نشریـه علمـی دانش مالی تحلیل اوراق بهادار
دوره ۱۶ / شماره ۵۹ / پاییز ۱۴۰۲
صفحه ۵۰ تا ۷۵

ارائه مدل سیاست گذاری فارنزیک بانکداری الکترونیک

افشین خدامرادی[۱]
علیرضا پورابراهیمی[۲]*
محمد علی افشار کاظمی[۳]

تاریخ دریافت: ۱۴۰۱/۰۸/۰۷ تاریخ پذیرش: ۱۴۰۱/۱۲/۰۳

چکیده

در صنعت بانکداری امروز با توجه به پیچیدگی ابزارها و تنوع فعالیت‌های بانکی و ارتباطات درون سیستمی، حفظ سلامت و ثبات نظام بانکی از مهمترین دلایل نظارت بر بانک ها و مؤسسات اعتباری است، از طرف دیگر مجرمان اینترنتی می‌توانند صدمات شدیدی وارد نمایند. این تحقیق توصیفی-کمّی است که از دو روش تفکر عمیق و مطالعه‌ی پیمایشی بهره برده ودر جمع‌آوری از ابزار مختلف (مصاحبه، مشاهده، پرسشنامه و بررسی اسناد) استفاده شده است. جامعه آماری این تحقیق بررسی لاگ های رخدادهای سایبری طی یک سال اخیر می‌باشد و نمونه‌گیری خاصی صورت نگرفته است. پس از ارائه مدل، با توجه به نیازمندی‌های پروژه، از شبیه‌سازهای معمول و مخصوصاً *Matlab* استفاده و نتایج بر اساس سرعت اجرا بررسی می‌شود. انتظار می‌رود سامانه‌ی طراحی شده برای تشخیص گونه‌های مختلف جرم‌شناسی ناشی از رخداد های سایبری در اینترنت انعطاف‌پذیری بالایی داشته و بتواند برای انواع دیگر وبگاه‌ها مورد استفاده قرار گیرد.

کلمات کلیدی: تجارت الکترونیکی، جرم‌شناسی، رخداد های سایبری، وبگاه، بانکداری

[۱]دانشجوی دکتری مدیریت فناوری اطلاعات دانشگاه آزاد اسلامی واحد بین الملل قشم *akmoradi231@gmail.com*
[۲]استادیار وعضوهیئت علمی دانشکده مدیریت و حسابداری دانشگاه آزاد اسلامی واحد کرج *support@apebrahimi.com*
[3]دانشیار گروه مدیریت صنعتی دانشگاه آزاد اسلامی واحد تهران مرکزی *m_afsharkazemi@iauec.ac.ir*

مقدمه

رشد و گسترش روزافزون فناوری اطلاعات و ارتباطات، انقلابی را در ابعاد مختلف زندگی انسانها و عملکرد سازمان ها ایجاد کرده است. این فناوری روش های کارکرد و نگرش افراد، سازمانها و دولت ها را دگرگون ساخته و باعث ایجاد صنایع نوین، مشاغل جدید و خلاقیت در انجام امور شده است. ظهور پدیده هایی چون آموزش الکترونیکی، کسب و کار الکترونیکی، تجارت الکترونیکی و بانکداری الکترونیک از نتایج عمده نفوذ و گسترش فناوری اطلاعات در ابعاد مختلف است که البته بانکداری الکترونیک یکی از مهمترین پدیده های یاد شده می باشد[۱]. هر فناوری جدید برای متداول شدن و توسعه یافتن، پیش از پذیرش عمومی نیازمند مقبولیت قانونی است تا کلیه ظرفیت های آن مورد استفاده قرار گیرد. یعنی اگر به دنبال فرآیند بانکداری الکترونیک با استقبال عمومی می باشیم، می بایست بسترهای قانونی مورد نیاز را فراهم نماییم و با شناخت تمامی احتمالات روند بانکداری الکترونیک، درصد ریسک و ناپایداری آن حوزه را کاهش دهیم[۲]. در حال حاضر وجود مجرمانی که قصد بدست آوردن اطلاعات فضای مجازی را داشته باشند امری بدیهی و غیر قابل انکاراست. با گسترش اینترنت یک مبحث قدیمی که حتی قبل از وجود اینترنت وجود داشت، وارد دنیای دیجیتال شد. و آن مبحثی به نام فارنزیک می باشد[۳]. فارنزیک در لغت به معنی دادگاه است، اما در اصطلاح و علوم مختلف آن را جرم شناسی می گویند. فارنزیک فرآیندی جهت جمع آوری اطلاعات و شواهد به منظور چرایی و چگونگی اتفاق افتادن واقعه ای است، که در شاخه ها و علوم مختلف کاربرد دارد. فارنزیک یا جرم شناسی در شاخه کامپیوتر به مجموعه تکنیک ها و روش ها جهت گردآوری، نگهداری و تحلیل اطلاعات دیجیتال گفته می شود[۱].

با توجه به وجود ابهام و خلاء های بسیار در شناسایی جرم های سایبری و دیجیتالی در سطح کشور و حوزه پر اهمیت بانکداری الکترونیک و دیجیتال، تدوین مدل و الگویی نظام مند و علمی جهت شناسایی این جرایم که یک نیاز ملی می باشد ضروری به نظر می رسد. در این تحقیق، اطلاعات مربوط به مولفه‌های پژوهش و پیشینه آن از روش‌های کتابخانه‌ای و استفاده از مقالات موجود در پایگاه اطلاعاتی معتبر(مانند *Science Direct*، *Springer*، *IEEE*، . . .)، انجام مصاحبه با نخبگان، مدیران و کارشناسان خبره حوزه فارنزیک بانکداری الکترونیک جمع آوری شده و در پایان پس از تحلیل چگونگی رخدادها، دلایل فنی وقوع رخداد، تحلیل نوع رخداد، و دسته بندی آن ها به منظور ارتقای سطح تشخیص جرم‌شناسی در بانکداری الکترونیک مدلی جهت سیاست گذاری جرم شناسی بانکداری الکترونیک ارائه خواهد گردید.

بیان مسئله

در دنیای امروز مسائل و مشکلات بانکی نه تنها در درون مرزهای ملی به دیگر بانک‌ها و سازمانهای مشابه سرایت می‌کند، بلکه از مرزهای ملی فراتر رفته و مؤسسات مالی سایر کشورها را نیز تحت تاثیر قرار می‌دهد[۳]. بانک‌ها و مؤسسات اعتباری نقش محوری دررشد و شکوفایی اقتصاد کشورها ایفا می‌کنند. صنعت بانکداری در کشور ما در سال‌های اخیر دچار تحولات چشمگیری شده است. از مهمترین تحولات در زمینه بانکداری می‌توان به تعامل گسترده بانک های داخلی با بانک ها و سازمان های بین‌المللی و مبارزه با پدیده پولشویی، تعدد روزافزون بانک ها و مؤسسات اعتباری، رقابت شدید بین آن‌ها، استفاده از ابزارهای جدید بانکداری و گسترش فعالیت بانکداری الکترونیک اشاره کرد. طبیعی است که همگام با تحولات صنعت بانکداری، نظارت براین صنعت نیز دستخوش تحولات شگرف شود و بر اهمیت آن افزوده شود. با عنایت به تأثیر قابل ملاحظه بانک ها و مؤسسات اعتباری بر رشد و شکوفائی اقتصادی وتأثیرگذاری آن‌ها بر متغیرهای کلان اقتصادی از قبیل رشدنقدینگی، تورم وبیکاری، نیاز به تحول درنظارت بانکی به منظور انطباق بانک ها و مؤسسات اعتباری با سیاست‌های پولی و بانکی وجلوگیری از تخلف آن‌ها از قوانین و مقررات احتیاطی و نظارتی و حفظ ثبات وسلامت سیستم بانکی و صیانت از منافع سپرده‌گذاران بیش ازپیش احساس می‌شود[۴]. از طرفی دیگر مجرمان اینترنتی می‌توانند صدمات شدیدی به رایانه های شرکت‌ها و حتی اشخاص بدون بر جای گذاشتن کوچکترین ردپائی وارد نمایند. اینترنت این توانایی را دارد که به رهبران گروه‌ها، مجریان ارشد مؤسسات مالی، قانونگذاران، مأمورین امنیتی در سطح بالا، مدیران

ریسک و دلالان یا واسطه‌های بیمه کمک نمایند یا اینکه ضرر و زیان برسانند اینترنت یا سایر پروتکل‌های انتقال داده‌ها، سبب تسهیل درجریان پردازش اطلاعات شده‌اند. در اقتصاد جدید اطلاعات سرمایه اولیه و مایع حیاتی (همانند خون در شریان‌ها) در هر شرکتی است و شرکت‌ها محتاطانه از آن محافظت می‌کنند. حتی شرکت‌هایی که به خوبی اداره و کنترل می‌شوند نیز به مباحثه و گفتگو درباره امنیت اطلاعات و مسائلی چون فناوری اطلاعات که به راه حل های اطلاعاتی نیاز دارد علاقه نشان می‌دهند[۴].

اطمینان از امنیت اطلاعاتی و ساختار اطلاعاتی سازمان موضوعی است که در سطح کل شرکت ها مطرح است و مسئولیت آن بر عهده مدیران عالی رتبه(اعضای هیات مدیره) و سایر اشخاص مهم در سازمان است. هر گونه اشکالی در امنیت شبکه اطلاعاتی سازمان اثرات گسترده و مخربی درسراسر سازمان دارد. در کل، نقص در خدمت رسانی یا قطع آن می تواند تا حدود زیادی بر سطح عملیاتی سازمان اثر بگذارد به گونه ای که یقیناً در چنین حالتی اگر اخبار و اطلاعاتی دچار نقص و اختلال گردند نام تجاری و شهرت سازمان آسیب خواهد دید[۵]. شبکه بانکی نیز مانند بسیاری دیگر از سازمانها و شرکتها از مشکلات و جرائم مرتبط با اینترنت فارغ نیست. امروزه و یا در آینده نه چندان دور، اکثر نقل و انتقال‌های پولی و مالی در بازار اقتصاد از طریق رایانه انجام می‌پذیرد. نتیجه این که توسعه داده‌های رایانه‌ای در بانک‌ها می‌تواند موجب ترس از قریب الوقوع بودن استفاده از روش‌های اجرایی از سوی بزهکاران متخصص شود[۶].

در عصرارتباطات به رغم این که شاهد گسترش وسایل و راه‌های ارتباطی پیشرفته هستیم و دستاوردهای ارتباطی این قرن را مورد بهره برداری شایان قرار می-دهیم، به نوعی، با برخی مشکلات که بعضاً هنوز نیز بدون حل باقی مانده‌اند، دست به گریبانیم. اصطلاح-هایی مانند جرایم اینترنتی که به گوش بسیاری از ما آشناست و هر از گاهی خبر یا گزارشی که در مورد ارتکاب چنین جرایمی از سوی مجرمان انتشار می‌یابد. بنابراین با توجه به مطالب ذکر شده و نیز با توجه به اینکه بانک‌ها صدمات و خسارت‌های زیادی را از ناحیه جرائم اینترنتی متحمل شده‌اند، شناسایی این جرائم و توجه کردن به روش‌های جلوگیری از این جرائم ضروری به نظر می‌رسد، از این رو اهمیت پژوهش حاضر احساس می شود[۳].

پیشینه موضوع

اسدی (۱۳۹۸) در پژوهشی تحت عنوان اینترنت و شکل گیری باندهای جرم و فساد در فضای مجازی به این نتایج رسید که با ورود رایانه به زندگی اجتماعی بشر، تغییرات شگرفی را در جامعه بشری شاهد بودیم. به تبع این تغییرات زندگی بشر به فضای جدیدی منتقل شده و یا در حال انتقال است به همین سبب جرائم در اجتماع شکل جدیدی یافته و روش های جدیدی را برای پیشگیری و کشف می‌طلبد و آینده پژوهی برای ترسیم وضعیت جرائم در آینده اجتناب ناپذیر به نظر می‌رسد. زندگی جدید، قوانین و مقررات اجتماعی جدیدی را در پی خواهد داشت که قوانین کشورهای مختلف برای مقابله با جرائم فضای مجازی ازجمله این قوانین است که کشورما ایران نیز از این موضوع غافل نبوده و قوانین متناسب را به تصویب رسانده و برای اجرا ابلاغ شده است. درفضای جدید، زندگی پلیس نقشی متفاوت از گذشته داشته و مراقبت از خیابان مانع ارتکاب وکشف جرم را در پی نخواهد داشت. بنابراین، پلیس باید وارد فضای مجازی شده و گشت‌های خود را در این فضا طراحی و اجرا کندو چاره‌ایی جز کشف جرم در فضای مجازی ندارد[۷].

ساروخانی (۱۳۹۷) در پژوهشی مطرح نمود که اینکه ۸۱ درصد انگیزه مجرمانه در فضای اینترنتی مربوط به جرایم مالی است، خاطر نشان کرد: تامین امنیت فضای تولیدوتبادل اطلاعات کشور، صیانت از هویت دینی، ملی وارزش‌های انسانی جامعه در فتا، حفظ حریم خصوصی وآزادی‌های مشروع، صیانت از منافع، اسرارو اقتدارملی درفضای تولیدو تبادل اطلاعات، حفظ زیرساخت‌های حیاتی کشور در مقابل حملات سایبری واعتماد وآسودگی خاطر آحاد شهروندان جامعه برای انجام تمامی امور قانونی به منظور صیانت ازحکمیت و اقتدار ملی از جمله اهداف تشکیل پلیس فتا به شمار می-آید[۸].

عموزاد و همکاران (۱۳۹۷) در پژوهشی دیگر مطرح نمود که سرقت اطلاعات کارت های بانکی از جمله شماره کارت، رمز دوم، کد $CVV2$، از طریق صفحات جعلی(فیشینگ)، "اسکمیر" (کپی کردن غیرقانونی داده

های کارت بانکی)، سوء استفاده از اعتماد افراد و دریافت کارت و رمز آن، روشهای پیچیده مجرمان در فریب افراد و تکنیکهای مهندسی اجتماعی از جمله شگردهای مجرمان است که به برداشت غیرمجاز منجر می‌شود[۹].

براساس مطالعه *Li* و همکاران در سال ۲۰۲۰، تحقیقات بر روی یازده دیتاست که از تاریخ ۱۹۹۸ موجود بوده صورت پذیرفت. بسیاری از این دیتاست ها قدیمی و بلااستفاده تشخیص داده شدند. برخی دیگر از دیتاست ها کمبود بر روی ترافیک شبکه داشتند. برخی انواع حمله را نداشتند و صرفا مجموعه‌ای از رکوردهای متشکل از چند نوع حمله بودند[۱۰].

Megha و همکاران در سال ۲۰۱۹، رویکردی برای تشخیص دسترسی مجازشماری نشده ارائه گردیده است که مبتنی بر نوعی دسته‌بندی آماری موجی شکل کار می کند. در راهکار پیشنهادی این تحقیق، در ابتدا اتصالات فعال شبکه در دوره های زمانی خاص ثبت می شوند تا یک فرم موجی شکل را تشکیل دهند. در ادامه، در هر دوره زمانی ویژگی هایی از اتصالات و رفتار آن ها مورد بررسی قرار می گیرد که بیان کننده رفتار کاربران بوده تا بتوان از آن ها جهت تشخیص دسترسی های مجاز شماری نشده استفاده نمود[۱۱].

Paliath و همکاران در سال ۲۰۲۰ یک شبکه مجازی‌سازی توابع[1] که جایگزین سخت افزاری بشود که از فرآیند ارسال بسته‌ها در شبکه را برعهده دارد. با کاهش هزینه محاسبات و انعطاف پذیری بیشتری که به شبکه می دهد خود را روشی موفق نشان میدهد. در واقع اینکار برای نشان دادن ارزش و کیفیت استفاده از واحد پردازنده‌های گرافیکی[2] است[۱۲].

Olufemi و همکاران در سال ۲۰۱۸، یک روش را توصیه میکند که در آن آنرمالی و رکوردهای غیرمتداول بدون نظارت[3] تشخیص داده میشوند. آنها از پردازش طبیعی زبان[4] کیفیت و نحوه کار را به عاریه میگیرند. اهمیت این کار در استفاده از دیتاست بروز شده *CICIDS2017* است[۱۳].

Nisha و همکاران در سال ۲۰۱۶، رویکردی با عنوان موتور شناسایی نفوذ فازی *FIRE* ارائه شده است که پایه آن تشخیص مخرب بودن و یا مغرضانه بودن رفتار کاربران در شبکه توسط استفاده از یک سیستم استنتاج مبتنی بر منطق فازی است. راهکار اصلی تشخیص نفوذ در این تحقیق، استفاده از تکنیک تشخیص ناهنجاری است[۱۴].

Gaharwar و همکاران (۲۰۲۰) در پژوهشی مطرح نمود که تقریباً می‌توان گفت به ازای هر کدام از روش-های حقه بازی و کلاهبرداری در جامعه، روش‌ها و ترفندهای متناظری در عالم اینترنت و شبکه پیدا می-شوند که به همان اندازه متنوع و متفاوت از یکدیگرند. مواردی که تاکنون در زمینه خلاف کاری‌های اینترنتی در جهان (عمدتاً اقتصادی) گزارش شده‌اند، بسیار زیاد بوده اما از این میان، آن تعداد که مورد پیگرد قضایی قرارگرفته و مسیر حقوقی خود شده‌اند، بسیار زیاد بوده اما از این میان، آن تعداد که مورد پیگرد قضایی قرار گرفته و مسیر حقوقی خود شده‌اند[۱۵].

Prashanth و همکاران (۲۰۱۹) در پژوهشی دیگر عنوان نمود که درزندگی اجتماعی امروز بشر تحول‌هایی صورت گرفته و به تاثیر از آن جرایم نیز اشکال متفاوتی به خود گرفته است که جرایم رایانه‌ای مصداق بارز این تحول‌ها در زندگی اجتماعی انسان‌ها می‌باشد. با ورود رایانه‌ها به زندگی شخصی افراد و گسترش فناوری اطلاعات(اینترنت) سوء استفاده از این وسایل اشکال گوناگونی به خود گرفته است که تحت عنوان جرایم رایانه‌ای از آن بحث می شود. به گزارش ایسکانیوز از جمله شایع‌ترین این جرایم که روز به روز نیز افزایش می‌یابد کلاهبرداری اینترنتی است، البته در کنار آن جرایم دیگری چون جعل کامپیوتری، سرقت اینترنتی، افشای اطلاعات نیز از شایع ترین این موارد است[۱۶].

شکاف تحقیقاتی:

انقلاب بانکداری الکترونیک با ارائه مزایای فراوان برای مشتریان و فرصت های تجاری جدید برای بانک ها، تجارت بانکداری را به طور اساسی تغییر داد. با این حال، ریسک‌های بانکداری سنتی و چالش‌های زیادی را به خصوص از نظر مسائل امنیتی تحمیل می‌کند. مدل های مختلفی برای کشف و پیشگیری از تقلب توسط تحقیقات بسیاری معرفی و پیشنهاد شده است که در آنها برخی در بهبود دقت تشخیص و پیشگیری از تقلب

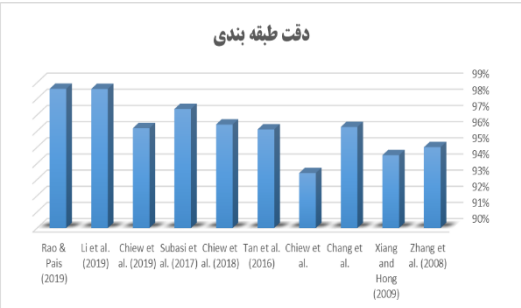
[1] *Network Function Virtualization (NFV)*
[2] *Graphics Processing Units (GPUs)*
[3] *unsupervised*
[4] *natural language processing*

موثر بوده اند. با این حال، هیچ استراتژی یا روش واحدی وجود ندارد که تمام خطرات یا حملات مختلف را که پلتفرم‌های بانکداری الکترونیک را تهدید می‌کنند، پوشش دهد. محققان تکنیک‌های متنوعی را برای احراز هویت پیشنهاد کردند، که در آن روش‌های چندگانه هنگام استفاده از تکنیک‌های بیومتریک در امنیت توصیه می‌شود.(جدول ۱)

جدول ۱: مدل های مرسوم امنیتی بانکداری اینترنتی

مدل	شرح
کیبورد های مجازی	اطلاعات تایپ شده در دستگاه را بر اساس جاوا و رمزنگاری مبتنی بر نرم‌افزار ضبط می شود تا استفاده کارآمد از ثبت‌کننده‌های کلید را خنثی نماید.
سر وقت (کارت های رمز عبور)	فاکتور دوم احراز هویت را فراهم می نماید. برای تولید رمزهای عبور پویا هزینه کمتری دارد.
محافظت از مرورگر	با نظارت بر ناحیه حافظه اختصاص داده شده توسط مرورگر، از کاربر و مرورگر او در برابر بدافزارهای شناخته شده محافظت می نماید.
گواهی های دیجیتال	برای احراز هویت کاربران و خود سیستم بانکی با استفاده از زیرساخت کلید عمومی (*PKI*) و یک مرجع صدور گواهی (*CA*) استفاده می شود.
سر وقت (رمز عبور)	دستگاه‌هایی که معمولاً به‌عنوان عامل دوم احراز هویت با تغییر پویا رمز عبور استفاده می‌شوند.
دستگاه (شناسایی)	همراه با ثبت دستگاه اعمال می شود اما همچنین به عنوان یک راه حل مستقل استفاده می شود. این بر اساس ویژگی های فیزیکی دستگاه های کاربران است.
مثبت (شناسایی)	کاربر را ملزم می نماید تا اطلاعاتی را وارد نمایند که فقط برای شناسایی خود او شناخته شده است.
کلمه عبور	تکنیک مبتنی بر اطلاعات نگهداری شده توسط کاربر که در معاملات جابجایی پول استفاده می شود.
ثبت دستگاه	دسترسی به سیستم های بانکی را برای دستگاه های شناخته شده و ثبت شده قبلی محدود می کند.
CAPTCHA	(تست تورینگ عمومی کاملاً خودکار برای تشخیص رایانه‌ها و انسان‌ها) حملات خودکار را در برابر جلسات تأیید اعتبار ناکارآمد ارائه می‌کند.
خدمات پیامک (پیام کوتاه)	کاربران را در مورد تراکنش هایی که به مجوز آنها نیاز دارد مطلع می کند.
نظار بر تراکنش	شامل بسیاری از رویکردها مانند هوش مصنوعی، تجزیه و تحلیل تاریخچه تراکنش ها و روش های دیگر برای شناسایی الگوهای تقلب است.

تان و همکاران از استخراج کلمات کلیدی هویت و یاب نام دامنه هدف استفاده کردند و میزان موفقیت ۹۶,۱٪ را گزارش کردند. سوباسی و همکاران روشی را در سال ۲۰۱۷ پیشنهاد کرد که از طبقه‌بندی‌کننده جنگل تصادفی استفاده می‌کرد. آنها می توانند با مدل پیشنهادی به دقت ۹۷,۳۶ درصد برسند. مطالعه دیگری که از شبکه عصبی کانولوشن (*CNN*) استفاده کرد مقاله لی و همکاران است. که در سال ۲۰۱۹ منتشر شده است. آنها می توانند به میزان موفقیت ۹۸,۶۰٪ برسند. در آن زمان نرخ بالایی بود. ***Rao & Pais*** ، مقاله ای را در سال ۲۰۱۹ با استفاده از ***Jail-Phish*** منتشر کردند و توانستند به حداکثر ۹۸,۶۱ درصد موفقیت دست یابند. این مقاله یکی از مطالعات تشخیص فیشینگ است که از رویکرد طبقه‌بندی‌کننده‌های گروهی در تشخیص وب‌سایت فیشینگ استفاده می‌کند. مطالعات متعددی وجود دارد که از روش‌های طبقه‌بندی مختلف استفاده می‌کنند، اما وقتی مطالعه خود را با مطالعه قبلی مقایسه می‌کنیم، می‌توانیم ببینیم که روش پیشنهادی نسبت به بسیاری از مطالعات قبلی بهتر عمل کرده است



مرجع مطالعه	روش	دقت طبقه بندی

Zhang et al. (2008)	سیستم لیست سیاه بر اساس طرح رتبه بندی مرتبط	٪۹۵
Xiang and Hong (2009)	روش تشخیص فیش ترکیبی بر اساس استخراج اطلاعات و بازیابی اطلاعات	٪۹۴,۵
Chang et al.	هویت وب سایت با استفاده از تصویر وب	٪۹۶,۲۵
Chiew et al.	لوگوی وب سایت	٪۹۳,۴
Tan et al. (2016)	استخراج کلمات کلیدی هویت و یاب نام دامنه هدف	٪۹۶,۱
Chiew et al. (2018)	با جستجوی تصویر گوگل از فاویکون استفاده می کند	٪۹۶,۴
Subasi et al. (2017)	جنگل تصادفی	٪۹۷,۳۶
Chiew et al. (2019)	جنگل تصادفی	٪۹۶,۱۷
Li et al. (2019)	*CNN*	٪۹۸,۶۰
Rao & Pais (2019)	*Jail-Phish*	٪۹۸,۶۱

روش انجام کار

این پژوهش از حیث روش تحقیق، تحقیقی توصیفی- کمّی است، که از دو روش تفکر عمیق و مطالعه‌ی پیمایشی بهره برده است. در جمع‌آوری داده ها نیز از ابزار های مختلفی همچون: مصاحبه، مشاهده، پرسشنامه و بررسی اسناد استفاده شده است. لازم به ذکر است جامعه آماری این تحقیق بررسی لاگ های رخداد های سایبری بانک های و طی یک سال اخیر می باشد و نمونه گیری خاصی صورت نگرفته است. پس از ارائه مدل، با توجه به نیازمندی‌های پروژه، از شبیه‌سازهای معمول و مخصوصاً *Matlab* استفاده خواهد شد و نتایج بر اساس سرعت اجرا بررسی خواهد شد. در ادامه، تحقیق با ایجاد چند شبیه‌سازی در سیستم مورد بررسی قرار خواهد گرفت و نتایج به صورت مشروح و همچنین با نمودارهای مرتبط توضیح داده خواهد شد. پس از استخراج ویژگی ها و اعمال الگوریتم ها، با استفاده از معیار صحت، فراخوانی به بررسی روش پیشنهادی پرداخته می شود.

تجزیه و تحلیل

- ویژگی‌های مؤثر در تشخیص جرم‌شناسی ناشی از رخداد های سایبری

مهاجمان در حمله‌ی جرم‌شناسی ناشی از رخداد های سایبری تلاش می‌کنند وبگاه جعلی را به گونه‌ای طراحی کنند که کاربران متوجه تفاوت آن با وبگاه اصلی نشوند و اطلاعات محرمانه‌ی خود را به آسانی افشا کنند. به رغم این تلاشِ عوامل رخداد های سایبری، نشانه‌ها و ویژگی‌هایی در وبگاه‌های جعلی وجود دارند که برای تشخیص عدم اصالت آنها به ما کمک می‌کنند. بدیهی است برای طراحی سامانه‌ای که قادر باشد هرگونه جرم‌شناسی ناشی از رخداد های سایبری را شناسایی کرده و به کاربران اخطار دهد، در گام نخست باید ویژگی‌های وبگاه جرم‌شناسی ناشی از رخداد های سایبری شده را تعیین کنیم. لذا در اولین قدم با بررسی مقالات ارائه شده در زمینه‌ی تشخیص جرم‌شناسی ناشی از رخداد های سایبری و بررسی نمونه‌های حقیقی از وبگاه‌های جرم‌شناسی ناشی از رخداد های سایبری شده که در وبگاه فیش‌تنک[1] موجود است، فهرستی اولیه از تمامی ویژگی‌های حملات جرم‌شناسی ناشی از رخداد های سایبری استخراج شد. این شاخص‌ها در جدول ۱ آمده است.

جدول ۱ ویژگی‌های حملات جرم‌شناسی ناشی از رخداد های سایبری

[1] *PhishTank: http://www.phishtank.com/phish_archive.php*

ردیف	شاخص های جرم شناسی	ردیف	شاخص های جرم شناسی
۱	استفاده از نشانی اینترنتی (*IP*) در یوآر اِل	۲۱	استفاده از نویسه‌های مشابه در یوآر اِل
۲	غیرعادی بودن یوآر اِل درخواست (*request URL*)	۲۲	اضافه کردن پیشوند و پسوند
۳	غیرعادی بودن یوآر اِل لنگر	۲۳	استفاده از نشانه‌ی @ در یوآر اِل
۴	رکورد دی‌اِن‌اِس غیرعادی	۲۴	استفاده از کدهای شانزده‌تایی
۵	یوآر اِل غیرعادی	۲۵	استفاده از درگاه سوییچینگ
۶	استفاده از گواهی *SSL* (وجود نشانگر قفل در پایین صفحه و یا *https:*\\ در نوار نشانی صفحه)	۲۶	تأکید افراطی بر امنیت در وبگاه
۷	گواهی‌دهنده (*CA*)	۲۷	عمومی بودن رایانامه
۸	کوکی غیرعادی	۲۸	در دست گرفتن زمان برای دسترسی به حساب‌ها
۹	جزئیات موجود در گواهی دیجیتالی	۲۹	در خواست اطلاعات محرمانه در رایانامه
۱۰	بازهدایت صفحات وب	۳۰	پیوست بودن پرونده‌های اِچ‌تی‌اِم‌اِل در رایانامه که به صورت محلی روی کارخواه باز می‌شوند
۱۱	حمله‌ی تزریق کد (*XSS*)	۳۱	دریافت خطای *SSL*
۱۲	حمله‌ی فارمینگ	۳۲	دریافت خطای «اطلاعات نامعتبر است» پس از ورود و ارسال اطلاعات
۱۳	پنهان شدن پیوند صفحه با قرار گرفتن نشانگر موس بر آن	۳۳	وجود اسم نمانام‌های معتبر در نشانی یوآر اِل
۱۴	*SFH* غیرعادی	۳۴	وبگاه‌هایی که خدمات مالی ارائه می‌دهند
۱۵	خطاهای نگارشی و نحوی در رایانامه یا وبگاه	۳۵	برچسب <*iframe*> در کد وبگاه
۱۶	کپی کردن وبگاه	۳۶	برچسب <*script*> در کد وبگاه
۱۷	وجود فرم‌هایی با کلید «*submit*»	۳۷	استفاده از کد *email* در وبگاه
۱۸	استفاده از پنجره‌های بالاپَر	۳۸	وجود *https* در کد وبگاه
۱۹	غیرفعال بودن کلیک راست	۳۹	کد غیرقانونی *pop-up*
۲۰	طولانی بودن نشانی یوآر اِل		

- **تعیین متغیرهای ورودی**

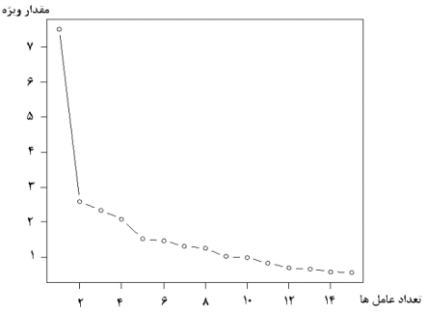
در این مرحله از پژوهش باید ویژگی‌هایی که از نظر خبرگان مهم‌تر و تأثیرگذارتر هستند، مشخص شود. همچنان که گفته شد فهرست اولیه شامل ۳۹ شاخص جرم‌شناسی ناشی از رخداد های سایبری بود. برای حذف شاخص‌های دارای افزونگی، فهرست اولیه شامل ۲۸ شاخص مهم‌تر که سایر شاخص‌ها را پوشش می-دادند به صورت پرسشنامه درآمد و بین خبرگان توزیع گردید تا مهم‌ترین و کارآمدترین شاخص‌ها از دیدگاه آنان مشخص شود. در مرحله اول (مرحله سنجش اعتبار) باتوجه به محدود بودن نفرات دارای بالاترین صلاحیت در صنعت، ۱۰ خبره انتخاب و راجع به صحت موارد و تعاریف نظر دادند و اصلاحات مورد نظر آنها در پرسشنامه اعمال شد و برای سنجش پایایی، آلفای کرونباخ محاسبه گردید. از آنجا که آلفای کرونباخ عدد ۰/۸۴۹ محاسبه شد، لذا پرسشنامه صحت و پایایی مورد نیاز را داراست.

پرسشنامه برای ۱۰۰ نفر ارسال شد که از این میان، ۴۳ نفر از متخصصین به آن پاسخ دادند. لازم به ذکر است، هریک از پرسشنامه‌های پر شده پس از دریافت مورد بازبینی دقیق قرار گرفته و در صورت مشاهده کوچکترین تناقض در پاسخ‌ها، پرسشنامه‌ی مذکور حذف شده و مورد استفاده قرار نمی‌گرفت. مشخصات پاسخ‌دهندگان در جدول ۲ آمده است.

جدول ۲ اطلاعات دموگرافی خبرگان شرکت کننده در نظرسنجی

	جنسیت		سطح تحصیلات			سابقه‌ی فعالیت در حوزه‌ی فناوری اطلاعات			
	زن	مرد	کارشناسی	کارشناسی ارشد	دکتری	کمتر از ۳ سال	۳ تا ۵ سال	۵ تا ۱۰ سال	بیش از ۱۰ سال
فراوانی	۶	۳۷	۱۴	۲۶	۳	۱۹	۱۲	۸	۴
درصد فراوانی	٪۱۴	٪۸۶	٪۳۳	٪۶۰	٪۷	٪۴۴	٪۲۸	٪۱۹	٪۹

برای تحلیل پرسشنامه، ابتدا میانگین تک تک شاخص‌ها محاسبه شد (جدول ۳)، این میانگین عددی بین ۵ تا ۸ (معادل محدوده متوسط و زیاد) است. با توجه به اهمیت نسبی تمام شاخص‌های فهرست اولیه، این نتیجه تا حدودی قابل پیش‌بینی بود. از آنجا که محاسبه‌ی میانگین، برتری شاخص‌ها را نسبت به هم نشان نداد، لازم شد برای رتبه‌بندی شاخص‌ها براساس میزان اهمیت و تأثیرگذاری، از روش دیگری استفاده کنیم. روش مورد استفاده ما تحلیل عاملی اکتشافی است که روشی آماری برای کاهش داده‌ها است. برای تعیین تعداد عوامل، نمودار سنگریزه‌ای مقادیر ویژه، در مقابل تعداد عوامل استخراج گردید که در شکل ۱ نشان داده شده است. با توجه به شکل ۱، تحلیل عاملی با دو عامل پیشنهاد می‌گردد. به همین منظور حامل‌ها برای این دو عامل در جدول ۳ نشان داده شده است.



شکل ۱- نمودار سنگریزه‌ای مقادیر ویژه

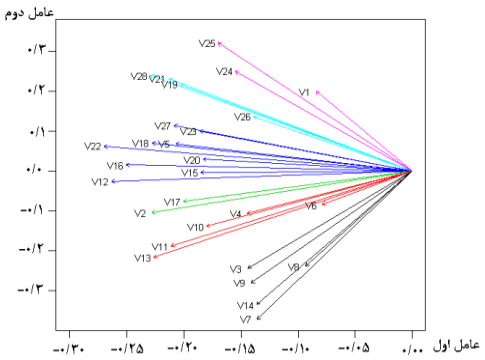
جدول ۳ میانگین شاخص‌ها و محاسبه‌ی حامل‌ها برای دو عامل

ردیف	شاخص‌های جرم‌شناسی ناشی از رخداد های سایبری	میانگین نظر خبرگان	حامل‌ها	
			عامل اول	عامل دوم
۱	استفاده از نشانی آی‌پی	۵/۴۶	-۰/۰۸۴۰۱۷۷۴	۰/۱۹۹۰۵۴۰۴۶
۲	یوآر اِل غیرعادی درخواست	۷/۱۲	-۰/۲۲۸۲۶۵۸۳	-۰/۱۰۴۹۶۴۳۶۲
۳	یوآر اِل غیرعادی لنگر	۶/۱۲	-۰/۱۴۳۹۴۵۱۳	-۰/۲۴۴۰۷۰۲۶۸
۴	رکورد دی‌اِن‌اِس غیرعادی	۶/۲۳	-۰/۱۴۴۳۷۶۴۸	-۰/۱۰۶۶۶۴۳۳۳
۵	یوآر اِل غیرعادی	۷/۳۹	-۰/۲۰۷۳۴۷۲۳	۰/۰۶۸۶۷۸۱۴۶
۶	استفاده از گواهی *SSL*	۶/۷۷	-۰/۰۷۸۳۸۱۳۰	-۰/۰۸۴۵۲۵۲۱۱
۷	گواهی‌دهنده	۷/۰۷	-۰/۱۳۵۷۶۲۶۴	-۰/۳۷۱۳۱۷۲۷۵
۸	کوکی غیرعادی	۵/۳۰	-۰/۰۹۳۳۲۸۸۸	-۰/۲۳۸۶۱۱۸۹۱
۹	جزئیات موجود در گواهی	۶/۱۲	-۰/۱۴۰۹۱۵۶۵	-۰/۲۷۹۸۰۱۱۸۷
۱۰	وبگاه‌های بازهدایت	۶/۶۳	-۰/۱۸۰۵۴۸۲۲	-۰/۱۳۸۵۵۵۰۸۶
۱۱	حمله‌ی تزریق کد	۶/۸۶	-۰/۲۱۱۲۲۳۰۴	-۰/۱۸۷۹۷۵۱۴۳
۱۲	حمله‌ی فارمینگ	۶/۱۶	-۰/۲۶۳۴۸۴۵۷	-۰/۰۲۵۵۷۱۳۸۰
۱۳	پنهان شدن با نشانگر موس	۵/۴۶	-۰/۲۲۶۷۵۰۴۷	-۰/۲۱۶۲۷۲۴۳۷
۱۴	*SFH* غیرعادی	۶/۰۷	-۰/۱۳۶۳۰۷۳۰	-۰/۳۳۴۳۷۰۲۶۵
۱۵	خطاهای نحوی و نگارشی	۶/۸۱	-۰/۱۸۵۴۶۸۹۷	-۰/۰۰۳۵۸۷۷۷۴
۱۶	کپی کردن وبگاه	۶/۸۸	-۰/۲۵۸۵۸۷۷	۰/۰۱۴۷۷۱۸۵۳
۱۷	وجود فرم‌های دریافت اطلاعات	۶/۹۱	-۰/۲۰۱۶۸۴۱۰	-۰/۰۷۶۹۴۵۳۹۵
۱۸	استفاده از پنجره‌های بالاپَر	۶/۴۶	-۰/۲۲۷۹۹۳۹۵	۰/۰۶۹۷۸۹۶۰۶
۱۹	غیرفعال شدن کلیک راست	۵/۲۵	-۰/۲۰۲۸۵۷۴۱	۰/۲۱۵۵۸۴۹۴۲
۲۰	نشانی طولانی یوآر اِل	۵/۱۴	-۰/۱۸۳۴۴۸۱۶	۰/۰۲۹۳۲۳۲۹۳
۲۱	نویسه‌های مشابه	۶/۳۵	-۰/۲۱۳۵۹۸۷۵	۰/۲۳۰۵۲۰۳۵۶

۲۲	اضافه کردن پیشوند و پسوند	۷/۱۸	-۰/۲۷۰۴۱۹۶۶	۰/۰۶۱۸۵۸۱۲۷
۲۳	استفاده از نشانه‌ی @	۵/۸۸	-۰/۱۸۶۱۴۹۲۰	۰/۰۹۹۸۴۰۹۷۶
۲۴	کدهای شانزده‌تایی	۶/۲۳	-۰/۱۵۵۱۸۳۹۶	۰/۲۵۰۰۵۳۴۸۷
۲۵	استفاده از درگاه سوییچینگ	۵/۶۹	-۰/۱۷۰۲۵۵۲۴	۰/۳۲۰۹۷۸۴۲۷
۲۶	تأکید افراطی بر امنیت	۵/۰۵	-۰/۱۳۹۸۴۶۳۶	۰/۱۳۶۱۱۰۰۷۶
۲۷	رایانامه‌ی عمومی	۶/۴۴	-۰/۲۰۸۸۲۲۷۹	۰/۱۱۴۱۶۶۸۰۸
۲۸	در دست گرفتن زمان	۵/۹۳	-۰/۲۲۹۶۲۹۶۸	۰/۲۳۹۳۳۲۱۰۶

جهت و میزان تأثیر هر متغیر با توجه به مدل ارائه شده در نمودار برداری حامل‌ها در شکل ۲ نشان داده شده است.

نرم‌افزار R، متغیرها را با توجه به جهت تاثیرگذاری‌شان به ۶ دسته تقسیم می‌کند که در نمودار شکل ۲ با رنگ-های مختلف نشان داده شده‌اند. با توجه به آنچه که بیان گردید دسته‌ها در جدول ۴ معرفی می‌گردند. متغیرها همان شاخص‌های جرم‌شناسی ناشی از رخداد های سایبری هستند.



شکل ۲ نمودار برداری حامل‌ها به ازای دو عامل

جدول ۴ دسته‌بندی متغیرها بر اساس جهت تأثیر

ردیف	دسته	متغیرها[1]
۱	دسته شماره ۱	متغیرهای (۳، ۷، ۸، ۹، ۱۴)
۲	دسته شماره ۲	متغیرهای (۴، ۶، ۱۰، ۱۱، ۱۳)
۳	دسته شماره ۳	متغیرهای (۲، ۱۷)
۴	دسته شماره ۴	متغیرهای (۵، ۱۲، ۱۵، ۱۶، ۱۸، ۲۰، ۲۲، ۲۳، ۲۷)
۵	دسته شماره ۵	متغیرهای (۲۶، ۱۹، ۲۱، ۲۸)
۶	دسته شماره ۶	متغیرهای (۱، ۲۴، ۲۵)

[1] *Variables*

به هر اندازه که بردار مربوط به هر متغیر بزرگتر باشد تاثیر آن متغیر نیز در مدل ارائه شده بیشتر خواهد بود. با توجه به آنکه مقیاس مربوط به عوامل در نمودار برداری حامل‌ها یکسان نیست مستقیماً نمی‌توان از این نمودار برای تعیین تأثیر متغیرها استفاده نمود. برای این منظور محموله‌های مربوط به هر متغیر استخراج و به ترتیب نزولی مرتب گردید که در جدول ۵ نشان داده شده‌اند.

جدول ۵ رتبه‌بندی شاخص‌ها به ترتیب نزولی

ردیف	شاخص جرم‌شناسی ناشی از رخداد های سایبری	محموله	ردیف	شاخص جرم‌شناسی ناشی از رخداد های سایبری	محموله
۱	قابلیت اعتماد به گواهی دهنده	۰/۰۷۸۱۵۴۰۱	۱۵	کپی کردن وبگاه	۰/۰۳۱۵۷۴۱۷
۲	استفاده از درگاه سوییچینگ	۰/۰۶۶۰۰۷۰۰	۱۶	یوآر اِل غیرعادی درخواست	۰/۰۳۱۵۶۱۴۰
۳	*SFH* غیرعادی	۰/۰۶۵۱۹۱۵۸	۱۷	استفاده از پنجره‌های بالاپر	۰/۰۲۸۴۲۵۹۲
۴	در دست گرفتن زمان	۰/۰۵۵۰۰۴۸۲	۱۸	رایانامه‌ی عمومی	۰/۰۲۸۳۲۰۵۱
۵	استفاده از نویسه‌های مشابه در یوآر اِل	۰/۰۴۹۳۸۲۰۳	۱۹	وبگاه‌های بازهدایت	۰/۰۲۵۸۹۷۵۹
۶	پنهان شدن پیوند با قرار گرفتن نشانگر موس	۰/۰۴۹۰۹۴۷۷	۲۰	یوآر اِل غیرعادی	۰/۰۲۳۸۵۴۷۸
۷	جزئیات موجود در گواهی	۰/۰۴۹۰۷۲۹۶	۲۱	استفاده از نشانی آی‌پی در یوآر اِل	۰/۰۲۳۳۴۰۷۵
۸	غیرفعال شدن کلیک راست	۰/۰۴۳۸۱۴۰۰	۲۲	وجود فرم‌های دریافت اطلاعات	۰/۰۲۳۰۹۷۳۵
۹	کدهای شانزده‌تایی	۰/۰۴۳۳۰۴۴۰	۲۳	استفاده از نشانه @ در یوآر اِل	۰/۰۲۲۳۰۹۸۷
۱۰	یوآر اِل غیرعادی لنگر	۰/۰۴۰۱۴۵۲۵	۲۴	تأکید افراطی بر امنیت	۰/۰۱۸۹۱۶۰۲
۱۱	حمله‌ی تزریق کد	۰/۰۳۹۹۷۴۹۱	۲۵	نشانی طولانی یوآر اِل	۰/۰۱۷۲۵۶۵۴
۱۲	اضافه کردن پیشوند و پسوند	۰/۰۳۸۴۷۶۶۱	۲۶	خطاهای نحوی و نگارشی	۰/۰۱۷۲۰۵۸۱
۱۳	حمله‌ی فارمینگ	۰/۰۳۵۰۳۹۰۱	۲۷	رکورد دی‌اِن‌اِس غیرعادی	۰/۰۱۶۱۱۰۹۲
۱۴	کوکی غیرعادی	۰/۰۳۲۸۲۲۹۶	۲۸	استفاده از گواهی *SSL*	۰/۰۰۶۶۴۴۰۷

با توجه به جدول ۵، ملاحظه می‌شود متغیر «قابلیت اعتماد به گواهی‌دهنده» دارای بیشترین میزان تأثیر و متغیر «استفاده از گواهی *SSL*» دارای کمترین میزان تأثیر در تشخیص جرم‌شناسی ناشی از رخداد های سایبری است. برای تعیین تأثیرگذارترین دسته، از مجموع محموله‌های مربوط به هر دسته استفاده گردید که محموله‌ها در جدول ۶ به صورت نزولی مرتب شده است.

جدول ۶ محموله‌های مربوط به دسته‌ها

ردیف	دسته	محموله
۱	دسته شماره ۱	۰/۲۶۵۳۸۶۸
۲	دسته شماره ۴	۰/۲۴۲۴۶۳۲
۳	دسته شماره ۵	۰/۱۶۷۱۱۶۹
۴	دسته شماره ۲	۰/۱۳۷۷۲۲۳
۵	دسته شماره ۶	۰/۱۳۲۶۵۲۱
۶	دسته شماره ۳	۰/۰۵۴۶۵۸۷۵

از این رو دسته سیاه دارای بیشترین اهمیت و دسته‌های آبی، آبی فیروزه‌ای، قرمز، صورتی و سبز به ترتیب در رتبه‌های بعدی قرار دارند.برای انتخاب تعدادی از شاخص‌های برتر در این مرحله، علاوه بر نتایج حاصل از تحلیل عاملی که یک رتبه‌بندی از شاخص‌های تأثیرگذار بر اساس نظر خبرگان ارائه می‌دهد (جدول ۵)، دو جنبه‌ی دیگر مدّ نظر قرار گرفت: یکی تجربیات وقوع جرم‌شناسی ناشی از رخداد های سایبری در بانک‌های ایرانی و دیگری تحقیقات پیشین در حوزه‌ی جرم‌شناسی ناشی از رخداد های سایبری در بانکداری الکترونیکی. مثلاً شاخص «استفاده از گواهی *SSL*» گرچه پایین‌ترین رتبه را در جدول ۵ کسب کرده اما با توجه به موارد واقعی جرم‌شناسی ناشی از رخداد های سایبری در ایران، به هیچ وجه قابل حذف نیست. در سایر نمونه‌های جرم‌شناسی در وبگاه بانک‌های ایرانی هم این نکته کاملاً بارز است که عوامل رخداد های سایبریی که بانک‌های ایرانی را هدف قرار می‌دهند اغلب برای گرفتن گواهی‌هایی با اعتبار کم خود را به زحمت نمی‌اندازند. به عبارتی شاخص مورد بحث در حملات جرم‌شناسی ناشی از رخداد های سایبری در بانک‌های ایرانی تأثیری غیر قابل انکار دارد و باید در سامانه در نظر گرفته شود. ازسویی باید اشاره کرد شاخص «خطاهای نحوی و نگارشی» در تشخیص جرم‌شناسی این پایان‌نامه نقش تأثیرگذاری ندارد، زیرا عوامل رخداد های سایبری بانک‌های ایرانی، خود ایرانی هستند و به زبان فارسی کاملاً مسلط هستند و در نمونه‌های واقعی جرم‌شناسی ناشی از رخداد های سایبری در ایران تا به حال خطای نحوی و نگارشی مشاهده نشده است. از طرفی این شاخص در جدول ۵ رتبه‌ی بسیار پایینی دارد. لذا با اطمینان می‌توان این شاخص را از فهرست حذف کرد. شایان ذکر اینکه این شاخص در وبگاه بانک‌های انگلیسی‌زبان بسیار مهم و تأثیرگذار است و بررسی‌ها نشان می‌دهد در ۸۰ درصد موارد جرم‌شناسی ناشی از رخداد های سایبری اتفاق می‌افتد زیرا عوامل رخداد های سایبری معمولاً از کشورهای غیرانگلیسی‌زبان هستند. به علاوه ماهیت زبان انگلیسی این وبگاه‌ها را مستعد خطاهای نگارشی و نحوی می‌کند.

شکل ۳ نسخه‌ی جرم‌شناسی ناشی از رخداد های سایبری شده‌ی دروازه‌ی پرداخت بانک ملت

در نهایت ۸ متغیر از ۲۸ متغیر در این مرحله حذف گردیدند. ۲۰ متغیر مهم باقیمانده در این مرحله در جدول ۷ فهرست شده اند.

جدول ۷ شاخص های مؤثر در تشخیص جرم‌شناسی ناشی از رخداد های سایبری در بانک‌های ایرانی

ردیف	شاخص‌های جرم‌شناسی ناشی از رخداد های سایبری	ردیف	شاخص‌های جرم‌شناسی ناشی از رخداد های سایبری

۱	میزان اعتبار *CA*	۱۱	یوآر اِل غیرعادی درخواست
۲	یوآر اِل غیرعادی لنگر	۱۲	یوآر اِل غیرعادی
۳	کوکی غیرعادی	۱۳	استفاده از پنجره‌های بالاپَر
۴	جزئیات موجود در گواهی	۱۴	نشانی یوآر اِل طولانی
۵	*SFH*[1] غیرعادی	۱۵	اضافه کردن پیشوند و پسوند
۶	رکورد غیرعادی دی‌اِن‌اِس	۱۶	استفاده از سمبل @ برای گیج کردن
۷	استفاده از گواهی *SSL* (وجود نشانگر قفل[2] در پایین صفحه و یا *https:*// در نوار نشانی صفحه)	۱۷	استفاده از نویسه‌های مشابه در یوآر اِل
۸	بازهدایت صفحات وب	۱۸	استفاده از نشانی اینترنتی(*IP*)
۹	حمله‌ی تزریق کد	۱۹	استفاده از کدهای شانزده‌تایی
۱۰	پنهان شدن پیوند صفحه با قرار گرفتن نشانگر موس بر آن	۲۰	استفاده از پورت سوییچینگ

- **تعیین متغیرهای خروجی**

هدف از طراحی سامانه‌ی خبره، شناسایی حملات جرم‌شناسی ناشی از رخداد های سایبری با بیشترین میزان چابکی و دقت است. متغیر خروجی موتور استنتاج فازی، «میزان خطر جرم‌شناسی وبگاه» است که واژه-های «قانونی»، «کمی مشکوک»، «مشکوک»، «بسیار مشکوک» و «جعلی» به آن تخصیص داده شده اند. به عبارت دیگر این سامانه وبگاه را با یکی از واژه‌های زبانی زیر دسته‌بندی می‌کند:

الف- قانونی: وبگاه به اندازه‌ی کافی امن است و می‌توان به اعتبار آن اطمینان کرد.

ب- کمی مشکوک: وبگاه کاملاً قابل اعتماد نیست و بهتر است قبل از ورود هرگونه اطلاعات در مورد اعتبار و قانونی بودن آن به طور کامل اطمینان حاصل کرد.

ج- مشکوک: وبگاه ویژگی‌هایی دارد که قانونی بودن آن را نقض می‌کند.

د- بسیار مشکوک: وبگاه با احتمال بالایی جعلی است. به هیچ وجه نباید اطلاعاتی وارد گردد.

ه- جعلی: وبگاه کاملاً جعلی است.

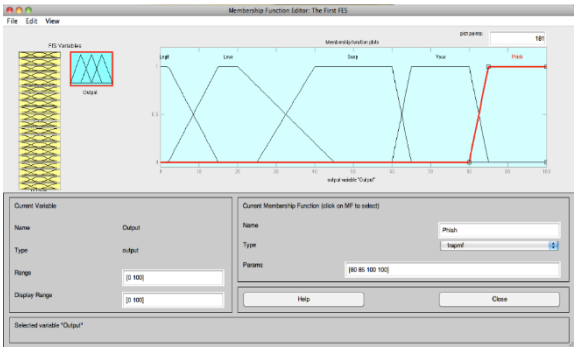
براساس توضیحات فوق نحوه‌ی دسته‌بندی وبگاه‌ها و بازه‌ی هریک از آنها بر اساس عدد قطعی خروجی مطابق جدول ۸ است. لذا همان‌طور که گفته شد خروجی این سامانه «میزان جرم‌شناسی» وبگاه مورد بررسی است که عددی قطعی است. شکل ۴ توابع عضویت متغیّر خروجی را نشان می‌دهد. چگونگی نگاشت نظریات خبرگان به اعداد فازی ذوزنقه‌ای جدول ۸، در بخش بعدی به تفصیل شرح داده می‌شود.

جدول ۸ دسته‌بندی واژه‌های زبانی خروجی بر اساس عدد قطعی خروجی (درصد جرم‌شناسی)

متغیر خروجی	واژه زبانی خروجی	عدد فازی متناظر

[1] *Server Form Handler*
[2] *Padlock Icon*

میزان جرم‌شناسی وبگاه (درصد)	قانونی	[۰ ۰ ۲ ۱۵]
	کمی مشکوک	[۲ ۱۵ ۲۰ ۴۵]
	مشکوک	[۲۵ ۴۰ ۶۰ ۶۵]
	خیلی مشکوک	[۶۰ ۶۵ ۸۰ ۸۵]
	جعلی	[۸۰ ۸۵ ۱۰۰ ۱۰۰]



شکل ۴ توابع عضویت متغیّر خروجی

- ارزیابی سامانه‌ی خبره‌ی فازی شناسایی جرم‌شناسی ناشی از رخداد های سایبری

در این مرحله، سامانه‌ی خبره‌ی فازی بر چندین نمونه‌ی حقیقی از وبگاه‌های بانک‌های ایرانی و همچنین بر نمونه‌هایی از حملات جرم‌شناسی ناشی از رخداد های سایبری ثبت شده در وبگاه فیش‌تَنک[1] آزمایش شد که نتایج آزمایش آن بر ۲۲ وبگاه در جدول ۹ آمده است. در این بخش یک نمونه‌ی آزمایشی برای نمایش میزان حساسیت سامانه و نیز دو نمونه‌ی واقعی دیگر با ذکر جزئیات بیان شده است. لازم به ذکر است که در ارزیابی سامانه‌ی خبره، ملاک مقایسه و بررسی صحت نتایج، نظر خبرگان است. چراکه یک سامانه‌ی خبره تلاش می‌کند نزدیک‌ترین تصویر از یک خبره را شبیه‌سازی کند. لذا همانطور که در ستون آخر جدول ۹ مشاهده می‌شود، نتایج خروجی سامانه برای تأیید به خبرگان داده شد.

الف) نمونه‌ی اول: نمونه‌ی آزمایشی

در این قسمت ویژگی‌های یک وبگاه فرضی به گونه‌ای در نظر گرفته می‌شود که عوامل رخداد های سایبری در آن تلاش کرده‌اند تا وبگاه «جعلی» بیشترین شباهت را به وبگاه قانونی داشته باشد. ویژگی‌های این وبگاه در ردیف ۲۲ جدول ۹ آمده است. وبگاه تقلبی دارای یوآرالِی به طول ۲۰ است، این عدد در سامانه‌ی طراحی شده‌ی این پایان‌نامه در محدوده‌ی «کم» قرار می‌گیرد که برای یک وبگاه بانکی مقدار بسیار مطلوبی است، همچنین دارای گواهی SSL است و گواهی‌دهنده‌ی آن دارای اعتبار «زیاد» است. گرچه در بهترین حالت ممکن عوامل رخداد های سایبری نخواهند توانست از یک گواهی‌دهنده‌ی «خیلی» معتبر برای وبگاه جعلی خود گواهی بگیرند اما فرض بر این است که آنها از یک گواهی منقضی شده استفاده می‌کنند لذا جزئیات موجود در گواهی «متوسط» است. شاخص «یوآرالِ غیرعادی درخواست» در محدوده‌ی «کم» است و «یوآرالِ لنگرِ غیرعادی» در کمترین مقدار ممکن خود و در گستره‌ی «زیاد» است. وبگاه دارای «رکورد عادی دی‌اِن‌اِس» است و نیز هیچ ویژگی غیرعادی در یوآرالِ وجود ندارد. در مجموعه کد[2] این وبگاه و برچسب $Form$، اس‌اِف‌اِچ غیرعادی است در نتیجه برابر با عدد فازی «یک» است. خروجی سامانه‌ی فازی، «میزان جرم‌شناسی وبگاه» است که می‌تواند عددی بین صفر تا صد باشد که هرچه این عدد به صد نزدیک‌تر باشد از میزان اعتبار وبگاه کاسته شده و اطمینان به جعلی بودن آن بیشتر می‌شود. نحوه‌ی محاسبه‌ی خروجی به این صورت است که ابتدا برای هر متغیر ورودی مقدار تابع عضویت محاسبه می‌شود. مثلا برای یوآرالِ این وبگاه که مقدار آن در گستره‌ی واژه‌ی «کم» قرار می‌گیرد، درجه‌ی تعلّق از رابطه‌ی زیر محاسبه می‌شود:

$$\mu_{Low}(x) = \begin{cases} 1 & 0 < x \leq 20 \\ -0.1x + 3 & 20 < x \leq 30 \end{cases}$$

$$\mu_{Lenght\ of\ URL=Low}(20) = 1$$

[1] *PhishTank: http://www.phishtank.com/phish_archive.php*

[2] *Source Code*

و برای «یوآرال لنگرِ غیرعادی» که در گستره‌ی واژه‌ی «زیاد» قرار می‌گیرد، مقدار تابع عضویت از رابطه‌ی زیر محاسبه می‌شود:

$$\mu_{Many}(x) = \begin{cases} 0.5x - 1 & 2 < x \leq 4 \\ 1 & 4 < x \leq 10 \end{cases}$$

$$\mu_{Abnormal\ URL\ of\ anchor=many}(3.2) = 0.6$$

از آنجا که SFH ، غیرعادی است، داریم:

$$\mu_{SFH}(x) = \begin{cases} -2x + 1 & 0 \leq x < 0.5 \\ 2|x - 1| + 1 & 0.5 \leq x < 1.5 \\ 0 & e.w \end{cases}$$

$$\mu_{SFH}(1) = 1$$

در نتیجه قاعده‌ی شماره‌ی ۱ و ۱۵۹ آتش[1] می‌شود. این دو قاعده عبارتند از:

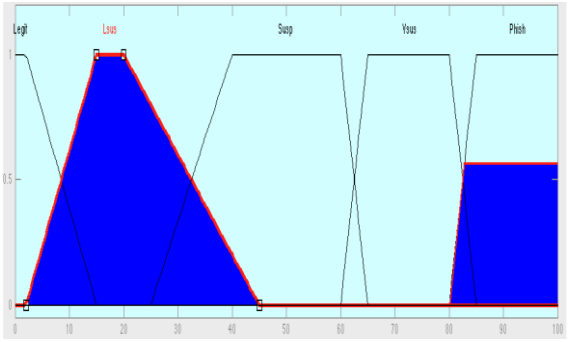
قاعده‌ی ۱: اگر یوآرال لنگر «زیاد» غیرعادی باشد، آنگاه وبگاه «جعلی» است.

قاعده‌ی ۱۵۹: اگر SFH غیرعادی «باشد»، آنگاه وبگاه «کمی مشکوک» است.

و با استفاده از موتور استنتاج کمینه‌ی ممدانی داریم:

$$\mu_{\acute{B}}(y) = max\{\mu_{Rule1}, \mu_{Rule\ 159}\} = \max\{min\{0.6, \mu_{Phish}\}, min\{1, \mu_{Lsus}\}\}$$

در این مرحله مساحت سطح زیر نمودار ماکزیمم (بخش آبی رنگ در شکل ۸) توسط انتگرال محاسبه شده و سپس درون رابطه‌ی وافازی‌ساز گرانیگاه قرار می‌گیرد تا درصد جرم‌شناسی (y^*) محاسبه شود.



شکل ۵ خروجی حاصل از موتور استنتاج کمینه‌ی ممدانی

$$y^* = \frac{\int_y y.\mu_{\acute{B}}(y)dy}{\int_y \mu_B(y)dy} = \frac{\int_2^{15} \frac{1}{13}(y-2)y\,dy + \int_{15}^{20} y\,dy + \int_{20}^{45} (\frac{-1}{25}y + 21)y\,dy + \int_{80}^{83} (0.2y - 16)y\,dy + \int_{83}^{100} 0.6y\,dy}{\text{مساحت}} = 43.$$

در وضعیتی که در بالا برای وبگاه آزمایشی شرح داده شد، حتی یک فرد خبره هم ممکن است در تشخیص اصالت وبگاه با ظاهری شبیه به وبگاه اصلی به خطا بیفتد اما همینطور که عدد خروجی (۴۳/۷) نشان می‌دهد، سامانه‌ی خبره‌ی فازی به خوبی «مشکوک» بودن وبگاه را اعلام می‌کند که وبگاه دارای ویژگی‌هایی است که قانونی بودن آن را نقض می‌کنند. یادآوری می‌شود در این مثال تمامی شاخص‌ها در نزدیک‌ترین حالت به یک وبگاه قانونی در نظر گرفته شدند.

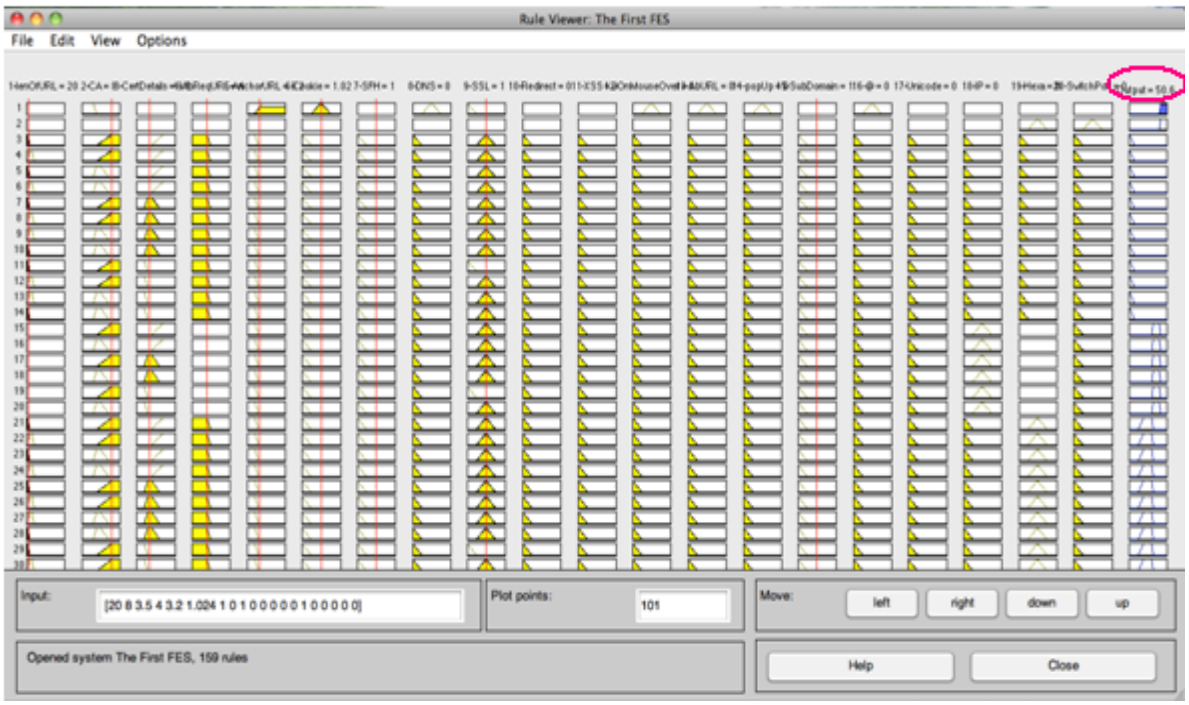
[1] *Rule fire*

جدول ۹ نتایج اجرای سامانه‌ی خبره‌ی فازی شناسایی جرم‌شناسی ناشی از رخداد های سایبری

ردیف	طول یوآرال	میزان اعتبار گواهی‌دهنده	جزئیات موجود در گواهی	یوآرال غیرعادی درخواست	یوآرال غیرعادی لنگر	کوکی غیرعادی	*SFH* غیرعادی	رکورد غیرعادی *DNS*	استفاده از گواهی *SSL*	*XSS*	بازهدایت صفحات وب	پنهان شدن پیوند صفحه با موس	یوآرال غیرعادی	استفاده از پنجره‌های بالاپر	اضافه کردن پیشوند و پسوند	استفاده از نشانه‌ی @	استفاده از نویسه‌های مشابه در	استفاده از نشانی *IP*	استفاده از کدهای شانزده‌تایی	استفاده از پورت سوییچینگ	میزان خطر جرم‌شناسی خروجی	تشخیص	صحت نتیجه
۱	۴۹	۷/۷۵	۸/۹۵	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۴/۸۶	قانونی	درست
۲	۸۰	۶	۵	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۲۲/۱	کمی مشکوک	درست
۳	۴۶	۳/۵	۲	۰	۰	۰	۰	۰/۸	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۹۱/۴	جعلی	درست
۴	۳۰	۲/۵	۲	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۹۱/۴	جعلی	درست
۵	۱۱۹	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۱	۰	۱	۰	۰	۰	۰	۰	۹۱/۴	جعلی	درست
۶	۵۱	۸/۲	۸/۱	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۸/۳۸	قانونی	درست
۷	۲۶	۸/۹	۹/۱	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۵/۵۱	قانونی	درست
۸	۴۷	۹	۹/۵	۰	۱/۵	۰	۰	۰	۱	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۴/۷۸	قانونی	درست
۹	۵۴	۸/۹	۹/۵	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۱۴/۶	کمی مشکوک	نادرست (قانونی)
۱۰	۶۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۱	۰	۰	۰	۰	۱	۰	۰	۹۱/۴	جعلی	درست

۱۱	۱۱۹	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۱	۰	۰	۰	۰	۰	۰	۰	۹۱/۴	جعلی	درست
۱۲	۲۹	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۹۱/۴	جعلی	درست
۱۳	۵۵	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۱	۰	۰	۰	۰	۰	۰	۰	۹۱/۴	جعلی	درست
۱۴	۵۸	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۹۱/۴	جعلی	درست
۱۵	۱۰۵	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۱	۰	۰	۰	۱	۰	۰	۰	۰	۹۱/۴	جعلی	درست
۱۶	۶۳	۰	۰	۰	۰	۰	۰	۰	۰	۰/۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۹۱/۴	جعلی	درست
۱۷	۳۴	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۹۱/۴	جعلی	درست
۱۸	۶۳	۰	۰	۰	۰	۰	۰	۰	۰	۰/۲	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۹۱/۴	جعلی	درست
۱۹	۲۶۵	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۱	۰	۱	۰	۰	۹۱/۴	جعلی	درست
۲۰	۵۸	۷/۹	۹/۱	۰	۲/۷	۰	۰	۰	۱	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۴۵/۳	مشکوک	نادرست (قانونی)
۲۱	۳۱	۸/۹	۹/۵	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۴/۷۸	قانونی	درست
۲۲	۲۰	۸	۳/۵	۴	۳/۲	۰	۱	۰	۱	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۴۳/۷	مشکوک	درست

شکل ۶ خروجی این نمونه‌ی آزمایشی را در سامانه‌ی خبره‌ی فازی شناسایی جرم‌شناسی نشان می‌دهد. همان‌طور که در این شکل مشاهده می‌شود، هر ستون مربوط به یک متغیر است. درصد جرم‌شناسی وبگاه در بالای ستون آخر که مربوط به متغیر خروجی است، نوشته شده است.

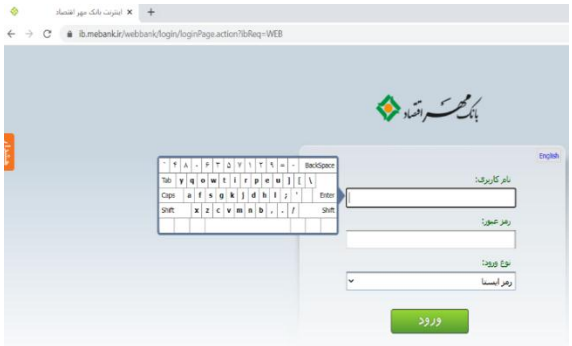


شکل ۶ قواعد سامانه‌ی خبره‌ی فازی شناسایی جرم‌شناسی پس از اجرای نمونه‌ی آزمایشی

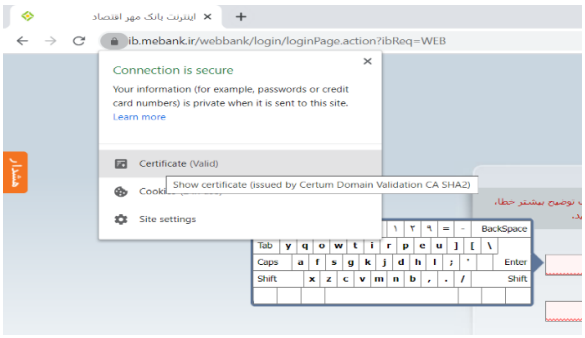
ب) نمونه‌ی دوم: وبگاه بانک مهر اقتصاد

وبگاه پرداخت اینترنتی بانک مهر اقتصاد در شکل ۷ نشان داده شده است. ویژگی‌های مربوط به این وبگاه استخراج شده و در ردیف ۲۱ جدول ۹ قابل مشاهده است. همانطور که در جدول ۹ هم آمده «طول یوآرال» این صفحه‌ی وب، ۳۱ است که در محدوده‌ی «متوسط» قرار می‌گیرد. علاوه بر این، در نشانیِ یوآرال آن هیچ ویژگی و نویسه‌ی غیرعادی وجود ندارد ولی یوآرال، دارای «پیش‌وند یا پس‌وند (زیردامنه)» است. همچنین این وبگاه دارای گواهی کاملاً معتبر است (شکل ۸) که با کلیک بر روی «*More Information*» و سپس «*View Certificate*» (شکل ۹) می‌توان جزئیات گواهی را مشاهده کرد. همان‌طور که در شکل ۹ مشاهده می‌شود، گواهی دارای تاریخ صدور و انقضای معتبر بوده و اطلاعات کافی در آن موجود است در نتیجه «جزئیات موجود درگواهی» در محدوده‌ی واژه‌ی «زیاد» است. از جمله ویژگی‌های مهم دیگر این وبگاه، نبود کدهای مخرب و نیز «عادی بودن *SFH*» است. با مراجعه به یک وبگاه *WHOIS* می‌توان به آسانی از «عادی بودن رکورد دی‌اِن‌اِس» آن نیز اطمینان حاصل کرد.

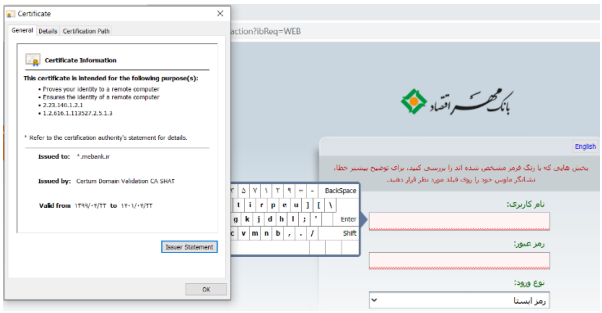
سامانه‌ی فازی ابتدا برای هریک از ۲۰ متغیر ورودی درجه‌ی تعلّق را محاسبه می‌کند و پس از استفاده از موتور استنتاج کمینه‌ی ممدانی و وافازی‌ساز گرانیگاه میزان جرم‌شناسی وبگاه به دست می‌آید. در نهایت سامانه‌ی فازیِ طراحی شده، درصد جرم‌شناسی ۴/۷۸ را برای این وبگاه محاسبه می‌کند. این عدد بیانگر «قانونی» بودن وبگاه است و نتیجه‌ی سامانه صحیح است.



شکل ۷ وبگاه پرداخت اینترنتی بانک مهر اقتصاد



شکل ۸ گواهی بانک مهر اقتصاد

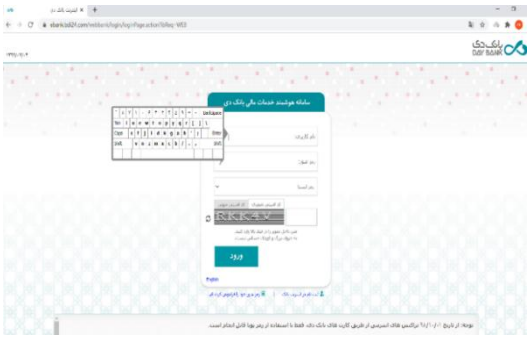


شکل ۹ جزئیات گواهی بانک مهر اقتصاد

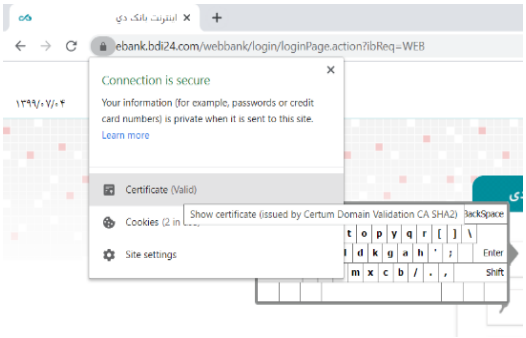
ج) نمونه سوم: وبگاه بانک دی

مقادیر هریک از ۲۰ متغیر ورودی (ویژگی‌های وبگاه بانک دی) در ردیف ۹ جدول ۹ آمده است. در بخش نشانی یوآرال وبگاه بانک دی *https:*۱۱ وجود دارد. پس *SSL* برابر با «یک» است. با کلیک بر روی نشانه‌ی قفل، اطلاعات مربوط به گواهی و گواهی‌دهنده قابل مشاهده است (شکل ۱۰). به همین ترتیب با کلیک بر روی «اطلاعات بیشتر» می‌توان جزئیات گواهی را دید لذا همانطور که در ردیف ۹ جدول ۹ مشاهده می‌شود، «اعتبار گواهی‌دهنده» و «جزئیات موجود در گواهی» در محدوده‌ی واژه‌ی «زیاد» هستند. همچنین وبگاه دارای زیردامنه است در نتیجه شاخص «اضافه کردن پیشوند و پسوند» نیز برابر با «یک» است. نبود سایر شاخص‌ها مانند عدم «غیرعادی بودن دی‌اِن‌اِس» باعث شده که این شاخص‌ها برابر با «صفر» باشند.

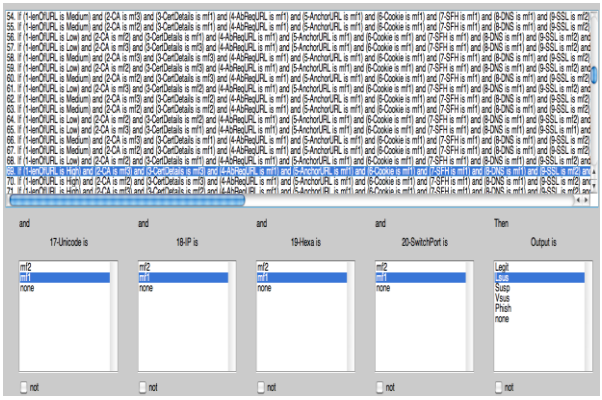
در نهایت درصد جرم‌شناسی برابر با ۱۴/۶ شده است. در این نمونه، سامانه باید درصد جرم‌شناسی پایین‌تری را به عنوان خروجی می‌داد و وبگاه به عنوان «قانونی» شناسایی می‌شد اما به دلیل اینکه تعداد نویسه‌های یوآرال، ۵۴ است و در محدوده‌ی «متوسط» و «زیاد» قرار می‌گیرد، دو قاعده‌ی شماره‌ی ۵۸ و ۶۹ در پایگاه قواعد آتش[۱۵] می‌شود و نتیجه «کمی مشکوک» تشخیص داده شده است. لازم به ذکر است همانطور که پیش از این شرح داده شد، اینکه چه عددی نشان‌دهنده‌ی یوآرال طولانی است بر اساس نظر خبرگان در سامانه لحاظ شده است.



شکل ۱۰ اینترنت بانک دی



شکل ۱۱ اطلاعات مربوط به گواهی



شکل ۱۲ پایگاه قواعد سامانه‌ی خبره‌ی فازیِ شناسایی جرم‌شناسی

شایان ذکر است نتایج ارزیابی سامانه روی ۵۰ نمونه وبگاه مورد آزمایش، نشان می‌دهد که سامانه دارای دقت تشخیص ۸۸٪ است و در حدود ۱۲٪ خطا دارد. هرچند در ادامه با شرح نمونه‌ی بانک دی اشاره خواهد شد که خطای موجود، مربوط به برداشت خبرگان بوده و ناشی

[15] *Rule fire*

از پیاده‌سازی نظریات آنها است. لازم به ذکر است، محدودیت دسترسی به خبرگان، محدودیت دسترسی به نمونه‌های واقعی وبگاه‌های بانکداری برای ارزیابی سامانه با اطمینان بالاتر، تخمین‌های بکار رفته در طراحی و فقدان استانداردی مشخص و دقیق در ایران برای طراحی وبگاه‌های بانکی که از حساسیت امنیتی بالایی برخوردارند، از دلایل ایجاد این میزان از خطا است.

هربار اجرای این سامانه و محاسبه‌ی درصد جرم‌شناسی وبگاه در محیط نرم افزار متلب روی رایانه‌ای با پردازنده‌ی *2.3 GHz Intel Core i7* و حافظه‌ی ۴ گیگابایتی[16]، ۱۶ ثانیه طول می‌کشد. زمان محاسبه‌ی خروجی، متناسب با تعداد متغیرها و تعداد قواعد فازی است زیرا سامانه‌ی فازی در هر مرتبه اجرا، مقدار تمام متغیرها را به ازای هریک از قواعد محاسبه می‌کند. لذا کُندی تشخیص در سامانه‌ی خبره‌ی فازی به دلیل تعداد زیاد متغیرهای ورودی و در نتیجه حجم زیاد قواعد در پایگاه قواعد فازی است.

- **بهبود سامانه‌ی خبره‌ی فازی به کمک نظریه‌ی مجموعه‌های ژولیده**

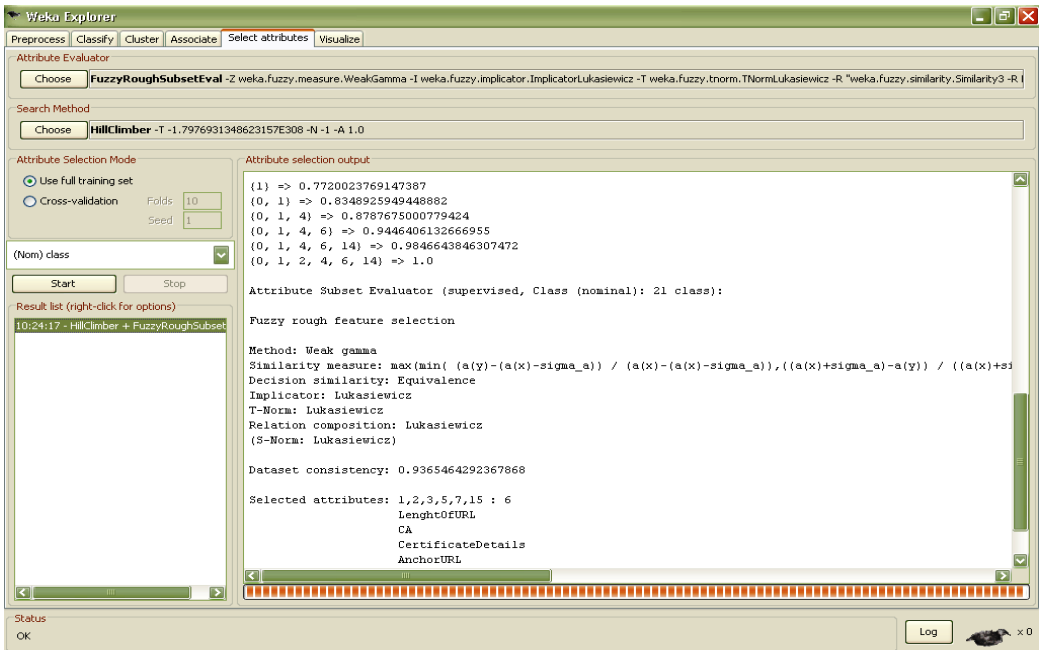
همانطور که نتایج ارزیابی در جدول ۹ نشان داد سامانه دارای کارایی ۸۸٪ است و به خوبی می‌تواند حملات جرم‌شناسی ناشی از رخداد های سایبری در وبگاه‌های بانکی را تشخیص دهد. اما همان‌طور که در بخش‌های قبلی اشاره شد، سامانه حاوی ۱۵۹ قاعده و ۲۰ شاخص ورودی است. این درحالی است که در عمل این سامانه باید به صورت برخط و در کوتاه‌ترین زمان ممکن، نتیجه‌ی تشخیص اعتبار وبگاه را اعلام کند تا بتوان بطور کاملاً بی‌درنگ از وارد شدن خسارات مالی به مشتریان بانک جلوگیری کرد. لذا در این بخش با استفاده از نظریه‌ی مجموعه‌های ژولیده[17]، آن دسته از متغیّرهای ورودی که دارای افزونگی هستند، شناسایی شده و حذف می‌شوند و بدین ترتیب سامانه‌ی خبره‌ی فازی طراحی شده در بخش قبل از نظر تعداد قوانین و زمان محاسبه‌ی خروجی بهبود داده می‌شود. در ادامه به شرح مراحل طراحی سامانه‌ی فازی-ژولیده می‌پردازیم.

الف) کاهش متغیرهای ورودی با استفاده از نظریه‌ی مجموعه‌های ژولیده

در این مرحله سعی بر این است با استفاده از الگوریتم انتخاب ویژگی فازی-ژولیده[18] برای موارد حقیقی حملات جرم‌شناسی ناشی از رخداد های سایبری، شاخص‌های غیر مؤثر و دارای افزونگی در جدول ۳ شناسایی و حذف شوند و در نتیجه تعداد متغیرهای ورودی به سامانه‌ی فازی و در نتیجه تعداد قواعد تا حد امکان کاهش پیدا کند و در نتیجه زمان اعلام نتیجه‌ی تشخیص اعتبار وبگاه، کاهش یافته و سامانه چابک‌تر عمل کند. در این راستا از الگوریتم مجموعه‌های ژولیده-ی فازی[19] استفاده شد تا آن دسته از متغیرهای ورودی که بیشترین تأثیر را بر خروجی سامانه‌ی فازی شناسایی جرم‌شناسی می‌گذارند، مشخص شده و قواعد سامانه بر روی این شاخص‌ها تعریف شود. برای پیاده‌سازی الگوریتم فازی-ژولیده، ۶۰ مورد از وبگاه‌های حقیقی حوزه‌ی بانکداری الکترونیکی را که بیش از ۵۰ درصد آنها مربوط به بانک‌های ایرانی و بقیه مربوط به حملات جرم‌شناسی ناشی از رخداد های سایبری به سایر وبگاه-های بانکی در سراسر جهان بودند استخراج شده و به نسخه‌ی ویژه‌ای از نرم‌افزار داده‌کاوی وِکا[20] داده شد. لازم به ذکر است در این مرحله برای هر وبگاه، مقادیر تمام ۲۸ شاخص اولیه که در جدول ۳ آمده است، در نظر گرفته و برای تحلیل به نرم‌افزار مذکور داده شد. پس از اجرای الگوریتم فازی-ژولیده، خروجی نمایش داده شده در شکل ۱۳ دریافت شد. این بار شش شاخص تأثیرگذار به دست آمده از الگوریتم فازی-ژولیده عبارتند از: طول یوآرال، میزان اعتبار گواهی‌دهنده، جزئیات موجود در گواهی، یوآرال غیرعادی لنگر، *SFH* غیرعادی و اضافه کردن پیش‌وند و پس‌وند (وجود زیردامنه).

---

[16] *4 GB, RAM*
[17] *Rough Set Theory*
[18] *Fuzzy-rough Set Feature Selection*
[19] *Fuzzy-rough set*
[20] *Weka Software*



شکل ۱۳ خروجی نرم‌افزار وِکا

ب) طراحی سامانه‌ی خبره‌ی فازی-ژولیده

در این مرحله با استفاده از شش شاخص اصلی گام قبل، سامانه‌ی خبره‌ی فازی-ژولیده طراحی شد. پایگاه قواعد سامانه‌ی خبره‌ی فازی-ژولیده، شامل ۴۰ قاعده اگر-آنگاه (با ترکیب‌کننده «**و**») است. بخشی از پایگاه دانش در جدول ۱۰ آمده است.

لازم به ذکر است، به غیر از مجموعه‌ی ورودی‌های سامانه و پایگاه قواعد، تمامی اجزای سامانه‌ی خبره‌ی فازی-ژولیده، اعم از متغیّر خروجی، توابع عضویت، فازی‌ساز، وافازی‌ساز و موتور استنتاج فازی، کاملا مشابه سامانه‌ی خبره‌ی فازی است.

جدول ۱۰ بخشی از قواعد پایگاه دانش فازیِ سامانه‌ی خبره‌ی فازی-ژولیده

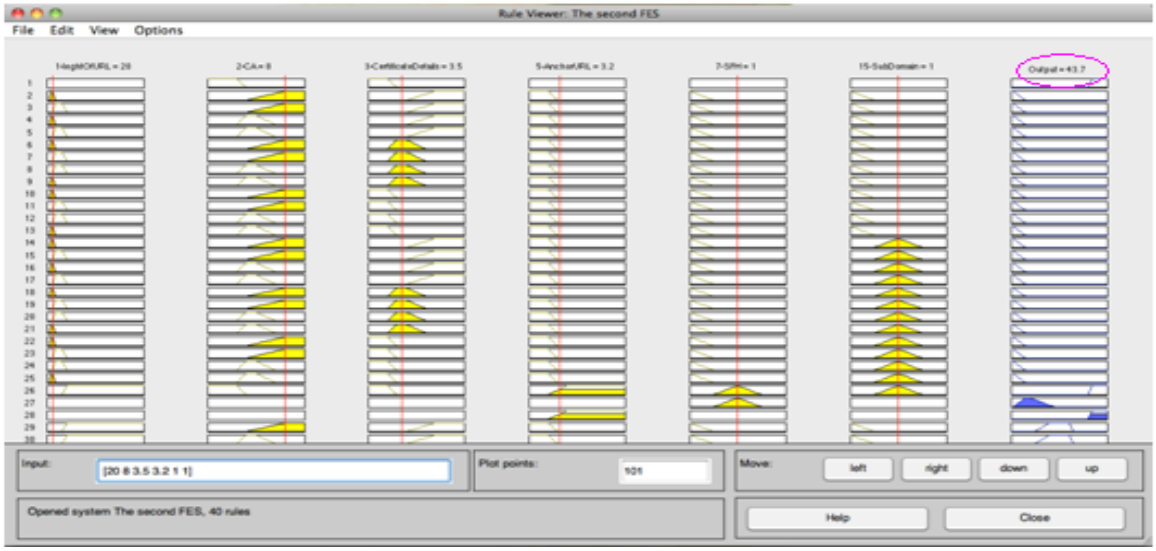
ردیف	شرح قاعده
۱	**اگر** اعتبار گواهی‌دهنده کم باشد **و** جزئیات موجود در گواهی دیجیتالی کم باشد، **آنگاه** وبگاه **جعلی** است.
۲	**اگر** یوآرال لنگر زیاد غیرعادی باشد، **آنگاه** وبگاه **جعلی** است.
۳	**اگر** اعتبار گواهی‌دهنده زیاد باشد **و** یوآرال لنگر کمی غیرعادی باشد **و** جزئیات موجود در گواهی دیجیتالی زیاد باشد **و** *SFH* غیرعادی نباشد **و** طول یوآرال کم باشد **و** از زیردامنه استفاده نشده باشد، **آنگاه** وبگاه **قانونی** است.
۴	**اگر** اعتبار گواهی‌دهنده زیاد باشد **و** یوآرال لنگر کمی غیرعادی باشد **و** جزئیات موجود در گواهی دیجیتالی زیاد باشد **و** *SFH* غیرعادی نباشد **و** طول یوآرال متوسط باشد **و** از زیردامنه استفاده نشده باشد، **آنگاه** وبگاه **قانونی** است.
۵	**اگر** اعتبار گواهی‌دهنده متوسط باشد **و** یوآرال لنگر کمی غیرعادی باشد **و** جزئیات موجود در گواهی دیجیتالی زیاد باشد **و** *SFH* غیرعادی نباشد **و** طول یوآرال متوسط باشد **و** از زیردامنه استفاده شده باشد، **آنگاه** وبگاه **قانونی** است.
۶	**اگر** اعتبار گواهی‌دهنده متوسط باشد **و** یوآرال لنگر کمی غیرعادی باشد **و** جزئیات موجود در گواهی دیجیتالی زیاد باشد **و** *SFH* غیرعادی نباشد **و** طول یوآرال کم باشد **و** از زیردامنه استفاده شده باشد، **آنگاه** وبگاه **قانونی** است.

۷	**اگر** اعتبار گواهی‌دهنده زیاد باشد **و** یوآرال لنگر کمی غیرعادی باشد **و** جزئیات موجود در گواهی دیجیتالی کم باشد **و** *SFH* غیرعادی نباشد **و** طول یوآرال زیاد باشد **و** از زیردامنه استفاده شده باشد، **آنگاه** وبگاه **خیلی مشکوک** است.
۸	**اگر** *SFH* غیرعادی باشد، **آنگاه** وبگاه **کمی مشکوک** است.
۹	**اگر** اعتبار گواهی‌دهنده زیاد باشد **و** یوآرال لنگر کمی غیرعادی باشد **و** جزئیات موجود در گواهی دیجیتالی کم باشد **و** *SFH* غیرعادی نباشد **و** طول یوآرال زیاد باشد **و** از زیردامنه استفاده نشده باشد، **آنگاه** وبگاه **مشکوک** است.
۱۰	**اگر** اعتبار گواهی‌دهنده زیاد باشد **و** یوآرال لنگر کمی غیرعادی باشد **و** جزئیات موجود در گواهی دیجیتالی زیاد باشد **و** *SFH* غیرعادی نباشد **و** طول یوآرال زیاد باشد **و** از زیردامنه استفاده نشده باشد، **آنگاه** وبگاه **مشکوک** است.

ج) ارزیابی سامانه‌ی خبره‌ی فازی-ژولیده

در این مرحله سامانه‌ی خبره‌ی فازی-ژولیده بر ۵۰ وبگاه بانکداری الکترونیکی آزمایش شد و نتایج آن با نتایج ارزیابی سامانه‌ی فازی مقایسه شد. این مقایسه نشان می‌دهد که سامانه‌ی خبره‌ی فازی-ژولیده دقیقاً با همان دقّتِ سامانه‌ی خبره‌ی فازی قادر به تشخیص میزان اعتبار وبگاه است. نتایج ارزیابی این سامانه بر ۱۰ نمونه وبگاه بانکی در جدول ۱۱ آمده است.

شکل ۱۴ نتیجه‌ی اجرای نمونه‌ی آزمایشی شرح داده شده در بخش قبل را در سامانه‌ی فازی ژولیده نشان می‌دهد. همان‌طور که در ردیف ۱۰ جدول ۱۱ مشاهده می‌شود، درصد جرم‌شناسی این وبگاه آزمایشی ۴۳/۷ محاسبه شده و وبگاه «مشکوک» است. یکسان بودن عدد خروجی با خروجی سامانه‌ی فازی قبلی به خوبی اثبات می‌کند شاخص‌هایی که از ورودی‌های سامانه‌ی فازی حذف شده اند، تأثیر قابل توجهی در نتیجه‌ی پایانی آن نداشته و صرفاً تعداد محاسبات را افزایش داده است. نقش شاخص‌ها در پایگاه قواعد سامانه‌ی فازی-ژولیده نسبت به قواعد سامانه‌ی فازی تغییری نکرده است، به همین دلیل در صورت یکسان بودن مقادیر ورودی به ازای شاخص‌های مشترک، نتیجه‌ی نهایی تشخیص سامانه‌ی فازی-ژولیده متفاوت از سامانه‌ی فازی نیست. لذا مزیّت استفاده از سامانه‌ی فازی-ژولیده، سرعت آن در تشخیص جرم‌شناسی است که در ادامه شرح داده می‌شود. در شکل ۱۴، شش ستون از متغیرهای ورودی و ستون خروجی آمده است و مشاهده می‌شود که وضعیت هر متغیر در هر قانون به ازای مقادیر ورودی محاسبه شده و با خطوط قرمز مشخص شده است. در بالای ستون آخر، عدد خروجی مشخص شده است.



شکل ۱۴ قواعد سامانه‌ی خبره‌ی فازی- ژولیده پس از اجرای نمونه‌ی آزمایشی

جدول ۱۱ نتایج اجرای سامانه‌ی خبره‌ی فازی-ژولیده

ردیف	طول *URL*	میزان اعتبار گواهی دهنده	جزئیات موجود در گواهی	*URL* غیرعادی لنگر	*SFH* غیرعادی	اضافه کردن پیشوند و پسوند	میزان خطر جرم‌شناسی خروجی سامانه‌ی فازی- ژولیده (درصد)	تشخیص	صحت نتیجه
۱	۶۴	۰	۰	۰	۰	۰	۹۱/۴	جعلی	درست
۲	۲۸	۰	۰	۰	۰	۱	۹۱/۴	جعلی	درست
۳	۶۰	۸/۳	۷	۰	۰	۱	۱۹/۳	کمی مشکوک	نادرست (قانونی)
۴	۴۵	۹	۹/۶	۰	۰	۱	۴/۷۸	قانونی	درست
۵	۲۵	۸/۹	۹/۵	۰	۰	۱	۵/۷۶	قانونی	درست
۶	۳۷	۸/۹	۹/۵	۱	۰	۱	۴/۷۸	قانونی	درست
۷	۵۵	۰	۰	۰	۰	۱	۹۱/۴	جعلی	درست
۸	۳۸	۸/۹	۹/۵	۰	۰	۱	۴/۷۸	قانونی	درست
۹	۳۰	۱/۹	۷/۶	۱/۲	۰	۰	۹۱/۴	جعلی	نادرست (قانونی)
۱۰	۲۰	۸	۳/۵	۳/۲	۱	۱	۴۳/۷	مشکوک	درست

نتایج اجرای سامانه خبره‌ی فازی-ژولیده روی ۵۰ نمونه وبگاه بانکی نشان می‌دهد که دقت تشخیص سامانه ۸۸٪ و میزان خطای آن ۱۲٪ است. اشاره شد که دستاورد مهم استفاده از نظریه‌ی مجموعه‌های ژولیده، کاهش زمان محاسبه‌ی خروجی است و همچنان که بیان شد، زمان محاسبه‌ی خروجی، متناسب با تعداد متغیرها و تعداد قواعد فازی است. سامانه‌ی فازی- ژولیده‌یِ طراحی شده برای تشخیص جرم‌شناسی، که شش متغیر ورودی و ۴۰ قاعده دارد، نیز همچون سامانه‌ی فازی قبلی در محیط نرم افزار متلب روی رایانه‌ای با حافظه‌ی ۴ گیگابایتی و دارای پردازنده‌ی *Intel Core i7* با سرعت ۲/۳ گیگا هرتز پیاده‌سازی و اجرا شد و مشاهده شد که این سامانه نتیجه را ظرف یک ثانیه محاسبه و اعلام می‌کند. حال آنکه محاسبه‌ی درصد جرم‌شناسی و اعلام وضعیت وبگاه در سامانه‌ی خبره‌ی فازی با ۲۰ متغیر ورودی و ۱۵۹ قاعده، حداقل ۱۶ ثانیه طول می‌کشید. بنابراین بدیهی است سامانه‌ی خبره‌ی فازی-ژولیده گزینه‌ی بسیار مناسب‌تری برای استفاده در شرایط برخط است زیرا برای افشای اطلاعات حساس و محرمانه‌ی کاربران در فضای مجازی تنها چند ثانیه کفایت می‌کند و شناسایی به موقع و بی‌درنگ وبگاه تقلبی بسیار حائز اهمیت است.

- **نتیجه گیری**

یکی از عوامل مهم در مقبولیت و گسترده شدن فرایندهای بانکداری الکترونیکی توسعه نرم‌افزاری و افزایش امنیت در سامانه‌های آن محسوب می شود. در صورتی که زمینه لازم برای تأمین این دو نیاز فراهم شود کاربرد عمومی از سامانه‌های الکترونیکی گسترش و تسهیل می‌یابد و ریسک استفاده از چنین سامانه‌هایی با حفظ درجه‌ی امنیت بالا کاهش می‌یابد و اعتماد و رضایتمندی مشتری افزایش می‌یابد. تحقیقات نشان می‌دهد که بانک‌ها قبل از هرچیز باید این اعتماد را در مشتریان خود ایجاد کنند که بانکداری الکترونیکی و عملیات صورت گرفته در آن دارای امنیت کافی است. پیشرفت‌های گسترده در زمینه‌ی فنّاوری، کمک زیادی به افزایش سطح امنیت داده‌های انتقال یافته در بانکداری الکترونیکی کرده است. عموماً بانکداری اینترنتی و برخط می‌تواند مخاطره‌های فراوانی برای مؤسسات و بنگاه‌های اقتصادی به همراه داشته باشد. اطلاعات مربوط به مشتریان و معاملات مالی بسیار حساس و محرمانه بوده و انجام این‌گونه معاملات از طریق اینترنت چالش‌هایی را در زمینه‌ی امنیت و اطمینان معاملات به وجود آورده است. بدون وجود امنیت بانکداری الکترونیکی نه تنها فایده‌ای نخواهد داشت بلکه خسارت‌های فراوانی هم وارد می‌کند. هرچند امنیت مطلق وجود ندارد اما لااقل برای برخورداری از یک وضعیت غیرشکننده می‌باید هزینه‌هایی صرف نمود. در این پژوهش مستخرج از پایان نامه تلاش شده تا برای تشخیص و کنترل یکی از مهم‌ترین انواع حملات اینترنتی که بیشترین آسیب را بر اعتماد مشتریان در حوزه‌ی تجارت الکترونیکی و بخصوص بانکداری الکترونیکی وارد می‌کند، راه حلی مؤثر پیشنهاد شود. برای افزایش دقت در تشخیص حملات جرم‌شناسی ناشی از رخداد های سایبری در این پژوهش از نظریه‌ی فازی بهره برده شده است و برای اولین بار سامانه‌ی خبره‌ی فازی برای تشخیص حملات جرم‌شناسی ناشی از رخداد های سایبری را با استفاده از نظریه مجموعه-های ژولیده بهبود دادیم. نتایج این پژوهش به صورت خلاصه در زیر ارائه شده است:

الف- خروجی حاصل از سامانه خبره فازی طراحی شده به نحوه طراحی قواعد پایگاه دانش فازی بستگی دارد که بر اساس نظریات خبرگان در حوزه‌ی بانکداری اینترنتی طراحی شده است.

ب- مدل پیشنهادی پژوهش در محیط نرم افزار متلب شبیه‌سازی شده است و به همین دلیل به سادگی می-توان برای هر داده‌ی ورودی مقادیر جریان‌ها را محاسبه و نتیجه‌ی خروجی را به‌دست آورد. سامانه‌ی خبره فازی می‌تواند با اتصال به یک پایگاه داده محلی، به صورت خودکار اطلاعات ورودی را دریافت کرده و نتایج خروجی را نیز به صورت خودکار ثبت نماید. لذا پردازش تعداد زیادی داده در زمانی کوتاه امکان‌پذیر است.

ج- آزمایش سامانه با استفاده از داده‌های مربوط به حملات واقعی جرم‌شناسی ناشی از رخداد های سایبری بر روی وبگاه بانک‌ها انجام شده است.

د- عوامل مؤثر برای تشخیص حملات جرم‌شناسی ناشی از رخداد های سایبری در بانکداری الکترونیکی ایران استخراج شده است.

منابع

بست، جان (۱۳۹۵)، روشهای تحقیق در علوم تربیتی و رفتاری، ترجمه حسن پاشا شریفی و نرگس طالقانی، تهران، رشد.

ساروخانی، لیلا ؛ منتظر، غلامعلی (۱۳۹۶)، طراحی و پیاده سازی سیستم هوشمند شناسایی رفتار مشکوک در بانکداری اینترنتی به کمک نظریهٔ مجموعه های فازی، فصلنامه فنّاوری اطلاعات و ارتباطات ایران، سال اول، شماره های ۱و ۲، پاییز و زمستان ۱۳۹۶.

Gupta, K., & Arora, N. (2019). Investigating consumer intention to accept mobile payment systems through unified theory of acceptance model. South Asian Journal of Business Studies.

Banu, R., Anand, M., Kamath, A., Ashika, S., Ujwala, H. S., & Harshitha, S. N. (2019, May). Detecting Phishing Attacks Using Natural Language Processing And Machine Learning. In 2019 International Conference on Intelligent Computing and Control Systems (ICCS) (pp. 1210-1214). IEEE.

Adil, M., Khan, R., & Ghani, M. A. N. U. (2020, February). Preventive Techniques of Phishing Attacks in Networks. In 2020 3rd International Conference on Advancements in

Computational Sciences (ICACS) (pp. 1-8). IEEE.

Subasi, A., & Kremic, E. (2020). Comparison of Adaboost with MultiBoosting for Phishing Website Detection. Procedia Computer Science, 168, 272-278.

اسدی صومعه، آ. (۱۳۹۸). توسعه‌ی مدل پرامیتی به کمک نظریه‌ی فازی شهودی و به کارگیری آن در بهبود کیفیت وبگاه‌های دانشگاهی. پایان‌نامه‌ی کارشناسی ارشد مهندسی فناوری اطلاعات. تهران، دانشگاه تربیت مدرس.

ساروخانی، ل. (۱۳۹۷). تشخیص رفتارهای مشکوک مشتریان در بانکداری الکترونیکی با استفاده از نظریه‌ی فازی. پایان‌نامه‌ی کارشناسی ارشد مهندسی فناوری اطلاعات. تهران، دانشگاه تربیت مدرس.

عموزاد خلیلی، ح، ر. توکلی مقدم و ف. مطلبی. (۱۳۹۷). "اثرات بهبود امنیت بانکداری الکترونیکی در جلب رضایت مشتریان الکترونیکی" . دومین کنفرانس جهانی بانکداری الکترونیکی. تهران، ایران.

Li, Q., Cheng, M., Wang, J., & Sun, B. (2020). LSTM based Phishing Detection for Big Email Data. IEEE Transactions on Big Data.

Megha, N., Babu, K. R., & Sherly, E. (2019, July). An Intelligent System for Phishing Attack Detection and Prevention. In 2019 International Conference on Communication and Electronics Systems (ICCES) (pp. 1577-1582). IEEE.

Paliath, S., Qbeitah, M. A., & Aldwairi, M. (2020). PhishOut: Effective Phishing Detection Using Selected Features. arXiv preprint arXiv:2004.09789.

Olufemi, R., Adebowale, J., & Victoria, K. (2018). Detection and Prevention of Phishing Attack Using Linkguard Algorithm. Journal of Information, 4(1), 10-23.

Nisha, S., & Madheswari, A. N. (2016, February). Prevention of phishing attacks in voting system using visual cryptography. In 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS) (pp. 1-4). IEEE.

Gaharwar, R. S., & Gupta, R. (2020). Vulnerability assessment of android instant messaging application and network intrusion detection prevention systems. Journal of Statistics and Management Systems, 23(2), 399-406.

Prashanth Kumar, P., & Vinay, M. (2019). Enhanced Technique for Detection and Prevention of Phishing on Websites. Journal of Computational and Theoretical Nanoscience, 16(5-6), 2614-2618.

Journal of Financial Knowledge of Securities Analysis
Vol. 16 / No. 59, Autumn 2023

Presentation of electronic banking forensic policy model

Afshin Khodamoradi[1]
Alireza Pourebrahimi[2] ❋
Mohammad Ali Afshar Kazemi[3]

Abstract
Given the complexity of tools as well as the variety of banking activities and intra-system communications, maintaining the banking system's health and stability refers to one of the key reasons for monitoring banks and credit institutions in today's banking industry; on the other hand, cybercriminals may cause serious harm. This is a descriptive-quantitative research employing two of deep thinking and survey study methods and different tools (interview, observation, questionnaire, and document review) for data collection. Its statistical population includes the investigation of cyber incident logs over the recent year, and no special sampling has been carried out. After presenting the model, the usual simulators, particularly MATLAB, are utilized based on the project needs and the results are reviewed according to the execution speed. The system designed to detect various criminology types caused by cyber incidents on the Internet is expected to have high flexibility and to be applied to other types of websites.

Keywords: *E-commerce, Criminology, Cyber Incidents, Website, Banking*

[1] *Corresponding author, PhD Student of Information Technology Management, Islamic Azad University, Qeshm International Branch, akmoradi231@gmail.com*
[2] *Assistant Professor and Faculty Member, Management and Accounting Department, Islamic Azad University, Karaj Branch, support@apebrahimi.com*
[3] *Associate Professor, Department of Industrial Management, Islamic Azad University, Central Tehran Branch, m_afsharkazemi@iauec.ac.ir*