پژوهشنامه‌ی مدیریت اجرایی
علمی – پژوهشی
سال سوم، شماره‌ی۶، نیمه ی دوم۱۳۹۰

طراحی سیستم دانش محور کشف تقلب در شرکت های بیمه: رویکرد فازی

عزیزا.. معماریانی*
ابوذر زنگویی نژاد**

تاریخ دریافت:۱۳۸۹/۱۰/۱۱ **تاریخ پذیرش:۱۳۹۰/۱۰/۲۸**

چکیده

گسترش فناوری اطلاعات در صحنه ی صنعت بیمه موجب ایجاد تحولات گسترده‌ای در شیوه‌های انجام معاملات و توسعه ی بیمه ی الکترونیکی شده است. از طرف دیگر، ارتباطات الکترونیکی دائماً در معرض انواع مختلف تقلب قرار دارند؛ بنابراین ابداع سیستم‌ها و استانداردهای قانونی که به شناسایی و پیشگیری از تقلب و سوء استفاده در بیمه ی الکترونیکی کمک کند بسیار مورد توجه است. بر این اساس، هدف اصلی این تحقیق تشخیص رفتارهای مشکوک کاربران بیمه ی الکترونیکی به کمک تئوری فازی است. روش انجام کار شامل طراحی سیستمی خبره فازی برای تشخیص رفتارهای مشکوک کاربران بیمه الکترونیکی به صورت هوشمند خواهد بود؛ نتایج نشان می‌دهد این سیستم امکان مدلسازی رفتار کاربران در پنج دسته ی مختلف را داراست که با دقت بیشتری نوع رفتار کاربر را پیش‌بینی می‌کند. بنابراین می‌توان مشتریان را بر اساس نوع رفتار آن ها دسته‌بندی و رفتارهای غیرمعمول را بر اساس شدّت و ضعف آنان در دسته‌های مختلف طبقه بندی کرد.

واژه های کلیدی: بیمه ی الکترونیک، سیستم دانش‌محور، کشف تقلب، سیستم خبره ی فازی، رویکرد نظریه ی فازی

---

* استاد گروه مدیریت دانشگاه تربیت مدرس
** نویسنده مسئول - دانشجوی دکتری مدیریت سیستم ها دانشگاه تربیت مدرس

۱- مقدمه

یکی از ابعاد «عصر اطلاعات»، تغییرات عمیقی است که در روابط اقتصادی بین افراد، شرکت‌ها و دولت‌ها به‌وجود آمده است(وانگ و وانگ[1]، ۲۰۰۸). نظام‌های بانکی و بیمه‌ای به عنوان نهادهایی که ارتباطی مستقیم با موضوع توسعه در ابعاد جهانی، اقتصاد خدماتی دانش‌محور و فناوری اطلاعات دارند برای تطبیق خود با شرایط رقابتی بسیار فشرده در ارائه ی خدمات به مشتریان، با جنبش کاربردی کردن فنّاوری اطلاعات در خدمات مالی و بانکی همراه شده‌اند(ریلی و همکاران[2] ، ۲۰۰۹: ۹۳). حاصل این تلاش همه جانبه رسیدن به مفهوم جدیدی به نام بیمه ی الکترونیکی است که به عنوان مفهومی عام در توسعه ی دیجیتالی خدمات بیمه گران به شمار می‌رود.

یکی از زیرساخت‌های مهم در مقبولیت و گسترده شدن فرایندهای بیمه ی الکترونیکی، افزایش امنیت و کنترل رفتارهای غیر قانونی در این نوع سیستم‌ها است(لابوسچگن و الوف[3]،۲۰۰۰: ۱۰۸-۱۱۰). پیشرفت‌های گسترده در زمینه ی فناوری، کمک زیادی به افزایش سطح امنیت داده‌های انتقال یافته در بیمه ی الکترونیکی کرده است؛ با این وجود چالش‌های پیش‌روی گسترش و توسعهٔ بیمه الکترونیکی کماکان باقی است(پارک و همکاران[4]، ۲۰۰۹). تاکنون سیستم‌های مختلفی برای شناسایی تقلب در رفتار کاربران بیمه ی الکترونیکی و به کار گرفته شده است. این گونه سیستم‌ها معمولاً قابلیت تشخیص شدّت و ضعف رفتارها را ندارند، به همین دلیل در این تحقیق به موضوع شناسایی رفتارهای مشکوک کاربران در بیمه گری الکترونیکی پرداخته شده است. بر این اساس، در بخش دوم پیشینه ی تحقیق و در بخش سوم متدولوژی تحقیق تشریح می شود. در بخش چهارم، یک سیستم خبره فازی برای شناسایی رفتارهای غیر معمول مشتریان در بیمه گری و بیمه گذاری الکترونیکی توسعه داده شده است؛ در بخش پایانی، نتیجه گیری و پیشنهادها به منظور بهبود عملکرد شرکت های بیمه در زمینه ی بیمه ی الکترونیکی مطرح می‌شود.

1- Wang & Wang
2- Riley & et al
3-Labuschagne & Eloff
4-Park & et al

۲- پیشینه ی تحقیق

۲-۱- بیمه ی الکترونیکی

بیمه ی الکترونیکی[۱] به معنای عام به عنوان کاربرد اینترنت و تکنولوژی اطلاعات در تولید و توزیع خدمات بیمه‌ای اطلاق می‌شود(آدولوجو و همکاران[۲]، ۲۰۰۹) و در معنای خاص بیمه ی الکترونیکی را می‌توان به عنوان تأمین یک پوشش بیمه‌ای از طریق بیمه‌نامه‌ای است که به طور برخط درخواست، پیشنهاد، مذاکره و قرارداد آن منعقد می‌شود (سزوچری و همکاران[۳]،۲۰۰۴).

بیمه ی الکترونیکی به عنوان کانال جدید توزیع محصولات بیمه‌ای ایجاب می‌کند که جریان مبادلات شتاب یابد؛ اما تهدیدهای زیادی برای کلاهبرداری و تقلب ایجاد می شود (رایس[۴] ، ۲۰۰۱: ۶۲-۸۲). از این رو شرکت‌های بیمه‌ای به سرعت در حال بهبود بخشیدن و سرمایه‌گذاری بر روی سیستم‌های ضد سرقت خود هستند و با توجه به رشد تهدیدات و حملات کامپیوتری که با انگیزه‌های مالی انجام می‌شود امنیت صنعت بیمه باید به عنوان یک موضوع مهم شناخته شود(بیگنل[۵]، ۲۰۰۶). چرا که از دست‌دادن اعتماد مشتریان به دلیل وقوع کلاهبرداری در این نوع خدمات، باعث به خطر افتادن اقتصاد عمومی می شود. بدین‌لحاظ روش‌های مختلفی برای پیشگیری و شناسایی تقلب، رفتارهای غیرمعمول و مغایر با قانون کاربران وجود دارد؛ این روش‌ها معمولاً شماره ی شناسایی شخصی(PIN)[۶] یا همان رمز عبور که شامل بررسی عددی است که مشتری به عنوان رمزعبور برای خود در نظر گرفته است و روش‌های زیست‌سنجی[۷] است(کوها و سری گانش[۸]، ۲۰۰۷). روش‌های زیست‌سنجی شامل شناسایی کاربران به صورت خودکار است. در این روش‌ها افراد بر اساس ویژگی‌های زیستی و رفتاری منحصر به فرد خود شناسایی می‌شوند. روش زیست سنجی در واقع یک سیستم تشخیص الگوست که با شناسایی الگوهایی که قبلاً در سیستم ثبت شده

1-Electronic Insurance(E-Insurance)
2-Aduloju & etal
3-Czuchry & etal
4-Rice
5-Bignell
6-Personal Identification Number(PIN)
7-Biometrics
8-Quah and Sriganesh

می‌تواند مجوّز ورود را برای افراد صادر کند. این الگوها می‌تواند شامل شناسایی اثرانگشت مشتری، عنبیه ی چشم، چهره، صدا و امضای شخص باشد(دانداش و همکاران[1]،۲۰۰۸).

یکی از روش‌های مورد استفاده در تشخیص تقلب، استفاده از روش‌های داده‌کاوی است که بر تحلیل‌های آماری و کشف رفتار مشتریان و استفاده از الگوها برای شناسایی جرم تمرکز دارند(چن و دو[2]، ۲۰۰۹ و پون و همکاران[3]، ۲۰۰۹). این روش‌ها مبتنی بر بر یادگیری قواعدی خاص هستند و قادرند شاخص‌های رفتار فریب‌آمیز را از پایگاه داده‌های بزرگ تراکنش های کاربران کشف کنند. این شاخص‌ها برای ایجاد سیستم‌های پایشگر[4] استفاده می‌شوند تا رفتارهای غیرمعمول مشتریان را ثبت و رفتارهای مشکوک را از میان آن ها شناسایی کنند. در نهایت خروجی این سیستم‌ها می‌تواند برای اعلام هشدار و اخطار درخصوص کاربران متخلف استفاده شود(فانگ و همکاران[5]، ۲۰۰۷). روش دیگری که تاکنون برای شناسایی و تشخیص جرم استفاده شده شبکه‌های عصبی مصنوعی است که قابلیت استخراج الگو از پایگاه داده‌های حاوی تراکنش‌های گذشته ی مشتریان را دارند. این شبکه‌ها آموزش پذیرند و قابلیت انطباق با شکل های جدید جرم را دارا هستند(یه و لین[6]،۲۰۰۹).

۲-۲- سیستم های دانش‌محور

سیستم‌های دانش محور به عنوان یک سیستم کامپیوتری طراحی شده برای پیروی از روش حل مسأله از سوی انسان از طریق ترکیب هوش مصنوعی[7] و یک پایگاه داده[8] از دانش موضوعات خاص تعریف می‌شوند(وانگ و همکاران، ۲۰۰۸).اجزای اصلی سیستم-های دانش محور، دانش‌محوری[9] و مکانیسم‌های استنباط/استدلال[10] است(کلارک و

1-Dandash et al
2-Chen & Du
3-Poon & etal
4-monitoring
5-Fang et al
6-Yeh and Lien
7-Artificial Intelligence
8-Database
9-Knowledge-base
10-Inference/reasoning mechanism

سلیمان[1]،۱۹۹۹: ۶۹). بنابراین دانش محوری، قلب یا عنصر اصلی سیستم‌های دانش-محور است و دربرگیرنده ی دانش خبره ی ذخیره شده از طریق تکنیک‌های بازنمایی[2] گوناگون است، (مانند شبکه های معنایی[3]، قواعد و منطق[4]) و به طور وسیعی از تکنیک-تکنیک‌ها یا روش «اگر(شرط) پس(عمل)»[5] برای تولید قانون[6] استفاده می‌کنند(چائو و و آلبرمانی[7]،۲۰۰۲). در این تحقیق به منظور توسعه ی سیستم دانش‌محور کشف تقلب در شرکت‌های بیمه‌ای از ترکیب سیستم‌های خبره با رویکرد فازی در قالب تکنیک داده کاوی استفاده می‌شود.

سیستم‌های خبره یا سیستم‌های مبتنی بر قاعده، سیستم‌هایی هستند که از دانش افراد خبره برای حل مشکلات دنیای واقعی، که معمولاً به هوش انسان نیاز دارند استفاده می‌کنند(لی آئو[8]، ۲۰۰۴» ۱۰۱-۱۰۵). دانش خبره معمولاً به شکل قواعد یا داده‌هایی برای رایانه تعریف می‌شوند. این نوع سیستم ها در حال حاضر نقش بسیار مهمی در سیستم‌های هوشمند بازی می‌کنند و معمولاً برای اهداف برنامه ریزی، طراحی، تشخیص خطا و غیره استفاده می‌شوند(آبراهام[9]،۲۰۰۵). بر این اساس، سیستم خبره ی فازی یک سیستم خبره است که برای استدلال داده‌ها از مجموعه‌ای از توابع عضویت و قواعد فازی به جای منطق دودویی استفاده می‌کند(ای شال و موریس[10]،۲۰۰۰).

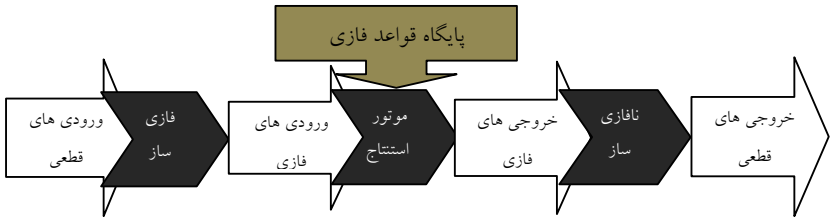
۲-۳- رویکرد فازی در صنعت بیمه

امروزه با گسترش سیستم‌های پایگاهی و حجم بالای داده ها ی ذخیره شده در این سیستم‌ها، نیاز به ابزاری است تا بتوان داده‌های ذخیره شده پردازش کرد و اطلاعات

1-Clark & Soliman
2-Representation techniques
3-Semantic networks
4-Frames and logic
5-If (condition) then (action)
6-Rule
7-Chau & Albermani
8-Liao
9-Abraham
10-Ei-Shal & Morris

حاصل از این پردازش را در اختیار کاربران قرار داد(لارس[1]،۲۰۰۵ :۲۵۳- ۲۶۰). سیستم سیستم خبره ی فازی[2] یکی از مهم‌ترین این روش‌ها است که به وسیله ی آن الگوهای مفید در داده‌ها با حداقل دخالت کاربران شناخته می‌شوند و اطلاعاتی را در اختیار کاربران و تحلیل‌گران قرار می‌دهند تا براساس آن ها تصمیمات مهم و حیاتی در سازمان‌ها اتّخاذ شوند(مارتنز و همکاران[3]، ۲۰۰۸). برای پیاده سازی چنین فرایندی باید باید از روش نظام یافته استفاده کرد. سیستم خبره ی فازی یک سیستم خبره است که برای استدلال داده‌ها از مجموعه‌ای از توابع عضویت و قواعد فازی به جای منطق دودویی استفاده می‌کند(ای شال و موریس[4]، ۲۰۰۰). شکل شماره ی یک معماری پایه پایه ی یک سیستم خبره ی فازی را نمایش می‌دهد که اجزای اصلی آن عبارتند از: (هوآنگ و همکاران[5]، ۲۰۰۷ و سیلرو و باکلی[6]،۲۰۰۵).

فازی ساز: در فرایند فازی‌سازی روابط بین ورودی‌ها و متغیّرهای زبانی با استفاده از توابع عضویت تعریف می‌شود. در این مرحله مقادیر ورودی به درجه ی تعلق متغیّرهای زبانی متناظر تبدیل می‌شوند. در واقع متغیّرهای ورودی از طریق واحد فازی‌ساز به اعداد فازی تبدیل می‌شوند.



شکل شماره ی دو - معماری یک سیستم خبره ی فازی

1-Larose
2-Fuzzy expert system
3-Martens & etal
4-Ei-Shal and Morris
5-Huang et al
6-Siler and Buckley

پایگاه قواعدفازی (پایگاه دانش): پایگاه دانش از ترکیب دانش خبرگان حوزه ی مورد بحث به وجود می‌آید و به شکل قواعدی از متغیّرهای زبانی تشکیل می‌شود. بدین‌معنا که نظریات خبرگان جمع‌آوری و با استفاده از آن ها و به کارگیری عملگرهای سه گانه ی فازی (شامل "یا"، "و"، "نه") در میان آن ها، قواعد "اگر- آنگاه" ایجاد می‌شوند؛ این قواعد برای بیان ارتباط میان مجموعه‌های فازی ورودی و خروجی استفاده می‌شود. قواعد اگر- آنگاه فازی و استدلال فازی ستون فقرات سیستم‌های خبره هستند و به عنوان مهم ترین ابزار مدل‌سازی بر اساس نظریه ی مجموعه‌های فازی شناخته می‌شوند. به عبارت دیگر قاعده ی اگر-آنگاه فازی، عبارتی اگر-آنگاه است که برخی از کلمات آن توسط توابعِ عضویت مشخص شده‌اند.

موتور استنتاج (منطق تصمیم گیر): این بخش واحد تصمیم‌گیرنده ی سیستم فازی است. یک موتوراستنتاج قابلیت استنتاج خروجی‌ها با استفاده از قواعد و عملگرهای فازی را داراست؛ بدین معنا که عملگرهایی مانند: کمینه، بیشینه و مجموع را ترکیب و خروجی فازی را از مجموعه‌های فازی ورودی و روابط فازی استخراج کرده و از این طریق توانایی تصمیم‌گیری در انسان را شبیه‌سازی می‌کند. یک سیستم استنتاج فازی پایه می‌تواند ورودی‌ها را به صورت فازی یا قطعی دریافت کند ولی خروجی‌هایی که تولید می‌شوند همواره مجموعه های فازی هستند. به زبان ساده تر موتور استنتاج فازی بررسی چگونگی نتیجه‌گیری از روی یک مجموعه از قواعد است.

نافازی ساز: این مرحله عکس فرایند فازی‌سازی را انجام می‌دهد. نافازی‌ساز، یک خروجی با مقدار قطعی از مجموعه‌های فازی که خروجی موتور استنتاج هستند تولید می‌کند. در این مرحله خروجی قطعی استخراج می‌شود که بهترین نمایشگر مجموعه‌های فازی باشد. در نافازی ساز با مجموعه‌ای مبهم مواجه هستیم که رسیدن به یک عدد را مشکل می کند و همین امر باعث می‌شود که کار این بخش از بخش فازی ساز مشکل‌تر باشد.

روش شناسی سیستم‌های خبره ی فازی به علت توانایی در طراحی، مدل‌سازی و اجرای الگوریتم های مدیریت فروش، شامل؛ نرخ دهی و تعیین کارمزد، مدیریت روابط

مشتری، و مدیریت ریسک، شامل؛ مدیریت شکایات، مدیریت تقلب و اعتبار سنجی، به مدیریت شرکت های بیمه ای در بازار رقابتی کمک کند (ان گایی و همکاران[1]، ۲۰۰۹).

۳- روش شناسی تحقیق

۳-۱- سؤال‌های تحقیق

دست‌یابی به اهداف فوق مستلزم پاسخ گویی به سؤالات متعددی از قبیل: سیستمی که برای شناسایی رفتارهای مشکوک طراحی می‌شود باید دارای چه خصوصیاتی باشد تا هم اجرای آن عملی باشد و هم از اعتبار مناسبی برخوردار باشد؟ دانش موجود در سیستم بیمه ی الکترونیکی چیست و چگونه باید جمع‌آوری شود؟ جزئیات اجزای مختلف سیستم خبره ی فازی برای فازی ساز، استنتاج و نافازی ساز چیست؟ و اعتبار سیستم فازی طراحی شده در نزد خبرگان بیمه ی الکترونیکی تا چه حدی است؟ می‌باشد.

۳-۲- اهداف تحقیق

هدف اصلی این تحقیق تشخیص رفتارهای مشکوک کاربران بیمه ی الکترونیکی به کمک سیستم دانش محور با رویکرد سیستم خبره ی فازی است. بدین منظور، ضمن بررسی نظریه ی فازی و کاربرد آن در شناسایی تقلب بیمه‌ای، رفتارهای مختلف کاربران در بیمه ی الکترونیکی، تشخیص تراکنش‌های غیرمعمول و مشکوک در سامانه ی بیمه ی الکترونیکی و تشخیص رفتارهای غیرمعمول کاربران در سامانه ی بیمه ی الکترونیکی با استفاده از سیستم خبره ی فازی طراحی و انجام خواهد گرفت.

۳-۳- روش تحقیق و گردآوری داده ها

این تحقیق از حیث روش تحقیق، تحقیقی توصیفی- کمّی است که از دو روش تحلیل منطقی و مطالعه ی پیمایشی بهره برده است. در جمع آوری داده‌ها نیز از ابزارهای مختلف این فن یعنی: مصاحبه، پرسش نامه و بررسی اسناد استفاده شده است.

1-Ngai & et al

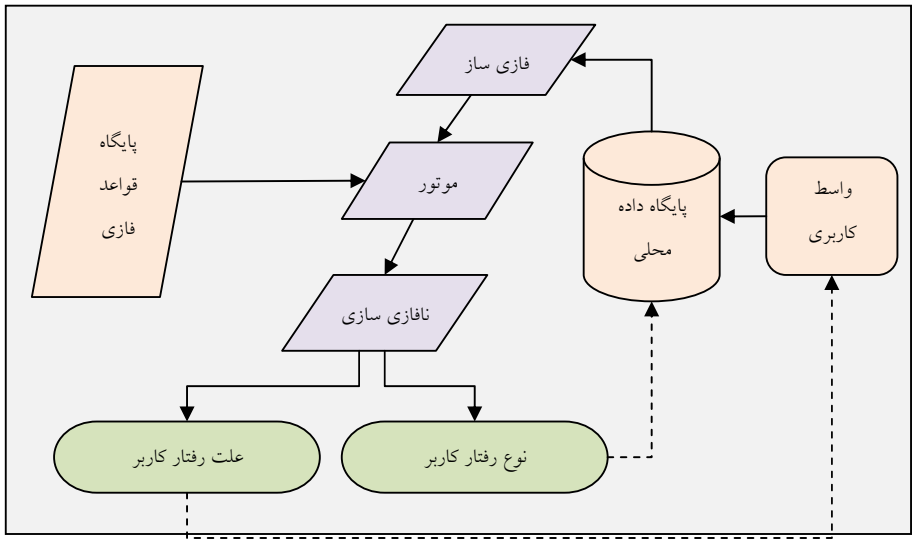
در این تحقیق، پیمایش داده‌ها به دو روش «پرسش‌نامه»[1] و «مصاحبه»[2] انجام شده است؛ به طوری که با تکمیل پرسش‌نامه و نیز مصاحبه از سوی خبرگان و متخصصان، به شناسایی عوامل مؤثر در شناسایی رفتارهای کاربران سیستم بیمه ی الکترونیکی پرداخته شده است. در این مرحله به کمک پرسش‌نامه و مصاحبه، می‌توان درباره ی مسأله و راه حل‌های آن اشراف کامل پیدا کرده و سپس برای طراحی، تست و اجرای سیستم خبره با رویکرد فازی برای تشخیص رفتارهای مشکوک کاربران بیمه ی الکترونیکی از متدلوژی سیستم‌های خبره ی فازی در قالب نرم افزار متلب استفاده گردید. انتخاب خبرگان برای انجام تحقیق، بر مبنای نمونه برداری تئوریک که در متدلوژی سیستم‌های خبره معمول می باشد، انجام شده است. نمونه برداری تئوریک عبارت است از، «گردآوری داده ها بر اساس مفاهیم شکل دهنده ی تئوری اولیه صورت می گیرد و بر مقایسه استوار است که هدف آن، بهینه ساختن مفاهیم شکل دهنده ی تئوری نهایی است و تلاش می کند به مفاهیم استحکام بیشتری ببخشد.» یعنی تا زمانی نمونه برداری ادامه می یابد که نمونه ی بعدی، مطلب تکمیل کننده ای به اجزای تشکیل دهنده ی تئوری نیفزاید که در بخش طراحی سیستم خبره ی فازی، به آن اشاره خواهد شد.

۴- طراحی سیستم کشف تقلب

۴-۱- طراحی

در این بخش اجزای سیستم خبره ی فازی طراحی شده برای تشخیص رفتارهای مشکوک کاربران بیمه ی الکترونیکی مطابق شکل شماره ی دو تشریح شده است. بدیهی است سیستم با هدف استفاده و آزمایش در سامانه ی بیمه ی الکترونیکی طراحی شده است؛ لذا در این بخش ابتدا نحوه ی تعیین متغیّرهای ورودی در سامانه ی بیمه ی الکترونیکی و مراحل فازی‌سازی آن ها توضیح داده شده است و سپس نحوه ی طراحی پایگاه دانش سیستم بیان می شود و در گام پایانی، سیستم با استفاده از داده‌های سامانه ی بیمه ی الکترونیکی شبیه سازی شده، مورد ارزیابی قرار گرفته است.

1-Questionnaire
2-Interview



شکل شماره ی دو - معماری سیستم شناسایی رفتارهای مشکوک

۴-۱-۱-تعیین عوامل ورودی

برای تعیین عوامل ورودی، سامانه ی بیمه ی الکترونیکی و جداول حاوی تراکنش-های انجام شده در یک سامانه به طور کامل مورد تحقیق قرار گرفت. برای استخراج متغیّرهای ورودی که در طراحی سیستم فازی مورد نیاز بود از نظر ۲۰ خبره ی بیمه ی الکترونیکی استفاده شد که در نتیجه ی آن برخی عوامل حذف و برخی اضافه شدند. از آن جا که واسطی کاربری، اطلاعات مربوط به متغیرهای ورودی سیستم را به شکل اعدادی قطعی دریافت می‌کند بعد از تحلیل نهایی، هفت عامل که در تعیین رفتار کاربر در سامانه ی بیمه ی الکترونیکی نقش دارد به عنوان متغیّرهای ورودی و یک عامل (رفتار کاربر) به عنوان متغیّر خروجی در سیستم تعیین شدند که نام و مفهوم هریک از آن ها مطابق جدول شماره ی یک است. لازم به ذکر است که با ذخیره ی اطلاعات این جدول در یک پایگاه داده ی محلی و اتصال آن به نرم افزار متلب، داده‌ها

و اقلام اطلاعاتی ورودی به صورت خودکار خوانده شده و مورد پردازش سیستم فازی طراحی شده قرار می‌گیرند.

جدول شماره ی یک - نام و مفهوم متغیّرهای زبانی ورودی و خروجی

ردیف	نام متغیّرها	نماد	واحد	مفهوم
۱	تعداد اشتباه	Mis	بار	تعداد خطاهای کاربر هنگام ورود به سیستم
۲	تعداد حواله	FtCnt	بار	تعداد حواله های اینترنتی که کاربر انجام داده است.
۳	مبلغ حواله	FtAmnt	صدهزاریال	مبلغ حواله های اینترنتی که کاربر انجام داده است.
۴	تعداد IP	IPCnt	-	تعداد IPهای مختلفی که در هنگام ورود کاربر به سامانه ثبت شده است.
۵	تعداد ISP	ISPCnt	-	تعداد ISPهای مختلفی که در هنگام ورود کاربر به سامانه ثبت شده است.
۶	تعداد مرورگر	BrwsrCnt	-	تعداد مرورگری که کاربر در یک روز استفاده کرده است.
۷	تعداد ورود	LCnt	بار	تعداد ورود موفق کاربر به سیستم
۸	رفتارکلی کاربر	Result	-	خروجی کلی – رفتاری که به کاربر تخصیص می‌یابد.

۴-۱-۲-تعیین متغیّرهای خروجی

هدف از طراحی این سیستم شناسایی رفتارهای مشکوک کاربران بیمه ی الکترونیکی است. همان گونه که مشخص است در شناسایی رفتارهای مشکوک، این واژه کاملاً مبهم است و ممکن است بر اساس نظر برخی از خبرگان طیف وسیعی از کاربران را در برگیرد و برعکس بر اساس نظریات برخی دیگر شامل تعداد کمی از کاربران باشد. از این جهت لازم بود تا این واژه با کمک نظریه ی فازی از حالت مبهم و پیچیده خارج شود؛ بر این اساس و با استفاده از قابلیت سیستم فازی در شناسایی رفتارهای مشکوک، نخست کلیه ی رفتارهای کاربران اعم از عادی و غیرعادی تعریف و در پنج سطح مختلف دسته‌بندی شد.

رفتارعادی: شامل کاربرانی است که عملیات آن ها به صورت عادی، بدون اشتباه و کامل انجام شده است. بدین معنا که این کاربران بدون انجام هیچ گونه اشتباهی وارد سامانه شده و پس از انجام تراکنش‌ها، از سیستم خارج شده‌اند، و می‌بایست طیف بسیار وسیعی از کاربران را دربرگیرند.

رفتارکمی مشکوک: شامل کاربرانی است که در هنگام ورود خطا دارند و به تلاش برای ورود غیر مجاز مظنون هستند. و یا بدون مشکل وارد سامانه می شوند ولی مشخصات مکانی آنان قابل شناسایی نیست.

رفتار مشکوک: شامل کاربرانی است که در هنگام ورود خطاهای پی‌درپی دارند و به تلاش برای ورود غیرمجاز مظنون هستند و یا بدون هیچ گونه مشکلی مرتباً و بیش از حد متوسط سایر کاربران وارد سامانه می شوند ولی تراکنشی انجام نمی دهند.

رفتار بسیارمشکوک: شامل کاربرانی است که به تلاش برای ورود غیرمجاز مشکوک هستند و هم چنین عملیات خاصی را خارج از عرف معمول تکرار می کنند؛ بدین معنا که در انجام یک تراکنش خاص مشکوک هستند.

رفتار خطرناک: شامل کاربرانی است که در بسیاری از فعالیت‌هایی که انجام داده‌اند مورد ظن می باشند یعنی رفتارهای یک کاربر مشکوک را دارند و یا پس از تلاش‌های بسیار زیاد موفق به ورود به سامانه می شوند و حتی تراکنشی نیز انجام می دهند.

همان‌طور که از معانی واژه‌ها بر می‌آید شدّت غیرمعمول بودن رفتارها به ترتیب از حالت عادی به خطرناک زیاد می‌شود. از آن جا که این واژه‌ها کاملاً غیرقطعی هستند به کمک اعداد فازی مدل شده و به عنوان متغیّرهای زبانی در خروجی سیستم فازی به کار گرفته شده‌اند؛ بدین معنا که نتیجه ی استنتاج سیستم فازی تخصیص کاربر به یکی از این پنج دسته خواهد بود. با توجه به توضیحات فوق نحوه ی دسته‌بندی رفتارها و بازه ی هریک از آن ها بر اساس عدد قطعی خروجی مطابق جدول شماره ی دو است. لازم به ذکر است که پس از پردازش ورودی ها با سیستم فازی نتایج خروجی نرم افزار متلب، به صورت خودکار به جدولی در یک پایگاه داده ی محلی منتقل می‌شوند.

جدول شماره ی دو - دسته بندی واژه های زبانی خروجی بر اساس عددقطعی خروجی

ردیف	نام متغیّرها	بازه
۱	عادی	[۰ ۰/۲)
۲	کمی مشکوک	[۰/۲ ۰/۴)
۳	مشکوک	[۰/۴ ۰/۶)

ردیف	نام متغیّرها	بازه
۴	بسیارمشکوک	(۰/۶ ۰/۸]
۵	خطرناک	[۰/۸ ۱]

با توجه به مواردی که ذکر شد سه خروجی مکمّل برای کمک به شناسایی بهتر علل رفتارهای مشکوک کاربران طراحی شدند. این خروجی‌ها شامل رفتارهای پرداخت کاربر، رفتارهای هنگام ورود کاربر و رفتارهای مربوط به مشخصات غیرمالی کاربر است. سپس هریک از این خروجی ها به چهار دسته ی A, B, C, D تقسیم شدند که جزئیات هر گروه به همراه مفهوم دسته‌ها در ادامه آمده است.

رفتارهای پرداخت در سامانه: شامل متغیّرهایی است که عملیات مالی کاربران مانند مبلغ و تعداد حواله‌ها را در بر می‌گیرد.

رفتارهای ورود به سامانه: شامل متغیّرهایی است که در هنگام ورود کاربر به سامانه ی بیمه ی الکترونیکی مورد توجه است، مانند تعداد ورود به سامانه و یا تعداد اشتباه در هنگام ورود.

رفتارهای مربوط به نحوه ی اتصال کاربر به سامانه: شامل متغیرهایی است که نحوه ی اتصال کاربر به سامانه را در برمی‌گیرد مانند تعداد IP و مرورگر کاربر.

این خروجی‌های مکمّل کمک می‌کنند تا کاستی‌های عدم دانایی در مورد جزئیات رفتار کاربران کمرنگ و توانایی تصمیم‌گیری بیشتر شود. در ادامه، هریک از دسته هایی که برای این خروجی‌ها تعریف شده‌اند تشریح می شوند. دسته ی A یا عادی : کلیه ی رفتارهای این گروه از هر دسته کاملاً عادی است؛ دسته ی B یا نیمه عادی: رفتارهای این گروه از کاربران در هر دسته ی جداگانه نیمه عادی و با کمی خطا همراه است؛ دسته ی C یا غیرعادی: رفتارهای این گروه از کاربران متفاوت از دیگران و یا همراه با خطاهای قابل توجه است؛ دسته ی D یا بسیارغیرعادی: رفتارهای این گروه از کاربران بسیار متفاوت از دیگران و یا همراه با خطاهای بسیار است. با توجه به توضیحات فوق نحوه ی دسته‌بندی رفتارها و بازه ی هریک از آن ها بر اساس عدد قطعی خروجی مطابق جدول شماره ی سه است.

جدول شماره ی سه - دسته بندی واژه های زبانی خروجی بر اساس عددقطعی خروجی

ردیف	نام متغیّرها	بازه
۱	عادی	[۱ ۲/۵)
۲	نیمه عادی	[۲/۵ ۵)
۳	غیرعادی	[۵ ۷/۵)
۴	بسیار غیرعادی	[۷/۵ ۱۰]

۴-۱-۳- فازی‌سازی[1]

در فرایند فازی‌سازی روابط بین ورودی‌ها و متغیّرهای زبانی با استفاده از توابع عضویت تعریف می‌شود. در این مرحله مقادیر ورودی به درجه ی تعلق متغیّرهای زبانی متناظر تبدیل می‌شوند. در واقع متغیّرهای ورودی از طریق واحد فازی‌ساز به اعداد فازی تبدیل می‌شوند. وظیفه ی واحد فازی ساز در این سیستم خواندن مقدار قطعی متغیّر ورودی و تبدیل آن به یکی از مقادیر واژگان فازی موجود در قواعد پایگاه دانش سیستم خبره ی فازی است. فازی ساز باید حجم محاسباتی زیادی نداشته و حتی در محاسبات مربوط به موتور استنتاج اثر مثبت داشته باشد. در این تحقیق هر متغیّر ورودی به علت محاسبات ساده‌تر به یک عدد فازی مثلثی تبدیل شده است. هرعدد فازی‌مثلثی با سه‌تایی $\tilde{A}=(a_1,a_2,a_3)$ نشان داده می‌شود که در آن $a_1 \le a_2 \le a_3$ است و تابع عضویت آن به شکل زیر نمایش داده می‌شود:

$$\mu_{\tilde{A}}=\begin{cases}0 & x<a_1\\ (x-a_1)\big/(a_2-a_1) & a_1\le x\le a_2\\ (x-a_3)\big/(a_2-a_3) & a_2\le x\le a_3\\ 0 & x>a_3\end{cases} \qquad (۱)$$

1-Fuzzification

هم چنین برای فازی‌سازی عوامل ورودی از فازی‌ساز تکین[1] به شکل زیر استفاده شده است این فازی ساز نقطه ی قطعی $X^* \in U$ را به مجموعه ی فازی A' در U به شکل زیر می‌نگارد:

$$\mu_A(x) = \begin{cases} 1 & X = X^* \\ 0 & e.w. \end{cases} \qquad (۲)$$

۴-۱-۴- تولید پایگاه قواعد فازی

در یک سیستم خبره ی فازی، پایگاه قواعد فازی یکی از مهم‌ترین بخش‌های سیستم به شمار می‌آید. در واقع پایگاه دانش[2] از ترکیب دانش خبرگان حوزه ی مورد بحث به وجود می‌آید و به شکل قواعدی از متغیّرهای زبانی تشکیل می‌شود. در سیستم طراحی شده در این تحقیق متغیّرهای زبانی و حدود آن ها با بهره گیری از نظریات خبرگان تعیین شد که در بخش عوامل ورودی و خروجی به طور کامل تشریح شده است. برای ایجاد پایگاه قواعد فازی در سیستم حاضر، قواعد مبهمی که در سامانه ی بیمه ی الکترونیکی برای تشخیص و شناسایی رفتارهای غیرمعمول کاربرد دارد با کمک نظریات خبرگان جمع‌آوری و استخراج شده و با به کارگیری عملگرهای سه‌گانه ی فازی (شامل "یا"، "و"، "نه") در میان هفت متغیّرزبانی ورودی، ۲۱۰ قاعده ی "اگر- آنگاه" ایجاد شد که اغلب از قواعد مرکب (با ترکیب کننده ی "و") تشکیل شده است. نیمی از این قواعد برای شناسایی نوع رفتار کاربر و نیمی دیگر برای تشخیص علت رفتار کاربر طراحی شده اند. نمونه ای از قوانین پایگاه دانش فازی عبارت است از:

اگر کاربری، بدون اشتباه و تعداد حواله کم و مبلغ حواله کم و تعداد آی پی کم و تعداد ورود کم و تعداد مرورگر کم وتعداد آی اس پی کم باشد آنگاه رفتار عادی است.

۴-۱-۵- نافازی‌ساز[3]

در این تحقیق مقادیری که از موتور استنتاج سیستم خبره به دست می‌آیند فازی است و لازم است تا این مقادیر به مقادیر غیرفازی مناسب تبدیل شوند؛ در واقع این

1-singleton fuzzifier
2-Knowledge base
3-Defuzzifier

مرحله عکس فرایند فازی‌سازی را انجام می‌دهد. نافازی‌ساز، یک خروجی با مقدار قطعی از مجموعه‌های فازی که خروجی موتوراستنتاج هستند تولید می‌کند؛ بدین‌معنا که خروجی موتور استنتاج (نتایج به‌دست آمده از قواعد) ورودهای بخش نافازی‌ساز است.

۴-۱-۶- موتور استنتاج[1]

همان طور که گفته شد این بخش واحد تصمیم‌گیر سیستم‌فازی است. در این تحقیق از بین دو روشی که برای استنتاج وجود دارد از استنتاج مبتنی بر قواعد جداگانه استفاده شده است، چراکه هدف به دست آوردن قواعد از نتیجه ی تمام قواعدی است که هریک توانایی تولید خروجی فازی موردنظر را دارد. همه ی قواعد موجود در پایگاه قواعد به شکل رابطه‌ای یکتا و به صورت اگر-آنگاه خلاصه می‌شوند و از عملگر اجتماع برای ترکیب قواعد استفاده شده است تا محافظه کارانه عمل کند و از تمامی قواعد در نتیجه گیری نهایی استفاده شود. دراین تحقیق موتوراستنتاج ممدانی[2] به عنوان هسته ی سیستم خبره ی فازی تشخیص رفتارهای مشکوک کاربران در سامانه ی بیمه ی الکترونیکی انتخاب شد که حاوی مشخصاتی از جمله: استنتاج مبتنی بر قواعد جداگانه است که از ترکیب اجتماع استفاده می‌شود. با این عمل هر قاعده قبل از ادغام شدن در سایر قواعد در تعیین خروجی نقش دارد؛ استلزام از نوع کمینه ِی ممدانی است تا شرایط تخصیص کاربران به هر دسته دقیق‌تر باشد؛ از عملگر کمینه برای تمامی عملگرهای نرم t استفاده شده است تا محافظه کارانه عمل شود؛ از عملگر بیشینه برای همه ی عملگرهای نرم s استفاده شده است تا از حداکثر توان استفاده شود.

۴-۲- ارزیابی سیستم

در این مرحله سیستم خبره ی فازی با استفاده از اطلاعاتی که از محیط واقعی سیستم به‌دست آمده بود به مرحله ی اجرا درآمد. برای ارزیابی سیستم، چندین نمونه از عناوین اطلاعاتی مربوط به کاربران مختلف که از پایگاه داده ی یکی از شرکت‌های بیمه وجود داشت به سیستم داده شد که در ادامه تشریح می‌شود. برای آزمایش عملکرد سیستم خبره ی طراحی شده، بیش از ۱۰۰۰۰ رکورد حاوی اطلاعات رفتاری مشتریان

1-Inference engine
2-Mamdani

به عنوان ورودی به سیستم داده شد که نتایج آن ها به همراه نظر خبرگان در مورد آن ها در جدول شماره ی چهار آمده است. لازم به ذکر است که اطلاعات مربوط به رفتارهای عادی به دلیل این که طیف بسیار وسیع (بیش از ۹۹ درصد) کاربران را دربرگرفته که از این تعداد ۵ رکورد به عنوان نمونه در ردیف های ۱ تا ۵ جدول نمایش داده شده است. هم چنین رفتارهای کمی مشکوک به ۸ کاربر از ردیف ۶ تا ۱۳ جدول اختصاص یافته است، رفتارهای مشکوک شامل کاربران ردیف های ۱۴ تا ۲۰ است و ۳ کاربر دیگر از ردیف ۲۱ تا ۲۳ بسیار مشکوک بوده‌اند. علاوه بر این، یک کاربر رفتار خطرناک داشته است که مشخصات آن در ردیف آخر جدول نمایش داده شده است .

بدیهی است هرچه خروجی سیستم (ستون نتیجه) به ۱ نزدیک تر باشد رفتار کاربر با شدت بیشتری مشکوک است (بر مبنای جدول شماره ی دو، قابل تحلیل خواهد بود). ستون آخر جدول به نظر خبرگان در مورد این خروجی ها اختصاص یافته است که همان طور که مشاهده می شود به جز دو رکورد بقیه ی خروجی ها مورد قبول کارشناسان بیمه ی الکترونیکی و طبق نظر آن ها نتایج این سیستم تا حدود ۹۲ درصد با واقعیت هم خوانی دارد.

جدول شماره ی چهار - نتیجه ی اجرای سیستم به همراه نظر خبرگان

ردیف	تعداد قبض	تعداد ISP	تعداد IP	تعداد مرورگر	تعداد تلاش ناموفق	تعداد ورود موفق	متوسط مبلغ حواله ها	تعداد حواله	نتیجه (خروجی سیستم)	نظر خبرگان
۱	0	1	1	1	0	2	280001	4	0/061	T
۲	0	1	1	1	0	8	0	0	0/076	T
۳	0	1	1	1	0	2	3500000	2	0/061	T
۴	0	1	1	1	0	1	4000000	2	0/071	T
۵	6	1	2	1	0	5	1500000	2	0/061	T
۶	0	2	2	1	2	5	3500000	2	**0/213**	T
۷	0	2	2	1	2	5	0	0	**0/213**	T
۸	0	2	2	1	2	4	16633333	6	**0/213**	T
۹	0	1	1	1	0	24	0	0	**0/267**	T
۱۰	118	1	1	1	0	24	3000000	3	**0/267**	T
۱۱	8	1	6	1	0	8	0	0	**0/308**	T
۱۲	42	1	2	1	2	14	0	0	**0/311**	T

ردیف	تعداد قبض	تعداد ISP	تعداد IP	تعداد مرورگر	تعداد تلاش ناموفق	تعداد ورود موفق	متوسط مبلغ حواله ها	تعداد حواله	نتیجه (خروجی سیستم)	نظر خبرگان
۱۳	31	1	1	1	2	8	0	0	**0/315**	T
۱۴	0	1	1	1	3	3	4924000	3	**0/490**	F
۱۵	209	1	1	1	0	40	5650000	4	**0/5**	T
۱۶	0	1	1	1	1	35	0	0	**0/5**	T
۱۷	0	1	1	1	0	37	0	0	**0/5**	T
۱۸	303	1	1	1	0	47	5000000	10	**0/5**	T
۱۹	0	1	1	1	0	78	0	0	**0/5**	T
۲۰	0	4	4	1	4	14	0	0	**0/512**	T
۲۱	9	2	2	1	3	7	0	0	**0/603**	T
۲۲	0	1	1	1	3	1	0	0	**0/603**	T
۲۳	0	3	3	1	5	9	0	0	**0/725**	F
۲۴	0	1	1	1	8	1	0	0	**0/911**	T

در این بخش معماری سیستم خبره ی فازی طراحی شده برای تشخیص رفتارهای مشکوک کاربران بیمه ی اینترنتی تشریح شده است. استفاده از نظریه ی مجموعه‌های فازی در طراحی سیستم خبره، روشی را برای محاسبه ی داده‌ها و اطلاعات غیر قطعی و مبهم ارائه می‌کند؛ ضمن این که سازوکار استنتاج، برای استدلال را براساس مجموعه‌ای از قواعد "اگر-آنگاه" فراهم می‌سازد. این قواعد به کمک مجموعه‌های فازی تعریف می‌شوند که در آن ها هریک از اعضای مجموعه درجه ی تعلقی بین صفر و یک دارند. در سیستم طراحی شده در این تحقیق، نوع عملکرد کاربر در مواجهه با سیستم بیمه ی الکترونیکی، به عنوان ورودی سیستم فازی در نظر گرفته شده است. این سیستم هم چنین دو نوع خروجی دارد. خروجی اول، یکی از پنج دسته رفتار عادی، کمی مشکوک، مشکوک، بسیار مشکوک و خطرناک کاربر خواهد بود و خروجی دوم علت رفتار کاربر تشخیص داده می‌شود. مهم ترین مزیت این سیستم نسبت به روش های به کار رفته در سایر مقالات، نخست امکان مدلسازی رفتار کاربران در پنج دسته ی مختلف است که با دقت بیش تری نوع رفتار کاربر را پیش‌بینی می‌کند و دیگر آن که تشخیص حیطه ی مشکوک بودن رفتار کاربر، اطلاعات بیشتری در مورد کاربر خاطی در اختیار قرار خواهد داد که در نوع برخورد با کاربر فوق کمک زیادی خواهد کرد.

۵- نتیجه گیری

گسترش روند گرایش مردم برای انجام عملیات بانکی و بیمه ای به طور الکترونیکی برای بانک ها و بیمه ها هم یک تهدید است و هم یک فرصت. شرکت های مالی که در ارائه ی همگانی این‌گونه خدمات با شکست مواجه شوند در معرض خطرِ از دست دادنِ تعداد زیادی از مشتریان خود قرار خواهند گرفت و شرکت هایی که با سرعت به سوی ارائه و ارتقای خدمات برخط[1] می‌روند فرصت آن را خواهند داشت که مشتریان بیشتری جذب کنند، مناطق جغرافیایی وسیع تری را تحت پوشش قرار دهند و اعتبار خود را در مقابل مشتریان افزایش دهند. چالش های متعددی پیش‌روی پیاده سازی بیمه ی الکترونیکی قرار دارند که چالش های امنیتی از مهم‌ترین آن هاست؛ زیرا بیمه ها و مؤسسات مالی به حجم عظیمی از سوابق عملکرد و اطلاعات مالی مشتریان دسترسی دارند و امکان سوء استفاده از این اطلاعات یکی دیگر از چالش‌های پیش‌روی شرکت های مالی و مشتریان آن هاست.

خروجی حاصل از سیستم خبره ی فازی طراحی شده به نحوه ی طراحی قوانین پایگاه دانش فازی بستگی دارد که بر اساس نظریات خبرگان در حوزه ی بیمه ی الکترونیکی طراحی شده است. سیستم خبره ی طراحی شده می‌تواند کلیه ی رفتارهای کاربران را شناسایی و آن ها را در قالب پنج گروه عادی، کمی مشکوک، مشکوک، بسیار مشکوک و خطرناک دسته‌بندی کند. این سیستم در محیط نرم افزار متلب طراحی شده و با استفاده از قابلیت های نرم افزار قادر است تا با اتصال به یک پایگاه داده ی محلی بتواند به صورت خودکار اطلاعات ورودی را دریافت و نتایج خروجی را نیز به صورت خودکار در پایگاه داده ی محلی ثبت کند، لذا پردازش تعداد زیادی داده در زمانی کوتاه امکان پذیر است.

منابع

-Abraham, A. (2005) ***Rule-based Expert Systems Sydenham***, P. H. & Thorn, R. (Eds.) Handbook of Measuring System Design. John Wiley & Sons.

1-Online

-Aduloju, S. A., Odugbesan, A. O., Oke, S. A. (2009) «The effects of advertising media on sales of insurance products: A developing-country case», ***The Journal of Risk Finance***, Vol. 10, No. 3, PP. 210-227.

-Bignell, K. B. (2006) ***Authentication in an Internet Banking and Insurance Environment;*** Towards Developing a Strategy for Fraud -Detection, Internet Surveillance and Protection, 2006. ICISP '06. International Conference on. Cote d'Azur, IEEE Xplore.

-Chau, K. W., Albermani, F.(2002) «Expert system application of preliminary design of water retaining structures», E***xpert Systems with Applications***, Vol. 22, No. 2, PP. 169-178.

-Chen, W. S., Du, Y. K.(2009) «Using neural networks and data mining techniques for the financial distress prediction model», ***Expert Systems with Applications***, Vol. 36, PP. 4075- 4086.

-Clark, J. A., Soliman, F. (1999)«A graphical method for assessing knowledge-based systems investments», ***Logistics Information Management,*** Vol. 12, No. 1, PP. 63-77.

-Czuchry, A. W., Yasin, M. M., Sallmann, F. (2004) «An applied e-business approach for reinsurance services», ***Marketing Intelligence & Planning***, Vol. 22, No. 7, PP. 716-731.

-EI-Shal, S. M., Morris, A. S. (2000)«A fuzzy system for fault detection in statistical process control of industrial processes», ***IEEE Transactions on Systems***, Man, and Cybernetics- Part C: Applications and Reviews, Vol. 30, PP. 281-292.

-Fang, L., Cai, M., Fu, H. & Dong, J. (2007) ***Ontology-Based Fraud Detection***, Computational Science – ICCS 2007.

-Huang, Y.-P., Lu, C.-C. & Chang3, T.-W. (2007) «an Intelligent Approach to Detecting the Bad Credit Card Accounts», 25th

IASTED International Multi-Conference Artificial Intelligence and Applications, Innsbruck,Austria, IEEE.

-Kirkos, E., Spathis, C. & Manolopoulos, Y. (2007) «Data Mining techniques for the detection of fraudulent financial statements», ***Experts Systems with Application***, 32, 995-1003.

-Labuschagne, L., Eloff, J. H. (2000) «Electronic commerce: The information-security challenge», ***Information Management & Computer Security***, Vol. 8, No. 3, PP. 154-157.

-Larose, D. T. (2005) ***Discovering Knowledge in Data***, A John Wiley & Sons, Inc., Publication.

-Liao, S. H. (2004) «Expert system methodologies and applications: A decade review from 1995 to 2004», ***Expert Systems with Applications***, Vol. 28, PP. 93-103.

-Martens, D., Bruynseels, L., Baesens, B., Willekens, M., Vanthienen, J. (2008) «Predicting going concern opinion with data mining», ***Decision Support Systems***, Vol. 45, PP. 765- 777.

-Ngai, E. W. T., Xiu, L., Chau, D. C. K. (2009) «Application of data mining techniques in customer relationship management: A literature review and classification», ***Expert Systems with Applications***, Vol. 36, PP. 2592- 2602.

-Dandash, O., Wang, Y., Srinivasan, P. D. L. B. (2008) «Fraudulent Internet Banking and Insurance Payments Prevention using Dynamic Key», ***Journal of Networks***, Vol. 3, PP. 25-35.

-Park, J., Lee, S., Kang, H. B. (2009) «The insurance distribution systems and efficiency in the property-casualty insurance industry», ***Managerial Finance***, Vol. 35, No. 8, PP. 670-681.

-Phua, C. W. C. (2003) ***Investigative Data Mining in Fraud Detection***, School of Business Systems. Monash University.

-Poon, S. K., Davis, J. G., Choi, B. (2009) «Augmenting productivity analysis with data mining: An application on IT business value», ***Expert Systems with Applications***, Vol. 36, PP. 2213-2224.

-Quah, J. T. S., Sriganesh, M. (2007) «Real-time credit card fraud detection using computational intelligence», ***Expert Systems With Applications***, Vol. 35, No. 4, PP. 1721-1732.

-Rice, E. (2001) «The future of the insurance market- do insurance need crystal balls?», ***Balanced Sheet***, Vol. 9, No. 1, PP. 14-16.

-Riley, F. D., Scarpi, D., Manaresi, A. (2009) «Purchasing services online: A two-country generalization of possible influences», ***Journal of Services Marketing***, Vol. 23, No. 2, PP. 92-102.

-Siler, W. & Buckley, J. J. (2005) ***Fuzzy Expert Systems and Fuzzy Reasoning***, Hoboken, New Jersey., John Wiley & Sons, Inc.

-Wang, H. and Wang, S. (2008)«A knowledge management approach to data mining process for business intelligence», ***Industrial Management & Data Systems***, Vol. 108, No. 5, pp. 622-634.

-Wang, W. K., Huang, H. C., Lai, M. C.(2008) «Design of a knowledge-based performance evaluation system: A case of high-tech state-owned enterprises in an emerging economy», ***Expert Systems with Applications***, Vol. 34, PP. 1795-1803.

-Yeh, I-C., Lien, C.(2009)«The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients», ***Expert Systems with Application***, Vol. 36, PP. 2473-2480.