

طراحی سیستم خبره فازی برای مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی دولت و کسب و کارها

شعبان الهی^۱، مصطفی رشیدی^۲، محمود صادقی^۳

چکیده: مدیران عالی حریم خصوصی با نقش‌ها و مسئولیت‌های متنوع و متعددی مواجه‌اند. از این رو، به‌منظور آگاه‌کردن مدیر عالی حریم خصوصی از وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب و کارها، در این مقاله نوعی سیستم خبره فازی با نام «سیستم خبره فازی مدیر عالی حریم خصوصی» طراحی شده است. به‌منظور تدوین مدل پژوهش و پایگاه دانش سیستم خبره یادشده، مفاهیم شایستگی مدیر عالی حریم خصوصی، نیت جرایم الکترونیکی، نوع تبادلات الکترونیکی بین دولت و کسب و کارها، اخلاق مداری حرفه‌ای طرفین تبادلات الکترونیکی و فناوری‌های محافظ حریم خصوصی شرکت، مؤلفه‌های وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب و کارها شناسایی شدند. به‌منظور اعتبارسنجی سیستم خبره فازی مدیر عالی حریم خصوصی، مقایسه‌ای از خروجی‌های سیستم پیشنهادشده با نظر خبرگان به عمل آمد. این سیستم، به تحلیل حریم خصوصی تبادلات الکترونیکی دولت و کسب و کارها و ارائه توصیه‌های دقیق‌تر، کمک می‌کند.

واژه‌های کلیدی: تبادلات الکترونیکی دولت و کسب و کار، سیستم خبره، مدیر عالی حریم خصوصی، منطق فازی.

۱. دانشیار مدیریت فناوری اطلاعات، دانشکده مدیریت و اقتصاد، دانشگاه تربیت مدرس، تهران، ایران

۲. کارشناس ارشد مدیریت فناوری اطلاعات، دانشکده مدیریت و اقتصاد، دانشگاه تربیت مدرس، تهران، ایران

۳. دانشیار حقوق خصوصی، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران

تاریخ دریافت مقاله: ۱۳۹۳/۱۲/۰۹

تاریخ پذیرش نهایی مقاله: ۱۳۹۴/۰۴/۱۳

نویسنده مسئول مقاله: شعبان الهی

E-mail: Elahi@modares.ac.ir

مقدمه

در قلب فرهنگ اینترنت، نیرویی وجود دارد که می‌خواهد هرچیزی را درباره شما، کشف کند. اطلاعات شخصی افراد و اسرار تجاری شرکت‌ها، دارایی‌های با ارزشی هستند که دیگران را برای تجارت درباره آن اطلاعات و اسرار، وسوسه می‌کند. آندره گرو، یکی از مدیران اجرایی شرکت اینتل، نسبت به مسئله حریم خصوصی در اینترنت ابراز نگرانی می‌کند و می‌گوید: حریم خصوصی، یکی از بزرگ‌ترین مسائل در عصر الکترونیکی جدید است. اگر برخی از شرکت‌ها، به اندازه کافی نسبت به مسئله حریم خصوصی ذی‌نفعان (مشتریان)، کارکنان، سهامداران، شرکای تجاری، تأمین‌کنندگان و سایر اشخاص حقیقی و حقوقی توجه نکنند، سهم بازارشان را از دست می‌دهند (بامبرگر و مولیگان، ۲۰۱۱؛ رزمیرسکی و سیسه، ۲۰۰۲؛ آوازو و دسوزا، ۲۰۰۴ و ردیک و روی، ۲۰۱۳). مدیران عالی حریم خصوصی کسب‌وکار با مسائلی از جمله ترکیب نقش‌های چون مسئول حریم خصوصی، مسئول رسیدگی به شکایت‌ها در دعاوی حقوقی بین شرکت و نهاد‌های دولتی، سرپرست اسناد و مدارک شرکت و نیز، چندبرابری خطر تبادلات آنلاین دولت با اشخاص حقیقی و حقوقی نسبت به مبادلات تجاری، مواجه‌اند. از سویی، سیستم‌های خبره، برنامه‌های هوشمند رایانه‌ای هستند که از دانش و رویه‌های استنتاج برای حل مسائلی استفاده می‌کنند که به اندازه کافی دشوارند و به تخصص خاص انسانی، نیاز دارند. این سیستم‌ها می‌توانند کاربر را در حل مسئله راهنمایی کنند و دانشی را که از اسناد و متخصصان دریافت کرده‌اند را در اختیار کسانی قرار دهند که به آن دانش نیاز دارند. در واقع سیستم‌های خبره می‌توانند مانند مشاور در کنار متخصصان انواع حوزه‌ها، به کار گرفته شوند (الهی، خدیور و حسن‌زاده، ۱۳۹۰؛ دن باتر، لیو و تان، ۲۰۱۲؛ شمسی، ۱۳۹۲؛ قدس‌الهی، ۱۳۸۹ و جالتا، بودوریک و ژانگ، ۲۰۰۶). در اینجا نیاز به نوعی سیستم خبره به منظور آگاه‌سازی مدیر عالی حریم خصوصی از وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها، احساس می‌شود. سؤال‌های زیر به منظور شناخت بهتر مسئله مطرح شده‌اند:

۱. چگونه می‌توان شبکه مفاهیم مرتبط با کار مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی دولت و کسب‌وکارها را طراحی کرد؟
۲. چگونه می‌توان دانش و تخصص مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی دولت و کسب‌وکارها را مدل‌سازی کرد؟
۳. چگونه سیستم خبره می‌تواند به مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی دولت و کسب‌وکارها کمک کند؟

به منظور رعایت انسجام ساختار پژوهش، این مقاله بدین شرح نگاشته شده است؛ در ادامه، سیستم‌های خبره در نشریه‌های معتبر بررسی می‌شود، روش‌شناسی پژوهش بخش بعدی را شکل می‌دهد و پس از آن به چگونگی استخراج مدل مفهومی و سیستم خبره فازی پیشنهادشده این پژوهش با عنوان «سیستم خبره فازی مدیر عالی حریم خصوصی»^۱ اشاره می‌شود، این مقاله با ارائه یافته‌ها و نتایج به پایان می‌رسد.

پیشینه نظری پژوهش

مقاله وارن و براندیس در سال ۱۸۹۰ با عنوان «حق مصونیت حریم خصوصی»، اولین بحث جدی و صریحی بود که موضوع حریم خصوصی افراد را در چارچوب قوانین حقوقی مطرح کرد. در سال ۱۹۶۷ وستین با انتشار کتاب حریم خصوصی و آزادی، ضمن تکمیل تعریف حوزه حریم خصوصی، مبنای چهارگانه‌ای برای حریم خصوصی افراد تعیین کرد. وستین، انقلاب و سیر تحول حریم خصوصی اطلاعات را با پیروی از انقلاب فناوری اطلاعات، طی چهار مرحله زیر شرح داد (جالتا، بودوریک و ژانگ، ۲۰۰۶؛ جنسن، پاتز و جنسن، ۲۰۰۵ و اصلانی، ۱۳۸۴: ۲۶-۱۸ و ۶۶-۵۹):

۱. آغاز و مبنای حریم خصوصی (۱۹۶۰-۱۹۴۵): اعتماد زیاد به بخش کسب‌وکار و دولت و راحتی جمع‌آوری اطلاعات همراه با توسعه‌های فناوری اطلاعات محدود؛
۲. اولین دوره توسعه حریم خصوصی معاصر (۱۹۷۹-۱۹۶۱): مطرح‌شدن ریسک حریم خصوصی اطلاعات با عنوان مسئله قانونی، سیاسی و اجتماعی صریح، تشخیص اولیه از جناح‌های تاریک فناوری‌های جدید و تدوین چارچوبی برای راهکارهای اطلاعاتی منصفانه و تنظیم قانون حریم خصوصی در سال ۱۹۷۴؛
۳. دومین دوره توسعه حریم خصوصی معاصر (۱۹۸۹-۱۹۸۰): طراحی سیستم‌های رایانه‌ای، قابلیت‌های پایگاه‌های داده‌ای و شبکه‌کردن فناوری‌های جدید درون راهکارهای اطلاعاتی منصفانه؛
۴. سومین دوره توسعه حریم خصوصی معاصر (۲۰۰۳-۱۹۹۰): تغییر چشم‌انداز مبادله اطلاعات توسط اینترنت و وب ۲/۰ و حمله‌های تروریستی ۱۱ سپتامبر. اروین آلمن در سال ۱۹۷۵ با هدف توصیف این موضوع که چرا مردم گاهی ترجیح می‌دهند در تنهایی بمانند و گاهی مایل‌اند در تعاملات اجتماعی درگیر شوند، نظریه مقررات حریم

خصوصی^۱ را توسعه داد و بیان کرد، حریم خصوصی ایستا و ثابت نیست، بلکه کنترل‌گزینی از دسترسی به اطلاعات شخصی فرد است. در واقع مبانی نظری درباره حریم خصوصی تبادلات دولت و کسب‌وکار، هنوز در دوران کودکی قرار دارد و اغلب تبادلات دولت و کسب‌وکارها در اتحادیه اروپا تا سال ۲۰۰۷، غیرالکترونیکی و مبتنی بر کاغذ بوده است (بلداد، جانگ و استیهودر، ۲۰۱۰؛ بلنجر و هیلر، ۲۰۰۶ و الهی و حسن‌زاده، ۲۰۰۹)؛ به طوری که تاکنون سیستمی به منظور بررسی حریم خصوصی تبادلات دولت و کسب‌وکار طراحی نشده است.

پیشینه تجربی

با توجه به پژوهش‌های پیشین در حوزه سیستم‌های خبره و حریم خصوصی و امنیت شرکت‌ها، در این بخش به بررسی انتقادی آنها پرداخته شده است. لانگلی و ریگیبای (۱۹۹۲) با استفاده از برنامه پرولوگ و مدل مبتنی بر قاعده، به طراحی سیستم خبره‌ای برای به‌کارگیری طرح‌های مدیریت کلید در مدل‌های امن سیستم‌های رمزنگاری در شبکه‌ها اقدام کردند. در سال ۱۹۹۵ کابلائی و جارات، به منظور مدیریت و تحلیل ریسک امنیت رایانه‌ای، نوعی سیستم خبره کیفی برای سازمان‌های تجاری کوچک و متوسط توسعه دادند. کارات، کارات، برودیه و فنگ در سال ۲۰۰۵، به منظور تسهیل تألیف، قبول پایش، پیاده‌سازی و به‌کارگیری خطمشی حریم خصوصی و شناسایی احتیاجات حریم خصوصی سازمانی، سیستمی طراحی کردند که به روشی منعطف به رعایت حریم خصوصی به منظور تواناسازی فناوری‌های شرکت کمک می‌کرد. در سال ۲۰۱۴ لی و همکارانش، برای بهره‌برداری از داده‌های حریم خصوصی حفاظت‌شده و کنترل دسترسی به داده‌های رمزگذاری‌شده، نوعی معماری ترکیبی ارائه کردند. کریمی و زاپاتا (۲۰۱۵) به شناسایی نوع جدیدی از حمله به حریم خصوصی و حمله‌های مختل‌کننده خدمات و سیستم‌های شرکت پرداختند و چالش‌های جدید امنیت در آینده اینترنت را بررسی کردند.

یکی از دلایل استفاده از منطق فازی در این سیستم خبره، این است که فهم و پروسه تصمیم‌گیری انسان‌ها در بسیاری از موقعیت‌ها کاملاً قطعی نیست و بسته به زمان و مکان آن، گاهی درست و گاهی نادرست است (زیدوناس و همکاران، ۲۰۰۹؛ آریانس آراندا و همکاران، ۲۰۱۰؛ اسپاتزر، ۱۹۹۰ و میا، کر و گامک، ۲۰۰۹)؛ زیرا در تفکر، استنتاج و ادراک افراد، همیشه درجه معینی از فازی بودن وجود دارد. به منظور بررسی انتقادی مرتبط‌ترین پژوهش‌های پیشین با پژوهش حاضر، شرح کوتاهی از آنها در جدول ۱ به نمایش گذاشته شده است.

جدول ۱. بررسی انتقادی مرتبطترین پژوهش‌های مبانی نظری در مقایسه با پژوهش حاضر

عنوان پژوهش	منبع	اعتبار رتبه‌بندی سیستم		اعتبار رتبه‌بندی سیستم خبره		مدیر عالی حریج خصوصی	جرایم الکترونیکی	بررسی در فضای الکترونیکی	تبادلات دولت با کسب‌وکارها (B2C)	تبادلات دولت با کسب‌وکارها (G2B)	استفاده از منطق فازی	تکنیک‌ها و آزمون‌های آماری
		اعتبار رتبه‌بندی سیستم	سیستم خبره	بررسی جزئی	بررسی جزئی							
بررسی تأثیر ادراک مشتریان از امنیت و اعتماد بر استفاده از سیستم‌های پرداخت الکترونیکی شعب بانک کشاورزی شهر تهران	کریمی، سیدزاد و حق‌نژاد (۱۳۹۱)	-	-	مخاطبات فنی بر امنیت ادراک شده مشتریان	ممنوع	اعتماد تراکنش‌های الکترونیکی	اشاره جزئی	سیستم پرداخت الکترونیکی	-	-	-	مدل معادلات ساختاری
بررسی تأثیر امنیت ادراک شده بر اعتماد به سیستم‌های پرداخت الکترونیکی مشتریان بانک (اصطلاحی درباره بانک صادرات شهر سمنان)	دانشانی و سیداصطلاحی کجوری (۱۳۹۱)	-	-	امنیت ادراک شده مشتریان بانک	-	اعتماد تراکنش‌های الکترونیکی	اشاره جزئی	بانکداری اینترنتی	-	-	-	مدل معادلات ساختاری
بررسی آمیخت در سیستم‌های اطلاعاتی توسعه‌یافته با روش معماری سرویس‌گرا (SOA)	تقوا و ایزدی (۱۳۹۲)	-	-	ایجاد امنیت سیستم‌های اطلاعاتی	-	-	اشاره جزئی	-	-	-	-	معماری سرویس‌گرا (SOA) گردآوری داده‌ها با آزمون تی
بررسی تأثیر خصوصیات مشتریان بر تمایل آنها به پذیرش خرید اینترنتی (اصطلاحی برای سیستم‌های اطلاعاتی)	حسنعلی پور و همکاران (۱۳۹۲)	-	-	ادراکات از امنیت وب	-	تکراری‌های حریج خصوصی	اشاره جزئی	خرید اینترنتی	-	-	-	همبستگی و رگرسیون طبقه‌بندی ماشین‌ها
ریشه‌یابی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات و بررسی میزان آداکمی مدیریت اطلاعات	تاجفر و همکاران (۱۳۹۲)	-	-	سیستم مدیریت امنیت اطلاعات (ISMS)	-	محرمانه‌بودن اطلاعات سازمان	اشاره جزئی	خرید اینترنتی	-	-	-	ریشه‌یابی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات
بررسی شاخص‌های تأثیرگذار بر موفقیت راهکارهای خدمات بانکداری برون از دیوار و نتجکان بانک انصار	نادری و قاسمی‌زاد (۱۳۹۳)	-	-	امنیت سیستم برون بانکی	-	-	اشاره جزئی	خدمات بانکداری برون	-	-	-	ریشه‌یابی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات
شناسایی نقش در کارتهای بانکی با استفاده از شبکه‌های عصبی مصنوعی	وفاق، عقیق‌پور و البرزی (۱۳۹۲)	-	-	امنیت کارتهای بانکی	-	-	تقلبهای بانکی	تراکنش‌های بانکی	-	-	-	شبکه‌های عصبی مصنوعی
An automatic search for security flaws in key management schemes	لانگی و ریجکی (۱۹۹۲)	#	#	امنیت کارتهای بانکی	-	-	-	شبکه‌های رایانشی	-	-	-	برنامه پروتوک و مدل سنتی بر قایده

جنبه‌های نوآوری پژوهش



تابلوه جدول ۱

فصلنامه‌های نوآوری پژوهش														
موضوع	منبع	سیستم فخره	اعتبارسنجی سیستم	بررسی جزئی	بررسی پروژه	بررسی حوزه امنیت		مدیر عالی	جرایم الکترونیکی	بررسی در فضای الکترونیکی	تابلوه دوت یا (۳۳B)	تابلوه دوت کسپروکارها یا دوت (۳۳C)	استفاده از منطقه فازی	تکنیکها و آزمون‌های اداری
						امنیت شبکه	امنیت هویت							
عنوان پژوهش	NADIR: An automatic system for detecting network intrusion and misuse- (۱۹۹۳)	•	•	•	•	•	•	•	•	•	•	•	•	سیستم فخره ناخفای شبکه
	کاراچی و جانت (۱۹۹۹)	•	•	•	•	•	•	•	•	•	•	•	•	مدیریت سیستم فخره
	کین و همکاران (۲۰۰۶)	•	•	•	•	•	•	•	•	•	•	•	•	نظریه خاکستری سناسی سریع فخره
	کاروتایین، بلسون و کویتاالس (۲۰۱۱)	•	•	•	•	•	•	•	•	•	•	•	•	آزاده چارچوب جهت‌ی اختیارات فخره خصوصي و امنیت
	مانسی و مانگ (۲۰۱۲)	•	•	•	•	•	•	•	•	•	•	•	•	طراحی سیستم استنتاج فازی
	لی و همکاران (۲۰۱۲)	•	•	•	•	•	•	•	•	•	•	•	•	آزاده مندری ترکیبی
	کریمی و زابا (۲۰۱۵)	•	•	•	•	•	•	•	•	•	•	•	•	سیستم تشخیصی بالخطی فازی PSO-Kmeans
	الهی، رشتی و صادقی (۲۰۱۵)	•	•	•	•	•	•	•	•	•	•	•	•	طراحی سیستم فخره CPOEX

طراحی سیستم فخره CPOEX
 طراحی آراز فازی کتده اولیا بین
 مطالعه فخره‌ها: مختلف دانش
 آراز انتشارسنجی سیستم فخره

مدل مفهومی پژوهش

بر اساس ترکیب مفاهیم مرتبط با کار مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی دولت و کسب و کارها، مدل مفهومی پژوهش تدوین شد (شکل ۱) که در ادامه به معرفی مؤلفه‌های آن پرداخته می‌شود.



شکل ۱. مدل مفهومی پژوهش

اخلاق مداری حرفه‌ای طرفین تبادلات الکترونیکی بین دولت و کسب و کارها؛ توجه اعضای شرکت و طرفین تبادلات الکترونیکی بین دولت و کسب و کارها به منشور اخلاقی شرکتشان و اندازه پای‌بندی آنها به وجدان اخلاقی، به‌منزله بزرگ‌ترین عامل برقرارکننده عدالت اجتماعی و رعایت اصول اخلاقی در انواع تبادلات الکترونیکی بین دولت و کسب و کارها. سنجه‌های این مؤلفه عبارت‌اند از: خطامشی اخلاقی سازمان نسبت به مصرف‌کننده و مشتریان، خطامشی اخلاقی سازمان نسبت به پیمانکاران و مؤسسه‌های نظارتی، خطامشی اخلاقی سازمان نسبت به کارکنان و مدیران، توجه به وجدان اخلاقی (به‌منزله بزرگ‌ترین عامل برقرارکننده عدالت اجتماعی و کنترل‌کننده انگیزه‌های زودگذر)، توجه سازمان به استفاده از سیستم‌های

اطلاعاتی اخلاقی و خطامشی استفاده اخلاقی از رایانه به منزله یکی از خطامشی های الکترونیکی سازمان (حسینی دولت آبادی، ۱۳۷۰ و آذر، فانی و داج خوش، ۱۳۹۱).

نیت جرایم الکترونیکی در حوزه تبادلات الکترونیکی بین دولت و کسب و کارها؛ تمام تخلفها و جرمه هایی است که با نیت خرابکاری و نابودی سیستم های شرکت، جاسوسی الکترونیکی و نفوذ (بدون خرابکاری) به اسرار تجاری و نقض حریم خصوصی شرکت، اخلال در سیستمها و عملیات اصلی شرکت و ایجاد هرگونه مشکل برای ادامه فعالیت های شرکت در حوزه تجارت الکترونیکی، سالانه خسارت های مادی (کاهش فروش) و معنوی (بدنامی و صدمه به شهرت شرکت) زیادی را بر شرکت تحمیل می کند. به طور خلاصه انواع جرایم الکترونیکی عبارتند از: نفوذ، گردآوری غیرمجاز دادهها (گردآوری داده های شخصی از طریق روش های غیرقانونی)، تغییر غیرمجاز دادهها (ورود به سایت و انتشار محتوای کذب)، سرقت هویت (دسترسی به شناسه و رمز عبور دیگران و وانمود کردن خود به جای آنها)، انتقال و افشای غیرمجاز دادهها و رعایت نکردن ضوابط امنیتی و سایر حقوق اشخاص حقیقی و حقوقی (اصلائی ۱۳۸۴: ۲۰۷-۱۸۶؛ بلنجر و هیلر، ۲۰۰۶؛ بلا، گیوستولیسی و ریکوبنه، ۲۰۱۱؛ کالونیاتیس، بلسیس و گریترالیس، ۲۰۱۱).

شایستگی مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی بین دولت و کسب و کارها؛ از ترکیب مفاهیمی چون وظایف، مهارت ها و فنون به کار برده شده مدیر عالی حریم خصوصی در مبانی نظری موضوع شکل گرفته است. در اینجا به بررسی توانایی مدیر عالی حریم خصوصی شرکت در به کارگیری فنون و روش های مرتبط با کار، پرداخته می شود (دیمیک، ۲۰۱۲ و آوازو و دسوزا، ۲۰۰۴).

فناوری های محافظ حریم خصوصی تبادلات الکترونیکی بین دولت و کسب و کارها؛ تأثیر استفاده از فناوری هایی مانند سیستم های تشخیص و جلوگیری از نفوذ، نرم افزارهای امنیتی، سخت افزارها و بسترهای مبادله های امن و بی نام و سایر ابزار الکترونیکی که شرکت برای رعایت حریم خصوصی اسرار تجاری و تبادل های الکترونیکی امن و بی نام به کار می برد. در این پژوهش به بررسی مؤلفه های استفاده از سیستم های اطلاعاتی امن (مطمئن)، سخت افزار و بستر پیام رسانی آنی رمزی، شبکه های پنهان سازی جریان اطلاعات، نرم افزار ضبط حرکات و کلیک های ماوس و صفحه کلید، فناوری متوقف کردن سایت های شخص ثالث ردیاب در سراسر وب، گذرواژه های یکبار مصرف، فناوری های حفاظت از حریم خصوصی انتشار و ثبت کردن اطلاعات حساس سازمان، فناوری پیام خودانهدام متنی، صوتی و تصویری (به منظور حفاظت از

حریم خصوصی ابزار موبایل سازمان) پرداخته شده است (کایلائی و جارات، ۱۹۹۵؛ سامرز، استنلی و کوزبان، ۱۹۹۸ و هاجبرگ و همکاران، ۱۹۹۳).

نوع تبادلات الکترونیکی بین دولت و کسب و کارها؛ میزان خطرپذیری و ریسک تبادل الکترونیکی بین دولت و کسب و کارها، از طریق درگاه‌های دولتی و سایر روش‌های تبادل الکترونیکی بین دولت و کسب و کارها است. در پژوهش پیش رو، سنجه‌هایی چون فرمول‌ها، تألیفات منتشرنشده و طرح‌های تجاری و نیز نرم‌افزارها، فرایندها و روش‌های تجارت شرکت، محتوای تبادلات در نظر گرفته شدند و به بررسی مبادله الکترونیکی از طریق وب‌سایت، رایانامه، تلفن و ... پرداخته شده است (بلا، گیوستولیس و ریکونه، ۲۰۱۱؛ ردیک و روی، ۲۰۱۳ و دینو و هارت، ۲۰۰۶).

روش‌شناسی پژوهش

از آنجا که تحقیقات طراحی، به روش‌شناسی منحصر به فردی نیاز دارد، در این مقاله با بررسی پارادایم‌های اصلی زیربنای فلسفی پژوهش‌های علوم اجتماعی و مدیریت و روش پژوهش سیستم‌های اطلاعاتی، از ترکیب نظریه انتقادی و رویکرد پژوهشی علم طراحی^۱ استفاده شده است. در واقع از دید هستی‌شناسی - پارادایم پژوهشی انتقادی، در این مقاله واقعیت و مسائلی که مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی دولت و کسب و کارها با آنها سروکار دارد را هاله‌ای از عوامل اجتماعی، سیاسی، فرهنگی، اقتصادی، اخلاقی و ... احاطه کرده است که این عوامل تأثیرگذار بر تصمیم‌های مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی دولت و کسب و کارها، در گذر زمان و در صورت تعامل با اعضای شرکت، شفاف می‌شوند. در واقع این پژوهش از نظر ماهیت، کاربردی است؛ زیرا نتایج و یافته‌های آن برای حل مسائل مختص به مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی دولت و کسب و کارها که یکی از مشکلات خاص سازمان‌ها به‌شمار می‌رود، به کار برده می‌شود. از دید شناخت‌شناسی، پژوهشگر به بررسی جامع پدیده مد نظر به شیوه‌ای تعاملی با خبرگان این حوزه اقدام می‌کند و خبرگان نیز نظرشان را درباره درستی و ارتباط مفاهیم و قواعد پرسشنامه بیان می‌کنند. در اینجا ذهنیت‌گرایی و ارزش‌های خبرگان حوزه مطالعه، بر پدیده تأثیر می‌گذارد. شناخت‌شناسی در رویکرد پژوهشی علم طراحی این مقاله به دو مسئله اشاره می‌کند؛ یکی دانستن از طریق ساختن سیستم خبره و دیگری سازه‌های عینی محدود درون مضمون حریم خصوصی. از دید ارزش‌شناسی، به خلق دانش جدید درباره حوزه کاری مدیر عالی حریم خصوصی، پیشرفت و بهبود در وضعیت حریم

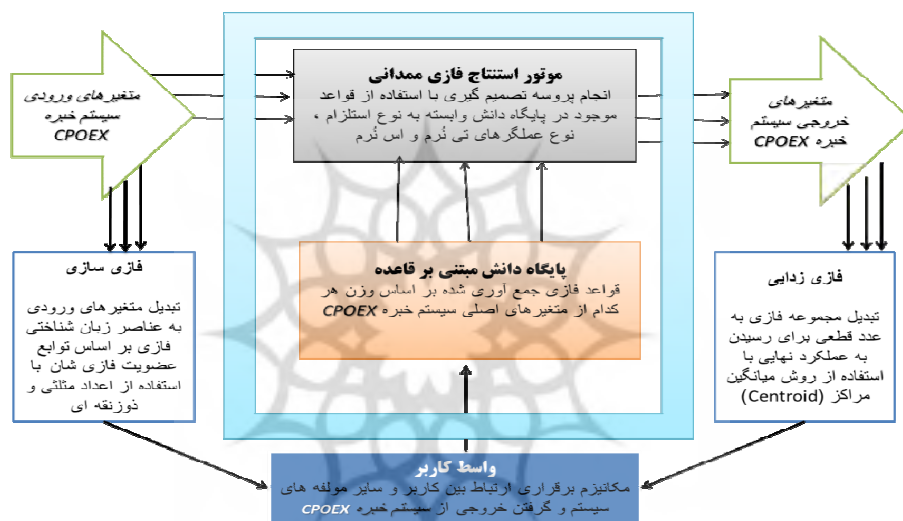
خصوصی تبادلات الکترونیکی بین دولت و کسب و کارها و فهم مسائل کاری مدیر عالی حریم خصوصی پرداخته شده است (واشناوی و کوچلر، ۲۰۰۸: ۲۰-۱۴ و کاتز، ۲۰۰۶: ۳۰۴-۳۰۲). در واقع روش اجرای این پژوهش از نظر هدف، توصیفی - ارزشیابی است؛ زیرا از سویی اقدام به توصیف دقیق مفاهیم و قواعد حوزه مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی دولت و کسب و کارها می‌پردازد و از سوی دیگر، روابط بین این مفاهیم و قواعد را با استفاده از پرسشنامه و مصاحبه با خبرگان ارزیابی و تعیین می‌کند. در واقع روش نمونه‌گیری در این مقاله ترکیبی از دو روش نمونه‌گیری غیر احتمالی هدفمند و نمونه‌گیری گلوله برفی است. گفتنی است، حجم نمونه این پژوهش را سه گروه معرفی شده از خبرگان در دسترس و مایل به همکاری در جامعه آماری شکل می‌دهد. برای دستیابی به مدل، از اسناد موجود در مجله‌های مرتبط با کار مدیر عالی حریم خصوصی در حوزه کسب و کار الکترونیکی، توصیه‌های سازمان توسعه همکاری‌های اقتصادی (OECD)، هشدارهای پلیس بین‌الملل درباره حریم خصوصی در فضای الکترونیکی، مرکز اطلاعاتی حریم خصوصی الکترونیکی (EPIC) و قانون تجارت الکترونیکی ایران، استفاده شده است. به منظور ارزیابی مفاهیم مرتبط با کار مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی دولت و کسب و کارها، از نظر ۱۷۲ نفر از متخصصان دانشگاهی، از جمله استادان حقوق دانشگاه‌های تربیت مدرس و شهید بهشتی، مرکز تحقیقات صنایع انفورماتیک و همچنین متخصصان بخش دولتی مانند پلیس فتا (فضای تبادل اطلاعات)، معاونت امنیت فضای تبادل اطلاعات وزارت ارتباطات و فناوری اطلاعات و... بهره برده شد. داده‌های پرسشنامه اول در فاصله زمانی شهریور ۱۳۹۳ تا آبان ۱۳۹۳ و داده‌های پرسشنامه دوم در آذرماه ۱۳۹۳ جمع‌آوری شده است. ضریب آلفای کرونباخ ۹۳ گزینۀ پرسشنامه برای پایایی مؤلفه‌های تعیین‌کننده وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب و کارها، ۰/۷۳ به دست آمد که قابلیت اعتماد بالای پرسشنامه را نشان می‌دهد.

یافته‌های پژوهش و طراحی سیستم خبره فازی

در این پژوهش سیستم خبره در پنج مرحله طراحی شده است که عبارت‌اند از: فازی‌سازی، پایگاه قواعد فازی، موتور استنتاج فازی و غیرفازی‌سازی و اعتبارسنجی سیستم خبره طراحی شده. با توجه به تحلیل ساختار سیستم‌های خبره به کاررفته در مجله‌های معتبر در حوزه سیستم‌های خبره^۱ (ژو و همکاران، ۲۰۰۷؛ لی بلنک و جلاسی، ۱۹۹۱؛ لیائو، ۲۰۰۵ و ژیدوناس و همکاران،

۲۰۰۹)، اجزای ساختار سیستم خبره این پژوهش طراحی شد که در شکل ۲ به نمایش گذاشته شده است.

فازی سازی: بعد از طراحی مدل مفهومی پژوهش، به تعریف متغیرهای ورودی و خروجی سیستم خبره اقدام می‌شود. در واقع مازول «وضعیت حریم خصوصی تبدلات الکترونیکی دولت و کسب و کارها»، خروجی سیستم خبره پیشنهادی را شکل می‌دهد. جدول ۲ افزایش متغیرهای زبانی مرتبط با متغیر خروجی سیستم خبره پژوهش را بر اساس نظر خبرگان به نمایش گذاشته است.



شکل ۲. ساختار پیشنهادی سیستم خبره پژوهش حاضر

جدول ۲. متغیرهای زبانی مرتبط با وضعیت حریم خصوصی تبدلات الکترونیکی دولت و کسب و کارها

شماره	متغیر زبانی	معادل انگلیسی	علامت اختصاری	توابع عضویت اعداد مثلثی و دوزنقه‌ای
۱	نا امن	InSecure	Worst	(۰/۱۵, ۰/۰۳, ۰, ۰)
۲	ریسک زیاد	High Risk	H-R	(۰/۳, ۰/۲, ۰/۱)
۳	ریسک متوسط	Medium Risk	M-R	(۰/۷, ۰/۵, ۰/۳)
۴	کم ریسک	Low Risk	L-R	(۰/۹, ۰/۸, ۰/۷)
۵	امن	Secure	Best	(۱, ۱, ۰/۹۷, ۰/۸۵)

پایگاه قواعد فازی: پایگاه قواعد فازی مجموعه‌ای از قواعد اگر - آنگاه است که قلب سیستم خبره این پژوهش به‌شمار می‌رود. در اینجا احتمال وقوع حالت‌های مختلف بین متغیرهای اصلی سیستم خبره، یکسان در نظر گرفته شده است. نحوه تولید قواعد پایگاه دانش ماژول اصلی سیستم خبره (وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها) به شرح زیر است:

محاسبه وزن هر یک از متغیرهای اصلی با بهره‌مندی از نظر خبرگان: با توجه به جدول وزن نهایی متغیرهای اندازه‌گیری‌کننده، وزن هر یک از متغیرهای اصلی به‌دست آمد که در جدول ۳ مشاهده می‌شود.

جدول ۳. وزن هر یک از متغیرهای اصلی پژوهش

شماره	متغیر اصلی	سنجدها	وزن نهایی متغیر
۱	اخلاق‌مداری حرفه‌ای طرفین تبادلات الکترونیکی	۷	۰/۸۱۱
۲	شایستگی مدیر عالی حریم خصوصی شرکت	۲۸	۰/۷۷۹
۳	نوع تبادلات الکترونیکی دولت و کسب‌وکارها	۲۴	۰/۷۷۲
۴	فناوری‌های حافظ حریم خصوصی شرکت	۱۷	۰/۷۷۱
۵	نیت جرایم الکترونیکی	۱۷	۰/۷۶۸

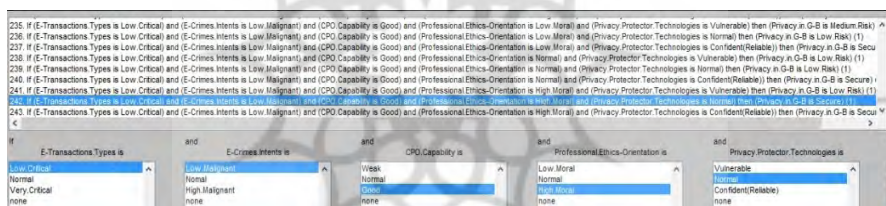
محاسبه مقدار متغیر خروجی بر اساس وزن هر یک از متغیرها: با توجه به وزن هر یک از پنج متغیر اصلی سیستم خبره، می‌توان وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها را در حالت‌های مختلف بررسی کرد. جدول ۴ نحوه محاسبه وزن حالت‌های ممکن برای تولید قاعده در پایگاه دانش سیستم خبره را نشان می‌دهد.

با توجه به توابع عضویت متغیرهای زبانی خبرگان، $0/247636$ در بازه تعریف‌شده برای متغیر زبانی «ریسک زیاد» جانمایی شده است. از این رو، وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها در حالت بالا (جدول ۴) در «ریسک زیاد» قرار دارد. سایر قواعد پایگاه دانش این سیستم خبره نیز به این ترتیب تولید شدند و در پرسشنامه‌ای به مقایسه پاسخ‌های سیستم خبره با میانگین نظر خبرگان پرداخته شد. شکل ۳ نحوه تولید قواعد پایگاه دانش ماژول اصلی سیستم خبره را نشان می‌دهد.

جدول ۴. نحوه محاسبه وزن حالت‌های ممکن برای تولید قاعده در پایگاه دانش سیستم خبره

حالت‌های ممکن برای تولید قاعده	تأثیر بر متغیر خروجی	وزن متغیر × مقدار قطعی متغیر	وزن حالت مفروض
اگر «نیت جرائم الکترونیکی» با بد خواهی زیاد باشد.	رابطه منفی	0.768×0.25	0.192
و «شایستگی مدیر عالی حریم خصوصی» در وضعیت معمولی باشد.	رابطه مثبت	0.779×0.5	0.3893
و «اخلاق مداری حرفه‌ای طرفین تبادلات الکترونیکی» زیاد باشد.	رابطه مثبت	0.811×0.975	0.7911
و «نوع تبادلات الکترونیکی دولت و کسب‌وکارها» خیلی مهم باشد.	رابطه منفی	0.772×0.25	0.193
و «فناوری‌های محافظ حریم خصوصی شرکت» ضعیف باشند.	رابطه مثبت	0.771×0.25	0.193

میانگین وزن حالت‌های مفروض:
 $0.19297625 + 0.3893375 + 0.791197375 + 0.1932685 + 0.19197375 = 0.1927175$
 در چه وضعیتی قرار دارد؟
 $0.1927175 \div 5 = 1/2381179$

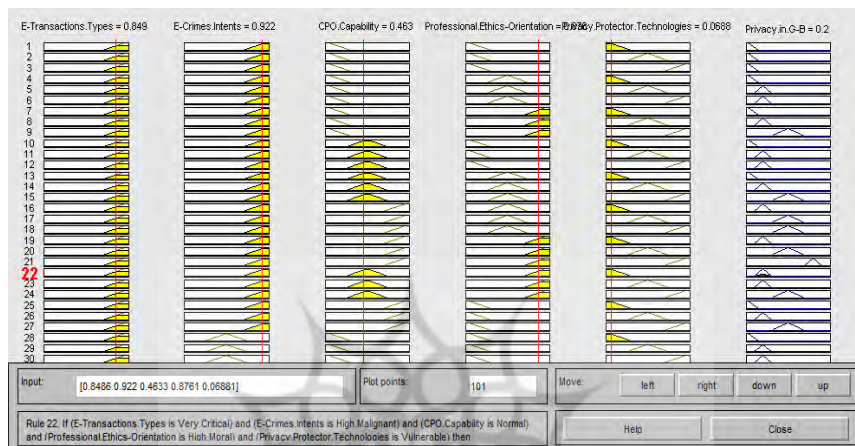


شکل ۳. نحوه تولید قواعد پایگاه دانش ماژول اصلی سیستم خبره

موتور استنتاج فازی: در بخش جعبه فازی نرم‌افزار متلب، به منظور اتصال قواعد فازی سیستم با استفاده از عملگر «و» و «Sum»، سبک تجمیع قواعد فازی انتخاب شده است. بدین ترتیب، مجموع دقیق تر هر مجموعه خروجی قواعد در نظر گرفته می‌شود، نه حداکثر آنها. دلیل اصلی استفاده از سیستم استنتاج فازی ممدانی این است که موتور استنتاج فازی ممدانی، معایب سیستم فازی خالص و سیستم فازی سوگنو را برطرف کرده است، ضمن آنکه یک فازی‌ساز در ورودی و یک غیرفازی‌ساز در خروجی سیستم قرار می‌دهد. برای انتخاب نوع استنتاج در نرم‌افزار متلب از Prod استفاده می‌شود؛ زیرا عملگر مینیمم مجموعه فازی خروجی را کوتاه و ناقص می‌کند. در واقع دلیل استفاده از Prod، مقیاس‌بندی دقیق تر خروجی مجموعه‌های فازی است (سیوناندام،

1. Aggregation

سوماتی و دیپا، ۲۰۰۷: ۱۲۷-۱۱۳). غیرفازی‌ساز، خروجی فازی را به عدد قطعی تبدیل می‌کند. در قسمت غیرفازی‌ساز نرم‌افزار متلب، روش Centroid انتخاب می‌شود. شکل ۴ نمایی از تحلیل رفتار متغیر خروجی در ماژول وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها، به صورت عددی و زبانی، بر اساس پنج متغیر اصلی سیستم خبره را نشان می‌دهد.



شکل ۴. تحلیل رفتار متغیر وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها

ارزیابی نهایی پاسخ‌های سیستم خبره: بعد از طراحی سیستم خبره پژوهش با انتخاب تصادفی ۱۰ قاعده از سیستم خبره، خروجی‌های سیستم خبره در پرسشنامه جداگانه‌ای (جدول ۵) با نظر ۱۸ نفر از خبرگان مقایسه شد. همان‌طور که در جدول ۶ مشاهده می‌شود، اختلاف نهایی بین خروجی‌های سیستم خبره و میانگین نظر خبرگان معنادار نیست (۰/۰۶۴۷۵). این نتیجه نشان می‌دهد سیستم خبره فازی مدیر عالی حریم خصوصی، از اعتبار کافی برخوردار است.

جدول ۵. ابزار اعتبارسنجی سیستم خبره از طریق مقایسه پاسخ‌ها با نظر خبرگان

شماره قاعده	متغیرهای ورودی سیستم خبره					نظر شما
	الف	ب	ج	د	ه	
۳	زیاد	کم	کم	زیاد	زیاد	؟
...						

الف: نیت جرایم الکترونیکی
ب: شایستگی مدیر عالی حریم خصوصی
ج: اخلاق‌مداری حرفه‌ای
د: نوع تبادلات الکترونیکی
ه: فناوری‌های محافظ حریم خصوصی
و: حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها

جدول ۶. نظر خبرگان درباره وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب و کارها

شماره قاعده	میانگین پاسخ‌های خبرگان	خروجی‌های سیستم خبره	اختلاف پاسخ‌ها بر اساس مقیاس پنج‌تایی	میانگین اختلافها
۳	۱/۲۲	۱	$۰/۰۵۵ = ۴ / ۰/۲۲$	
۴۵	۲/۷۲	۳	$۰/۰۶۷۵ = ۴ / ۰/۲۸$	
۷۹	۲/۷۸	۳	$۰/۰۵۵ = ۴ / ۰/۲۲$	
۸۶	۱/۶۷	۲	$۰/۰۸۲۵ = ۴ / ۰/۲۲$	
۱۰۳	۱/۶۷	۲	$۰/۰۸۲۵ = ۴ / ۰/۲۲$	۰/۰۶۴۷۵
۱۴۰	۲/۷۸	۳	$۰/۰۵۵ = ۴ / ۰/۲۲$	
۱۵۷	۳	۳	$۰ = ۴ / ۰$	
۲۱۹	۲/۹۴	۳	$۰/۰۱۵ = ۴ / ۰/۰۶$	
۲۲۴	۳/۳۹	۴	$۰/۱۵۲۵ = ۴ / ۰/۶۱$	
۲۳۵	۲/۶۷	۳	$۰/۰۸۲۵ = ۴ / ۰/۲۲$	

مقایسه یافته‌ها: به منظور مقایسه نتایج مرتبط‌ترین پژوهش‌های مبانی نظری با یافته‌های پژوهش حاضر، شرح مختصری از آنها در جدول ۱ به نمایش گذاشته شد. پژوهش‌های مندرج در جدول ۱ بر اساس این جنبه‌ها بررسی و مقایسه شدند: طراحی سیستم خبره، اعتبارسنجی سیستم، بررسی حوزه امنیت، بررسی فنون به کاررفته مدیر عالی حریم خصوصی، شناسایی جرایم الکترونیکی مرتبط با حوزه، بررسی در فضای الکترونیکی، تبادلات دولت با کسب و کارها (G2B)، تبادلات کسب و کارها با دولت (B2G) و استفاده از منطق فازی. نتایج مقایسه‌های جدول ۱ ضمن کمک به شناسایی شکاف‌های این حوزه، نشان می‌دهد یافته‌های پژوهش حاضر، بخشی از کاستی‌های پژوهش‌های پیشین در این حوزه را رفع می‌کند.

نتیجه‌گیری و پیشنهادها

نوع و میزان ارتباط مفاهیم کار مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی دولت و کسب و کارها، تابع منطق فازی است؛ زیرا عوامل بسیاری در فرایند انتخاب و به کارگیری فناوری‌ها، روش‌ها و نظریه‌های به کاربرده شده وی تأثیر می‌گذارند که هر یک از این عوامل از ابهام و پیچیدگی بسیاری برخوردارند. مهم‌ترین نتیجه این پژوهش را می‌توان تحلیل وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب و کارها، بر اساس مؤلفه‌های شایستگی مدیر عالی حریم خصوصی، نیت جرایم الکترونیکی، نوع تبادلات الکترونیکی دولت و کسب و کارها، اخلاق مداری حرفه‌ای طرفین تبادلات الکترونیکی و فناوری‌های محافظ حریم خصوصی شرکت،

بیان کرد. با توجه به بررسی پایگاه‌های اطلاعاتی اسکوپوس، اشپرینگر، ساینس دایرکت، ایران داک و غیره، می‌توان برخی از جنبه‌های نوآوری این مقاله را به این شرح بیان کرد: ۱. طراحی سیستم خبره برای مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی دولت و کسب‌وکارها بر اساس مهم‌ترین نرم‌افزارها؛ ۲. روش‌ها و جرایم فضای کسب‌وکار الکترونیکی؛ ۳. شناسایی مفاهیم مرتبط با کار مدیر عالی حریم خصوصی در حوزه تبادلات الکترونیکی دولت و کسب‌وکارها و مدل‌سازی جامع پایگاه دانش سیستم خبره بر اساس آنها؛ ۴. استفاده از رویکرد منطق فازی به منظور ارائه توصیه‌هایی دقیق‌تر درباره وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها.

در پایان می‌توان گفت، سازمان‌هایی که با نهادها و سازمان‌های دولتی تبادلات الکترونیکی دارند، می‌توانند با استفاده از سیستم خبره طراحی شده این پژوهش، وضعیت حریم خصوصی تبادلات الکترونیکی بین دولت و سازمان‌شان را بررسی و ارزیابی کنند و با توجه به رویکرد جامع مدل این سیستم، ریسک تبادلات الکترونیکی را مدیریت کنند. به علاوه، به کارگیری سیستم خبره این پژوهش در سازمان‌های فعال در حوزه امنیت اطلاعات و ارتباطات، می‌تواند به کاهش هزینه کسب تجربه کاربران سازمانی کمک کند؛ زیرا سیستم‌های خبره دائمی و پایدارند و مانند انسان‌های خبره نمی‌میرند و فناپذیرند. یکی دیگر از مزیت‌های این سیستم، سهولت انتقال آن به مکان‌های جغرافیایی گوناگون است. این امر برای توسعه کشورهای که استطاعت خرید دانش متخصصان را ندارند، بسیار اهمیت دارد و در کاهش هزینه‌های آنها مؤثر است. با توجه به مطالب بیان شده، مهم‌ترین توصیه و پیشنهاد برای پژوهش‌های بعدی را می‌توان، ادغام سیستم خبره این پژوهش با روش‌های هوش مصنوعی، به ویژه شبکه عصبی مصنوعی و الگوریتم‌های حوزه هوش مصنوعی برای افزایش غنای محتوای سیستم خبره یادشده و بهبود فرایند استنتاج فازی آن، بیان کرد.

References

- Arias-Aranda, D., Castro, J.L., Navarro, M., Sánchez, J.M., Zurita, J.M. (2010). A Fuzzy expert system for business management. *Expert Systems with Applications*, 37 (12): 7570–7580.
- Aslani, H.R. (2006). *Information Technology Laws*. Tehran: Mizan Publications. (in Persian)
- Awazu, Y. & Desouza, K. C. (2004). The Knowledge Chiefs: CKOs, CLOs and CPOs. *European Management Journal*, 22(3): 339–344.

- Bamberger, K.A. & Mulligan, D.K. (2011). New governance, chief privacy officers, and the corporate management of information privacy in the United States: An initial inquiry. *Law & Policy*, 33(4): 477-508.
- Belanger, F. & Hiller, J.S. (2006). A framework for e-government: privacy implications. *Business process management journal*, 12 (1): 48-60.
- Beldad, A., de Jong, M. & Steehouder, M. (2010). Reading the least read? Indicators of users' intention to consult privacy statements on municipal websites. *Government Information Quarterly*, 27(3): 238-244.
- Bella, G., Giustolisi, R. & Riccobene, S. (2011). Enforcing privacy in e-commerce by balancing anonymity and trust. *Computers & Security*, 30 (8): 705-718.
- Damghanian, H. & Siah Sarani Kojuri, M. A. (2012). A Study on the Effect of Perceived Security on the Trust of Female Customers in the Internet Banking: (A Survey of the SADERAT BANK in Semnan). *Journal of Information Technology Management*, 4(13): 71-88. (in Persian)
- Den Butter, F. A. G., Liu, J., & Tan, Y.H. (2012). Using IT to engender trust in government-to-business relationships: The Authorized Economic Operator as an example. *Government Information Quarterly*, 29(2): 261-274.
- Dimick, C. (2012). The new privacy officer. *Journal of AHIMA/American Health Information Management Association*, 83(4): 20-25.
- Diney, T. & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17 (1): 61-80.
- Elahi, Sh. & Hassanzadeh, A. (2009). A framework for evaluating electronic commerce adoption in Iranian companies. *International Journal of Information Management*, 29(1): 27-36.
- Ghodselahi, A. (2011). *Designing a Fuzzy Expert system for Risk Management in Banking Industry*. [Master thesis]. Supervisor: Elahi, Sha'ban. Tehran: Tarbiat Modares University, Faculty of Management and Economic. (in Persian)
- Hasangholipour, T., Amiri, M., Fahim, F.S. & Ghaderi Abed, A. (2013). Effects of Consumer Characteristics on their Acceptance of Online Shopping: A Survey in Faculty of Management, University of Tehran. *Journal of Information Technology Management*, 5(4): 67-84. (in Persian)
- Hashemi, M. & Malek, M.R. (2012). Protecting location privacy in mobile geoservices using Fuzzy inference systems. *Computers. Environment and Urban Systems*, 36(4): 311-320.

- Hochberg, J., Jackson, K., Stallings, C., McClary, J.F., DuBois, D. & Ford, J. (1993). NADIR: An automated system for detecting network intrusion and misuse. *Computers & Security*, 12(3): 235-248.
- Hosseini Dolwlat Abadi, F. (2001). *The Ethical Conscience and ways of fostering it*. [Master thesis]. Supervisor: Dr Hojati. Tehran: Tarbiat Modares Uni. (in Persian)
- Jensen, C., Potts, C. & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1-2): 203-227.
- Jutla, D.N., Bodorik, P. & Zhang, Y. (2006). PeCAN: An architecture for users' privacy-aware electronic commerce contexts on the semantic web. *Information Systems*, 31 (4): 295-320.
- Kailay, M. P. & Peter, J. (1995). RAMEX: a prototype expert system for computer security risk analysis and management. *Computers & Security*, 14(5): 449-463.
- Kalloniatis, Ch., Belsis, P. & Gritzalis, S. (2011). A soft computing approach for privacy requirements engineering: The Pris framework. *Applied Soft Computing*, 11(7): 4341-4348.
- Karami, A. & Guerrero-Zapatab, M. (2015). A Fuzzy anomaly detection system based on hybrid PSO-Kmeans algorithm in content-centric networks. *Neurocomputing*, 149: 1253-1269.
- Karat, J., Karat, C.M., Brodie, C. & Feng, J. (2005). Privacy in information technology: Designing to enable privacy policy management in organizations. *International Journal of Human-Computer Studies*, 63(1): 153-174.
- Le Blanc, L. A. & Jelassi, T. (1991). an evaluation and selection methodology for expert system shells. *Expert Systems with Applications*, 2(2-3): 201-209.
- Li, J., Li, J., Chen, X., Liu, Zh. & Jia, CH. (2014). Privacy-preserving data utilization in hybrid clouds. *Future Generation Computer Systems*. (30): 98-106.
- Liao, SH. (2005). Expert system methodologies and applications-a decade review from 1995 to 2004. *Expert Systems with Applications*, 28 (1): 93-103.
- Longley, D. & Rigby, S. (1992). An automatic search for security flaws in key management schemes. *Computers & Security*. 11(1): 75-89.

- Majdalawieh, M. (2010). The Integrated Privacy Model: Building a Privacy Model in the Business Processes of the Enterprise. *International Journal of Information Security and Privacy archive*, 4 (3): 1-21.
- Miah, Sh., Kerr, D. & Gammack, J.G. (2009). A methodology to allow rural extension professionals to build target-specific expert systems for Australian rural business operators. *Expert Systems with Applications*. 36(1): 735-744.
- Naderi, A & Ghaseminezhad, Y. (2014). Investigating the Indicators Affecting the Success of Modern Banking Services Strategies from the View Point of Managers and Experts of Ansar Bank. *Journal of Iranian Technology Management*, 6(3): 487-504.
- Qin, B., Zhou, X., Yang, J. & Song, C. (2006). Grey-theory based intrusion detection model. *Journal of Systems Engineering and Electronics*, 17(1): 230-235.
- Reddick, C.G. & Roy, J. (2013). Business perceptions and satisfaction with e-government: Findings from a Canadian. *Government Information Quarterly*, 30(1): 1-9.
- Reza Karimi, M., Sepandarand, S. & Haghshenas, F. (2012). Study of the Effects of Customers' Perceptions of Security and Trust on their Use of the Agriculture Bank of Iran's e-Payment System. *Journal of Iranian Technology Management*, 4(11): 135-154.
- Rezmierski, V. E. & Marshall, R. S. (2002). University systems security logging: who is doing it and how far can they go? *Computers & Security*, 21 (6)1: 557-564.
- Shamsi, Z. (2014). *Designing a Fuzzy expert system for selecting new IT product development projects*. [Master thesis]. Supervisor: Elahi, Sha'ban. Tehran: Tarbiat Modares University, Faculty of Management and Economic. (in Persian)
- Sivanandam, S. N., Sumathi, S. & Deepa, S.N. (2007). *Introduction to Fuzzy Logic using MATLAB*. Springer-Verlag Berlin Heidelberg.
- Summers, R. C. & Kurzban, S.A. (1988). Potential applications of knowledge-based methods to computer security. *Computers & Security*, 7(4): 373-385.
- Taghva, M.R. & Izadi, M. (2013). Investigating Security in Developed Information Systems through Service oriented Architecture (SOA). *Journal of Information Technology Management*, 5(3): 25-42. (in Persian)
- Tajfar, A. H., Mahmoudi Maymand, M., Rezasoltani, F. & Rezasoltani, P. (2015). Ranking the barriers of implementing Information Security Management

- System and Investigation of readiness rate of exploration management. *Journal of Information Technology Management*, 6(4): 551-566. (in Persian)
- Vaishnavi, V. K. & Kuechler, Jr. W. (2008). *Design Science Research Methods and Patterns, Innovating Information and Communication Technology*. Auerbach Publications, Taylor & Francis Group.
- Vosough, M., Taghavi Fard, M. T. & Alborzi, M. (2015). Bank card fraud detection using artificial neural network. *Journal of Information Technology Management*, 6(4): 721-746. (in Persian)
- Xidonas, P., Ergazakis, E., Ergazakis, K., Metaxiotis, K., Askounis, D., Mavrotas, G. & Psarras, J. (2009). On the selection of equity securities: An expert systems methodology and an application on the Athens Stock Exchange. *Expert Systems with Applications*, 36(9): 11966-11980.
- Xu, D.L., Liu, J., Yang, J.B., Liu, G.P., Wang, J., Jenkinson, I. & Ren, J. (2007). Inference and learning methodology of belief-rule-based expert system for pipeline leak detection. *Expert Systems with Application*, 32(1): 103-113.