر شود. در حالتی که سطح امنیت برابر با یک باشد، تمام ویژگی‌های امنیتی برقرار و فرآیند کاملاً در برابر اخلال‌ها محافظت می‌شود. انتخاب ویژگی امنیتی و راهکار مناسب برای اجرای هر مکانیسم در هر یک از فعالیت‌های فرآیند، از یک‌سو هزینه ایجاد امنیت را افزایش می‌دهد و از سوی دیگر هزینه‌های ناشی از عدم امنیت را کاهش می‌دهد و در مجموع باعث می‌شود تا سطح امنیت فرآیند در یک سطح مشخص در بازه بین صفر و یک، تعیین شود. مسئله‌ای که در این بخش مدل آن ارائه می‌شود، عبارت است از اینکه برای رسیدن به یک سطح مشخص از امنیت موردنظر در کل فرآیند با در نظر گرفتن محدودیت‌های هزینه‌ای سازمان، برای هر یک از فعالیت‌های فرآیند چه ویژگی‌ها و مکانیسم‌های امنیتی انتخاب شوند و ویژگی‌ها و مکانیسم‌های انتخاب‌شده بر اساس کدام راهکار پیاده‌سازی شوند. در ادامه اندیس‌ها و پارامترهای مورداستفاده در مدل ریاضی، متغیر تصمیم، تابع هدف و مهدویت‌های مدل ریاضی معرفی می‌شوند.

اندیس‌ها و پارامترهای مدل

i : شماره فعالیت‌های ففرآیند $(= 1,2, \dots, m)$

k : عنوان ویژگی امنیتی

sk :راهکار اجرای ویژگی امنیتی k

h_i :تعداد ویژگی امنیتی مرتبط با فعالیت i

$l_{i,k}$: تعداد راهکارهای مختلف برای پیاده‌سازی ویژگی امنیتی k در فعالیت i

$CN_{i,k}$: میزان خسارت واردشده به فرآیند در صورت نبود ویژگی امنیتی k در فعالیت i

$CN_{i,k,sk}$: میزان پوشش خسارت واردشده به فرآیند توسط راهکار sk از ویژگی امنیتی k در

فعالیت i

$C_{i,k,sk}$:هزینه ایجاد راهکار sk از ویژگی امنیتی k در فعالیت i

$P_{i,k} = \begin{cases}1\\0\end{cases}$: پارامتر تعیین‌کننده مصداق ویژگی امنیتی k برای فعالیت i (در صورت مصداق داشتن برابر با یک و در غیر این صورت برابر با صفر)

ll_p : داقل سطح امنیت مورد انتظار در فرآیند p

متغیرهای مدل

γ_k :وزن ویژگی امنیتی k در فرآیند

$\sigma_{k,p} = \begin{cases}1\\0\end{cases}$: ضعیت استقرار ویژگی امنیتی k در کل فرآیند p (در صورت انتخاب برابر با یک در غیر این صورت برابر با صفر)

$\hat{\sigma}_p$: جمع اوزان ویژگی‌های امنیتی بر اساس راهکارهای انتخاب‌شده در فرآیندp

متغیر تصمیم

$\sigma_{i,k,sk} = \begin{cases}1\\0\end{cases}$ **:** بربر با یک اگر راهکار $\boldsymbol{sk}$ برای ویژگی امنیتی $\boldsymbol{k}$ در فعالیت $\boldsymbol{i}$ انتخاب شود و در غیر این صورت برابر با صفر.

فرضیات

در مدل ارائه شده فرض می‌شود از بین $\boldsymbol{l_{i,k}}$ راهکار موجود برای پیاده‌سازی ویژگی امنیتی $\boldsymbol{k}$ در فعالیت $\boldsymbol{i}$، تنها یک راهکار انتخاب می‌شود. بنابراین با توجه متغیر تصمیم در نظر گرفته شده در مدل طبق رابطه (۱) خواهیم داشت:

$$\sum_{sk=1}^{l_{i,k}} \sigma_{i,k,sk} = 1 \qquad i = \{1, \dots, m\} \qquad k = \{1, \dots, h_i\} \qquad \text{رابطه ۱)}$$

تابع هدف

فرض کنید در طراحی فرآیند برای فعالیت $\boldsymbol{i}$، $\boldsymbol{h_i}$ ویژگی امنیتی در نظر گرفته شده باشد. میزان

خسارت واردشده به فرآیند در صورت نبود ویژگی امنیتی $\boldsymbol{k}$ در فعالیت $\boldsymbol{i}$ برابر با $\boldsymbol{CN_{i,k}}$ خواهد بود. این میزان خسارت در صورت پیاده‌سازی ویژگی امنیتی $\boldsymbol{k}$ در فعالیت $\boldsymbol{i}$ توسط راهکار $\boldsymbol{sk}$ به میزان $\boldsymbol{CN_{i,k,sk}}$ پوشش پیدا می‌کند و میزان خسارت واردشده به فرآیند کاهش یافته و برابر خواهد شد با $\boldsymbol{CN_{i,k}} - \boldsymbol{CN_{i,k,sk}}$. لذا بخشی از تابع هدف کمینه‌سازی مقدار $\boldsymbol{CN_{i,k}} - \boldsymbol{CN_{i,k,sk}}$ برای ویژگی‌های مختلف روی هر فعالیت است. اما از سوی دیگر پیاده‌سازی ویژگی امن؛ ی $\boldsymbol{k}$ در فعالیت $\boldsymbol{i}$ توسط راهکار $\boldsymbol{sk}$ هزینه‌ای به میزان $\boldsymbol{C_{i,k,sk}}$ برای فرآیند ایجاد می‌کند که در تابع هدف کمینه شدن آن دنبال می‌شود. با توجه به اینکه از بین $\boldsymbol{l_{i,k}}$ راهکار مختلف که برای پیاده‌سازی ویژگی امنیتی $\boldsymbol{k}$ وجود دارد، تنها یک راهکار انتخاب می‌شود مقدار تابع هدف برابر با رابطه (۲) خواهد بود.

$$\min Z = \sum_{i=1}^{m}\sum_{k=1}^{h_i}\left(CN_{i,k} - \sum_{sk=1}^{l_{i,k}} \left(CN_{i,k,sk} - C_{i,k,sk}\right)\sigma_{i,k,sk} \right) \qquad \text{رابطه ۲)}$$

محدودیت‌ها

حداقل سطح امنیت فرآیند: حداقل سطح امنیت مورد انتظار منتج از انتخاب راهکارهای امنیتی در فرآیند یعنی ll_p، اولین محدودیت در نظر گرفته شده در این مقاله است. سطح امنیت فرایند بر اساس تحقیق الشافی و بوبک[1](۲۰۲۰)، از رابطه (۳) محاسبه می‌شود.

$$s_p = 1 - e^{-\hat{\sigma}_p} \qquad 0 \le s_p \le 1 \qquad \text{رابطه ۳)}$$

مقدار سطح امنیت فرآیند ($\boldsymbol{s_p}$)، در بازه‌ای بین صفر تا یک متغیر است. سطح امنیت صفر بیانگر پایین‌ترین سطح امنیت و عدد یک بیانگر بالاترین سطح امنیت است. $\boldsymbol{\hat{\sigma}_p}$ بیانگر مجموع اوزان ویژگی‌های امنیتی بر اساس راهکارهای انتخابی است. هرچقدر $\boldsymbol{\hat{\sigma}_p}$ افزایش یابد، سطح امنیت فرآیند به عدد یک نزدیک‌تر می‌شود. $\boldsymbol{\hat{\sigma}_p}$ مطابق رابطه (۴) محاسبه می‌شود.

1. Elshaafi & Botvich

$$\widehat{\sigma}_p = \sum_{k=1}^{h_i} \gamma_k \times \sigma_{k,p}$$ رابطه ۴)

درصورتی‌که ویژگی امنیتی k از منظر طراحی برای فعالیت i مصداق داشته باشد یعنی $P_{i,k} = 1$، آنگاه ویژگی امنیتی k تنها با یکی از $l_{i,k}$ راهکاری که برای پیاده‌سازی مکانیسم این ویژگی در نظر گرفته شده است، اجرا می‌شود و در نتیجه $\sigma_{i,k,sk} = 1$. با اجرای راهکار امنیتی sk از ویژگی k در فعالیت i بخشی از هزینه‌های بالقوه خسارت واردشده به فرآیند در صورت نبود ویژگی امنیتی k در فعالیت i به میزان $CN_{i,k,sk}$ پوشش داده می‌شود. لذا درصد پوشش خسارت‌های ناشی از نبود ویژگی امنیتی k در هر یک از فعالیت‌ها با استفاده از راهکارهای امنیتی پیاده‌سازی شده در هر فعالیت برابر γ_k است که از رابطه (۵) محاسبه می شود.

$$\gamma_k = \frac{\sum_{i=1}^{m} \sum_{sk=1}^{l_{i,k}} (CN_{i,k,sk} \times \sigma_{i,k,sk})}{\sum_{i=1}^{m} CN_{i,k}} \quad ، k = 1، \dots ،h$$ رابطه ۵)

فرض بر آن است که اگر ویژگی امنیتی k از منظر طراحی برای فعالیت i مصداق داشته باشد یعنی $P_{i,k} = 1$ و هیچ‌کدام از راهکارهای اجرایی ویژگی امنیتی k در فعالیت i انتخاب نشود یعنی $\sum_{sk=1}^{l_{i,k}} \sigma_{i,k,sk} = 0$ باشد، آنگاه وضعیت استقرار ویژگی امنیتی k در کل فرآیند یعنی $\sigma_{k,p}$ برابر صفر خواهد بود. چراکه اگر حتی امکان بروز اخلال از منظر ویژگی امنیتی k در تمام فعالیت‌ها جز یک فعالیت گرفته شده باشد، اخلال در فرآیند از طریق همین یک فعالیت می‌تواند باعث شود تا کل فرآیند دچار خسارت شود. بنابراین:

$$\sigma_{k,p} = \min_{i=1}^{m} \sigma_{i,k,sk} \ \ if \ \ P_{i,k} = 1$$ رابطه ۶)

محدودیت تأمین هزینه‌های استقرار راهکارهای امنیتی: حداکثر منابع مالی در اختیار برای استقرار راهکارهای امنیتی فرایند مقدار B واحد پولی است. با توجه به اینکه هزینه اجرای راهکار

امنیتی $\boldsymbol{sk}$ در فعالیت $\boldsymbol{i}$ برابر با مقدار $\boldsymbol{C_{i,k,sk}}$ است، مجموع هزینه استقرار راهکارهای امنیتی در ارتباط با تمام ویژگی‌های امنیتی در تمام فعالیت‌های فرآیند عبارت است از $\sum_{i=1}^{m}\sum_{k=1}^{h_i}\sum_{sk=1}^{l_{i,k}} \boldsymbol{C_{i,k,sk}} \times \boldsymbol{\sigma_{i,k,sk}}$. بنابراین محدودیت تأمین هزینه‌های استقرار راهکارهای امنیتی مطابق رابطه (۷) در مدل در نظر گرفته می‌شود.

رابطه ۷) $$\sum_{i=1}^{m}\sum_{k=1}^{h_i}\sum_{sk=1}^{l_{i,k}} \boldsymbol{C_{i,k,sk}} \times \boldsymbol{\sigma_{i,k,sk}} \leq \boldsymbol{B}$$

مدل ریاضی

با در نظر گرفتن متغیرهای تصمیم، تابع هدف، محدودیت‌ها و فرضیات معرفی شده، مدل ریاضی تحقیق به شکل زیر خواهد بود.

رابطه ۲) $$\min Z = \sum_{i=1}^{m}\sum_{k=1}^{h_i}\left(CN_{i,k} - \sum_{sk=1}^{l_{i,k}} \left(CN_{i,k,sk} - C_{i,k,sk}\right)\sigma_{i,k,sk} \right)$$

Subject to

رابطه ۳) $$ll_p \ll 1 - e^{-\hat{\sigma}_p}$$

رابطه ۴) $$\hat{\sigma}_p = \sum_{k=1}^{h_i} \gamma_k \times \sigma_{k,p}$$

رابطه ۵) $$\gamma_k = \frac{\sum_{i=1}^{m}\sum_{sk=1}^{l_{i,k}}(CN_{i,k,sk} \times \sigma_{i.k,sk})}{\sum_{i=1}^{m} CN_{i,k}} \quad , k = 1, \dots, h$$

رابطه ۶) $$\sigma_{k,p} = \min_{i=1}^{m} \sigma_{i,k,sk} \;\; if \;\; P_{i,k} = 1$$

رابطه ۷) $$\sum_{i=1}^{m}\sum_{k=1}^{h_i}\sum_{sk=1}^{l_{i,k}} C_{i,k,sk} \times \sigma_{i,k,sk} \leq B$$

رابطه ۸) $$\sum_{sk=1}^{l_{i,k}} \sigma_{i,k,sk} = 1 \qquad i = \{1, \dots, m\} \qquad k = \{1, \dots, h\}$$

رابطه۹) $$\sigma_{i,k,sk} = \{0,1\}$$

$$\sigma_{k,p} = \{0,1\}$$ رابطه ۱۰)

مثال عددی

در این مقاله بر اساس اطلاعات فرآیند خرید اینترنتی از یکی از فروشگاه‌های اینترنتی مطرح کشور، مدل ارائه شده مورد ارزیابی و اعتبارسنجی قرار گرفته است. گروه‌های مختلف کالا مانند کالای دیجیتال، لوازم خانگی، لوازم شخصی، فرهنگ و هنر و ورزش و سرگرمی با تنوع زیاد در این فروشگاه عرضه می‌شود. در فرآیند خرید و پرداخت اینترنتی این فروشگاه، خریدار پس از مراجعه به سایت فروشنده و مطالعه‌ی مشخصات و ویژگی‌های کالا، نسبت به ثبت سفارش و خرید اقدام می‌کند. فرآیند خرید اینترنتی مورد مطالعه دارای ۱۳ فعالیت اصلی است. برای ارتقا سطح امنیت فرآیند در برخی از فعالیت‌ها، ویژگی امنیتی در نظر گرفته شده است. برای هر ویژگی امنیتی یک مکانیسم و برای هر مکانیسم یک یا چند راهکار برای استقرار مکانیسم می‌تواند انتخاب شود. در ادامه شرح فعالیت‌ها و ویژگی‌های امنیتی در صورت مصداق، مکانیسم‌ها و راهکارهای پیاده‌سازی شرح داده شده است:

۱- ارسال درخواست[1] از سمت کاربر به سایت فروشنده اینترنتی

۲- تأیید درخواست از طرف سایت فروشنده اینترنتی به کاربر

- ویژگی امنیتی: "شناسایی وقوع حمله "
- مکانیسم ایجاد ویژگی: شناسایی، ثبت و اطلاع‌رسانی حملات و جلوگیری از سرازیر شدن تقاضاهای زیاد به یک سرور و استفاده بیش‌ازحد از منابع (پردازنده، پایگاه داده، پهنای باند، حافظه و...) و پیش‌گیری از دسترس خارج شدن سایت
- راهکارهای ایجاد مکانیسم:

۱. فایروال لایه ۳: با هدف مسدود نمودن دسترسی برخی از **IP** ها و حملات **DDOS**

1. Request

۲. **"WAF"**[1] لایه ۷: با هدف فیلتر کردن تمام دسترسی‌ها به برنامه وب با ابزارهای امنیتی و کنترل ترافیک ورودی به برنامه وب‌سایت فروشنده و ترافیک پاسخ از سمت برنامه وب کاربر (خریدار) و جلوگیری از حملات " مرد میانی[2] "، " تزریق به پایگاه داده[3] " و حملات **DDOS**

۳. سیستم توزیع‌شده: جلوگیری از حملات **DDOS** و جایگزینی نزدیک‌ترین سرور با سرور از کار افتاده

۴. راهکار ترکیبی: به‌کارگیری ترکیبی از راهکارهای فوق

۳-ثبت‌نام کاربر شامل وارد کردن مشخصات، کد پستی، آدرس، تلفن و ایمیل

- ویژگی امنیتی: " احراز ویژگی اصل بودن اطلاعات "
- مکانیسم ایجاد ویژگی: اطمینان از اینکه اطلاعات توسط خریدار در حال ارسال به سایت فروشنده است.
- راهکارهای ایجاد مکانیسم:

۱. گزینه **"I am not robot"**: اطمینان از ربات نبودن کاربر در شرایطی که الگوی رفتاری خریدار در صفحه فروشنده از حالت عادی دور باشد و منجر به ایجاد شک شود.

۲. کد امنیتی[4] **"CAPTCHA"**: که به معنای آزمون همگانی کاملاً خودکار شده تورینگ برای مجزا کردن انسان و رایانه است.

۳. ارسال لینک فعال‌سازی به پست الکترونیکی: هدایت کاربر برای طی مراحل "فعال‌سازی لینک ارسال‌شده به پست الکترونیکی کاربر "، "ارجاع کاربر سایت موردنظر " و "ثبت‌نام با مشاهده پیام [ثبت‌نام با موفقیت انجام گردید]"

۴- ورود به سایت فروشنده اینترنتی با زدن نام کاربری و رمز عبور

۵- جستجو بین کالاهای موردنظر توسط کاربر و انتخاب کالای موردنظر (تعیین تعداد کالا، رنگ، مدل و ...) و اضافه نمودن کالای انتخاب‌شده به سبد خرید

1. Web Application Firewall
2. Man in the Maddle
3. SQL Injection
4. Completely Automated Public Turing to Tell Computers and Humans Apart

۶- بررسی موجود بودن یا نبودن کالا در انبار شرکت فروشنده اینترنتی و قرار دادن کالا در فهرست علائق در صورت موجود نبودن برای دریافت اطلاع

۷- ارزیابی نهایی کالای انتخابی و تصمیم به خرید یا ویرایش مجدد کالای انتخاب‌شده

۸- ثبت و تأیید آدرس محل تحویل کالا و مشخصات نحوه بسته‌بندی کالا (به‌صورت هدیه یا معمولی)، بازه زمانی و روز تحویل و نوع ارسال (شامل پست پیشتاز، پست اکسپرس، پیک موتوری)

۹- تعیین درگاه پرداخت اینترنتی و کلیک بر روی دکمه پرداخت اینترنتی

- ویژگی امنیتی: " جلوگیری از افشای اطلاعات به افراد غیرمجاز "
- مکانیسم ایجاد ویژگی: حفظ محرمانگی اطلاعات از طریق رمزنگاری بین کاربر و سایت فروشنده
- راهکارهای ایجاد مکانیسم:

۱. استفاده از پروتکل[1] **"HTTPS"**: با هدف رمزنگاری اطلاعات تبادلی میان وب‌سایت فروشنده و کاربر

۱۰- دسترسی به صفحه پرداخت بانک انتخاب‌شده

- ویژگی امنیتی: " کنترل دسترسی به اطلاعات حفاظت‌شده "
- مکانیسم ایجاد ویژگی: کنترل دسترسی
- راهکارهای ایجاد مکانیسم:

۱. استفاده از **"Time"**: به‌منظور قطع خودکار ارتباط با سرور بانک در صورت طولانی شدن زمان و محدود کردن مدت‌زمان حمله توسط هکرها

۱۱-کامل نمودن اطلاعات مربوط به کارت‌بانکی

- ویژگی امنیتی اول: " جلوگیری از افشای اطلاعات به افراد غیرمجاز "
- مکانیسم ایجاد ویژگی اول: محرمانگی اطلاعات ورودی
- راهکارهای ایجاد مکانیسم:

1. Hyper Text Transfer Protocol Secure

۱. استفاده از کدهای "**ASCII**"[1] یا صفحه‌کلید مجازی: با هدف جلوگیری از خواندن اطلاعات توسط هکر

- ویژگی امنیتی دوم: " احراز ویژگی اصل بودن اطلاعات "
- مکانیسم ایجاد ویژگی دوم: اطمینان از اینکه اطلاعات توسط خریدار در حال ارسال به سایت فروشنده است.
- راهکارهای ایجاد مکانیسم:

۱. کد امنیتی "**CAPTCHA**"[2]

۱۲- اتمام پرداخت کالا با کلیک بر روی دکمه پرداخت درگاه موردنظر و برگشت به سایت فروشنده و مشاهده پیام موفقیت‌آمیز بودن پرداخت (شامل دریافت کد تراکنش به‌منظور پیگیری پرداخت در صورت بروز مشکل)

جدول ۱ هزینه خسارت ناشی از نبود ویژگی امنیتی، میزان پوشش این هزینه توسط هر یک از راهکارهای ایجاد مکانیسم‌های امنیتی مربوطه و هزینه استقرار راهکارها را در فرآیند نشان می‌دهد.

جدول ۱: اطلاعات فرآیند خرید الکترونیکی

شماره فعالیت	ویژگی امنیتی	مکانیسم ایجاد ویژگی امنیتی	هزینه خسارت ناشی از نبود ویژگی امنیتی ($CN_{i,k}$)	راهکارهای پیاده‌سازی مکانیسم	هزینه استقرار راهکار ($C_{i,k,sk}$)	پوشش خسارت راهکار ($CN_{i,k,sk}$)
۱	عدم مصداق	–	–	–	–	–
۲	شناسایی وقوع حمله	شناسایی، ثبت و اطلاع‌رسانی حملات	۳،۰۰۰،۰۰۰،۰۰۰	راهکار صفر	۰	۰
				فایروال لایه ۳	۶۰،۰۰۰،۰۰۰	۲۰۰،۰۰۰،۰۰۰
				"WAF" لایه ۷	۹۰،۰۰۰،۰۰۰	۳۰۰،۰۰۰،۰۰۰
				سیستم توزیع‌شده	۲،۰۰۰،۰۰۰،۰۰۰	۱،۰۰۰،۰۰۰،۰۰۰
				راهکار ترکیبی	۱۰۰،۰۰۰،۰۰۰،۰۰۰	۱،۰۰۰،۰۰۰،۵۰۰

1. American Standard Code for Information Interchange
2. Completely Automated Public Turing to tell Computers and Humans Apart

شماره فعالیت	ویژگی امنیتی	مکانیسم ایجاد ویژگی امنیتی	هزینه خسارت ناشی از نبود ویژگی امنیتی ($CN_{i.k}$)	راهکارهای پیاده‌سازی مکانیسم	هزینه استقرار راهکار ($C_{i.k.sk}$)	پوشش خسارت راهکار ($CN_{i.k.sk}$)
۳	احراز ویژگی اصل بودن اطلاعات	اطمینان از ربات نبودن کاربر	۱۰،۰۰۰،۰۰۰	گزینه " I am not robot"	۱۰۰،۰۰۰	۲،۰۰۰،۰۰۰
				راهکار صفر	۰	۰
				CAPTCHA	۲۰۰،۰۰۰	٤،۰۰۰،۰۰۰
				ارسال لینک فعال‌سازی به ایمیل	۳۰۰،۰۰۰	٤،۰۰۰،۰۰۰
۴ تا ۸	عدم مصداق	–	–	–	–	–
۹	احراز محرمانگی	حفظ محرمانگی اطلاعات	۲،۰۰۰،۰۰۰،۰۰۰	راهکار صفر	۰	۰
				استفاده از پروتکل "HTTPS"	۳۳۰، ۰۰۰	۲،۰۰۰،۰۰۰،۰۰۰
۱۰	کنترل دسترسی به اطلاعات حفاظت شده	کنترل دسترسی	۱۰۰،۰۰۰	راهکار صفر	۰	۰
				استفاده از "Time"	۵۰،۰۰۰	۱۰۰،۰۰۰
۱۱	جلوگیری از افشای اطلاعات به افراد غیرمجاز	محرمانگی اطلاعات ورودی	۵،۰۰۰،۰۰۰	راهکار صفر	۰	۰
				صفحه‌کلید مجازی	۲۵۰ ،۰۰۰	۵،۰۰۰،۰۰۰
	احراز ویژگی اصل بودن اطلاعات	اطمینان از ربات نبودن کاربر	٤۰۰،۰۰۰	راهکار صفر	۰	۰
				CAPTCHA	۲۰۰،۰۰۰	۴،۰۰۰،۰۰۰
۱۲	عدم مصداق	–	–	–	–	–

الگوریتم بهینه‌سازی مدل تصمیم انتخاب راهکارهای امنیتی در فرآیند کسب‌وکار

در این بخش الگوریتم جستجوی جواب بهینه مدل انتخاب راهکارهای امنیتی در فرآیند کسب‌وکار که در بخش ۴ ارائه شده است بر اساس الگوریتم ژنتیک، شرح داده می‌شود. الگوریتم ژنتیک با ایجاد یک جمعیت اولیه از جواب‌های متعدد برای مسئله موردنظر آغاز می‌شود. هر یک از این جواب‌ها یک کروموزوم نامیده می‌شوند و هر کروموزوم نیز از تعدادی ژن تشکیل می‌شود. جمعیت اولیه این امکان را پیدا می‌کند تا در شرایطی که قواعد انتخاب جواب و محدودیت‌های مسئله را رعایت می‌کند، یک نسل جدید ایجاد کند و میزان تابع برازندگی را بهتر کند. زمانی که بر اساس جواب اولیه یک نسل جدید ایجاد شد، بهترین کروموزوم‌ها بر اساس میزان تابع برازندگی انتخاب شده و زمینه ایجاد نسل جدیدی از این جواب‌ها را ایجاد می‌کنند. هر نسل جدید با استفاده از عملگر تقاطعی، به‌گونه‌ای که تعداد کروموزوم‌های نسل جدید با کروموزوم‌های نسل قبلی برابر باشد ایجاد می‌کند. این عملگر بدین شکل عمل می‌کند که دو تا از بهترین جواب‌های نسل اولیه را گرفته و از یک نقطه مشخص از طول رشته جواب، دو جواب دیگر تولید می‌کند. برای این منظور بخش اول از جواب اول با بخش دوم از جواب دوم ترکیب شده و یک کروموزوم جدید ایجاد می‌شود. این عمل با استفاده از عملگر تقاطعی برای بخش دوم جواب اول و بخش اول جواب دوم نیز انجام می‌شود. عملگر دیگری که در این الگوریتم نقش بازی می‌کند عملگر جهشی است. این عملگر جهت ایجاد یک جهش در ژن یک کروموزوم ایجاد شده است. مجموعه عملیاتی که این عملگرها انجام می‌دهند باعث می‌شود تا تهدید قرار گرفتن الگوریتم در فضایی که جواب بهینه محلی را می‌دهد، کاهش دهد. الگوریتم تا جایی ادامه پیدا می‌کند که یک جواب قابل‌قبول یافت شود و یا تعداد نسل‌های تولیدشده به مقدار مشخص از قبل تعیین شده برسد. برای استفاده از الگوریتم ژنتیک چند موضوع اساسی است که باید تعیین شوند: مفهوم و شکل کروموزوم[1]،

1. hromosome Representation

تولید جمعیت اولیه[۱]، تابع برازندگی[۲]، تابع انتخاب[۳]، عملگرهای ژنی[۴]، شرایط توقف[۵] الگوریتم (ابانی و سفت[۶]، ۲۰۰۳). در ادامه هر یک از بخش‌های اصلی الگوریتم بهینه‌سازی ارائه می گردد.

شکل کروموزوم: هر کروموزوم بیانگر یک جواب موجه یا غیرموجه برای انتخاب از بین راهکارهای مختلف ایجاد ویژگی‌های امنیتی در فرآیند مورد مطالعه است که در قالب رشته‌ای از اعداد باینری کدگذاری می‌شود (فان و همکاران[۷]،۲۰۰۳). هر ژن در کروموزوم بیانگر متغیر تصمیم یعنی $\sigma_{i,k,sk}$ است که می‌تواند مقدار صفر یا یک را به خود اختصاص دهد. در تولید کروموزوم برای نسل‌های مختلف، الگوریتم، عدد صفر یا یک را به شکل تصادفی به هر ژن تخصیص می‌دهد. تعداد ژن‌های هر کروموزوم برابر با مجموع تعداد راهکارهای امنیتی فعالیت-های هر فرآیند است. در مثال مورد مطالعه در این مقاله، تنها در ۵ فعالیت از ۱۲ فعالیت فرآیند، ویژگی‌های امنیتی مصداق دارند. در مجموع در این ۵ فعالیت همان‌گونه که در جدول ۱ نشان داده شد، ۱۱ راهکار مختلف برای پیاده‌سازی ۶ ویژگی امنیتی می‌تواند به‌عنوان راهکارهای بالقوه در نظر گرفته شود. از طرف دیگر ممکن است تصمیم گرفته شود تا از ایجاد یک ویژگی امنیتی برای یک فعالیت صرف‌نظر شود. لذا در کنار تمام راهکارهای تعریف‌شده برای هر یک از ویژگی‌های امنیتی، یک راهکار با نام "راهکار صفر" برای تمام ویژگی‌های امنیتی مطرح شده، در نظر گرفته می‌شود که انتخاب این راهکار نشان‌دهنده عدم انتخاب ویژگی امنیتی برای فعالیت موردنظر است. بنا؛ این اضافه بر ۱۱ راهکار استقرار ویژگی‌های امنیتی، لازم است تا ۶ راهکار صفر هم برای هر یک از ۶ ویژگی امنیتی مربوط به ۵ فعالیت دارای ویژگی امنیتی در نظر گرفته شود. ازاین‌رو هر کروموزوم در الگوریتم حل مدل در مطالعه موردی این مقاله، دارای ۱۷ ژن است.

1. Initial Population
2. Fitness Function
3. Selection Function
4. Genetic Operators
5. Termination Criterion
6. Abonyi and Szeifert
7. Fan et al.

جمعیت اولیه: مجموعه‌ای از کروموزوم‌ها یک جمعیت را تشکیل می‌دهند. با تأثیر عملگرهای ژنتیکی بر روی هر جمعیت، جمعیت جدیدی با همان تعداد کروموزوم به‌صورت تصادفی تشکیل می‌گردد. مقدار پارامتر جمعیت اولیه برای الگوریتم حل مثال مورد مطالعه در این مقاله، پس از بررسی تعداد جمعیت‌های اولیه مختلف، مقدار ۲۰۰ کروموزوم تعیین شد.

تابع برازندگی: در مسائل بهینه‌سازی، تابع هدف مسئله به‌عنوان تابع برازندگی برای الگوریتم در نظر گرفته می‌شود. در مسئله بهینه‌سازی مورد مطالعه، مقدار تابع برازندگی بر اساس مقدار تابع هدف معرفی شده در رابطه شماره ۲ در بخش ۴-۴ و متناسب با مقادیر متغیرهای تصمیم در هر کروموزوم تعیین می‌شود.

تابع انتخاب: انتخاب جواب از میان جواب‌های مختلف هر نسل برای تولید نسل بعدی نقش مهمی را در الگوریتم ژنتیک بازی می‌کند. در ادبیات طرح‌های مختلفی را می‌توان برای فرایند انتخاب مشاهده نمود (ابانی و سفت، ۲۰۰۳). از آن جمله می‌توان به روش‌های "چرخ رولت[1]"، "رتبه‌بندی[2]" و "نخبه‌گزینی[3]" و روش‌های توسعه داده شده مبتنی بر آن‌ها اشاره نمود. در این مقاله از روش دو نقطه‌ای استفاده شده است.

عملگرهای ژنی: عملگرهای ژنی یکی از اجزا مهم در الگوریتم ژنتیک هستند که بر مبنای آن‌ها جواب‌های جدید بر اساس جواب‌های موجود در جمعیت تولید می‌شوند. عملگر تقاطع[4] و جهش[5] دو عملگر اصلی ژنی هستند. عملگر تقاطع، دو جواب از جمعیت موجود را انتخاب می‌کند و دو جواب جدید تولید می‌کند و عملگر جهشی یک جواب را از جمعیت موجود انتخاب می‌کند و یک جواب تکی ایجاد می‌کند. در ادبیات عملگرهای متفاوتی برای جهش و تقاطع می‌توان یافت (فان و همکاران، ۲۰۰۳). در این تحقیق روش " جهش یکنواخت[6] " و "تقاطع حسابی[7] " مورد استفاده قرار گرفته است.

1. Roulette Wheel Selection
2. Ranking Methods
3. Tournament Elitist Models
4. Crossover
5. Mutation
6. Uniform Mutation
7. Arithmetic Crossover

تولید نسل جدید: بعد از اجرای عملگرهای تقاطعی و جهشی، به تعداد ۲۰۰ کروموزوم جدید تولید می‌شود. برای تولید نسل جدید، این کروموزوم‌ها به جمعیت فعلی اضافه شده و نسل جدید به اندازه ۲۰۰ کروموزوم از بهترین کروموزوم‌های موجود انتخاب می‌شود.

شرایط توقف الگوریتم: الگوریتم ژنتیک یک حلقه تکراری از مراحل ایجاد جمعیت، انتخاب از بین جمعیت موجود و تولید جمعیت جدید است که تا تحقق شرایط توقف و پیدا کردن جواب بهینه ادامه می‌یابد. یکی از شرایط توقف پراستفاده در ادبیات تعیین بیشینه تکرار ممکن برای اجرای الگوریتم است. یکی دیگر از شرایط توقف موجود شرط همپوشانی جمعیت‌ها است. در حالت کلی، الگوریتم ژنتیک کل جمعیت را به این سمت سوق می‌دهد تا به یک جواب یکتا دست یابد. زمانی که مجموع انحراف معیار جمعیت از یک آستانه مشخص کوچک‌تر شد، الگوریتم متوقف می‌شود. یکی دیگر از شرایط توقف الگوریتم می‌تواند بدین شکل باشد که اگر بهبود معناداری بین جواب بهینه تکرارهای مختلف ایجاد نشد، الگوریتم متوقف شود. برای تعیین شرایط توقف حتی می‌توان ترکیبی از روش‌های مختلف را استفاده کرد (فان و همکاران، ۲۰۰۳). در این تحقیق، الگوریتم بعد از تکرار یک حد مشخص برابر ۲۵۰ تکرار متوقف می‌شود.

اجرای الگوریتم: گام‌های اجرای الگوریتم ژنتیک برای مثال عددی مورد مطالعه به شرح ذیل است.

۱. تنظیم پارامترهای اجرای الگوریتم شامل تعداد جمعیت اولیه = ۲۰۰، احتمال تقاطع= ۰,۷، احتمال جهش= ۰,۰۳، تعداد اجرای الگوریتم= ۲۵۰

۲. تولید جمعیت اولیه

۳. تا زمانی که تعداد تکرار الگوریتم کمتر یا مساوی ۲۵۰ است حلقه زیر تکرار شود:

۳,۱. به تعداد جمعیت اولیه حلقه زیر برای هر کروموزوم از جمعیت اولیه تکرار شود.

۳,۱,۱. اگر کروموزوم از نظر محدودیت حداقل سطح امنیتی طبق رابطه (۳) موجه است الگوریتم ادامه یابد در غیر این صورت از جمعیت کروموزوم‌ها حذف شود.

۳,۱,۲. اگر کروموزوم از نظر محدودیت هزینه استقرار راهکار امنیتی طبق رابطه (۴) موجه است الگوریتم ادامه یابد در غیر از جمعیت کروموزوم‌ها حذف شود.

۳,۱,۳. برای هر کروموزوم مقدار تابع برازندگی محاسبه شود.

۳,۲. برای ۵۰٪ از کروموزوم‌ها با کمترین مقدار تابع برازندگی حلقه زیر تا رسیدن تعداد کروموزوم‌ها به تعداد جمعیت اولیه ادامه یابد.

۳,۲,۱. دو کروموزوم به‌صورت تصادفی انتخاب شود.

۳,۲,۲. عملگر جهش و تقاطع روی کروموزوم‌ها انجام شود.

۳,۳. جمعیت جدید کروموزوم‌ها جایگزین جمعیت اولیه شود.

۴. کروموزوم‌ها بر اساس مقدار تابع برازندگی مرتب شوند.

۵. مقادیر ژن‌های کروموزوم با کمترین مقدار تابع برازندگی به‌عنوان جواب مسئله در نظر گرفته شود.

نتایج اجرای الگوریتم برای مثال عددی مورد مطالعه: از بین ۱۲ فعالیت فرآیند خرید اینترنتی مورد مطالعه، تنها برای ۵ فعالیت ویژگی‌های امنیتی در نظر گرفته شده است. حل مدل ارائه شده در این مقاله برای مثال عددی مورد مطالعه، عبارت است از انتخاب راهکار WAF برای فعالیت دوم، انتخاب راهکار CAPTCHA برای فعالیت سوم، انتخاب راهکار HTTPS برای فعالیت نهم، انتخاب راهکار Time برای فعالیت دهم و انتخاب راهکار صفحه‌کلید مجازی و CAPTCHA برای فعالیت یازدهم. لازم به یادآوری است مدل برای فعالیت‌های نه تا دوازده از بین راهکار صفر و راهکارهای اشاره شده در جدول ۱، راهکارهای ذکرشده در جواب مدل را شناسایی کرده است. با توجه به راهکارهای انتخاب شده در جواب، سطح امنیت ایجاد شده (S_p)، مقدار ۰/۹۸۹۴ را به خود اختصاص داده است که با توجه به اینکه سطح امنیت به یک نزدیک است، فرآیند از امنیت بسیار بالا و قابل قبولی برخوردار است. همچنین، هزینه‌ی ایجاد راهکارهای امنیتی پیشنهاد شده در جواب برابر با ۹۰.۸۳۰.۰۰۰ تومان است که این میزان از مبلغ ۷۰۰.۰۰۰.۰۰۰ تومان که در محدودیت بودجه‌ای در نظر گرفته شده بود، کمتر است. در نهایت میزان تابع هدف بهینه به مبلغ ۲.۸۰۰.۶۳۰.۰۰۰ تومان به دست می‌آید.

جدول ۲: مقایسه جواب مدل و جواب خبرگان

شماره فعالیت	ویژگی امنیتی	مکانیسم ایجاد ویژگی امنیتی	راهکارهای پیاده‌سازی مکانیسم	جواب مدل	جواب خبرگان
۱	عدم مصداق	–	–	–	–
۲	شناسایی وقوع حمله	شناسایی، ثبت و اطلاع‌رسانی حملات	راهکار صفر		
			فایروال لایه ۳		
			"WAF" لایه ۷	*	*
			سیستم توزیع‌شده		
			راهکار ترکیبی		
۳	احراز ویژگی اصل بودن اطلاعات	اطمینان از ربات نبودن کاربر	گزینه " I am not robot"		*
			راهکار صفر		
			CAPTCHA	*	
			ارسال لینک فعال‌سازی به ایمیل		
۴ تا ۸	عدم مصداق	–	–	–	–
۹	احراز محرمانگی	حفظ محرمانگی اطلاعات	راهکار صفر		
			استفاده از پروتکل "HTTPS"	*	*
۱۰	کنترل دسترسی به اطلاعات حفاظت‌شده	کنترل دسترسی	راهکار صفر		
			استفاده از "Time"	*	*
۱۱	جلوگیری از افشای اطلاعات به	محرمانگی اطلاعات ورودی	راهکار صفر		
			صفحه‌کلید مجازی	*	*

شماره فعالیت	ویژگی امنیتی	مکانیسم ایجاد ویژگی امنیتی	راهکارهای پیاده‌سازی مکانیسم	جواب مدل	جواب خبرگان
	افراد غیرمجاز				
	احراز ویژگی اصل بودن اطلاعات	اطمینان از ربات نبودن کاربر	راهکار صفر		
			CAPTCHA	*	*
۱۲	عدم مصداق	–	–	–	–
سطح امنیت فرآیند ناشی از راهکارهای انتخاب شده				۰/۹۸۹۴ <	۰/۹۸۹۳
مقدار تابع هدف ناشی از راهکارهای انتخاب شده (تومان)				۲.۸۰۰.۶۳۰.۰۰۰ >	۰۰۰،۵۳۰،۸۰۲،۲
قدرت رمزنگاری[1]				۹۰ درصد <	۸۵ درصد

اعتبار سنجی نتایج: به‌منظور اعتبار سنجی مدل ارائه شده در این تحقیق، جلسه‌ای با یک گروه متشکل از چهار نفر متخصص امنیتی که به‌عنوان خبره انتخاب شده بودند، تشکیل و با آنان مصاحبه گردید. در این مصاحبه، فرآیند خرید اینترنتی از سایت فروشنده به همراه تمام راهکارهای امنیتی این فرآیند، برای اعضای گروه تشریح شد. سپس پرسش‌نامه‌ای متشکل از فعالیت‌ها و راهکارهای موجود، در اختیار آنان قرار گرفت تا راهکارهای پیشنهادی را بر اساس تجربیات خود با در نظر گرفتن محدودیت‌های مسئله انتخاب کنند. مقایسه جواب پیشنهادی توسط خبرگان با جواب پیشنهادی توسط مدل ارائه شده در این مقاله در جدول ۲ نشان داده شده است.

نتایج جدول ۲ نشان می‌دهد علی‌رغم همپوشانی نسبی جواب مدل پیشنهادی در این مقاله با جواب خبرگان، راهکارهای انتخاب شده توسط خبرگان سطح امنیت پایین‌تری را در مقایسه با راهکارهای منتخب مدل ساخته شده ایجاد می‌کند. همچنین میزان تابع هدف در مدل

1. Cipher Strength

طراحی شده، کمتر از میزان تابع هدف ناشی از جواب حاصل از نظر خبرگان است؛ بنابراین می‌توان در مثال مورد مطالعه اعتبار جواب حاصل از مدل ارائه شده در این مقاله را معتبر دانست.

به‌منظور ارزیابی سطح امنیت با استفاده از اطلاعات میدانی، گزینه امنیتی انتخاب شده توسط مدل و گزینه انتخابی توسط گروه خبرگان اجرا شد و نتایج اجرای هر دو گزینه توسط SSL Labs به‌صورت برخط مورد ارزیابی قرار گرفت. SSL Labs یکی از معتبرترین ابزارها برای اسکن SSL وب سرور است. این ابزار تحلیل عمیقی از قدرت رمزنگاری و امنیت برنامه‌های تحت وب را در اختیار قرار می‌دهد. پروتکل‌های SSL برای امن کردن ارتباط میان کاربر و سرور از طریق تصدیق هویت و رمزنگاری، طراحی و پیاده‌سازی می‌شوند. نتایج ارزیابی "قدرت رمزنگاری " در هر دو گزینه مورد ارزیابی، نشان از برتری قدرت رمزنگاری گزینه انتخابی توسط مدل ارائه شده در این مقاله است. افزون بر دو گزینه اشاره شده در جدول ۲، برای اعتبارسنجی مدل می‌توان گزینه‌های دیگر را که حاصل ترکیب‌های مختلف راهکارهای پیاده‌سازی مکانیسم‌ها هستند، پیاده‌سازی نمود و قدرت رمزنگاری هر یک را مورد ارزیابی قرار داد؛ اما با توجه به محدودیت محقق در اجرای همه گزینه‌ها، برای اعتبارسنجی نتایج مدل تنها به ارزیابی و مقایسه نتایج قدرت رمزنگاری در دو گزینه اشاره شده، پرداخته شده است.

نتیجه‌گیری و پیشنهادها

تحقیقات متعددی در رابطه امنیت با ابعاد دیگر کیفیت فرآیندهای کسب‌وکار در ادبیات موضوع وجود دارد؛ اما در محدوده مطالعات انجام شده در این مقاله، تحقیقات معدودی مشاهده شد که رابطه امنیت و هزینه، به‌عنوان دو بعد مهم کیفیت فرآیندهای کسب‌وکار ، هم‌زمان بررسی شود. یکی از مسائل مطرح در این زمینه، شناسایی سطح بهینه امنیت در کل فرآیند با توجه به توازن بین هزینه ناشی از افزایش امنیت و هزینه‌های بالقوه ناشی از نقص امنیتی در فرآیند است. در پاسخ به این خلأ تحقیقاتی در این مقاله مدلی ریاضی قطعی و غیرخطی به‌منظور انتخاب راهکار مناسب از بین راهکارهای قابل انتخاب برای ایجاد یک ویژگی امنیتی

در فرآیند کسب‌وکار، ارائه شد. در این مدل انتخاب بهینه راهکارهای امنیتی هر فعالیت در فرآیند، با توجه به بیشینه کردن سطح امنیت کل فرآیند و همچنین کمینه کردن هزینه‌های استقرار راهکارهای امنیتی انجام می‌شود. حداقل سطح امنیت در کل فرآیند و مجموع منابع مالی در اختیار برای استقرار راهکارهای امنیتی، دو محدودیت اصلی مدل در نظر گرفته شده‌اند. برای حل مدل الگوریتم ژنتیک مورد استفاده قرار گرفت و با استفاده از آن مدل پیشنهادی برای فرآیند خرید اینترنتی در یک فروشگاه اینترنتی اجرا شد. مقایسه نتایج حاصل از مدل و نتایج حاصل از انتخاب راهکارهای امنیتی برای فعالیت‌ها توسط خبرگان، نشان داد هم از نظر میزان هزینه‌های استقرار راهکارهای امنیتی و هم از نظر سطح امنیت ایجاد شده ناشی از راهکارهای پیشنهادی، نتایج مدل از وضعیت مناسب‌تری برخوردار است.

نوآوری تحقیق حاضر نسبت به تحقیقات موجود، ارائه مدلی است که به‌صورت عملیاتی با در نظر گرفتن اهداف کسب‌وکار و محدودیت‌های موجود، به‌صورت هوشمند کارآمدترین و اثربخش‌ترین راهکار امنیتی را برای استقرار در فرآیند کسب‌وکار انتخاب می‌کند. این در حالی است که در پیشینه تحقیق، محور تحقیقات عمدتاً بر تبیین چگونگی به‌کارگیری الزامات امنیتی و شیوه مدل‌سازی آن‌ها در فرآیند پرداخته است.

هرچند در این مقاله کاربرد مدل برای یک فرآیند الکترونیکی با تمرکز بر امنیت سایبری نشان داده شد، اما کاربرد مدل تنها محدود به امنیت سایبری در فرآیندهای کسب‌وکار نیست. با توجه به افزایش روزافزون تهدیدات تروریستی و خرابکارانه یا افزایش فعالیت‌های مجرمانه در فرآیندهای کسب‌وکار ، نیاز به ایجاد کنترل‌های فرآیندی بیش‌ازپیش احساس می‌شود. لذا این سؤال برای طراحان و مدیران فرآیندهای کسب‌وکار مطرح خواهد شد که از بین گزینه‌های مختلف برای هر فعالیت از فرآیند، چه کنترلی انتخاب شود. مدل ارائه شده در این تحقیق می‌تواند با در نظر گفتن هزینه‌های ایجاد کنترل و هزینه‌های نبود کنترل، پاسخگوی این سؤال باشد.

در تحقیق حاضر هزینه‌های ناشی از نقصان امنیت و میزان پوشش خسارت ناشی از راهکارهای امنیتی بر هزینه‌های ناشی از نبود ویژگی امنیتی به‌صورت قطعی در نظر گرفته شده است. این در حالی است که در دنیای واقعی این هزینه‌ها احتمالی است. لذا در نظر گرفتن هزینه‌های احتمالی، می‌تواند مدل پیشنهادی در این مقاله را توسعه دهد. از دیگر تحقیقات آتی پیشنهادی، توسعه مدل این مقاله با در نظر گرفتن جزییات بیشتری از هزینه‌های غیرمستقیم ناشی از استقرار الزامات امنیتی در فرآیندهای کسب‌وکار مانند هزینه‌های مورد نیاز برای به‌روزرسانی و نگهداری آتی نرم‌افزارها و سخت‌افزارهای مورد استفاده، هزینه‌های ناشی از افزایش پیچیدگی و یا هزینه‌های احتمالی ناشی از کند شدن فرآیند به دلیل رعایت الزامات امنیتی است. در نظر گرفتن تأثیرگذاری استقرار راهکارهای امنیتی بر میزان امنیت فعالیت‌های پسین یا پیشین و در مجموع بر امنیت کل فرآیند، در قالب شبکه راهکارهای امنیتی می‌تواند کاربرد مدل پیشنهادی را به واقعیت نزدیک کند.

منابع

پیکام، علیرضا و سلیمی فرد، خداکرم. (۱۳۹۵). ارائه چارچوبی برای بررسی عوامل درون‌سازمانی مؤثر بر امنیت سامانه‌های اطلاعاتی با استفاده از روش تحلیل سلسله مراتبی فازی. *مطالعات مدیریت* کسب و کار هوشمند، ۴(۱۶)،۱۷۶-۱۴۷.

لگزیان، محمد و موسوی، پریسا. (۱۳۹۷). مروری سیستماتیک بر رویکردهای سرمایه‌گذاری در امنیت اطلاعات. مطالعات مدیریت کسب و کار هوشمند،۷(۲۵)، ۱۸۲-۱۴۷.

وظیفه، زهرا.، مهدی، محمد و وکیلی، نادیا. (۱۳۹۷). الگوی امکان‌سنجی و استقرار اثربخش سیستم مدیریت امنیت اطلاعات بر مبنای روش فراترکیب. مطالعات مدیریت کسب و کار هوشمند،۷(۲۶)، ۹۹-۷۱.

Abonyi، J.، and Szeifert، F. (2003). Supervised fuzzy clustering for the identification of fuzzy classifiers. *Pattern Recognition Letters*، *24*(14)، 2195-2207.

Atluri، V. (2001). Security for workflow systems. *Information Security Technical Report*، *2*(6)، 59-68 .

Backes، M.، Pfitzmann، B.، and Waidner، M. (2003). Security in business process engineering. In *International Conference on Business Process Management* ، Springer، Berlin، Heidelberg، 168-183.

Basin، D.، Doser، J.، and Lodderstedt، T. (2006). Model driven security: From UML models to access control infrastructures. *ACM Transactions on Software Engineering and Methodology (TOSEM)*، *15*(1)، 39-91.

Campbell، K.، Gordon، L. A.، Loeb، M. P.، and Zhou، L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security، 11(3)، 431-448.

Elshaafi، H.، and Botvich، D. (2012). Aggregation of trustworthiness properties of BPMN-based composite services. In 2012 *IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (383-387). IEEE.

Fan، J. L.، Zhen، W. Z.، and Xie، W. X. (2003). Suppressed fuzzy c-means clustering algorithm. *Pattern Recognition Letters*، *24*(9-10)، 1607-1612.

Guan، X.، Cai، Y.، and Yang، W. (2014). On the reliability-security tradeoff and secrecy throughput in cooperative ARQ. *IEEE Communications Letters*، *18*(3)، 479-482.

Hájková، M. (2012). Business Process Management versus Quality Management System. In *Proceedings in EIIC-1st Electronic International Interdisciplinary Conference*، 32-36.

Heidari، F.، and Loucopoulos، P. (2014). Quality evaluation framework (QEF): Modeling and evaluating quality of business processes. *International Journal of Accounting Information Systems*، *15*(3)، 193-223.

Heravizadeh، M. (2009). *Quality-aware business process management* (Doctoral dissertation، Queensland University of Technology).

Heravizadeh، M.، Mendling، J.، and Rosemann، M. (2009، September). Dimensions of business processes quality (QoBP). In *International Conference on Business Process Management* (pp. 80-91). Springer، Berlin، Heidelberg.

Herrmann، G.، and Pernul، G. (1998). Towards security semantics in workflow management. In *Proceedings of the Thirty-First Hawaii International Conference on System Sciences*، 7، 766-767. IEEE.

Herrmann، G.، & Pernul، G. (1999). Viewing business-process security from different perspectives. *International Journal of Electronic Commerce*، *3*(3)، 89-103.

Herrmann، P.، and Herrmann، G. (2006). Security requirement analysis of business processes. *Electronic Commerce Research*، *6*(3-4)، 305-335.

Jürjens، J. (2002، September). UMLsec: Extending UML for secure systems development. In *International Conference on The Unified Modeling Language* (pp. 412-425). Springer، Berlin، Heidelberg.

Kedrosky، P. (2000). Hackers prey on our insecurities. *The Wall Street Journal*، A18.

Kindler، T.، and Soyez، T. A. (1996). Modelling security for integrated enterprise Workflow and Telecooperation Systems. In *IEEE Fifth Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*، *6*، *(WET ICE 96)*.

Knorr، K.، and Röhrig، S. (2001). Security requirements of e-business processes. In *Towards the E-Society* (pp. 72-86). Springer، Boston، MA.

McDermott، J.، and Fox، C. (1999). Using abuse case models for security requirements analysis. In *Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99)* (pp. 55-64). IEEE.

Mercuri، R. T. (2003). Analyzing security costs. *Communications of the ACM*، *46*(6)، 15-18.

Morselli، C.، Giguère، C.، and Petit، K. (2007). The efficiency/security trade-off in criminal networks. *Social Networks*، *29*(1)، 143-153.

Date، W.، and Note، W. (1992). Archived NIST Technical Series Publication. *NIST Special Publication*، *800*، 60.

Olovsson، T. (1992). *A structured approach to computer security*. Chalmers University of Technology.

Ribeiro، C.، and Guedes، P. (1999). Verifying workflow processes against organization security policies. In *Proceedings. IEEE 8th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE'99)* (190-191). IEEE.

Rodriguez، A.، Fernandez-Medina، E.، and Piattini، M. (2006، April). Security requirement with a UML 2.0 profile. In *First International Conference on Availability، Reliability and Security (ARES'06)* (pp. 8-pp). IEEE.

Rodríguez، A.، Fernández-Medina، E.، and Piattini، M. (2007). A BPMN extension for the modeling of security requirements in business processes. *IEICE transactions on information and systems*، *90*(4)، 745-752.

Rohm، A. W.، Herrmann، G.، and Pernul، G. (1999). A language for modelling secure business transactions. In *Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99)* (pp. 22-31). IEEE.

Röhrig، S.، and Knorr، K. (2004). Security analysis of electronic business processes. *Electronic Commerce Research*، *4*(1-2)، 59-81.

McDermott، J. (2000). Eliciting Security Requirements by Misuse Cases. *Proc. 37th Technology of Object-Oriented Languages and Systems (TOOLS-37 Pacific 2000)، Sydney، Australia*، 120-131.

Thompson، M. S.، and Fortess، E. E. (1980). Cost-effectiveness analysis in health program evaluation. *Evaluation Review*، *4*(4)، 549-568.

Wolter، K.، and Reinecke، P. (2010، June). Performance and security tradeoff. In *International School on Formal Methods for the Design of Computer، Communication and Software Systems* (135-167). Springer، Berlin، Heidelberg.