هفتمین کنفرانس ملی مباحث نوین در کامپیوتر و فناوری اطلاعات
7th National Conference on Advanced Topics in Computer and Information Technology
۲ آذر ماه ۱۴۰۲

جلوگیری از نفوذ بدافزارها در سامانه‌های کنترل صنعتی

داریوش غنی‌زاده حصار

چکیده : سامانه‌های کنترل صنعتی از جمله سامانه‌های کنترل نظارت و جمع‌آوری داده، سامانه‌های کنترل توزیع شده، سامانه‌های کنترل فرایند، سامانه‌های فیزیکی سایبری یا کنترل کننده‌های منطقی قابل برنامه‌ریزی هستند که اغلب در بخش‌های صنعتی و زیرساخت‌های حیاتی یافت می‌شوند این سامانه‌ها اساساً سامانه‌های کنترلی بوده که در صنایعی مانند برق آب و فاضلاب نفت و گاز شیمیایی حمل‌ونقل داروسازی، خمیر و کاغذ، مواد غذایی و آشامیدنی استفاده و عملیات تأسیسات صنعتی را برای مدیریت فرایندهای صنعتی مانند تولید جابجایی و توزیع کنترل و مدیریت می‌کنند. در طی چندین سال اخیر حملات سایبری بی‌شماری به سیستم‌های کنترل صنعتی ثبت گردیده است هرچند برخی از آنها خسارات چندانی بر جای نگذاشته‌اند اما برخی از حملات تهدید جدی پیش روی این سیستم‌ها را بیش از پیش نمایان ساخته‌اند. لذا در این مقاله بر آن شدیم جهت جلوگیری از نفوذ بدافزارها در سامانه‌های کنترل صنعتی از الگوریتم شبکه عصبی مصنوعی استفاده کنیم. نتایج بدست آمده از پیاده‌سازی روش پیشنهادی حاکی از آن است که روش پیشنهادی با دقت ۹۵.۵ درصد از عملکرد خوب و قابل قبولی در تشخیص حملات سایبری و نفوذ در سامانه‌های کنترل صنعتی برخوردار می‌باشد.

کلمات کلیدی: بدافزار، نفوذ، سامانه‌های کنترل صنعتی، شبکه عصبی مصنوعی

۱ – سامانه‌های کنترل صنعتی

سیستم‌های کنترل صنعتی که به اختصار ICS[1] نامیده می‌شوند در واقع مجموعه‌ای مرکب از سخت افزارها، نرم افزارها، شبکه و اپراتورها می‌باشند که به صورت کاملا هماهنگ و موزن برای انجام تعداد کثیری از توابع با هدف اجرای فعالیت‌ها و وظایف پیچیده صنعتی طراحی و توسعه یافته‌اند. حیطه گسترده‌ای از کاربردهای سیستم‌های کنترل صنعتی را می‌توان در صنعت تصفیه آب صنعت نفت و گاز و نیروگاه‌ها مشاهده نمود[۱]. سیستم‌های کنترل صنعتی بخش مهم و جدایی ناپذیر از زیرساخت‌های صنعتی می‌باشند سال‌های متمادی است که از آنها برای نظارت بر عملکرد ماشین‌آلات و فرآیندهای صنعتی استفاده می‌شود؛ در واقع از این سامانه‌ها برای مانیتورینگ، تعامل و همچنین برقراری تراکنش‌های بلادرنگ با موجودیت‌های زیرساخت صنعتی با هدف جمع‌آوری و تجزیه و تحلیل بلادرنگ داده‌های تولید شده توسط هر یک از اجزای زیر ساخت و انجام واکنش مناسب به آنها استفاده می‌شود[۲]. سامانه سرپرستی و گرداوری داده که به اختصار آن را اسکادا می‌نامیم، در واقع گسترده‌ترین و بزرگترین زیر مجموعه از سیستم‌های کنترل صنعتی می‌باشد که یک رابط کاربری گرافیکی[2] مناسب را از طریق سیستم‌هایی با نام رابط کاربری انسانی (HMI[3]) برای مانیتورینگ، پایش و انجام فعالیت‌های اپراتوری فراهم می‌نماید .یک سامانه اسکادا شامل چهار زیر سیستم است که عبارتند از:

- کنترل و نظارت[4] بعنوان مرکز کنترل مسئولیت کنترل پایش و امنیت زیرساخت را برعهده دارد.
- شبکه کنترل[5] شامل کنترلرهای PLC ،است و به صورت مستقیم به تجهیزات سخت افزاری متصل می‌باشد.

[1] Industrial Control Systems
[2] Graphical User Interface (GUI)
[3] Human-Machine Interface (HMI)
[4] Supervisory Control
[5] I/O Network

- شبکه ورودی/خروجی[6] شامل سنسورها و محرک‌ها به عنوان اجزای عملیاتی زیرساخت می‌باشد.
- شبکه اینترانت و اینترنت شرکت[7] که شامل سرورها سیستم‌ها و دیگر تجهیزات سازمان با اهدافی شامل انتقال فایل وب سایت و ... می‌باشد.

۲- انواع سیستم‌های صنعتی

در شبکه‌های صنعتی ممکن است سیستم‌های کنترلی گوناگونی وجود داشته باشد. این سیستم‌ها عبارتند از اسکادا سیستم‌های کنترلی توزیع شده و PLC [۳و۴].

سیستم‌های اسکادا به منظور نظارت از راه دور به شبکه‌های میدانی که از لحاظ جغرافیایی ممکن است گسترده باشند مورد استفاده قرار می‌گیرند اسکادا شامل ترمینال کارفرما تجهیزات ارتباطی مانند خط تلفن، ماهواره و یک یا چند شبکه میدانی تحت کنترل است. روند کلی کارکرد اسکادا به این صورت است که ترمینال کارفرما به طور متناوب پیغام‌های درخواستی به کنترل کننده‌های شبکه میدانی می‌فرستد و آنها بوسیله پیغام‌های جواب وضعیت شبکه میدانی را به ترمینال کارفرما می‌فرستند. اطلاعات جمع‌آوری شده، در ترمینال کارفرما ذخیره و پردازش می‌شود این اطلاعات همچنین به صورت گرافیکی یا به صورت نوشتاری در HMI به نمایش در می‌آید. اپراتور می‌تواند برنامه‌های موجود در سیستم کنترلی اسکادا را طوری تنظیم کند که این روند به صورت خودکار انجام شود همچنین می‌تواند به صورت دستی تغییراتی در این روند ایجاد کند به عنوان مثال می‌تواند اضافه بر پیغام‌هایی که به صورت متناوب فرستاده می‌شود پیغام درخواست به صورت دستی بفرستد. همچنین اپراتور می‌تواند الگوریتمهای موجود در اسکادا و آستانه‌ها را تغییر دهد.

سیستم‌های کنترلی توزیع شده به منظور کنترل سیستم‌های تولید کننده‌ای است که از لحاظ جغرافیایی گسترده نیستند به عنوان مثال می‌توان به پالایشگاه‌های نفت و پتروشیمی‌ها اشاره کرد. در سیستم‌های کنترلی توزیع شده از یک حلقه کنترلی و نظارتی مرکزی استفاده می‌شود این حلقه نقش یک واسطه را بین گروهی از کنترل کننده‌ها که فرآیند تولید را انجام می‌دهند بازی می‌کند. سیستم کنترلی توزیع شده با قسمت‌بندی سیستم تولیدی تحت کنترل باعث می‌شود با خرابی یک قسمت کل سیستم تولیدی تحت تاثیر قرار نگیرد. تفاوت سیستم‌های کنترل کننده توزیع شده با اسکادا بستگی به فاصله جغرافیایی است که توسط پیوندهای ارتباطی[8] پوشش داده می‌شود. همان طور که بیان شد اسکادا در شبکه‌های صنعتی با توزیع جغرافیایی زیاد کاربرد دارد و سیستم‌های کنترلی توزیع شده به منظور کنترل شبکه‌های صنعتی که در یک منطقه جغرافیایی هستند به کار برده می‌شوند.

کنترل کننده PLC در انواع شبکه‌های کنترلی از جمله اسکادا و سیستم‌های کنترلی توزیع شده استفاده می‌شوند. PLC شامل یک حافظه است که قابلیت برنامه‌ریزی توسط کاربر را دارد این حافظه به منظور ذخیره‌سازی دستوراتی استفاده می‌شود که برای پیاده‌سازی کارهای مختلف از جمله کنترل ورودی و خروجی، منطق، زمان‌بندی و شمارش مورد استفاده قرار می‌گیرد. این کنترل کننده توسط ایستگاه کاری مهندسی[9] قابل برنامه‌ریزی است و توسط یک شبکه فیلدباس به اجزاء شبکه متصل است.

۳- امنیت سیستم‌های کنترل صنعتی

امروزه شبکه‌های کنترل صنعتی که وظیفه کنترل و نظارت بر زیرساخت‌های بنیادی را برعهده دارند به طور فرآیندهای به شبکه‌های همگانی متصل می‌شوند و در نتیجه ریسک حملات سایبری به شبکه‌های کنترلی و زیرساخت‌های مرتبط با آن افزایش می‌یابد. از آنجایی که پروتکل‌های موجود در شبکه‌های کنترلی از لحاظ امنیتی به خودی خود ضعیف هستند و ملاحظات امنیتی در آنها رعایت نشده است، ارزیابی امنیتی اینگونه از سیستم‌ها از جایگاه ویژه‌ای برخوردار می‌شود[۵و۶]. مشکلات امنیتی شبکه‌های کنترل صنعتی را می‌توان در چند دسته قرار داد:

۱) دسته اول آسیب‌پذیری‌های موجود در پروتکل‌های مورد استفاده در شبکه‌های صنعتی است. در پروتکل‌های صنعتی بیشتر به بلادرنگ بودن و کارایی بالا اهمیت داده شده است و تقریبا توجهی به امنیت پروتکل نشده است؛ به عنوان مثال در پروتکل مدباس[10] که یکی از پرکاربردترین پروتکل‌های صنعتی است پیام‌های درخواست و پاسخ به صورت آشکار در شبکه رد و بدل می‌شوند و هیچگونه رمزنگاری یا احراز اصالت در این پروتکل در نظر گرفته نشده است.

[6] Control Network
[7] Corporate Network
[8] Communication Link
[9] Engineering Workstation
[10] Modbus

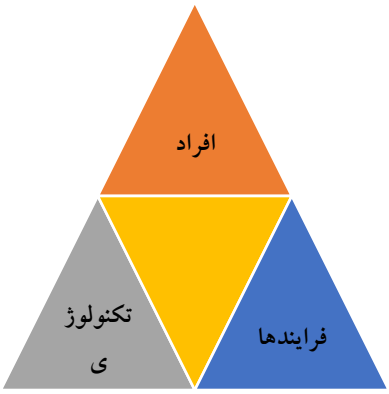
۲) دسته دوم آسیب‌پذیری‌های موجود در پیاده‌سازی‌های مختلف پروتکل‌های صنعتی است. پروتکل‌های صنعتی ممکن است طوری پیاده‌سازی شوند که باعث به وجود آمدن مشکلات امنیتی، نظیر سرریز بافر[11] شود.

۳) دسته سوم آسیب‌پذیری‌های مربوط به دستگاه‌های مورد استفاده در شبکه‌های صنعتی است. به عنوان مثال PLCهای موجود در شبکه صنعتی که نقش اساسی در اجرای فرآیندهای در حال اجرا دارند می‌توانند مورد سوء استفاده قرار بگیرند یا توسط افرادی که متخصص نیستند برنامه‌ریزی شوند و ایجاد مشکل نمایند. برای مثال حمله کننده می‌تواند با استفاده از پورت‌های باز در یک PLC به آن متصل شود و با کد خود آن را مجددا برنامه‌ریزی کند کاری که شبیه به آن در استاکسنت[12] انجام شد.

۴) دسته چهارم آسیب‌پذیری‌های مربوط به رسانه‌های ارتباطی در شبکه‌های صنعتی است. به عنوان مثال رسانه‌های بیسیم به راحتی می‌توانند شنود[13] شوند همچنین شبکه‌های اسکادایی که از طریق WAN[14] یا شبکه‌های بر پایه IP[15] با شبکه میدانی ارتباط برقرار می‌کنند می‌توانند مورد حملات سایبری قرار گیرند.

۴- جنبه‌های مختلف در امنیت اطلاعات

امنیت اطلاعات درای سه جنبه است که عبارتند از[۷]:



شکل ۲: جنبه‌های مختلف در امنیت اطلاعات

امروزه از تکنولوژی‌های متعددی به منظور ارائه سرویس‌های لازم در رابطه با ایمن‌سازی اطلاعات و تشخیص مزاحمین اطلاعاتی استفاده می‌گردد. سازمان‌ها و مؤسسات می‌بایست سیاست‌ها و فرایندهای لازم به منظور استفاده از یک تکنولوژی را مشخص کنند تا زمینه انتخاب و به کارگیری درست تکنولوژی در سازمان مربوطه فراهم گردد. در این رابطه می‌بایست به مواردی همچون سیاست امنیتی، اصول ایمن‌سازی اطلاعات، استانداردها و معماری ایمن‌سازی اطلاعات، استفاده از محصولات مربوط به ارائه دهندگان شناخته شده و خوشنام، راهنمای پیکربندی، پردازش‌های لازم برای ارزیابی ریسک سیستم‌های مجتمع و بهم مرتبط، توجه گردد. فرایندها منظور از عملیات مجموعه فعالیت‌های لازم به منظور نگهداری وضعیت امنیتی یک سازمان است. در این رابطه لازم است به موارد زیر توجه شود[۸] :

- ✓ پشتیبانی ملموس و به هنگام‌سازی سیاست‌های امنیتی
- ✓ اعمال تغییرات لازم با توجه به روند تحولات مرتبط با تکنولوژی اطلاعات
- ✓ مدیریت وضعیت امنیتی با توجه به تکنولوژی‌های استفاده شده در رابطه با ایمن‌سازی اطلاعات
- ✓ ارائه سرویس‌های مدیریتی اساسی و حفاظت از زیرساخت‌های مهم
- ✓ ارزیابی سیستم امنیتی
- ✓ هماهنگی و واکنش در مقابل حملات جاری
- ✓ تشخیص حملات و ارائه هشدار و پاسخ مناسب به منظور ایزوله نمودن حملات و پیشگیری از موارد مشابه
- ✓ بازیافت و برگرداندن امور به حالت اولیه

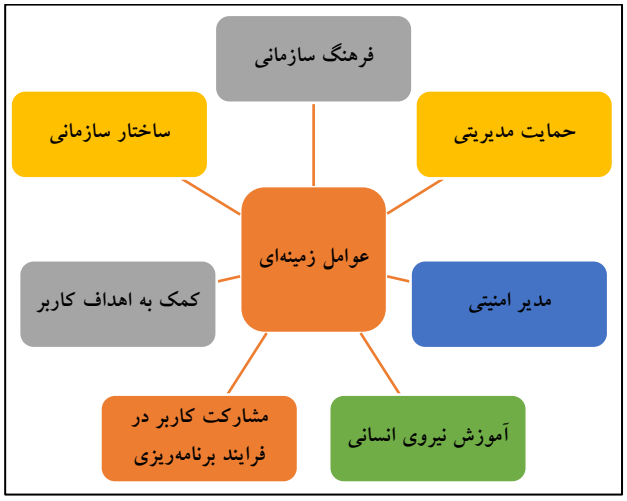
موفقیت در ایمن‌سازی اطلاعات با پذیرش مسئولیت و حمایت مدیریت مالی یک سازمان و براساس شناخت مناسب از تهاجمات حاصل می‌شود، نیل به موفقیت با پیگیری سیاست‌ها و روتین‌های مربوطه و تعیین وظایف و مسئولیت‌های آموزش منابع انسانی حساس و همچنین توجیه مسئولیت‌های شخصی کارکنان حاصل می‌گردد که در این راستا لازم است یک سیستم امنیتی فیزیکی و شخصی به منظور کنترل و هماهنگی در دستیابی به هر یک از عناصر حیاتی در محیط‌های مبتنی بر تکنولوژی اطلاعات نیز ایجاد گردد. ایمن‌سازی اطلاعات از جمله مواردی است که می‌بایست موفقیت خود را در عمل و نه در حرف نشان دهد بنابراین لازم

[11] Buffer Overflow
[12] Stuxnet
[13] Sniff
[14] Wide Area Network
[15] Internet Protocol

است که پس از تدوین سیاست‌ها و دستورالعمل‌های مربوطه پیگیری مستمر و هدفمند جهت اجرای سیاست‌ها و دستورالعمل‌ها دنبال گردد.

۵– نقش عوامل انسانی در امنیت اطلاعات

برخلاف دید غالب در مورد آسیب‌های اطلاعاتی مبنی بر کامپیوتر امنیت اطلاعات فقط اتخاذ روش‌های قوی رمزنگاری و کلمه رمز عبور قوی نیست؛ این موارد تنها بعد فنی امنیت اطلاعات است حتی در صورتی که شما حداکثر کنترل‌های فنی را در سازمان خود پیاده‌سازی کرده باشید ممکن است به دلیل عدم توجه به مسائل غیر فنی به نتایج دلخواه نرسد لذا امنیت فقط در بعد فنی آن خلاصه نمی‌شود و نیاز به روال‌های اداری و تشکیلات سازمانی و مدیریتی دارد. امنیت یک فرآیند مستمر است و برقراری امنیت در یک برهه زمان به معنای امنیت برای همیشه نیست لازم به ذکر است که در حال حاضر وضعیت امنیت فضای تبادل اطلاعات کشور به ویژه در حوزه سازمان‌های دولتی در سطح نامطلوبی قرار دارد؛ از جمله دلایل اصلی وضعیت موجود می‌توان به فقدان زیرساخت‌های فنی و اجرایی امنیت و عدم انجام اقدامات موثر در خصوص ایمن‌سازی فضای تبادل اطلاعات سازمان‌های دولتی، نبود سیستم‌های مدیریت امنیت اطلاعات، فقدان سیاست‌ها و استراتژی‌های امنیتی و عدم توجه به عوامل انسانی همچون عدم حمایت مدیریتی و بی توجهی به آموزش و ارتقاء سطح آگاهی‌های کاربران از امنیت اطلاعات اشاره نمود. در شکل زیر عوامل غیر فنی تأثیرگذار بر به کارگیری امنیت اطلاعات قابل مشاهده است که بیشتر مربوط به عوامل انسانی و مدیریتی است. ابزارها و ساز و کارهای امنیتی اثربخشی محدودی دارند زیرا امنیت در وهله اول مسئله‌ای انسانی و به همان میزان مسئله‌ای سازمانی و یا مدیریتی است، تحت این دیدگاه اهمیت مدیریت امنیت سیستم‌های اطلاعاتی به زمینه سازمانی بر می‌گردد که در آنجا وجود دارد که این امر لزوم توجه به منشا تهدیدات سازمانی و شناسایی ویژگی‌های داخلی و خارجی سازمان را برجسته می‌سازد. نقل قول معروفی این روزها وجود دارد که ۸۰ درصد یا حداقل بخش عظیمی از ریسک‌های سیستم‌های اطلاعاتی از داخل سازمان می‌باشد که این نقل قول راه‌کار پیشنهادی به همراه ندارد و همچنین عنوان نمی‌کند که باید بیشتر یا کمتر به تهدیدات بیرونی بپردازیم. معمولا تهدیدات بیرونی جدی‌تر می‌باشند و می‌توانند منجر به خرابی سیستم‌های اطلاعاتی شرکت یا سرقت اطلاعات محرمانه و غیره شوند هر چند انگیزه این افراد به طور کلی کمتر است و قوانین بازدارنده‌ای وجود دارد ولی تنوع و تعداد زیاد آنها موجب تهدیدات زیادی می‌شود. ویژگی مشترک آنها این است که شانس کمتری برای موفقیت در حملات دارند چون تنها از رخنه‌ها و نقاط ضعف سیستم‌های حفاظتی می‌توانند شانس کمتری برای موفقیت در حمله داشته باشند اما تهدیدات داخلی از دسترسی مجاز بهره‌مند است و موجب آسیب زدن راحت‌تر در مقیاس با تهدیدات خارجی می‌شود همچنین عموم دفاع سازمان در برابر آن ناکافی است و نوع دسترسی که موجبات تخریب را فراهم می‌آورند برای انجام وظایف آنها ضروری است البته نباید فراموش کرد که اکثر کارمندان به سازمان وفادارند و نباید با دید منفی به آنها نگریست [۹و۱۰].



شکل ۲-۲: فاکتور غیر فنی مؤثر بر امنیت سیستم‌های اطلاعاتی

۶ – آگاهی از امنیت اطلاعات

یکی از جنبه‌ها و راه‌های مهم برای حفاظت و مدیریت امنیت اطلاعات ارتقاء آگاهی کاربران از امنیت اطلاعات است در این صورت افراد آگاهی‌های لازم و مربوط به نقش و مسئولیت خویش در حفظ امنیت اطلاعات در کار مربوط به خود را کسب می‌کنند. آگاهی از امنیت اطلاعات در افراد منجر به ایجاد تغییر رفتار و تقویت فعالیت‌های خوب امنیتی می‌شود و به افراد اجازه می‌دهد تا نسبت به امنیت فناوری اطلاعات نگران و پاسخگو باشند و به تدریج به فرهنگ سازمان‌ها تبدیل خواهد شد لذا بایستی به موازات تمهیدات فنی اعمال شده جهت امنیت اطلاعات، در قوانین و سیاست‌های جاری نیز متناسب با جایگاه نوین فضای تبادل اطلاعات در امور مدیریتی و اطلاع‌رسانی تجدید نظر شود و آموزش‌های صحیح به کارگیری اطلاعات و تأمین امنیت آنها با اولویت بالاتری در سطح جامعه ترویج شود. آگاهی از امنیت اطلاعات طبق نظر

پارک و همکاران شامل سه بعد زیر است [۱۱] :

الف) آگاهی عمومی از امنیت اطلاعات به معنای آگاهی‌رسانی عمومی در زمینهٔ ابعاد امنیت از جمله اهداف یک سیستم مدیریت امنیت اطلاعات است که با هدف افزایش آگاهی عمومی کاربران و جامعهٔ مخاطبان سیستم‌های مدیریت امنیت اطلاعات صورت می‌گیرد.

ب) آگاهی از قوانین امنیت اطلاعات که یک مفهوم ساختاری جدید است که به آگاهی، درک و رعایت کارکنان از سیاست‌ها، قوانین و اطلاعات امنیتی سازمان مرتبط اشاره و بیان می‌کند که آگاهی کارکنان از سیاست امنیت اطلاعات سازمان تأثیر مثبتی بر نگرش کارکنان برای موافقت با سیاست‌های امنیتی شرکت دارد.

ج) آگاهی از شدت مجازات نقض امنیت اطلاعات به دانش و درک درست کارکنان از انواع مجازات و شدت مجازات‌های مرتبط با نقض امنیت اطلاعات سازمان اطلاق می‌شود.

۷–نفوذ در سامانه‌های کنترل صنعتی

به فرآیند پردازش رخدادهای اتفاق افتاده در یک سیستم یا در شبکه و آنالیز آنها به منظور پیدا کردن یک حادثه[۱۶] که این حادثه می‌تواند یک نقض قانون در شبکه یا سیستم باشد تشخیص نفوذ گفته می‌شود. حادثه‌هایی که اتفاق می‌افتد می‌توانند علل مختلفی از جمله یک بدافزار[۱۷] یا دسترسی غیرقانونی یک حمله کننده به سیستم داشته باشد. سیستم تشخیص نفوذ به نرم افزاری گفته می‌شود که فرآیند تشخیص نفوذ را به صورت خودکار انجام می‌دهد. این نرم افزارها با جمع‌آوری اطلاعات از منابع مختلف شبکه یا سیستم سعی در پیدا کردن مشکلات امنیتی موجود می‌کنند. به طور خلاصه سیستم تشخیص نفوذ کارهای زیر را به منظور پیدا کردن مشکلات امنیتی انجام می‌دهد[۱۲و۱۳]:

- نظارت و بررسی فعالیت‌های کاربر و سیستم
- رسیدگی کردن[۱۸] به تنظیمات سیستم و آسیب پذیری‌ها
- سنجش تمامیت[۱۹] سیستم و فایل‌های داده
- بررسی‌های آماری در الگوهای[۲۰] فعالیت بر اساس حمله‌های شناخته شده
- بررسی رفتار و فعالیت ناهنجار

با توسعه فناوری‌های اطلاعات و ارتباطات و افزایش دسترسی به اینترنت، سازمان‌ها در برابر انواع مختلف تهدیدات آسیب‌پذیر می‌شوند. در واقع دارایی‌های اطلاعات آنها در معرض حملات سایبری قرار می‌گیرد و خسارات ناشی از آنها همانطور که پیشتر بیان شد می‌تواند در ابعاد گسترده‌ای مانند از مدار خارج شدن تولید یک کارخانه تا تحولات سیاسی را شامل شود. آنچه که می‌توان به عنوان یک دید از بالا و موشکافانه به حملات داشت این است که یک اتفاق و رویداد ناگوار امنیتی حاصل در کنار هم قرار گرفتن سه عامل آسیب‌پذیری، تهدید و حمله می‌باشد. حملات در سیستم‌های کنترل صنعتی بسیار متنوع است و تحت تأثیر عوامل زیادی از جمله هدف مهاجم، توانایی‌های مهاجم، پیچیدگی فنون حمله و آشنایی وی با سیستم‌های کنترل صنعتی و فرآیندهای صنعتی قرار می‌گیرد. باید توجه داشت حمله به سامانه‌های کنترل صنعتی به سادگی نفوذ به یک شبکه ساده نیست بلکه برای رسیدن به یک حمله دقیق بایستی یک سری فعالیت و گام‌های مشخص انجام شود.

۸- شبکه عصبی مصنوعی

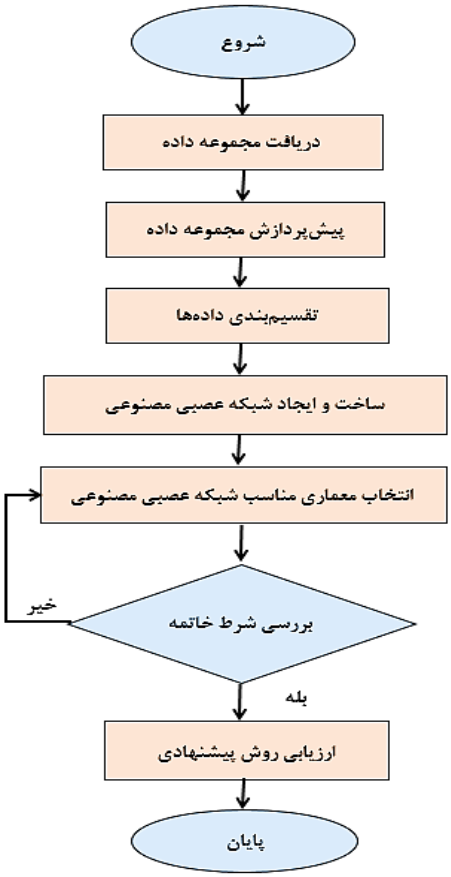
شبکه‌های عصبی مصنوعی[۲۱] یا به زبان ساده‌تر شبکه‌های عصبی سیستم‌ها، روش‌های محاسباتی نوینی هستند برای یادگیری ماشینی، نمایش دانش و در انتها اعمال دانش به دست آمده در جهت پیش‌بینی پاسخ‌های خروجی از سامانه‌های پیچیده ایده اصلی اینگونه شبکه‌ها (تا حدودی) الهام گرفته از شیوه کارکرد سیستم عصبی زیستی برای پردازش داده‌ها و اطلاعات به منظور یادگیری و ایجاد دانش قرار دارد. عنصر کلیدی این ایده ایجاد ساختارهایی جدید برای سامانه پردازش اطلاعات است. این سیستم از شمار زیادی عناصر پردازشی فوق العاده بهم پیوسته با نام نورون تشکیل شده که برای حل یک مسأله باهم هماهنگ عمل می‌کند. با استفاده از دانش برنامه نویسی رایانه می‌توان ساختار داده‌ای طراحی کرد که همانند یک نورون عمل نماید سپس با ایجاد شبکه‌ای از این نورون‌های مصنوعی بهم پیوسته ایجاد یک الگوریتم آموزشی برای شبکه کرده و با اعمال این الگوریتم به شبکه آن را آموزش داد[۱۴].

---

[16] Incident
[17] Malware
[18] Auditing
[19] lategrity
[20] Pattem
[21] Artificial Neural Networks

۹- چارچوب روش پیشنهادی

در این مقاله تلاش نمودیم تا با ارائه راهکاری موثر و مفید با استفاده از الگوریتم شبکه عصبی مصنوعی به تشخیص حملات سایبری و نفوذ در سامانه‌های کنترل صنعتی بپردازیم. شبکه عصبی پیشنهادی در این تحقیق از نوع پیش‌خور است. فلوچارت روش پیشنهادی در شکل (۱) نشان داده شده است.



شکل ۱: فلوچارت روش پیشنهادی

همانطور که مشاهده می‌شود در ابتدا به جمع‌آوری مجموعه داده مورد نظر پرداخته شد. بدین منظور داده‌های مورد نظر از سایت Kaggle[۲۲] گردآوری گردید. مجموعه داده دریافت شده شامل ۱۰۰۰۰۰ رکورد یا فایل می‌باشد که هر فایل دارای ۳۲ ویژگی است. در این مجموعه داده[۲۳] ۳۱ ویژگی به عنوان ویژگی‌های اصلی بوده و یک ویژگی آن به عنوان برچسب[۲۴] و تعیین کننده نوع فایل از جهت سالم و یا آلوده بودن به بدافزار می‌باشد. سپس داده‌ها را مورد نرمالسازی قرار دادیم در واقع نرمال‌سازی روشی است که داده‌ها در زمانی که در یک دامنه قرار ندارند را در دامنه مشابه قرار می‌دهد. برای این منظور با استفاده از روش نرمالسازی Max-Min داده‌های موجود در مجموعه داده را در بازه بین صفر و یک نرمالسازی کردیم که در رابطه ۱ نشان داده شده است.

$$\acute{V} = \frac{V - min(V)}{max(V) - min(V)} \qquad (۱)$$

که در این رابطه V مقدار اصلی ویژگی مربوط به رکورد یا فایلی که قرار است نرمال شود می‌باشد، $\acute{V}$ مقدار نرمال‌سازی شده ویژگی مربوط به رکورد مورد نظر است، $\max(V)$ حد بالای ویژگی و $\min(V)$ حد پایین مقدار ویژگی در بین کل رکوردهای مجموعه داده می‌باشد.

در ادامه با استفاده از روش هولداوت داده‌ها به دو مجموعه داده آموزشی و آزمایشی با نسبت ۷۰ به ۳۰ درصد تقسیم شدند. پس از تقسیم‌بندی داده‌ها به ایجاد و ساخت الگوریتم مورد استفاده پرداختیم و در ادامه به آموزش و ارزیابی طبقه‌بند موردنظر به تعداد ۱۰۰۰ مرتبه پرداخته پرداخته شد.

نحوه پردازش داده‌ها در شبکه عصبی مصنوعی به این صورت است که ابتدا هرکدام از ویژگی‌های انتخاب شده به عنوان یک ورودی در نظر گرفته شده و به هر ورودی یا نورون در لایه ورودی یک وزن دلخواه در بازه صفر و یک بصورت تصادفی تعلق می‌گیرد سپس این وزن‌ها در مقدار ورودی ضرب شده و مجموع این مقادیر به نرون‌های واقع در لایه پنهان رسیده و با یک مقدار به نام بایاس که در واقع وزن نورون بوده و معمولاً مقدار آن برابر یک است جمع می‌شود. به این مقدار مجدداً وزنی اختصاص یافته و به نورون بعدی در لایه پنهان بعدی یا لایه خروجی منتقل می‌شود و به این ترتیب مقادیر بدست آمده از همه نورون‌های لایه پنهان جمع می‌شوند و یک دوره آموزشی شبکه کامل می‌شود.

بنابراین با پایان یافتن یک دوره آموزش شبکه عصبی، پاسخ بدست آمده در لایه خروجی با پاسخ واقعی اندازه‌گیری و مورد مقایسه قرار گرفته می‌شود و از اختلاف آنها میانگین مربعات خطا (mse) مطابق با رابطه ۷ محاسبه می‌شود.

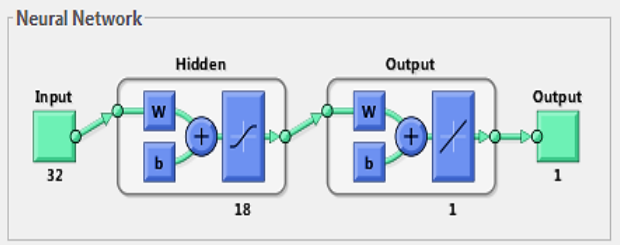
$$mse = \frac{1}{n}(\sum_{i=1}^{n} O_i - T_i) \qquad (۷)$$

که T_i و O_i به ترتیب مقدار تخمین زده شده و مقدار واقعی اندازه‌گیری شده است و N نیز تعداد داده‌های موجود می‌باشد.

این فرآیند تا زمانی که شرط خاتمه آموزش شبکه یعنی تعداد دوره‌های تعریف شده برای آموزش شبکه به پایان نرسد ادامه خواهد داشت، به

[22] www.kaggle.com/nsaravana/malware-detection
[23] Dataset
[24] Label

این ترتیب شبکه آموزش یافته و با تعداد دیگری از داده‌ها که خروجی آنها به شبکه داده نشده یعنی داده‌های آزمایشی مورد ارزیابی قرار گرفته و با مقایسه نتایج بدست آمده از شبکه عصبی و نتایج واقعی اندازه‌گیری شده، عملکرد شبکه عصبی طراحی شده جهت تشخیص حملات سایبری و نفوذ در سامانه‌های کنترل صنعتی مورد سنجش قرار می‌گیرد.



شکل ۴: معماری شبکه عصبی مصنوعی

۱۰- معیارهای ارزیابی روش پیشنهادی

از جمله معیارهایی که با توجه به ماتریس آشفتگی جهت سنجش و ارزیابی کارایی روش پیشنهادی در این مقاله می‌توان استفاده نمود معیارهای دقت، حساسیت و ویژگی می‌باشند. لازم به ذکر است که در معیارهای مذکور، مفاهیم TP تعداد درستی‌های مثبت، TN تعداد درستی‌های منفی، FP تعداد خطاهای مثبت و FN تعداد خطاهای منفی در تشخیص حملات سایبری و نفوذ در سامانه‌های کنترل صنعتی می‌باشند. طبق روابط ۳ تا ۵ استفاده می‌شود:

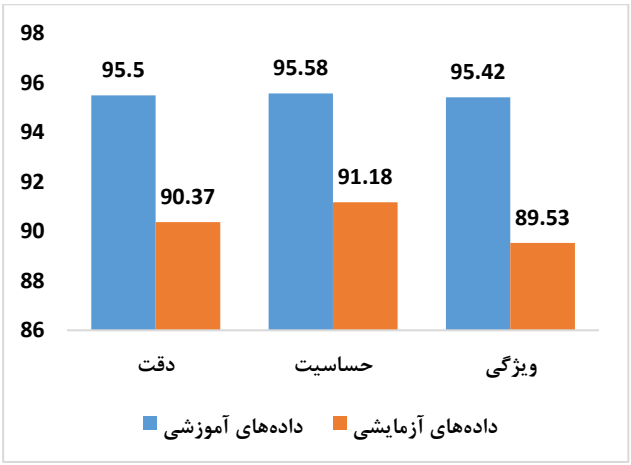
$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (۳)$$

$$Sensitivity = \frac{TP}{TP+FN} \times 100 \quad (۴)$$

$$Specificity = \frac{TN}{FP+TN} \times 100 \quad (۵)$$

۱۱- نتایج بدست آمده

باتوجه به معیارهای مورد بررسی جهت تشخیص حملات سایبری و نفوذ در سامانه‌های کنترل صنعتی، نتایج بدست آمده از پیاده‌سازی روش پیشنهادی و معیارهای ارزیابی برای داده‌های آموزشی و آزمایشی براساس درصد در شکل ۲ مشاهده می‌شود.



شکل ۲: نتایج بدست آمده

با توجه به نتایج بدست آمده از پیاده‌سازی روش پیشنهادی که در شکل ۲ نشان داده شده است مشاهده می‌کنیم از عملکرد خوب و قابل قبولی در تشخیص حملات سایبری و نفوذ در سامانه‌های کنترل صنعتی برخوردار می‌باشد.

۱۲- نتیجه‌گیری

امروزه شبکه‌های کنترل صنعتی که وظیفه کنترل و نظارت بر زیرساخت‌های بنیادی را برعهده دارند به طور فرآیندهای به شبکه‌های همگانی متصل می‌شوند و در نتیجه ریسک حملات سایبری به شبکه‌های کنترلی و زیرساخت‌های مرتبط با آن افزایش می‌یابد. از آنجایی که پروتکل‌های موجود در شبکه‌های کنترلی از لحاظ امنیتی به خودی خود ضعیف هستند و ملاحظات امنیتی در آنها رعایت نشده است، ارزیابی امنیتی اینگونه از سیستم‌ها از جایگاه ویژه‌ای برخوردار می‌شود. در طی چندین سال اخیر حملات سایبری بی‌شماری به سیستم‌های کنترل صنعتی ثبت گردیده است هرچند برخی از آنها خسارات چندانی بر جای نگذاشته‌اند اما برخی از حملات تهدید جدی پیش روی سیستم‌های کنترل صنعتی را بیش از پیش نمایان ساخته‌اند. لذا در این مقاله بر آن شدیم جهت جلوگیری از نفوذ بدافزارها در سامانه‌های کنترل صنعتی از الگوریتم شبکه عصبی مصنوعی استفاده کنیم. نتایج بدست آمده از پیاده‌سازی روش پیشنهادی حاکی از آن است که روش پیشنهادی با دقت ۹۵.۵ درصد از عملکرد خوب و قابل قبولی در تشخیص حملات سایبری و نفوذ در سامانه‌های کنترل صنعتی برخوردار می‌باشد.

مراجع

[1] Soliman, S., Oudah, W., & Aljuhani, A. (2023). Deep learning-based intrusion detection approach for securing industrial Internet of Things. *Alexandria Engineering Journal*, *81*, 371-383.

[2] Imran, M., Siddiqui, H. U. R., Raza, A., Raza, M. A., Rustam, F., & Ashraf, I. (2023). A performance overview of machine learning-based defense strategies for advanced persistent threats in industrial control systems. *Computers & Security*, *134*, 103445.

[3] Alzahrani, L., & Seth, K. P. (2021). The Impact of Organizational Practices on the Information Security Management Performance. *Information*, *12*(10), 398.

[4] Ali, R. F., Dominic, P. D. D., & Ali, K. (2020). Organizational governance, social bonds and information security policy compliance: A perspective towards oil and gas employees. *Sustainability*, *12*(20), 8576.

[5] Dhillon, G., Abdul Talib, Y. Y., & Picoto, W. N. (2020). The mediating role of psychological empowerment in information security compliance intentions. *Journal of the Association for Information Systems*, *21*(1), 5.

[6] Anthi, E., Williams, L., Burnap, P., & Jones, K. (2021). A three-tiered intrusion detection system for industrial control systems. *Journal of Cybersecurity*, *7*(1), tyab006.

[7] Dehlaghi-Ghadim, A., Moghadam, M. H., Balador, A., & Hansson, H. (2023). Anomaly detection dataset for industrial control systems. *IEEE Access*, *11*, 107982-107996.

[8] Alohali, M. A., Al-Wesabi, F. N., Hilal, A. M., Goel, S., Gupta, D., & Khanna, A. (2022). Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment. *Cognitive Neurodynamics*, *16*(5), 1045-1057.

[9] Hong, Y., & Furnell, S. (2022). Motivating information security policy compliance: Insights from perceived organizational formalization. *Journal of Computer Information Systems*, *62*(1), 19-28.

[10] Roy, S., Li, J., Choi, B. J., & Bai, Y. (2022). A lightweight supervised intrusion detection mechanism for IoT networks. Future Generation Computer Systems, 127, 276-285

[11] dos Santos Vieira, P., DIAS, M. D. O., Pereira, L. J. D., & da Silv, G. D. B. P. (2022). Brazilian Organizational Culture on Information Security: A Literature Review. *GPH-International Journal of Business Management (IJBM)*, *5*(01), 56-67.

[12] Syfert, M., Ordys, A., Kościelny, J. M., Wnuk, P., Możaryn, J., & Kukiełka, K. (2022). Integrated approach to diagnostics of failures and cyber-attacks in industrial control systems. *Energies*, *15*(17), 6212.

[13] Kumah, P. (2022). The role of human resource management in enhancing organizational information systems security. In *Research Anthology on Human Resource Practices for the Modern Workforce* (pp. 1251-1277). IGI Global.

[14] Kumar, R., Aggarwal, R. K., & Sharma, J. D. (2013). "Energy Analysis of a Building Using Artificial Neural Network: A Review". Energy And Buildings, 65, pp.352-358.