مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"

سال اول، شماره ۴، زمستان ۱۳۹۲، ص ۳۳-۲۳

به‌کارگیری شبکه‌های عصبی مصنوعی در ارزیابی ریسک امنیت اطلاعات

صدیقه اولین چهارسوقی[۱]، محمدعلی دوستاری[۲*]، علی یزدیان ورجانی[۳]، سید علیرضا مهدوی اردستانی[٤]

۱- دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، دانشکده فنی و مهندسی، دانشگاه شاهد ۲- استادیار دانشکده فنی و مهندسی، دانشگاه شاهد ۳- استادیار دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس ٤- کارشناسی ارشد مدیریت فناوری اطلاعات واحد الکترونیکی، دانشگاه آزاد اسلامی

(دریافت: ۹۱/۰۴/۲۵ ، پذیرش: ۹۱/۱۰/۲۷)

چکیده

یکی از مهم‌ترین اجزای سازنده سامانه مدیریت امنیت اطلاعات، فرایند ارزیابی ریسک است. فرایند ارزیابی ریسک به سازمان‌ها این امکان را می‌دهد که نقاط ضعف و تهدیدات امنیتی خود را شناسایی نمایند و متناسب با ریسک‌های تعیین شده، راه‌کارهای مناسب جهت مقابله با آنها را اتخاذ نمایند. از این‌رو به‌منظور مدیریت مطلوب‌تر امنیت اطلاعات باید روش‌های مناسبی جهت ارزیابی ریسک به‌کار گرفته شود تا با کمترین خطا بتوان به تحلیل و ارزیابی ریسک‌های شناسایی شده پرداخت. این مقاله با ارائه شاخص‌هایی برای تعیین احتمال وقوع تهدیدات و شدت آسیب‌پذیری‌ها و ترکیب آنها با پیامد حوادث، راهکار جدیدی را برای ارزیابی ریسک امنیت اطلاعات ارائه می‌دهد. محاسبه ریسک‌ها با استفاده از شبکه‌های عصبی مصنوعی صورت گرفته است. به‌منظور صحت‌سنجی درستی و دقت این روش، سه روش هوشمند دیگر شامل «ماشین بردارهای پشتیبان»، «درخت تصمیم» و « k- نزدیک‌ترین همسایه» نیز پیاده‌سازی و نتایج حاصل با شبکه عصبی مقایسه شده است.

واژه‌های کلیدی: امنیت اطلاعات، ارزیابی ریسک، شبکه‌های عصبی مصنوعی، روش‌های هوشمند

۱. مقدمه

مدیریت مناسب اطلاعات لازمه برقراری امنیت اطلاعات می‌باشد. بهترین راه مدیریت، اطلاع از وضعیت موجود و اتخاذ تصمیمات صحیح برای بهبود مستمر آن است. لازمه‌ی شناسایی وضعیت موجود، یک مکانیسم ارزیابی دقیق و مؤثر است که نتیجه‌ی آن هرچه بیشتر به واقعیت نزدیک باشد. ارزیابی ریسک مهم‌ترین بخش این ارزیابی است. آگاهی از اینکه ریسک‌های امنیت اطلاعات سازمان در چه وضعیتی قرار دارند، بسیار اهمیت دارد. از آنجا که این ارزیابی تاریخچه‌ی جدیدی دارد، مطالعات، استانداردها و متدولوژی‌ها در این زمینه در حال انجام بوده و روز به روز افزایش می‌یابند.

ارزیابی ریسک امنیت اطلاعات مبتنی بر استاندارد ایزو ۲۷۰۰۱ و در ترکیب با روش‌های فازی و سامانه‌های خبره، یک نمونه از این فعالیت‌ها است. این روش برای طبقه‌بندی دارایی ها، از مدل زکمن[1] استفاده کرده و پس از تعیین سطح ارزش دارایی‌ها، اثر تهدیدات و اثر آسیب‌پذیری‌ها با استفاده از تابع عضویت سه‌سطحی در مدل‌سازی فازی، ریسک نهایی با استفاده از سامانه خبره ارزیابی شده است[۱].

ادغام نتایج تحقیقات AHP[2] ریاضیات فازی و روش شبکه عصبی مصنوعی، یک روش دیگر برای ارزیابی ریسک امنیت اطلاعات می‌باشد[۲]. همچنین، از ترکیب تئوری RBF[3] شبکه عصبی و روش ارزیابی فازی بهینه‌سازی ازدحام ذرات، برای ارزیابی ریسک امنیت اطلاعات استفاده شده است[۳]. ارزیابی ریسک امنیت اطلاعات بر اساس مدل شبکه عصبی مصنوعی و AHP فازی نیز، یک روش دیگر ارائه شده می‌باشد[۴]. در روش دیگر، ریسک امنیت شبکه با استفاده از احتمالات، شدت اثر، تکنیک‌های AHP و آنتروپی شانون ارزیابی شده است. در این روش، اتخاذ تصمیمات با استفاده از منطق فازی و از طریق متغیرهای زبانی صورت گرفته است. هم‌چنین از آنتروپی برای اندازه‌گیری وزن معیار استفاده شده است[۵]. روش ارائه شده دیگر در این زمینه، برآورد ریسک امنیت اطلاعات با توجه به احتمال و عوامل اثرگذار می‌باشد.

1- Zackman

2- Analytic Hierarchy Process (AHP)

3- Radial Basis Function (RBF)

* رایانامه نویسنده پاسخگو: doostari@shahed.ac.ir

در این روش، عوامل ریسک با توجه به دسته‌بندی استاندارد ایزو ۱۷۷۹۹ شناسایی و سپس فرض شده است که تعیین احتمال هر ریسک، مشابه با تعیین وزن‌ها در مقایسه‌های دو به دو در روش AHP است. بر این اساس، احتمال یا وزن هر عامل ریسک، با استفاده از نظرات کارشناسان تعیین می‌شود. از طرف دیگر، آسیب‌پذیری هر دارایی اطلاعاتی برای هر عامل ریسک، با شدت اثر آن که مقدار نسبی‌اش از طریق متغیرهای زبانی و توسط کارشناسان به‌دست می‌آید، یکسان در نظر گرفته می‌شود [۶]. مدل فازی نیز برای ارزیابی برخط ریسک شبکه‌ها پیشنهاد شده است. بخش بیشتر این مطالعه، کنترل‌کننده‌های منطق فازی هستند که برای کمّی سازی ریسک‌های مختلف براساس تعداد متغیرهای حاصل از ورودی‌ها که ناشی از مؤلفه‌های گوناگون هستند، ایجاد شده‌اند [۷].

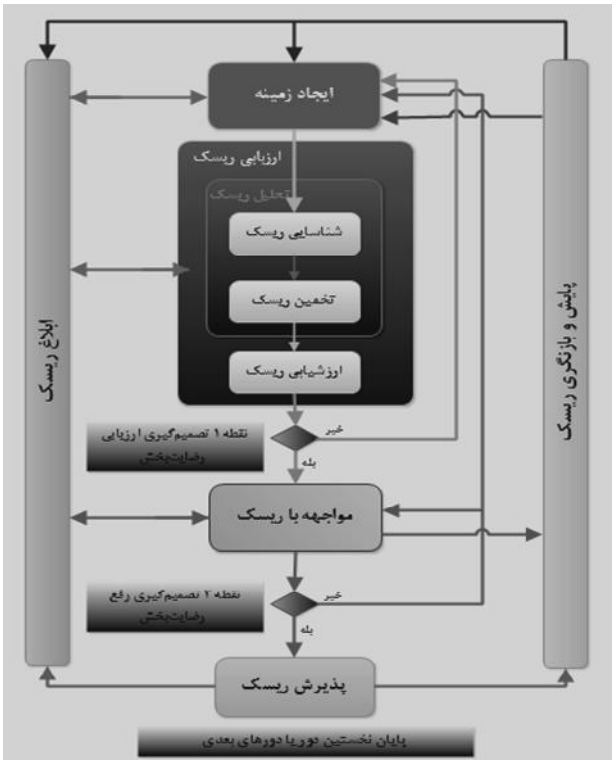
این مقاله مدل جدیدی برای ارزیابی ریسک امنیت اطلاعات با استفاده از شبکه‌های عصبی ارائه می‌دهد. در این مدل، شاخص‌هایی برای تعیین احتمال تهدید و سطح آسیب‌پذیری در نظر گرفته شده و با توجه به پیامد حادثه، ریسک مربوطه ارزیابی می‌گردد.

علاوه بر رویکرد مقایسه‌ای میان الگوریتم‌ها، روش جمع آوری داده‌ها و نقاط ضعف و قوت آنها یکی دیگر از جنبه‌های جدید این تحقیق می‌باشد.

در ادامه، مروری بر مفهوم ارزیابی ریسک امنیت اطلاعات ارائه می‌گردد. بخش سوم، به اختصار روش هوشمند شبکه عصبی مصنوعی را که الگوریتم اصلی این پژوهش می‌باشد، توصیف می‌نماید. مدل پیشنهادی برای ارزیابی ریسک امنیت اطلاعات در بخش چهارم ارائه و توصیف شده است. معرفی شاخص‌های مؤثر بر احتمال تهدید و سطح آسیب‌پذیری و هم‌چنین نحوه‌ی جمع آوری داده‌ها با استفاده از پرسش‌نامه نیز در این بخش به تفصیل بیان شده است. بخش پنجم حاوی نتایج آزمایشی حاصل از روش‌های هوشمند و بررسی و مقایسه‌ی آنهاست. در انتها نیز نتیجه‌گیری و مراجع مورد استفاده در این پژوهش آورده شده است.

۲. ارزیابی ریسک امنیت اطلاعات

ارزیابی ریسک، مهم‌ترین بخش از فرآیند مدیریت ریسک امنیت اطلاعات است. همان‌طور که در شکل ۱ نشان داده شده است، این فرآیند شامل ایجاد زمینه، ارزیابی ریسک، مواجهه با ریسک، پذیرش ریسک، ابلاغ ریسک و نظارت و بررسی ریسک می‌باشد[۸]. فرآیند مدیریت ریسک امنیت اطلاعات را می‌توان برای فعالیت‌های ارزیابی ریسک و یا رفع ریسک تکرار نمود[۹].



شکل ۱. فرآیند مدیریت ریسک امنیت اطلاعات [۸]

ارزیابی ریسک، از مراحل «شناسایی ریسک»، «تخمین ریسک» و «ارزشیابی ریسک» تشکیل شده است. هدف از شناسایی ریسک، تعیین تبعات ناشی از ایجاد یک ضرر بالقوه است و اینکه این ضرر، چگونه، کجا و چرا ممکن است رخ دهد. فعالیت‌هایی که باید در مرحله شناسایی ریسک انجام شوند، عبارتند از: «شناسایی دارایی‌ها»، «شناسایی تهدیدات»، «شناسایی آسیب پذیری ها»، «شناسایی پیامدها» و «شناسایی کنترل‌های موجود» [۹].

به‌منظور تخمین ریسک، از دو روش «کیفی» یا «کمّی» استفاده می‌شود. در تخمین کیفی، برای توصیف میزان پیامدهای بالقوه و احتمال وقوع حوادث، از مقیاس ویژگی‌های کیفی (به‌عنوان مثال: کم، متوسط و زیاد) استفاده می‌شود. مزیت تخمین کیفی، سادگی فهم آن توسط تمامی افراد سازمان و عیب آن، وابستگی به انتخاب ذهنی مقیاس است[۸].

تخمین کمّی برای پیامدها و نیز برای احتمال، از مقیاسی با مقادیر عددی (به جای مقیاس‌های توصیفی که در تخمین کیفی استفاده می‌شد) با استفاده از داده‌های حاصل از منابع متنوع استفاده می‌کند[۸]. لازم به ذکر است که در این مقاله، از رویکرد کیفی استفاده شده است. از همین‌رو، نظرات خبرگان بر اساس مدل‌های ذهنی مبنا قرار گرفته شده است.

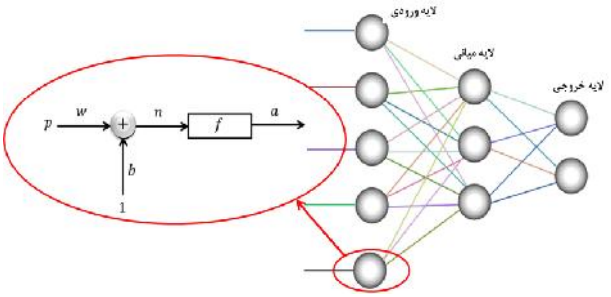
فعالیت‌های اصلی در مرحله تخمین ریسک، عبارتند از: «ارزیابی پیامدها»، «ارزیابی احتمال وقوع حوادث» و «تعیین سطح تخمین ریسک». در مرحله ارزشیابی ریسک، سطح ریسک ها باید با معیارهای ارزیابی ریسک و معیارهای پذیرش ریسک مقایسه شود [۹].

در ارزیابی ریسک، از روش‌های هوشمندی مثل فازی، سامانه‌های خبره، AHP و شبکه‌های عصبی استفاده می‌شود. برای مثال، هازلم[1] به کمک همکارانش، مدل فازی را برای ارزیابی برخط ریسک شبکه‌ها پیشنهاد کرده‌اند [۷]. همچنین، کانگفووی[2] و همکارانش، ریسک امنیت اطلاعات را بر اساس مدل شبکه عصبی مصنوعی و AHP فازی ارزیابی نموده‌اند [۴]. ادغام نتایج تحقیقات AHP، ریاضیات فازی و روش شبکه عصبی مصنوعی توسط وانگ[3] و زنگ[4]، نمونه دیگری از ارزیابی ریسک امنیت اطلاعات با استفاده از روش‌های هوشمند می‌باشد [۲].

۳. شبکه‌های عصبی مصنوعی

شبکه‌های عصبی مصنوعی یک سامانه پردازشی داده‌ها است که از مغز انسان ایده گرفته و پردازش داده‌ها را به عهده‌ی پردازنده‌های کوچک و بسیار زیادی سپرده است که به‌صورت شبکه ای به هم پیوسته و موازی با یکدیگر رفتار می‌کنند تا یک مسئله را حل نمایند. در این شبکه‌ها به کمک دانش برنامه‌نویسی، ساختمان داده‌ای طراحی می‌شود که می‌تواند همانند نورون[5] عمل کند. به این ساختمان داده، گره[6] گفته می‌شود. سپس با ایجاد شبکه‌ای بین این گره‌ها و اعمال یک الگوریتم آموزشی به آن، شبکه را آموزش می‌دهند [۱۰]. در ارائه‌ی مدل شبکه عصبی مصنوعی، تنوع بسیاری وجود داشته و تعیین سه عنصر «تعریف نورون»، «ساختار شبکه» و «الگوریتم آموزش» ضروری می‌باشد.

مدلی از شبکه عصبی مصنوعی در شکل۲ ارائه شده است. در این شکل، p نشان‌دهنده‌ی یک سیگنال ورودی است که پس از تقویت (یا تضعیف) به اندازه پارامتر w ، که پارامتر وزن نامیده می شود، به‌صورت یک سیگنال الکتریکی با اندازه pw وارد نورون می شود. سپس این سیگنال ورودی با سیگنال دیگری به اندازه b جمع می‌گردد. مجموع حاصل، یعنی سیگنالی به اندازه pw + b قبل از خارج شدن از سلول تحت عمل یا فرآیند دیگری واقع می‌شود که به



شکل ۲. ساختار شبکه عصبی مصنوعی

آن تابع انتقال[7] می‌گویند و معمولاً با علامت f نشان داده می شود. خروجی این تابع یا همان خروجی سلول، با علامت α نشانه‌گذاری شده است. در ریاضی، بخش آخر مدل‌ستازی توسط رابطه α = f(pw + b) نمایش داده می‌شود. تابع f می‌تواند به شکل های متفاوتی نظیر توابع sigmoid، arctan و arcsin انتخاب شود [۱۱]. در این پژوهش از تابع sigmoid استفاده شده است. معمولاً شبکه های عصبی حداقل دارای سه لایه می‌باشند. این سه لایه عبارتند از: لایه ورودی، لایه خروجی و لایه پنهان یا لایه میانی.

در این پژوهش از ساختار شبکه سه لایه پیشرو[8] استفاده شده است. فرآیند تنظیم وزن‌ها، یعنی تنظیم w و b در شکل۲، برای رسیدن به خروجی دلخواه به نام آموزش شبکه معروف است.

به‌طور کلی در اغلب کاربردها، آموزش شبکه به دو روش یادگیری با ناظر[9] و روش یادگیری بدون ناظر[10] انجام می‌شود [۱۰]. الگوریتم‌های متعددی برای آموزش شبکه وجود دارد. در این پژوهش از روش پس‌انتشار خطا[11] که یک روش یادگیری با ناظر می‌باشد، استفاده شده است.

۴. مدل پیشنهادی برای ارزیابی ریسک امنیت اطلاعات

ریسک، تابعی از میزان «احتمال حادثه» و «پیامد حادثه» است. «احتمال وقوع تهدید» و «سطح آسیب‌پذیری»، اجزاء سازنده احتمال حادثه می‌باشند[۹]. مسئله اصلی در ارزیابی ریسک، تعیین شاخص‌های تأثیرگذار بر احتمال وقوع تهدید و سطح آسیب‌پذیری است. در این مقاله، برای هریک از این دو جزء، چهار شاخص مهم و تأثیرگذار درنظر گرفته شده است. مدل پیشنهادی و شاخص های

1- Haslum
2- Kangfo Wei
3- Wang
4- Zang
5- Neuron
6- Node

7- Transfer Function
8- Feed Forward
9- Supervised Learning
10- Unsupervised Learning
11- Error Back Propagation

مربوطه در شکل۳ نشان داده شده است که در ادامه، به معرفی این شاخص‌ها پرداخته می‌شود.

۱.۴. احتمال تهدید

چهار شاخص در نظر گرفته شده برای احتمال تهدید عبارت‌اند از:

- **مهارت مهاجم:** نشان‌دهنده میزان توانمندی مهاجم و بهره‌مندی او از تخصص‌های امنیتی در ایجاد تهدید برای هدف مورد مخاطره است.
- **انگیزه مهاجم:** نشان‌دهنده میزان انگیزه مهاجم در ایجاد تهدید برای هدف مورد مخاطره است.
- **فرصت مهاجم:** نشان‌دهنده میزان منابع (شامل منابع مالی، انسانی، زمانی، تکنولوژیکی و ...) در دسترس مهاجم در ایجاد تهدید برای هدف مورد مخاطره است.
- **اندازه مهاجم:** نشان‌دهنده وسعت و بزرگی دامنه مهاجمان بالقوه تهدیدکننده هدف مورد مخاطره است.

لازم به ذکر است عوامل مؤثر بر احتمال وقوع تهدید منحصر به این چهار شاخص نمی‌شوند، اما به دو دلیل زیر، از این موارد به‌عنوان شاخص‌های اصلی در این مقاله استفاده شده است.

رویکرد این پژوهش، دریافت و تحلیل نتایج مبتنی بر نظرات خبرگان پایه‌ریزی شده است و در نتیجه، از روش‌های ذهنی تخمین احتمال وقوع تهدیدات استفاده شده است. از این‌رو، نوع تهدیدات مدنظر در این مقاله، از نوع تهدیدات با منشأ «انسانی» می‌باشند که شاخص‌های ذکر شده، به‌خوبی می‌توانند تبیین‌کننده احتمال وقوع چنین تهدیداتی باشند. بررسی منابع موجود [۱۴-۱۲]. نشان می‌دهد که اجماع قابل توجهی در میان متخصصین حوزه امنیت اطلاعات در خصوص این شاخص‌ها در سطح دنیا وجود دارد.

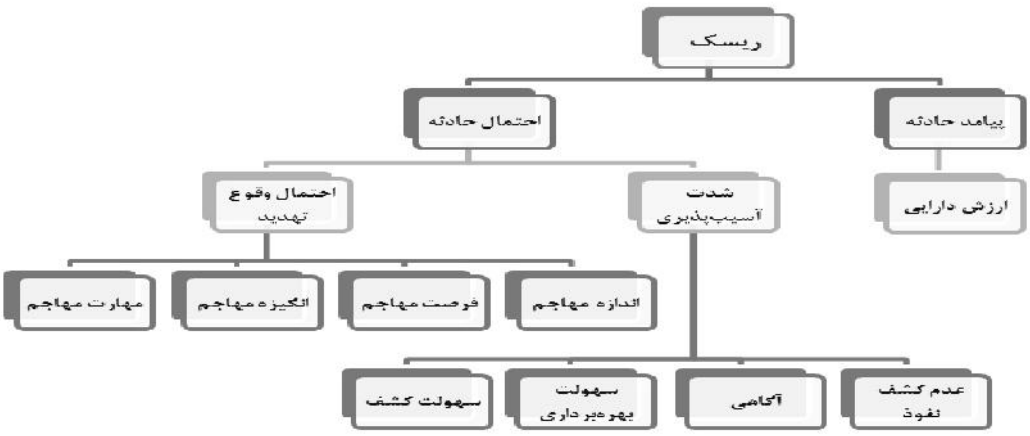
با توجه به این‌که رویکرد در نظر گرفته‌شده در این پژوهش بر اساس نظر خبرگان است، لذا مقیاس‌ها به‌صورت کیفی و در قالب ۵ سطح (برگرفته از مقیاس‌گذاری لیکرت [۱۵]) انتخاب و تعیین شده‌اند. در ادامه و در قالب جدول‌های ۱ تا ۴ توصیف هر یک از مقیاس‌های بالا برای شاخص‌ها ارائه شده است.

جدول ۱. توصیف مقیاس‌های مربوط به شاخص مهارت

مقیاس سنجش مهارت	توصیف
خیلی کم	گروه تهدیدکنندگان بدون مهارت فنی هستند.
کم	گروه تهدیدکنندگان دارای مهارت فنی اندک می‌باشند.
متوسط	تهدیدکنندگان، کاربران پیشرفته هستند.
زیاد	گروه تهدیدکنندگان دارای مهارت فنی شبکه و برنامه‌نویسی می‌باشند.
خیلی زیاد	گروه تهدیدکنندگان دارای مهارت نفوذ امنیتی می‌باشند.

جدول ۲. توصیف مقیاس‌های مربوط به شاخص انگیزه

مقیاس سنجش انگیزه	توصیف
خیلی کم	گروه تهدیدکنندگان انگیزه بسیار کمی برای تهدید دارند.
کم	گروه تهدیدکنندگان انگیزه کمی برای تهدید دارند.
متوسط	گروه تهدیدکنندگان انگیزه نه چندان زیادی برای تهدید دارند.
زیاد	گروه تهدیدکنندگان انگیزه زیادی برای تهدید دارند.
خیلی زیاد	گروه تهدیدکنندگان انگیزه بسیار زیادی برای تهدید دارند.



شکل ۳. مدل پیشنهادی برای ارزیابی ریسک

جدول ۳. توصیف مقیاس‌های مربوط به شاخص فرصت

مقیاس سنجش فرصت	توصیف
خیلی کم	گروه تهدیدکنندگان به منابع خاصی دسترسی ندارند.
کم	گروه تهدیدکنندگان به منابع خاص و محدودی دسترسی دارند.
متوسط	گروه تهدیدکنندگان دارای دسترسی یا منابع متوسط می‌باشند.
زیاد	گروه تهدیدکنندگان دارای دسترسی یا منابع ویژه می‌باشند.
خیلی زیاد	گروه تهدیدکنندگان از دسترسی کامل یا منابع بسیار ویژه‌ای برخوردارند.

جدول ۴. توصیف مقیاس‌های مربوط به شاخص اندازه

مقیاس سنجش فرصت	توصیف
خیلی کم	گروه تهدیدکنندگان محدود به توسعه‌دهندگان می‌باشند.
کم	گروه تهدیدکنندگان را مدیران سامانه تشکیل می‌دهند.
متوسط	گروه تهدیدکنندگان را کاربران اینترانت تشکیل می‌دهند.
زیاد	گروه تهدیدکنندگان، همه کاربران مجاز یا شرکا می‌باشند.
خیلی زیاد	گروه تهدیدکنندگان را کاربران اینترنتی تشکیل می‌دهند.

با توجه به این‌که در این پژوهش سعی شده است از روش های ذهنی مبتنی بر نظر خبرگان در تعیین احتمال وقوع تهدیدات استفاده شود، لذا گام‌های زیر در گردآوری و تحلیل نتایج برداشته شده است:

- **گام اول: طراحی و تدوین پرسشنامه**

از آنجائی که در رابطه با شاخص‌های موثر در احتمال تهدید که در بالا به آنها اشاره شد، داده‌هایی در دسترس نبود، روش گردآوری داده، از طریق پرسشنامه برگزیده شد.

باتوجه به شرایط خاصی که می‌بایست در ساختار داده های ورودی و خروجی چهار روش هوشمند منتخب رعایت می‌شد، نحوه طراحی پرسشنامه کمی متفاوت از پرسشنامه‌های مرسوم و متداول می‌باشد. به این ترتیب که نحوه پاسخ‌دهی به سؤالات به‌گونه‌ای است که با توجه به شاخص‌های در نظر گرفته شده در صورت هریک از سؤالات، از پاسخ‌دهنده خواسته شده است به‌عنوان یک فرد خبره در زمینه امنیت اطلاعات، میزان احتمال تهدید متناظر را تعیین نماید.

- **گام دوم: شناسایی خبرگان مرتبط و تجمیع اطلاعات**

با توجه به رویکرد این پژوهش بر به‌کارگیری نظرات خبرگان و تحلیل نتایج آنها، یکی از فعالیت‌های مهم این مقاله شناسایی خبرگان حوزه امنیت اطلاعات و مدیریت ریسک و معرفی طرح به آنها بوده است. از این‌رو، پس از بررسی‌های میدانی و جستجو در نهادها، سازمان‌ها و شرکت‌هایی که احتمال حضور چنین افرادی در آنها می‌رفت، در نهایت ۲۰ نفر از این خبرگان شناسایی شدند و پس از معرفی و ارائه طرح و پرسشنامه به آنها، از ایشان خواسته شد تا مبتنی بر نظرات کارشناسانه خود، اقدام به پاسخ‌گویی به پرسشنامه نمایند. شایان توجه است که هر یک از خبرگان به‌صورت مستقل اقدام به تکمیل پرسشنامه کردند، لذا پس از دریافت نظرات تمامی آنها، نسبت به جمع‌بندی و نرمالیزه کردن اطلاعات به‌منظور حذف پاسخ‌های با انحراف زیاد اقدام گردید.

- **گام سوم: پیاده‌سازی و تحلیل نتایج خبرگان بر اساس روش‌های هوشمند**

پس از دریافت جواب پرسشنامه‌ها از خبرگان، تجمیع و به هنجارسازی آنها، داده‌ها به الگوریتم شبکه عصبی مصنوعی داده شد تا با روش یادگیری با ناظر آموزش دیده و پس از پیاده سازی، نتیجه‌اش مورد تحلیل قرار گیرد. سپس، هریک از سه روش درخت تصمیم، k- نزدیک‌ترین همسایه و ماشین بردارهای پشتیبان برای سنجش کارایی روش شبکه‌های عصبی، پیاده‌سازی و مورد ارزیابی و مقایسه قرار گرفتند. داده‌های ورودی، دارای چهار ویژگی «مهارت»، «انگیزه»، «فرصت» و «اندازه» هستند که همان‌طور که در بالا ذکر شد، با اعداد متناظر برای ۵ سطح (برگرفته از مقیاس‌گذاری لیکرت [۱۵]) تعیین شده در آنها جایگزین شده‌اند. در ابتدا، برای خروجی احتمال تهدید نیز همان ۵ مقدار لحاظ شده بود، اما در تحلیل نتایج مشاهده شد که به‌علت پراکندگی موجود در جواب‌ها و میزان کم داده‌ها، بهتر است ۵ مقدار فوق، به ۳ مقدار کاهش یابد. به‌همین دلیل، نتایج احتمال تهدید در سه گروه «کم»، «متوسط» و «زیاد»، دسته‌بندی و تحلیل شدند. به این ترتیب که نتایج مربوط به مقادیر «خیلی کم» و «کم»، در دسته «کم» و نتایج مربوط به مقادیر «زیاد» و «خیلی زیاد»، در دسته «زیاد» قرار گرفته و نتایج مربوط به مقدار «متوسط»، به همان شکل باقی ماندند؛ بنابراین، خروجی در سه کلاس در نظر گرفته شده است. سپس داده های

به‌دست آمده، به فرم قابل آنالیز در نرم‌افزار WEKA [۱۶] تبدیل شدند. در این تحلیل، از نسخه ۷-۶-۳ استفاده شده است.

از آنجا که تعداد داده‌های جمع‌آوری شده نسبتاً کم می باشد، برای توزیع داده‌های آموزشی و آزمایشی از روش اعتبارسنجی متقاطع ۱۰ وجهی[1] [۱۷] استفاده شده است. لازم به ذکر است با توجه به اینکه نتایج حاصل از پیاده‌سازی الگوریتم‌های به‌کار گرفته شده کمّی هستند، لذا ابتدا این اعداد گِرد، و سپس به هر یک از این اعداد به ترتیب از ۱ تا ۳ عبارات کم، متوسط و زیاد منتسب شدند.

۲.۴. شدت آسیب‌پذیری

بر اساس بررسی‌های انجام شده می‌توان این گونه نتیجه گیری کرد که آسیب‌پذیری یک دارایی یا گروهی از دارایی‌ها، متشکل از چهار شاخص اصلی زیر است:

- **سهولت کشف:** نشان‌دهنده میزان سهولت در یافتن و کشف نقطه ضعف و آسیب‌پذیری در دارایی یا گروه دارایی‌های هدف است.
- **سهولت بهره‌برداری:** نشان‌دهنده میزان سهولت در سوء استفاده و بهره‌برداری از آسیب‌پذیری موجود در دارایی یا گروه دارایی‌های هدف است.
- **آگاهی:** نشان‌دهنده میزان معروفیت و آشنایی تهدیدکنندگان با آسیب‌پذیری موجود در دارایی یا گروه دارایی‌های هدف است.
- **عدم کشف نفوذ:** نشان‌دهنده میزان احتمال عدم کشف نفوذ بهره‌برداری صورت گرفته توسط مهاجم از آسیب پذیری دارایی یا گروهی از دارایی‌ها به‌وسیله صاحبان آنها است.

لازم به ذکر است که عوامل مؤثر در میزان آسیب پذیری، منحصر به این چهار شاخص نمی‌شوند، اما با توجه به جامعیت این شاخص‌ها و اجماع قابل توجهی که در میان متخصصان حوزه امنیت بر روی این عوامل وجود دارد [۱۴-۱۲]، لذا در این پژوهش از این شاخص‌ها به‌عنوان عوامل سازنده آسیب‌پذیری استفاده شده است. مقیاس‌های سنجش و اندازه‌گیری شاخص‌های سازنده سطح آسیب‌پذیری، به‌صورت کیفی و در قالب ۵ سطح (برگرفته از مقیاس-گذاری لیکرت [۱۵]) انتخاب و تعیین شده‌اند. در ادامه و در قالب جداول ۵ تا ۸، توصیف هر یک از مقیاس‌های فوق برای هر یک از شاخص‌ها ارائه شده است:

گردآوری و تحلیل نتایج در حوزه آسیب‌پذیری نیز مشابه گام‌های ارائه شده در گردآوری و تحلیل نتایج احتمال وقوع تهدیدات انجام پذیرفته است.

جدول ۵. توصیف مقیاس‌های مربوط به شاخص سهولت کشف

مقیاس سنجش سهولت کشف	توصیف
خیلی کم	کشف آسیب‌پذیری توسط گروه تهدیدکنندگان، عملاً غیرممکن است.
کم	کشف آسیب‌پذیری توسط گروه تهدیدکنندگان، دشوار است.
متوسط	کشف آسیب‌پذیری توسط گروه تهدیدکنندگان، امکان‌پذیر بوده اما به آسانی ممکن نیست.
زیاد	کشف آسیب‌پذیری توسط گروه تهدیدکنندگان، آسان است.
خیلی زیاد	کشف آسیب‌پذیری توسط گروه تهدیدکنندگان، توسط ابزارهای خودکار امکان‌پذیر است.

جدول ۶. توصیف مقیاس‌های مربوط به شاخص سهولت بهره‌برداری

مقیاس سنجش سهولت بهره‌برداری	توصیف
خیلی کم	بهره‌برداری از آسیب‌پذیری توسط گروه تهدیدکنندگان، فقط از نظر تئوری ممکن است.
کم	بهره‌برداری از آسیب‌پذیری توسط گروه تهدیدکنندگان، دشوار است.
متوسط	بهره‌برداری از آسیب‌پذیری توسط گروه تهدید کنندگان، امکان‌پذیر بوده اما به آسانی ممکن نیست.
زیاد	بهره‌برداری از آسیب‌پذیری توسط گروه تهدیدکنندگان، آسان است.
خیلی زیاد	بهره‌برداری از آسیب‌پذیری توسط گروه تهدید کنندگان، توسط ابزارهای خودکار امکان‌پذیر است.

جدول ۷. توصیف مقیاس‌های مربوط به شاخص پارامتر آگاهی

مقیاس سنجش آگاهی	توصیف
خیلی کم	آسیب‌پذیری موجود برای گروه تهدیدکنندگان، ناشناخته است.
کم	آسیب‌پذیری موجود برای گروه تهدیدکنندگان، پنهان است.
متوسط	آسیب‌پذیری موجود برای گروه تهدیدکنندگان، قابل آشکار شدن است.
زیاد	آسیب‌پذیری موجود برای گروه تهدیدکنندگان، واضح است.
خیلی زیاد	آسیب‌پذیری موجود برای گروه تهدیدکنندگان، به‌صورت یک دانش عمومی است.

1- 10-Fold Cross Validation

جدول ۸. توصیف مقیاس‌های مربوط به شاخص عدم کشف نفوذ

مقیاس سنجش عدم کشف نفوذ	توصیف
خیلی کم	امکان کشف فعال در برنامه‌ها توسط گروه تهدید شونده وجود دارد.
کم	وقایع توسط گروه تهدید شونده ثبت و بازبینی می‌شود.
متوسط	وقایع توسط گروه تهدید شونده ثبت می‌شود ولی به‌ندرت بازبینی می‌شود.
زیاد	وقایع توسط گروه تهدید شونده ثبت شده ولی بازبینی نمی‌شود.
خیلی زیاد	وقایع توسط گروه تهدید شونده ثبت نمی‌شود.

لازم به ذکر است با توجه به اینکه نتایج حاصل از الگوریتم های به‌کار گرفته شده به‌صورت کمّی هستند، لذا ابتدا این اعداد گرد و سپس به هر یک از این اعداد به‌ترتیب از ۱ تا ۳، عبارات کم، متوسط و زیاد منتسب می‌شوند. با توجه به آنکه احتمال حادثه، تابعی از سطح آسیب‌پذیری و احتمال تهدید است [۹]، لذا در این پژوهش و براساس نتایج حاصل از مراحل قبل، احتمال حادثه در ۵ سطح به‌صورت کیفی (برگرفته از مقیاس‌گذاری لیکرت [۱۵]) و در قالب ماتریس شکل ۴، تعیین و محاسبه می‌شود.

امکان تهدید	۳	متوسط	زیاد	خیلی زیاد
	۲	کم	متوسط	زیاد
	۱	خیلی کم	کم	متوسط
		۱	۲	۳
		سطح آسیب‌پذیری		

شکل ۴. ماتریس احتمال حادثه

۳.۴. پیامد حادثه

همان‌طور که پیش از این نیز اشاره شد، ریسک تابعی از دو پارامتر احتمال حادثه و پیامد حادثه است [۱۰]. روش تعیین و محاسبه احتمال حادثه به تفصیل در بالا تشریح گردید. نکته قابل توجه در خصوص این پژوهش این است که تمرکز اصلی بر روی محاسبه و تعیین احتمال حادثه و به‌کارگیری روش‌های هوشمند در تعیین احتمال وقوع تهدید و شدت آسیب‌پذیری می‌باشد. بنابراین، در خصوص پیامد حادثه فرض بر این است که متخصصان مربوطه از شیوه‌های رایج و معمول برای تعیین پیامدهای ناشی از وقوع یک حادثه می‌پردازند که در ادامه به‌طور خلاصه به توضیح آن پرداخته می‌شود. پیامد یک حادثه از میزان تأثیر حادثه بر روی دارایی مبتنی بر ارزش امنیتی آن شناسایی و تعیین می‌گردد. معمولاً و به صورت کلی، سه پارامتر محرمانگی، صحت و دسترس‌پذیری، به‌عنوان عوامل مهم در ارزش‌گذاری امنیتی دارایی محسوب می‌شوند. از این‌رو، پیامد هر حادثه ناشی از میزان تأثیرگذاری آن حادثه در جهت نقض هریک از این سه پارامتر می‌باشد. در این مقاله، به‌منظور یکسان سازی و جامعیت با دیگر شاخص‌های سازنده ریسک، پیامد حادثه در ۵ سطح به‌صورت کیفی (برگرفته از مقیاس‌گذاری لیکرت [۱۵]) و در قالب جدول ۹ تعریف می‌شود.

لازم به ذکر است به‌منظور توصیف بهتر پیامد حادثه، از شاخص‌هایی مانند وقفه در فعالیت‌های کاری و زیان مالی و تجاری جهت معرفی و توضیح میزان تأثیر حادثه استفاده شده است.

۴.۴. ارزیابی ریسک

آخرین مرحله از مراحل تحقیق در این مقاله، ارزیابی ریسک است. بر اساس اطلاعات گردآوری شده و نتایج حاصل از مراحل قبل، در این بخش به تعیین و محاسبه ریسک پرداخته می‌شود. جهت

جدول ۹. توصیف مقیاس‌های مربوط به پیامد حادثه

پیامد حادثه	توضیحات
خیلی کم	حوادث به‌وجود آمده از تهدیدات در این سطح قابل چشم‌پوشی می‌باشند. عوارض این نوع حوادث، وقفه‌های کاری بسیار کوتاه مدت و یا زیان مالی بسیار اندک به سازمان است که با واکنش مناسب و با هزینه بسیار اندک قابل جبران است.
کم	حوادث بوجود آمده از تهدیدات در این سطح چندان جدی نمی‌باشند. عوارض این نوع حوادث، وقفه‌های کاری کوتاه مدت و یا زیان مالی اندک به سازمان است که با واکنش مناسب و با هزینه اندک قابل جبران است.
متوسط	حوادث بوجود آمده از تهدیدات در این سطح نسبتاً جدی می‌باشند. عوارض این نوع حوادث، وقفه در کسب و کار سازمان، زیان مالی و خدشه به اعتبار سازمان است که با صرف هزینه متوسطی قابل جبران است.
زیاد	حوادث بوجود آمده از تهدیدات در این سطح جدی می‌باشند. عوارض این نوع حوادث، وقفه‌های بلندمدت و تأثیرگذار کاری، زیان مالی زیاد و از دست دادن اعتبار و وجهه عمومی سازمان است که جهت جبران نیاز به صرف هزینه‌های زیاد است.
خیلی زیاد	حوادث بوجود آمده از تهدیدات در این سطح بسیار جدی می‌باشند. عوارض این نوع حوادث، وقفه‌های بسیار بلند مدت و تأثیرگذار کاری، زیان مالی گزاف و از دست دادن اعتبار و وجهه عمومی سازمان در سطح گسترده است که بعضاً حتی با صرف هزینه‌های بسیار زیاد هم قابل جبران نیستند.

تعیین ریسک، از روش ماتریسی بر اساس دو پارامتر احتمال حادثه و پیامد حادثه استفاده می‌شود. ماتریس شکل ۵ نشان‌دهنده میزان ریسک می‌باشد.

امکان حادثه						
۵	متوسط	زیاد	زیاد	خیلی زیاد	خیلی زیاد
۴	کم	متوسط	زیاد	زیاد	خیلی زیاد
۳	کم	کم	متوسط	زیاد	زیاد
۲	خیلی کم	کم	کم	متوسط	زیاد
۱	خیلی کم	خیلی کم	کم	کم	متوسط
	۱	۲	۳	۴	۵
	پیامد حادثه				

شکل ۵. ماتریس ریسک

۵. پیاده‌سازی و ارزیابی نتایج آزمایشی

در نرم‌افزار شبیه‌سازی منتخب، از تابع Multilayer Perceptron به‌عنوان طبقه‌بندی کننده‌ی[1] شبکه‌های عصبی، که روش هوشمند مبنای این پژوهش برای بررسی داده‌های به‌دست‌آمده از پرسشنامه‌هاست، استفاده شده است. برای این الگوریتم با تغییر پارامتر کلیدیِ نرخ یادگیری[2]، نتایج حاصل از پیاده‌سازی با یکدیگر مقایسه شده‌اند.

همان‌طور که در بخش‌های قبل اشاره شد، پیاده‌سازی و تحلیل‌های این بخش از مقاله، با استفاده از نرم‌افزار WEKA [۱۶] که نرم‌افزار تخصصی یادگیری ماشین می‌باشد، انجام شده است. این نرم‌افزار توسط دانشگاه وایکاتو همیلتون[3] نیوزلند تهیه شده است. نسخه مورد استفاده ۷-۶-۳ می‌باشد.

برچسب کلاس‌ها به‌صورت low، med و high تعیین شده اند. کلاس اول نشان‌دهنده احتمال تهدید/ سطح آسیب‌پذیری کم، کلاس دوم نشان‌دهنده احتمال تهدید/ سطح آسیب‌پذیری متوسط و کلاس سوم نشان‌دهنده احتمال تهدید/ سطح آسیب‌پذیری زیاد می‌باشد.

۱.۵. تجزیه و تحلیل نتایج برای ارزیابی احتمال تهدید

در این بخش، داده‌های حاصل از پرسشنامه مربوط به ارزیابی احتمال تهدید، پیاده‌سازی و مورد تجزیه و تحلیل قرار گرفته اند. چهار پارامتر ورودی برای این ارزیابی عبارت‌انداز: «مهارت گروه تهدیدکننده»، «انگیزه گروه تهدیدکننده»، «فرصت و منابع موجود در اختیار گروه تهدیدکننده» و «اندازه گروه تهدیدکننده».

نتایج که نشان‌دهنده میزان احتمال تهدید می‌باشند، در سه کلاس «کم»، «متوسط» و «زیاد» دسته‌بندی شده‌اند که در ادامه، نتایج حاصل از پیاده‌سازی الگوریتم ذکر شده مورد تجزیه و تحلیل قرار می‌گیرد.

همان‌طور که ذکر شد، داده‌های آموزشی و آزمون، از روش اعتبارسنجی متقاطع ۱۰ وجهی [۱۷] توزیع شده‌اند و مستقیماً مورد تفکیک قرار نگرفته‌اند.

۱.۱.۵. تجزیه و تحلیل نتایج حاصل از پیاده‌سازی روش شبکه‌های عصبی مصنوعی

در این بخش، نتایج حاصل از پیاده‌سازی روش شبکه‌های عصبی مصنوعی ارائه می‌گردد. نتایج حاصل از نمونه‌های تست شده با این الگوریتم برای نرخ‌های یادگیری ۰/۱، ۰/۲، ۰/۳، ۰/۴ و ۰/۵ در جدول ۱۰ نشان داده شده است. همان‌طور که مشاهده می شود، این الگوریتم در نرخ یادگیری ۰/۴ بهترین پاسخ با بیشترین دقت را ارائه می‌دهد. نتایج نشان می‌دهد روش شبکه‌های عصبی مصنوعی در بهترین حالت توانسته است با دقت ۸۴/۷۵۶۱ ٪ ذهن خبره را مدل کند.

جدول ۱۰. نتایج حاصل از پیاده‌سازی روش شبکه‌های عصبی با نرخ یادگیری متفاوت برای ارزیابی احتمال تهدید

ردیف	نرخ یادگیری	میزان دقت (درصد)
۱	۰/۱	۸۱/۷۰۷۳
۲	۰/۲	۸۰/۴۸۷۸
۳	۰/۳	۸۲/۹۲۶۸
۴	۰/۴	۸۴/۷۵۶۱
۵	۰/۵	۸۲/۹۲۶۸

۲.۱.۵. تجزیه و تحلیل نتایج حاصل از اجرای سه روش هوشمند دیگر

برای بررسی دقت نتایج حاصل از روش شبکه‌های عصبی در ارزیابی احتمال تهدید، نتایج حاصل از پیاده‌سازی سه روش هوشمند دیگر نیز مورد تجزیه و تحلیل قرار گرفتند. توابع این سه روش عبارت‌اند از [۱۶]:

- J48 به‌عنوان تابعی از روش درخت تصمیم
- IBK به‌عنوان تابعی از روش k- نزدیک‌ترین همسایه
- SMO به‌عنوان تابعی از روش ماشین‌های برداری پشتیبان.

1- Classifier
2- Learning Rate
3- Waikato Hamilton University

برای هر یک از الگوریتم‌های فوق، با تغییر پارامترهای کلیدی نتایج حاصل از پیاده‌سازی هر الگوریتم، با یکدیگر مقایسه و در نهایت، بهترین نتیجه حاصل آورده شده است.

داده‌های به‌دست آمده از پرسشنامه‌ها با روش درخت تصمیم و با استفاده از تابع J48 با ضرایب اطمینان ۰/۱، ۰/۲۵، ۰/۵، ۰/۷۵ و ۱ پیاده‌سازی و مشاهده شد که بهترین نتیجه در ضرایب اطمینان ۰/۵، ۰/۷۵ و ۱/۰ و با مقدار ۷۶/۲۱۹۵٪ رخ می دهد. همچنین در پیاده‌سازی روش k- نزدیک‌ترین همسایه با استفاده از تابع IBK، تعداد همسایه‌های مختلف با مقادیر ۱، ۲، ۳، ۴، ۵ و ۶ اجرا و مشخص شد این الگوریتم با نزدیک‌ترین K همسایه برابر ۶، بهترین پاسخ با بیشترین دقت را ارائه می‌دهد. این مقدار برابر با ۷۹/۲۶۸۳٪ می‌باشد.

در پیاده‌سازی تابع SMO برای روش ماشین بردار پشتیبان با هسته‌های مختلف PolyKernel، PUK، RBFKernel و Normalized Poly Kernel نیز بهترین نتیجه در هسته PolyKernel و با مقدار ۸۳/۵۳۶۶٪ رخ می‌دهد. جدول ۱۱ نتایج حاصل از اجرای چهار روش هوشمند فوق در بهترین حالت را نشان می‌دهد.

جدول ۱۱. مقایسه نتایج حاصل از اجرای چهار روش هوشمند برای ارزیابی احتمال تهدید

ردیف	الگوریتم	میزان دقت در بهترین حالت (درصد)
۱	درخت تصمیم	۷۶/۲۱۹۵
۲	k- نزدیکترین همسایه	۷۹/۲۶۸۳
۳	شبکه‌های عصبی مصنوعی	۸۴/۷۵۶۱
۴	ماشین‌های بردار پشتیبان	۸۳/۵۳۶۶

همان‌طور که از جدول فوق مشخص است، بهترین نتیجه مربوط به روش شبکه‌های عصبی مصنوعی است. این روش توانسته است با دقت ۸۴/۷۵۶۱٪ ذهن خبره را مدل کند. این عدد در روش ماشین بردارهای پشتیبان ۸۳/۵۳۶۶٪، در روش k- نزدیک‌ترین همسایه ۷۹/۲۶۸۳٪ و در روش درخت تصمیم ۷۶/۲۱۹۵٪ می‌باشد.

۲.۵. تجزیه و تحلیل نتایج برای ارزیابی سطح آسیب‌پذیری

در این بخش داده‌های حاصل از پرسشنامه مربوط به ارزیابی سطح آسیب‌پذیری، پیاده‌سازی و مورد تجزیه و تحلیل قرار گرفته است. چهار پارامتر ورودی برای این ارزیابی عبارت‌اند از: «سهولت کشف آسیب‌پذیری»، «سهولت بهره‌برداری از آسیب‌پذیری»، «میزان آگاهی از آسیب‌پذیری» و «عدم کشف نفوذ توسط گروه تهدیدشونده». نتایج که نشان‌دهنده سطح آسیب‌پذیری می‌باشند، در سه کلاس «کم»، «متوسط» و «زیاد» دسته‌بندی شده‌اند. در ادامه، نتایج حاصل از چهار الگوریتم ذکر شده مورد تجزیه و تحلیل قرار می‌گیرند.

۱.۲.۵. تجزیه و تحلیل نتایج حاصل از پیاده‌سازی روش شبکه‌های عصبی مصنوعی

نتایج حاصل از نمونه‌های تست شده با تابع Multilayer Perceptron برای نرخ‌های یادگیری ۰/۱، ۰/۲، ۰/۳، ۰/۴ و ۰/۵ در جدول ۱۲ نشان داده شده است. همان‌طور که مشاهده می‌شود، این الگوریتم در نرخ یادگیری ۰/۲ بهترین پاسخ با بیشترین دقت را ارائه می‌دهد.

نتایج فوق نشان می‌دهد روش شبکه‌های عصبی مصنوعی در بهترین حالت توانسته است با دقت ۸۵/۹۷۵۶٪ ذهن خبره را مدل کند.

جدول ۱۲. نتایج حاصل از پیاده‌سازی روش شبکه‌های عصبی با نرخ یادگیری متفاوت برای ارزیابی سطح آسیب‌پذیری

ردیف	نرخ یادگیری	میزان دقت (درصد)
۱	۰/۱	۸۴/۷۵۶۱
۲	۰/۲	۸۵/۹۷۵۶
۳	۰/۳	۸۳/۵۳۶۶
۴	۰/۴	۸۳/۵۳۶۶
۵	۰/۵	۸۳/۵۳۶۶

۲.۲.۵. تجزیه و تحلیل نتایج حاصل از اجرای سه روش هوشمند دیگر

برای بررسی دقت نتایج حاصل از پیاده‌سازی روش شبکه های عصبی در ارزیابی سطح آسیب‌پذیری نیز، از همان سه روش هوشمند قبل با همان پارامترهای کلیدی استفاده شد.

در پیاده‌سازی روش درخت تصمیم با تابع J48، مشاهده شد که بهترین نتیجه در ضریب اطمینان ۰.۵ و با مقدار ۷۹/۸۷۸٪ رخ می‌دهد. همچنین در اجرای تابع IBK برای روش k- نزدیک‌ترین همسایه، مشخص شد این الگوریتم با نزدیک‌ترین k همسایه برابر ۴، بهترین پاسخ با بیشترین دقت را ارائه می‌دهد که این مقدار برابر با ۸۲.۳۱۷۱٪ می‌باشد.

در پیاده‌سازی روش ماشین بردارهای پشتیبان با تابع SMO نیز، بهترین نتیجه در هسته PolyKernel و با مقدار ۸۴/۷۵۶۱٪ رخ می‌دهد. جدول ۱۳ نتایج حاصل از اجرای چهار روش هوشمند فوق در بهترین حالت را نشان می‌دهد.

جدول ۱۳. مقایسه نتایج حاصل از اجرای چهار روش هوشمند برای ارزیابی سطح آسیب‌پذیری

ردیف	الگوریتم	میزان دقت در بهترین حالت (درصد)
۱	درخت تصمیم	۷۹/۸۷۸
۲	k- نزدیکترین همسایه	۸۲/۳۱۷۱
۳	شبکه‌های عصبی مصنوعی	۸۵/۹۷۵۶
۴	ماشین‌های بردار پشتیبان	۸۴/۷۵۶۱

همان‌طور که از این جدول مشخص است، بهترین نتیجه مربوط به روش شبکه‌های عصبی مصنوعی است. این روش توانسته است با دقت ۸۵/۹۷۵۶٪ ذهن خبره را مدل کند. این عدد در روش ماشین بردارهای پشتیبان ۸۴/۷۵۶۱٪، در روش k- نزدیک‌ترین همسایه ۸۲/۳۱۷۱٪ و در روش درخت تصمیم ۷۹/۸۷۸٪ می‌باشد.

۶. نتیجه‌گیری

تا کنون راهکارهای زیادی برای مقابله با معضل ارزیابی ریسک امنیت اطلاعات ارائه شده است. یکی از این راه‌کارها ارزیابی ریسک با استفاده از روش‌های هوشمند است. در این مقاله از روش شبکه‌های عصبی مصنوعی برای ارزیابی ریسک استفاده شد، با این راه‌کار جدید شاخص‌های واقعی‌تری برای عوامل مؤثر بر ریسک تعریف شدند که باعث دقیق‌تر شدن نتایج و نزدیکی آن به آنچه در واقعیت رخ می‌دهد می‌شود. هم چنین، بررسی منابع موجود [۱۲-۱۴] نشان می‌دهند که اجماع زیادی در میان متخصصین حوزه امنیت اطلاعات در خصوص این شاخص‌ها در سطح دنیا وجود دارد. داده‌های این پژوهش با استفاده از روش پرسشنامه‌ای که میان جامعه آماری متشکل از متخصصین حوزه ارزیابی ریسک امنیت اطلاعات توزیع شده بود به‌دست آمده است. بررسی‌های ما نشان داد که نتایج حاصل از شبکه‌های عصبی در مقایسه با سایر روش‌ها از دقت و کیفیت بالاتری برخوردار است. برای ارزیابی دقت نتایج حاصل از پیاده‌سازی این روش روی داده‌های موجود، سه روش هوشمند دیگر یعنی «درخت تصمیم»، «k- نزدیک‌ترین همسایه» و «ماشین بردارهای پشتیبان» نیز پیاده‌سازی و با آن مقایسه شد و مشاهده گردید که ادعای اولیه در مورد دقت بهتر این روش درست بوده است.

۷. مراجع

[1] Sendi. A. S, Jabbarifar. M , Shajari. M , and Dagenais. M, "FEMRA: Fuzzy Expert Model for Risk Assessment," Proc. Fifth International Conference on Internet Monitoring and Protection (ICIMP), 2010.

[2] Wangl. Z, Zeng. H, "Study on the Risk Assessment Quantitative Method of Information Security," Proc. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.

[3] Honghui. N, Yanling. S, "Research on risk assessment model of information security based on particle swarm algorithm -RBF neural network," Proc. Second Pacific-Asia Conference on Circuits, Communications and System (PACCS), 2010.

[4] Wei. G, Zhang. X, Zhang. X, Huang. Z, "Research on E-government information security risk assessment Based on Fuzzy AHP and Artificial Neural Network model," Proc. First International Conference on Networking and Distributed Computing, 2010.

[5] Zhao. D. M, Wang. J. H and Ma. J. F, "Fuzzy Risk Assessment of Network Security," Proc. Fifth International Conference on Machine Learning and Cybernetics, Dalian, China, 2006

[6] Guan. B. C, Lo. C. C. , Wang. P and Hwang. J. S, "Evaluation of information security related risk of an organization: the application of multi criteria decision making method," Proc. IEEE 37th Annual International Carnahan Conference, 2003.

[7] Haslum. K, Abraham. A and Knapskog. S, "Fuzzy Online Risk Assessment for Distributed Intrusion Prediction and Prevention Systems," Proc. Tenth International Conference on Computer Modeling and Simulation, Cambridge, USA, 2008.

[8] ISO/IEC, "ISO/IEC 27005:2008: Information technology - security techniques - information security risk management," International Organization for Standardization, Geneva, Switzerland, 2008.

[9] ISO/IEC, "ISO/IEC 27005:2011: Information technology - security techniques - information security risk management," International Organization for Standardization,Geneva, Switzerland, 2011.

[10] Mitchell. T, "Machine learning," NewYork, McGraw Hill, 1997.

[11] Bishop. C. M, "Pattern Recognition and Machine Learning," NewYork, Springer , 2006.

[12] Stoneburner. G, Goguen. A and Feringa. A, "Risk Management Guide for Information Technology Systems" NIST Special Publication 800-30, July, 2002.

[13] The Risk IT Framework, ISACA, [Online], (http://books.google.com), 2009 .

[14] OWASP, "Risk Rating Methodology" http://www.owasp .org, 2009.

[15] Clason. D. L and Dormody. T. J, "Analyzing data measured by individual Likert-type items" *Journal of Agricultural Education*, 35 (4), pp. 31-35, 1994.

[16] Mark. H, et. al., "The WEKA data mining software: an update," *ACM SIGKDD Explorations Newsletter*, vol. 11, no. 1, pp. 10-18, 2009.

[17] Braga-Neto. U. M and Dougherty. E. R, "Is cross-validation valid for small-sample microarray classification" *Oxford Journals, Bioinformatics* 20 (3), pp. 374-380, 2004.