عنوان سمینار: مروری بر روش های پیش بینی حملات سایبری

استاد راهنما : سرکار خانم مطهره دهقان

دانشجو : مهدی شاکرمی

شماره دانشجویی : ۴۰۱۶۶۲۲۱۰۰۳

سال تحصیلی :۱۴۰۲-۱۴۰۱

فصل اول :

فصل دوم :

بررسی روش های پیش بینی در امنیت سایبری بر اساس سیستم های تشخیص نفوذ :

فصل سوم :

پیش بینی حمله امنیت سایبری: رویکرد یادگیری عمیق

فصل چهارم : رسی رویکردهای امنیت سایبری برای تشخیص حمله :

فصل پنجم :

چکیده:

امنیت سایبری حفاظت از سیستم های متصل به اینترنت از قبیل سخت افزار، نرم افزار و داده ها از تهدیدات سایبری است. این روش توسط افراد و شرکت ها برای حفاظت در برابر دسترسی غیر مجاز به مراکز داده ها و دیگر سیستم های کامپیوتری استفاده می شود. یک استراتژی امنیت سایبری قوی می تواند وضعیت امنیتی خوبی را در مقابل حملات خرابکارانه که برای دسترسی، تغییر، حذف، تخریب یا گرفتن سیستم های کاربر یا سازمان و داده های حساس طراحی شده اند، فراهم کند،امنیت سایبری همچنین در جلوگیری از حملاتی که هدفشان از کار انداختن یا اخلال در عملیات های دستگاه یا سیستم است، مفید است.بنابر این امنیت همیشه یکی از بحث های مهم فضای سایبری بوده و در طول زمان و با پیشرفت تکنولوژی، توجهات بیشتری را به خود جلب کرده است.فلذا امنیت سایبری، ریشه ی اصلی تکنولوژی ها، فرآیندها و شیوه های طراحی شده برای محافظت از شبکه ها، کامپیوترها، برنامه ها و داده ها در مقابل حملات، خسارات و دسترسی های غیر مجاز است.

بیان مساله :

یکی از مسائل مهم با توجه به استفاده گسترده از شبکه های کامپیوتری، حملات سایبری و بحث امنیت در این شبکه ها و پایگاه داده ها است. نفوذ به شبکه های کامپیوتری با انگیزه های مختلف از جمله سیاسی، نظامی، مالی و یا نشان دادن سستی و ضعف امنیتی در برنامه های موجود میباشد. از اینرو، تکنیکهای متداول با توجه به ویژگی های مخرب جدید که به طور تصاعدی درحال افزایش میباشد بی اثر شده و روشهای سنتی قادر به حفظ امنیت نمیباشد. حملات امنیت سایبری به طور تصاعدی در حال افزایش است و مکانیسم های شناسایی موجود را ناکافی می سازد و نیاز به طراحی مدل ها ورویکردهای پیش بینی مرتبط تر را افزایش می دهد، امنیت سایبری حفاظت از سیستم های متصل به اینترنت از قبیل سخت افزار، نرم افزار و داده ها از تهدیدات سایبری است. این روش توسط افراد و شرکت ها برای حفاظت در برابر دسترسی غیر مجاز به مراکز داده ها و دیگر سیستم های کامپیوتری استفاده می شود. یک استراتژی امنیت سایبری قوی می تواند وضعیت امنیتی خوبی را در مقابل حملات خرابکارانه که برای دسترسی، تغییر، حذف، تخریب یا گرفتن سیستم های کاربر یا سازمان و داده های حساس طراحی شده اند، فراهم کند،امنیت سایبری همچنین در جلوگیری از حملاتی که هدفشان از کار انداختن یا اخالل در عملیات های دستگاه یا سیستم است، مفید است.بنابر این امنیت همیشه یکی از بحث های مهم فضای سایبری بوده و در طول زمان و با پیشرفت تکنولوژی، توجهات بیشتری را به خود جلب کرده است.فلذا امنیت سایبری، ریشه ی اصلی تکنولوژی ها، فرآیندها و شیوه های طراحی شده برای محافظت از شبکه ها، کامپیوترها، برنامه ها و داده ها در مقابل حملات، خسارات و دسترسی های غیر مجاز است. و امنیت شامل دو بخش امنیت سایبری و امنیت فیزیکی می شود.

هدف از تحقیق :

امروزه به خاطر اینکه افزایش دسترسی افراد به سیستم ها و سازمانها بیشتر شده و همه چی داره روی اینترنت می روه و هر کس از هرکجای دنیا میتونه به اونها دسترسی داشته باشه (تلویزیون ، گوشی موبایل ،کامپیوترها و ...) یا حتی بحث های IOT باعث شده که این اتفاق شدت و سرعت بیشتری بگیره یعنی تمامی Device هایی که هست قابلیت اتصال به سرویس های ابری را دارند و این باعث شده که افزایش دسترسی و از طرف دیگر استفاده از ابزارهایی که امنیت را به خطر می اندازند حملات زیادی در سالهای اخیر صورت بگیرد ، البته که این حملات می تواند دلایل مختلفی همچون

۱ - اهداف سیاسی(تغیر دولت ها)

۲ – اهداف اقتصادی(ضربه زدن به رقبا ، کسب اطلاعات رقبا)

۳ – اهداف شخصی(انتقام جویی)

داشته باشند ، لذا این اتفاقات باعث شدن تا ما به امنیت بیشتری نیاز داشته باشیم.

امنیت سایبری یک مساله بسیار مهم است،زیرا به حفاظت دارایی های اطلاعاتی سازمان از حملات دیجیتال کمک می کند.اطلاعاتی که اگر دیگران به آنها دست پیدا کنند،به سازمان یا افراد آسیب می رسد. امروزه اطلاعات پزشکی،دولتی،شغلی و سوابق مالی همه افراد نگهداری می شود.حملات سایبری ممکن است منجر به سرقت اطلاعات، حذف اطلاعات، کلاهبرداری و لطمه خوردن به اعتبار افراد و سازمان شوند.

بیان مفاهیم پایه :

۱-۱مفهوم امنیت :

امنیت سایبری به موضوعی مورد توجه و اهمیت جهانی تبدیل شده است. در حال حاضربیش از ۵۰ کشور رسماً نوعی از سند راهبردی را منتشر کرده اند که موضع رسمی خود را در موردفضای مجازی، جرایم سایبری،و/یاامنیت سایبری (کلیمبورگ، 2012)اخانه سفید (۲۰۱۱)یک استراتژی سایبری را ترسیم کرده است که موضع ایالات متحده آمریکا (ایالات متحده آمریکا) را در مورد مسائل مربوط به سایبری ارائه می دهد و یک رویکرد واحد را برای تعامل ایالات متحده با سایر کشورها در موردمسائل سایبری ترسیم می کند. بریتانیا (بریتانیا) امنیت سایبری را به عنوان اولویت اصلی فهرست کرده و متعهد شده است ۶۵۰ میلیون طی چهار سال برای یک برنامه تحول آفرین امنیت ملی سایبری (وزیر دفتر کابینه و مدیرکل پرداخت۲۰۱۱)، با این حال، به نظر می رسد تعداد بسیار کمی از این منابع بین مفاهیم مربوط به تمایز قائل شوندامنیت سایبری وامنیت اطلاعات یا رابطه بین آنها دربیشتر ادبیات، امنیت سایبری به عنوان یک اصطلاح فراگیر استفاده می شود.تعاریف این اصطلاح متفاوت است، به عنوان مثال فرهنگ لغت مریام وبستر آنرا به عنوان "اقداماتی که برای محافظت از رایانه یا سیستم رایانه ای (مانند اینترنت) در برابر دسترسی یا حمله غیرمجاز انجام می شود، تعریف می کند. اتحادیه بین المللی مخابرات(ITU) امنیت سایبری را به شرح زیر تعریف می کند:

امنیت سایبری مجموعه ای از ابزارها، سیاست ها، مفاهیم امنیتی، پادمان های امنیتی،دستورالعمل ها، رویکردهای مدیریت ریسک، اقدامات، آموزش، بهترین شیوه ها، تضمین و فناوری هایی است که می تواند برای حفاظت از محیط سایبری و سازمان و دارایی های کاربر استفاده شود. دارایی های سازمان و کاربر شامل دستگاه های محاسباتی متصل، پرسنل، زیرساخت ها، برنامه ها، خدمات،سیستم های مخابراتی و مجموع اطلاعات منتقل شده و/یا ذخیره شده درمحیط سایبری است.

بسیاری از نشریات فعلی که با امنیت سایبری سروکار دارنداز این اصطلاح استفاده می کنندکه امنیت سایبری به جای امنیت اطلاعات.اگر امنیت سایبری مترادف با امنیت اطلاعات باشد، منطقی است که فرض کنیم حوادث امنیت سایبری را می توان بر حسب ویژگی های مورد استفاده برای تعریف امنیت اطلاعات نیز توصیف کرد. بنابراین، یک حادثه امنیت سایبری، برای مثال، منجر به نقض محرمانه بودن، یکپارچگی یا در دسترس بودن اطلاعات نیز میشود.

امنیت سایبری یعنی محافظت از سیستمها، شبکه ها، برنامه ها و سامانه های نرم افزاری در برابر حملات دیجیتالی. هدف از امنیت سایبری، محافظت از اطلاعات در برابر سرقت و آسیب است. بدون وجود امنیت سایبری، سازمانها نمیتوانند از خود در برابر نقضهای دادهای و حمله های هکرها دفاع کنند و به هدفی ساده برای مجرمان سایبری تبدیل میشوند. مخاطرات امنیتی به دلیل گسترده تر شدن ارتباطات در مقیاس جهانی و استفاده از سرویسهای ابری برای ذخیره سازی اطلاعات حساس و شخصی رو به افزایش است . دسترسی، نابودی و تغییر در اطلاعات مهم، دریافت پول از کاربران و در نهایت ایجاد وقفه در روال کسبوکارها از اهداف حملات سایبری است. حفاظت از سامانه های اطلاعات در برابر آسیب رساندن به سخت افزار، نرم افزار و اطلاعات سامانه ها و محافظت در برابر این حملات، نمونه پارامترهایی هستند که امنیت رایانه ای را مورد سنجش قرار می دهند. تهدیدات سایبری با سرعت زیادی رشد میکند و هر ساله تعداد زیادی نفوذ به سیستم ها در حال رخ دادن است.

۲-۱استراتژی امنیت سایبری :

با افزایش حجم و پیچیدگی حملات سایبری، شرکتها و سازمانها به ویژه آنهایی که وظیفه حفاظت ازاطلاعات محرمانه مربوط به امنیت ملی و یا سوابق مالی را بر عهده دارند، باید اقدامات لازم بمنظور محافظت از این اطلاعات حساس را انجام دهند. ایجاد یک استراتژی امنیت سایبری منسجم برای یک سازمان ایده ای مناسب برای این منظور است که البته نیاز به تلاش بسیار زیادی دارد و از مراحل و گام های مختلفی تشکیل می شود. این گام ها عبارتند از:

گام اول: درک چشم انداز تهدیدات سایبری

قبل از اینکه بتوانید چشم انداز تهدیدات سایبری خود را درک کنید، باید درک درستی از این تهدیدات و انواع حملات سایبری را که امروزه سازمان شما با آن مواجه است را داشته باشید. این امر می تواند به این شکل نمایان شود که در حال حاضر کدام نوع از این تهدیدات بیشتر و شدیدتر بر سازمان شما تأثیر میگذارند:

بدافزار ، فیشینگ تهدیدات داخلی یا چیز دیگری است ؟ آیا سازمان ها و شرکت های مشابه شما اخیراً حوادث بزرگی داشته اند و اگر چنین است، چه نوع تهدیدهایی باعث آنها شده است؟

در مرحله بعد، با روندهای پیش بینی شده تهدیدات سایبری که بر سازمان شما تأثیر می گذارد، خود را آماده کنید. به عنوان مثال، بسیاری از محققان امنیتی احساس میکنند که با رونق گرفتن کسب وکارها، باج افزارها به تهدید بزرگتری تبدیل میشوند. همچنین نگرانیهای فزایندهای در مورد تهدیدات در حوزه زنجیره اطلاعات وجود دارد، به این صورت که اطلاعات آسیب دیده و استفاده از آن در منابع اطلاعاتی می تواند منجر به دریافت اطلاعات غیرواقعی و نادرست از سامانه ها شود. درک چشم انداز تهدیدات سایبری می تواند بطور فزاینده ای سازمان را در برابر این تهدیدات مقاوم سازد.

گام دوم: ارزیابی بلوغ امنیت سایبری سازمان متبوع :

هنگامی که متوجه شدید با چه چیزی روبرو هستید، باید یک ارزیابی کامل و دقیق از بلوغ امنیت سایبری سازمان خود انجام دهید. یک چارچوب امنیت سایبری را انتخاب نموده و از آن برای ارزیابی میزان بلوغ سازمان خود در دسته بندی و زیرمجموعه مختلفی از خط مشیها و حاکمیت گرفته تا فناوریهای امنیتی و قابلیتهای بازیابی حوادث استفاده کنید. این و سیستمهای ۲۲ ارزیابی باید شامل تمام فناوریهای شما، از فناوری اطلاعات سنتی گرفته تا فناوری عملیاتی، اینترنت اشیا فیزیکی سایبری باشد. در مرحله بعد، از

همان چارچوب امنیت سایبری استفاده کرده و تعیین نمایید که سازمان متبوع شما در سه تا پنج سال آینده از نظر بلوغ برای هر یک از آن دسته ها و زیرمجموعه ها در کجا قرار گیرد.

گام سوم: تعیین نحوه بهبود برنامه امنیت سایبری

اکنون که میدانید کجا هستید و میخواهید کجا باشید، باید ابزارهای امنیت سایبری و بهترین روشهایی را که به شما در رسیدن به اهدافتان کمک میکنند، پیدا کنید. در این مرحله، شما تعیین می کنید که چگونه برنامه امنیت سایبری خود را بهبود بخشید تا به اهداف استراتژیکی که تعریف کرده اید دست یابید. هر بهبودی در برنامه مذکور مستلزم صرف هزینه و منابع بوده لذا باید مزایا و معایب رسیدن به اهداف هر گزینه را بررسی نموده و تفکر لازم را در انتخاب آن انجام دهید. بطور مثال ممکن است به این نتیجه برسید که برخی یا همه وظایف امنیتی خود را برون سپاری کنید، در اینصورت مقدار هزینه و منابع صرف شده در این تصمیم را باید درنظر گرفته و سپس اقدامات خود را در آن راستا انجام دهید.

گام چهارم: مستند نمودن استراتژی امنیت سایبری

پس از تأیید مدیریت ارشد سازمان، باید اطمینان حاصل کنید که استراتژی امنیت سایبری شما به طور کامل مستند شده است. مستندسازی استراتژی امنیت سایبری شامل نوشتن یا بروزرسانی ارزیابیهای ریسک، برنامه های امنیت سایبری، سیاستها، دستورالعملها، رویه ها و هر چیز دیگری است که برای تعریف آنچه برای دستیابی به اهداف استراتژیک مورد نیاز یا توصیه میشود، نیاز دارید. روشن کردن وظایف هر فرد کلیدی است.

مطمئن باشید که هنگام نوشتن و به روز رسانی این اسناد، مشارکت فعال و بازخوردی از افرادی دریافت می کنید که کار مرتبط را انجام خواهند داد. همچنین باید برای آنها توضیح دهید که چرا این تغییرات ایجاد شده است و این تغییرات چقدر دارای اهمیت می باشد تا مردم بیشتر آن را پذیرفته و حمایت نمایند. همه افراد در سازمان نقشی در کاهش مسائل امنیتی و بهبود برنامه امنیت سایبری دارند. فراموش نکنید که استراتژی امنیت سایبری سازمان شما نیازمند به روز رسانی آگاهی و تلاشهای آموزشی در مورد امنیت سایبری است و همانطور که مشخصات ریسک شما تغییر می کند، فرهنگ امنیت سایبری شما نیز باید تغییر کند.

۳-۱مبانی امنیت داده :

نگرانی اصلی در سازگاری ابر برای داده ها، امنیت و حریم خصوصی است . برای سرویس ابری بسیار مهم است که از یکپارچگی داده ها، حریم خصوصی و حفاظت اطمینان حاصل کند .برای این منظور، چندین ارائه دهنده خدمات از سیاست ها و مکانیسم های مختلفی استفاده می کنند که به ماهیت، نوع و اندازه داده هابستگی دارد.

یکی از مزایای رایانش ابری این است که داده ها را می توان بین سازمانهای مختلف به اشتراک گذاشت. با این حال، این مزیت خود خطری برای داده ها ایجاد می کند. برای جلوگیری از خطرات احتمالی برای داده ها، حفاظت از مخازن داده ها ضروری است.

بااستفاده از ابر سازمانی داخلی این رویکرد می تواند با اعمال خط مشی استفاده از داده در محل به ایمن کردن داده ها کمک کند. با این حال، هنوز امنیت و حریم خصوصی کامل داده ها را تضمین نمی کند، زیرا بسیاری از سازمانها به اندازه کافی واجد شرایط نیستند تا تمام لایه های حفاظتی را به داده های حساس اضافه کنند.

امنیت داده در رایانش ابری بیش از رمزگذاری داده ها را شامل میشود. الزامات امنیت داده ها به سه مدل سرویس PaaS ، SaaSو IaaSبستگی دارد. دوحالت داده معمولاًامنیت آن را در ابرها تهدید می کند . Rest at Dataکه به معنای داده های ذخیره شده در ابر است و Transit in Data که به معنای داده هایی است که در داخل و خارج از ابر حرکت میکنند. محرمانه بودن و یکپارچگی داده ها بر اساس ماهیت مکانیسمها، رویه ها و فرآیندهای حفاظت از داده ها است. مهم ترین موضوع،قرار گرفتن در معرض داده ها در دو حالت فوق است.

داده های در حال استراحت:

داده در حالت استراحت به داده های موجود در فضای ابری یا هر داده ای که با استفاده از اینترنت قابل دسترسی است اشاره دارد. این شامل داده های پشتیبان و همچنین داده های زنده است. همانطور که قبلا ذکر شد، گاهی اوقات برای سازمان ها بسیار دشوار است که از داده ها در حالت استراحت محافظت کنند، اگر از یک ابر خصوصی نگهداری نکنند، زیرا کنترل فیزیکی روی داده هاندارند. با این حال، این مشکل را می توان با حفظ یک ابر خصوصی با دسترسی دقیق کنترل شده حل کرد.

داده های در حال انتقال :

داده های در حال انتقال معمولاً به داده هایی اطلاق می شود که به داخل و خارج از ابر حرکت می کنند. این داده ها می توانند به شکل یک فایل یا پایگاه داده ذخیره شده در ابر باشند و می توانند برای استفاده در مکان دیگری درخواست شوند.هر زمان که داده ها در فضای ابری بارگذاری می شوند، داده ها در زمان بارگذاری،داده های در حال انتقال نامیده می شوند. داده های در حال انتقال می توانندداده های بسیار حساسی مانند نام های کاربری و رمزهای عبور باشند و گاهی اوقات رمزگذاری شوند. با این حال، داده ها به صورت رمزگذاری نشده نیز دادههای در حال انتقال هستند. دادههای در حال انتقال گاهی بیشتر از داده های در حال سکون در معرض خطر هستند زیرا باید از یک مکان به مکان دیگر سفر کنند . روش های مختلفی وجود دارد که نرم افزار واسطه میتواند داده ها را استراق سمع کند و گاهی اوقات توانایی تغییر داده هارا در مسیر رسیدن به مقصد داشته باشد. به منظور محافظت از دادهها در حین انتقال، یکی از بهترین استراتژی ها رمزگذاری است:

اینروزها تکنیک های رمزنگاری مختلفی برای رمزگذاری داده ها استفادهمی شود. رمزنگاری سطح حفاظت از داده ها را برای اطمینان ازیکپارچگی، احراز هویت و در دسترس بودن محتوا افزایش داده است.در شکل اصلی رمزنگاری، متن ساده با استفاده از یک کلید رمزگذاری به متن رمزگذاری می شود و سپس متن رمزی حاصل با استفاده از یک کلید رمزگشایی که در شکل ۲ نشان داده شده است، رمزگشایی می شود.

۴-۱اهداف امنیت سایبری:

همانند هر عرصه دیگر، پدافند سایبری کشور باید آمادگی کامل خود را به منظور مصون سازی و نیز مقابله با تهدیدات و حملات دشمن در حد عالی حفظ کند، این آمادگی در همه سطوح کاری باید همراه با استقامت و پایداری و حفظ روحیه جهادی باشد. بنابر این هدف امنیت سایبری محافظت از اطلاعات در برابر سرقت و آسیب است. این اطلاعات شامل دادهای حساس، اطلاعات قابل شناسایی و تشخیص هویت افراد، سوابق پزشکی، اطلاعات شخصی، مالکیت معنوی، داده های مرتبط با فعالیت آژانس های دولتی و صنعتی می شود.بدون وجود امنیت سایبری سازمانها نمی توانند از خود در برابر نقض های داده ای(نقص داده ای به رویکردی اشاره دارد که باعث افشای داده های شخصی کاربران شده و به هکرها اجازه سوء استفاده از اطلاعات و جعل هویت افراد را می دهد)و حمله های هکری دفاع کنند و به هدفی ساده برای مجرمان سایبری تبدیل می شوند. مخاطرات امنیتی به دلیل گسترده تر شدن ارتباطات در مقیاس جهانی و استفاده از سرویس های ابری برای ذخیره سازی اطلاعات حساس و شخصی رو به افزایش است.پیکربندی غیر اصولی خدمات ابری باعث شده تا حمله های سایبری شکل پیچیده ای به خود بگیرند. هر سازمانی ممکن است قربانی یک حمله سایبری موفق شده و با مشکل نقض داده ای در مقیاس کلان روبرو شود. روز هایی که دیوارهای آتش ساده و نرم افزارهای ضد ویروس تنها راهکارهای امنیتی موثر بودند سپری شده و کارشناسان امنیتی نمی توانند همچون گذشته به مقابله با تهدیدات سایبری بپردازند و این تهدیدات می توانند از زوایای مختلفی به سازمانها آسیب زنند. امنیت سایبری با رویکردهای فنی و آموزشی به مقابله با چالش های امنیتی می پردازد مثال کارمندان درباره کلاه برداری های ساده ای مثل مهندسی اجتماعی و حملات پیچیده تر مثل حملات باج افزاری، بد افزارهای که برای سرقت مالکیت معنوی یا داده های شخصی طراحی شده اند آموزش های لازم را می بینند. امنیت سایبری دیگر مفهومی نیست که کسب و کارها به سادگی از آن چشم پوشی کنند.حوادث امنیتی به طور منظم بر عملکرد مشاغل مختلف در هر اندازه ای تاثیرگذار است و اغلب به اعتبار یک شرکت خدشه وارد می کند.

۵-۱انواع امنیت سایبری:

۱ - امنیت زیر ساخت های حیاتی: تامین امنیت سایبری زیر ساخت های حیاتی به معنای محافظت از شبکه های ارتباطی، شبکه انتقال انرژی، تصفیه آب، چراغ های راهنمایی، پایانه های فروش و مراکز بهداشتی است. این مراکز ممکن است به طور مستقیم با حمله های سایبری مرتبط نباشد، اما می توانند به عنوان بستری برای ورود بد افزار ها به نقاط پایانی سامانه هایی که به آنها متصل می شوند استفاده شوند.

۲ - امنیت شبکه: امنیت شبکه از شبکه کامپیوتری در برابر اختلال گران محافظت می کند حال این اختلال می تواند بدافزار باشد و یا هکر. امنیت شبکه مجموعه راهکارهایی است که سازمانها را قادر می سازد تا شبکه های رایانه ای را از دسترس افراد متجاوز، مهاجمان سازمان یافته و بد افزارها دور نگه دارند.

۶-۱حملات سایبری

حمله های سایبری، نوعی حمله است که در آن یک مؤلفه رایانه ای وجود دارد که سیستم های هدف را غیر قابل استفاده نموده، کارایی آنها را کم کرده و با تزریق اطلاعات غلط، دقت تصمیم گیری کاربران را کاهش می دهد و حتی منجر به سرقت اطلاعات می شوند. حمله های سایبری چند تفاوت عمده با شکل های معمول حمله دارند: اول اینکه حمله های سایبری توسط عوامل نامعلوم صورت می گیرد و رد یابی و یافتن محل اختفای آنها بسیار دشوار است. اینگونه حمله ها، فاصله و مکان را محو کرده و از بین میبرند. دوم اینکه حمله های سایبری بسیار ارزانتر از حمله درجنگ های معمولی است و در عین حال که فاقد آسیب پذیری و هز ینه هستند، بیشتر مورد توجه شخص مهاجم قرار می گیرند. سوم اینکه ساختارهای شبکه ای گروه های مهاجم، آنها را در مقابل هرگونه اقدام تلافی جویانه ایمن ساخته و باعث افزایش توان خود ترمیمی آنها می گردد.

حملاتی که منابع یه شبکه رخ میده از دیدگاه کلی به دو بخش حملات فعال و حملات غیر فعال تقسیم میشن.

حملات فعال Attack Active

به حملاتی که از همون لحظه اول شروع حمله علائم اشکاری از خودشون بروز میدن و کشف اونها امکان پذیره حملات فعال گفته میشه .به عنوان مثال حمله نوع وقفه با از کار انداختن شبکه خودشو نشون میده و در دسته حملات اکتیو دسته بندی میشه

حملات غیر فعال Attack Passive

حملات غیر فعال هیچ علامت اشکاری در شبکه از خودشون نشون نمیدن و ممکنه برای ساعتها و هفته ها مخفی بمونن .حمله استراق سمع از این دسته از حملات محسوب میشه. حملات غیر فعال بسیار خطرناک و موجب آسیب بسیار زیاد به موجودیت های شبکه میشن.

۷-۱انواع حملات سایبری :

۱ - **خرابکاری اینترنتی :** دشمن، امکان نفوذ و خرابکاری سیستم های اطلاعاتی نظامی و غیر نظامی خود را با قطع شبکه های اطلاعاتی، وبه ویژه قطع شبکه جهانی اینترنت، برای کشور مقابل سلب می کند.

۲ - **گردآوری داده ها:** دسترسی به اطلاعات طبقه بندی شده که امکان جاسوسی از نقاط مختلف جهان را فراهم می کند.

۳ – **حمله گسترده اخلال در سرویس دهی :** در این نوع حمله، شمار زیادی را از رایانه هادر یک کشور مبادرت به ایجاد اخلال در سرویس دهی به سیستم های کشور دیگر می شوند .

۴ – اخلال در تجهیزات : فعالیت های نظامی که در آنها از رایانه و ماهواره برای هماهنگی استفاده می شود، در خطر این نوع حمله قرار دارند؛ زیرا مهاجمان می توانند فرمان ها و ارتباطات را رهگیری کرده یا تغییر دهند.

۵ - **حمله به زیرساختارهای حیاتی:** نیروگاه های برق، تأسیسات آبرسانی و سوخت رسانی، ارتباطات و حمل و نقل در برابر این نوع حمله آسیب پذیری بالایی دارند.

۶ – رهگیری : در این روش، نفوذ گران می توانند به شکل مخفیانه از اطلاعات نسخه برداری کنند.

۷ - **افزودن و تغییر اطلاعات:** در این روش نفوذگر، اطلاعات اضافی را بر اطلاعات اصلی اضافه کرده و یا آن را تغییر می دهد.

۸ – وقفه : در این روش نفوذگر باعث اختلال در شبکه و تبادل اطلاعات میشود.

۹ - **افزایش سرعت در تصمیم گیری:** سیستم های اطلاعاتی کمک شایانی به بهبود سرعت و دقت در امر تصمیم گیری توسط فرماندهان میکنند.

فواید حملات سایبری :

۱ - محافظت از کسب و کار در مقابل حملات سایبری و درز کردن اطالعات و داده ها

۲ - محافظت از اطالعات داده ها و شبکه ها

۳ - جلوگیری از دسترسی کاربران غیر مجاز

۴ - بهبود زمان بازیابی پس از درز کردن احتمالی اطلاعات

۵ - محافظت از اطلاعات کاربران نهایی و سیستم های نقطه انتهایی

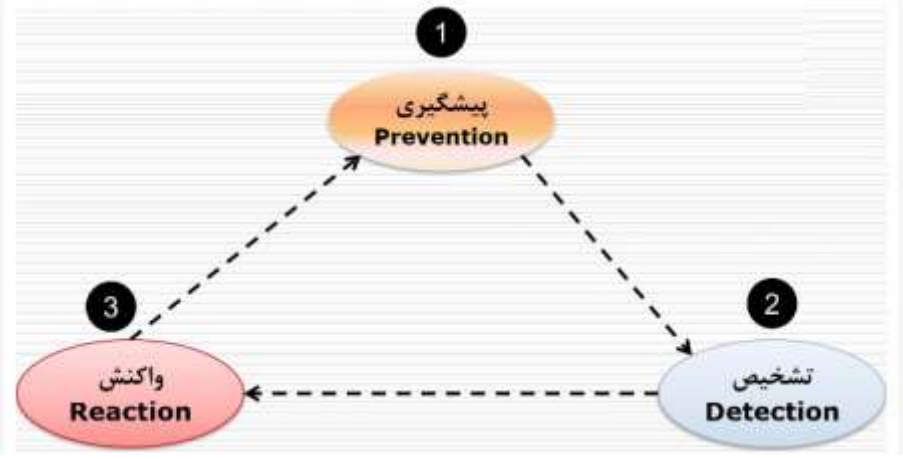
۶ - انطباق و همراستا بودن با رگولاتوری

۷ - تضمین تداوم کسب و کار

۸ - ایجاد اطمینان برای حفظ خوشنامی شرکت،همچنین جلب اعتماد توسعه دهندگان، شرکا، مشتریان، سهامداران و کارمندان.

مفاهیم امنیت سایبری :

تامین امنیت سایبری با توجه به شرایط موجود پیگیری می شود. پیش از وقوع حمله یا نفوذ، لازم است اقدامات پیشگیرانه انجام شود. در حین حمله و پس از آن نیز باید اقدامات تشخیص و ردیابی و در نهایت واکنش مناسب صورت پذیرد. در ادامه این مفاهیم را معرفی می کنیم.



پیشگیری(Prevention)

این رویکرد مربوط به زمان طراحی و پیاده‌سازی برنامه و یا شبکه است. پیش‌گیری با اتخاذ سیاست‌های امنیتی مناسب و بکارگیری مکانیزم‌های درست، از وقوع حمله و خسارت‌های متعاقب آن جلوگیری می‌کند.

تشخیص و ردیابی(Detection and Tracing)

تشخیص و ردیابی در زمان وقوع حمله و پس از آن صورت می‌گیرد. در زمان حمله، در صورت تشخیص باید پاسخ مناسب داده شود تا خسارت ناشی از حمله به حداقل برسد، به‌عنوان مثال دسترسی مهاجم قطع یا محدود شود. در موارد دیگر، شناسایی پس از وقوع حمله اتفاق می‌افتد. در این موارد باید زمان و علت حمله (آسیب پذیری‌های موجود)، میزان خسارت و هویت دشمن شناسایی شود.

واکنش(Reaction)

پس از شناسایی علل آسیب‌پذیری، باید در جهت رفع نقاط ضعف اقدام کرد تا از حملات مجدد جلوگیری شود. همچنین با استفاده از نسخه‌های پشتیبان، داده‌های آسیب‌دیده یا از بین رفته را ترمیم کرد و سیستم را به حالت درست قبلی برگرداند و یا نزدیک کرد.

دالیل ناامنی شبکه ها:

ضعف فناوری

پروتکل، سیستم عامل، تجهیزات

ضعف تنظیمات

رهاکردن تنظیمات پیشفرض، گذرواژه های نامناسب، عدم استفاده از رمزنگاری، راه اندازی سرویسهای اینترنت بدون اعمال تنظیمات الزم، ...

ضعف سیاستگذاری

عدم وجود سیاست امنیتی

عدم وجود طرحی برای مقابله و بازیابی مخاطرات

نداشتن نظارت امنیتی مناسب (مدیریتی و فنی)

فصل دوم

خلاصه :

:سیستم های تشخیص نفوذ شبکه NIDS برای محافظت از نیازهای امنیتی شبکه های سازمانی در برابر حملات سایبری طراحی شده اند. با این حال، شبکه های NIDS از محدودیت های متعددی رنج می برند، مانند ایجاد حجم بالایی از هشدارهای با کیفیت پایین. علاوه بر این، ٪۹۹ از هشدارهای تولید شده توسط NIDSها مثبت کاذب هستند. همچنین، پیش بینی اقدامات آتی یک مهاجم یکی از مهم ترین اهداف در اینجاست. این مطالعه پیشرفته ترین پیش بینی حملات سایبری را بر اساس هشدار نفوذNIDS ، مدل ها و محدودیت های آن بررسی کرده است. طبقه بندی همبستگی هشدار نفوذ ACمعرفی شده است که شامل رویکردهای مبتنی بر شباهت، مبتنی بر آمار، مبتنی بر دانش و مبتنی بر ترکیبی است.علاوه بر این، طبقه بندی مؤلفه های همبستگی هشدار نیز معرفی شد. مجموعه داده های همبستگی هشدار و مسیرهای تحقیقاتی آینده برجسته شده است AC .هشدارهای خام را برای شناسایی ارتباط بین هشدارهای مختلف دریافتمی کند، هر هشدار را به اطلاعات متنی مرتبط خود مرتبط می کند و هشدار/حمله آتی را پیش بینی می کند.

شبکه NIDS :

سیستم تشخیص نفوذ مبتنی بر شبکه (NIDS) Network Intrusion Detection System :
شناسایی و تشخیص نفوذهای غیرمجاز قبل از رسیدن به سیستم های بحرانی، به عهده سامانه تشخیص نفوذ مبتنی بر شبکه استNIDS .، به عنوان دومین نوعIDS ها، در بسیاری از موارد عملاً یک Sniffer هستند که با بررسی بسته ها و پروتکل های ارتباطات فعال، به جستجوی تلاش هایی که برای حمله صورت می گیرد می پردازند. به عبارت دیگر معیارNIDS ، تنها بسته هایی است که بر روی شبکه ها رد و بدل می گردد. از آن جایی که NIDS تشخیص را به یک سیستم منفرد محدود نمی کنند، عملاً گستردگی بیشتری داشته و فرایند تشخیص را به صورت توزیع شده انجام می دهند. با این وجود این سیستم ها در رویایی با بسته های رمزشده یا شبکه هایی با سرعت و ترافیک بالاکارایی خود را از دست می دهند.
سیستم تشخیص نفوذ شبکه ترافیک یک شبکه را برای پیدا کردن فعالیت های مشکوک مثل یک حمله یا فعالیت های غیر مجاز مانیتور می کند.
سرورهای بزرگ NIDS می تواند روی یک ستون فقرات به انگلیسی back bone :کارگزاری شود تا همهٔ ترافیک ها را مانیتور کند یا یک سیستم کوچکتر می تواند کارگزاری شود تا ترافیک یک بخشی از سرور را مانیتور کند، مثل سوئیچ و روتر.
به علاوه برای مانیتور کردن ترافیک ورودی و خروجی شبکه، سرور NIDS می تواند فایل های سیستم را اسکن کند تا فعالیت های غیر مجاز را پیدا کندو جامعیت داده ها و فایل ها را حفظ کند.

سرور NIDS می تواند تغییراتی را که در اجزای هسته سرور ایجاد می شود را شناسایی کند. علاوه بر مانیتور کردن ترافیک، سرور NIDS می تواند فایل های لاگ سرور را اسکن کند و ترافیک های مشکوک را پیدا کند.

سیستمهای تشخیص نفوذ شبکه NID به دلیل خطرات پیچیده مرتبط با حملات شبکه به سرعت در حالفراگیر شدن هستند. سیستم های تشخیص نفوذ شبکه NIDS برای محافظت از نیازهای امنیتی شبکه های سازمانی در برابر حملات سایبری طراحی شده اند. شبکه های NIDS از محدودیت های متعددی رنجمی برند، مانند تولید حجم بالایی از هشدارهای با کیفیت پایین. علاوه بر این، ٪۹۹ از هشدارهای تولید شده توسطNIDS ، مثبت کاذب هستند.

یک نفوذ را می توان به عنوان یک چارچوب تخطی از سیاست امنیتی که به مؤلفه های امنیتی اشاره دارد،که متعهد به شناسایی نقض امنیت چارچوب هستند، توصیف کرد. فعالیت های نفوذی مانند فعالیت هایعادی سیستم و فعالیت های غیرعادی سیستم نیست. سیستم های تشخیص نفوذ IDS جایگزین سایر استراتژی های امنیتی نمی شوند، به عنوان مثال، روش های پیشگیری از تأیید و کنترل دسترسی.

مدل های پیشرفته پیش بینی نفوذ :

طرح کتابخانه :

نمودار حمله شبکه

استخراج الگوهای توالی

یادگیری ماشین و داده کاوی

سری های زمانی

شبکه های بیضی

طرح کتابخانه :

این طرح برای پیش بینی رفتار مهاجم استفاده می شود چگونه یک کتابخانه طرح از حملات خاصرا برای پیش بینی یک طرح حمله تعریف کرد. کارشناس امنیتی موظف است کتابخانه طرح را به صورتدستی جمع آوری کند. با این حال، این می تواند زمان بر باشد و همیشه نمی تواند به شکل جدیدی از انواع حمله پاسخ دهد. پیچیدگی تطبیق طرح بهدلیل تنوع اقدامات از دست رفته در یک توالی حمله افزایش می یابد. بنابراین، انتظار می رود کتابخانه طرح به طور منظم به روز شود تا اطمینان حاصل شود که با توالی حمله جدید مطابقت دارد.

مدل های مارکوف :

یکی دیگر از رویکردهای رایج برای پیش بینی حملات بر اساس روش های پیش بینی بررسی مدل، استفاده از مدل های مارکوف است.مدل های مارکوف دسته بندی محبوبی از مدل ها را تشکیل می دهند،از جمله نمونه های معروف زنجیره های مارکوف و مدل های پنهان مارکوف .مدل های مارکوف اغلب به عنوان یک نمودار نشان داده می شوند که روش های مبتنی بر آنها را شبیه به روش های مبتنی بر نمودارهای حمله و شبکه های بیزی می کند .برخلاف روش های توصیف شده قبلی، مدل های مارکوف در حضور حالت هاو انتقال های غیرقابل مشاهده به خوبی عمل می کنند، که وابستگی روش های تشخیص نفوذ و پیش بینی حمله را به داشتن اطلاعات کامل حذف می کند. این امکان تشخیص نفوذ موفق و پیش بینی حمله را فراهم می کند، حتی اگر برخی از مراحل حمله شناسایی نشده باشند یا به طور کامل قابل استنباط نباشند.

بررسی ادبیات:

روش های مبتنی بر مدل های مارکوف همراه با روش های مبتنی بر نمودارهای حمله و شبکه های بیزی در اواخر سال 2000ظاهر شدند.فرهادی و همکاران در سال ۲۰۱۱ یک چارچوب پیچیده برای همبستگی و پیش بینی هشدار پیشنهاد کرد. در اینکار، از الگوبرداری متوالی برای استخراج سناریوهای حمله استفاده می شود،که سپس با استفاده از یک مدل مارکوف پنهان که برای شناسایی طرح حمله استفاده می شود، نمایش داده می شوند .نویسندگان ادعا می کنند که کار آنها اولین کاری است که از روشی بدون نظارت برای شناسایی طرح حمله استفاده می کند. کارهای تحقیقاتی مانند این بخشی از روند تحقیقاتی در زمینه پیش بینی ها در امنیت سایبری است که بر اشکال عمده کارهای قبلی غلبه می کند. به جای تکیه بر یک مدل از پیش تعریف شده ساخته شده یا تحت نظارت یک متخصص انسانی، از روش های بدون نظارت داده کاوی یا

یادگیری ماشین استفاده می کند. بنابراین، ما این اثر را به عنوان مطالعه توصیه شده برای نشان دادن این انتقال انتخاب کردیم .سندیو همکاران در سال ۲۰۱۲ روشی برای پیش بینی نفوذ درزمان واقعی پیشنهاد کرد که از HMM استفاده می کند. حملات چندمرحله ای علاقه اصلی در این کار است. یک ارزیابی تجربی نشان می دهدکه چگونه روش آنها می تواند حملات چند مرحله ای را پیش بینی کند، که به ویژه برای جلوگیری از کنترل بیشتر و بیشتر میزبان هادر شبکه توسط مهاجم مفید است.

مدل های پیوسته :

شامل سری های زمانی و مدل های خاکستری است که چنین رویکردهایی در بیشتر موارد برای پیش بینی وضعیت امنیت شبکه مناسب هستند. نتایج رایج پیش بینی تعداد،حجم و ترکیب حملات در شبکه و توزیع آنها در زمان است .روش دیگر، الگوهای مکانی و زمانی در سری های زمانی ممکن است برای پیش بینی حملات سایبری استفاده شود. سریهای زمانی ابزار بسیار جالبی برای تجزیه و تحلیل پیش بینی است که در زمینه های مختلف از جمله امنیت سایبری استفاده می شود.

سری های زمانی معمولا در تشخیص ناهنجاری استفاده می شود. یک سری زمانی نشان دهنده الگوهای رایج ترافیک شبکه است. متعاقباً، انحرافاتی که با مقادیر مورد انتظار ترافیک شبکه دریک لحظه معین مطابقت ندارند، به عنوان یک ناهنجاری اعلام می شوند.اگرچه اصطلاحات و روش های تشخیص ناهنجاری شبیه به پیش بینی حمله است، اما این دو مورد استفاده اساساً متفاوت هستند.از این رو، تحقیق در مورد تشخیص ناهنجاری در اینجا ارائه نشدهاست. سری زمانی مجموعه ای از نقاط داده متوالی است که به ترتیب زمانی نمایه می شوند و اغلب در نمودارهای خطی رسم میشوند. یک سری زمانی از سوابق تاریخی یک پدیده مشاهده شده ساخته شده است. در مورد ما، این می تواند فعالیت مهاجم یا وضعیت امنیت شبکه باشد که در یک مقدار عددی نشان داده شده است.روش های زیادی برای تحلیل سری های زمانی وجود دارد که می توان از آنها برای پیش بینی مقادیر یک سری زمانی در آینده نزدیک استفاده کرد. تعداد قابل توجهی از رویکردها از میانگین متحرک استفاده می کنند، یک محاسبه برای تجزیه و تحلیل داده ها با ایجاد یکسری میانگین از زیر مجموعه های سری زمانی. انواع تجزیه و تحلیل میانگین متحرک شامل میانگین متحرک ساده یا میانگین متحرک موزون نمایی است.

طبقه بندی :

رویکرد مبتنی بر شباهت

رویکرد دانش محور

رویکرد مبتنی بر آمار

رویکرد مبتنی بر ترکیبی

رویکرد همبستگی هشدار

مدل های همبستگی هشدار نفوذ :

برای اطمینان از بهبود کیفیت هشدارهایی که توسط NIDS در دسترس قرار گرفته اند، نیاز زیادی به همبستگیهشدار AC وجود دارد. پیش بینی سناریوهای حمله پیچیده نیازمند توسعه یک مدل همبستگی / پیش بینیهشدار مؤثر، کارآمد و دقیق است. مدل AC شامل چندین کار است که شامل عادی سازی، کاهش،شدت/اولویت بندی، تشخیص حمله و پیش بینی برای ارائه دیدگاهی از موقعیت های امنیتی شبکه است.

درمیان کارهای پیش پردازشی که توسط AC مورد مطالعه قرار گرفته است، قالب بندی هشدارها را میتوان به عنوان یک کار اولیه مهم در نظر گرفت. در حال حاضر، بیشتر سازمان ها انواع مختلفی از NIDS NIDS ناهمگنرا پیاده سازی می کنند، بنابراین هشدارها را در قالب های داده های مختلف تولید می کنند . نرمالسازی هشدار فرآیند تبدیل فرمت های مختلف داده های هشدار از سنسورهای نفوذ متعدد به فرمت هایاستاندارد مناسب و قابل قبول برای سایر اجزای همبستگی است.

سیستم‌های تشخیص نفوذ به عنوان عناصر اصلی برای افزایش امنیت در شبکه‌های کامپیوتری مطرح شدند. نقش این سیستم‌ها نظارت بر توافقات امنیتی شبکه و هدف آن‌ها تشخیص فعالیت مهاجمان و ایجاد هشدارهایی در این زمینه می‌باشد. یکی از مشکلات اساسی سیستم‌های تشخیص نفوذ تولید حجم زیادی از هشدارها است، که ممکن است بیش از ۹۹ درصد هشدارهای تولید شده نادرست باشند، که با عنوان هشدارهای مثبت کاذب مطرح می‌شوند. هشدارهای نادرست هر رفتار نرمال و مورد انتظار شبکه را به عنوان یک تهاجم معرفی می‌کنند. هنر مدیریت سیستم‌های تشخیص نفوذ استفاده از روش‌هایی به منظور کاهش هشدارهای نادرست است، بدون این‌که مانع تشخیص حملات واقعی به سازمان شوند. بنابراین، کنترل این

نوع هشدارها حائز اهمیت است و اخیراً محققان به ارائه روش‌هایی جهت تعداد هشدارها، پرداخته‌اند. در این مقاله به بررسی تکنیک‌های داده کاوی به منظور کاهش هشدار در سیستم‌های تشخیص نفوذ پرداخته می‌شود.

مروری بر ارزیابی ریسک :

ارزیابی ریسک:

ارزیابی ریسک بخش مهمی از فرآیند مدیریت ریسک برای ایمن سازی سیستم های اطلاعاتی است. فعالیت های ارزیابی ریسک به سازمانها کمک میکند تا سطح قابل قبول ریسک را تعیین کنند. درک وارزیابی ریسک یک فرآیند مهم برای بهبود امنیت اطلاعات در تصمیم گیری است که با عث شده تا پیش بینی ریسک بخش مهمی از سیستم امنیت اطلاعات شود. برای اینکه مرکز عملیات امنیتی محیط خود رادرک کند، تکنیک پیش بینی ریسک به آن ها کمک می کند تا درک جامعی از شبکه ها، سیستم ها، سرویس ها و برنامه هایی که مسئول نظارت بر آن هستند ایجاد کنند.

معرفی ریسک:

حملات سایبری در حال افزایش است وبه یک نگرانی فزاینده ای برای سازمان ها و بخش های دولتی تبدیل شده. زیرساخت های موجود به شدت بر زمان به روزرسانی سرویس، یکپارچگی داده ها وانطباق تأثیر می گذاردو سازمان ها را ملزم می کند تا اقدامات متقابلی را برای مقابله با این نگرانی های امنیتی اجرا کنند. حفاظت ازسیستم شبکه به یک چالش برای سازمان ها تبدیل شده است زیرا مهاجمان از روش های پیشرفته برای نفوذ به پایگاه های داده استفاده می کنند اگرچه مدیر شبکه اتصال را برای ورود به پایگاه داده ایمن می کند. چارچوب های مدیریت ریسک امنیت در فضای سایبری، کنترل های امنیتی و حریم خصوصی و قابلیت اطمینان منحصر به فردی را ایجاد میکنند .و شامل بیش از ۸۰۰ کنترل برا ی انتخاب هستند که بسیاری از آنها برا ی برخی سیستم ها اعمال نمی شوند. درصورتی که برخی از این مؤلفه ها در چارجوبهای مذکور در فضای سایبری و با توجه به تهدیدهای روز به روز فزاینده، الزامی انکار ناپذیرند؛ ارزیابی های ترکیبی ایمنی، امنیت و قابلیت اطمینان می تواند شناسایی موثرتر و به موقع عیوب طراحی

اولیه را بیان کنند، .لذا شناخت این چارچوبها کمک میکند که هر سازمانی با توجه به فعالیتهای خود و سیستم های مورد نظرش تصمیم بگیرد که کدام مؤلفه های این چارچوبها را اعمال کند یا خیر.

مراحلی که در چهارچوب مدیریت ریسک موجود می باشند :

یک مرحله مقدماتی برای اطمینان از آمادگی سازمان ها برا ی اجرا ی فرآیند و شش مرحله اصلی. هر هفت مرحله برا ی اجرا ی موفقیت آمیز چارچوب مدیریت ریسک ضروری است.

مراحل عبارتند از

۱ - با ایجاد زمینه و اولویت ها برا ی مدیر یت خطر امنیت و حریم خصوصی، برای اجرا ی چارچوب مدیریت ریسک از دیدگاه سازمان و سطح سیستم آماده شوید .

۲ - سیستم و االطلاعات پردازش، ذخیره و ارسال شده توسط سیستم بر اساس تجزیه و تحلیل تاثیر ضرر را طبقه بندی کنید .

۳ - یک مجموعه اولیه از کنترل ها را برای سیستم انتخاب کنید و کنترل ها را بر اساس ارزیابی ریسک تا حد قابل قبولی کاهش دهید .

۴ - کنترل ها را اجرا کنید و نحوه بکارگیری کنترل ها در سیستم و محیط عملیاتی آن را شرح دهید .

۵ - کنترل ها را ارزیابی کنید تا مشخص کنید که آیا کنترل ها به درستی اجرا می شوند، همانطور که در نظر گرفته شده عمل می کنند و نتایج مورد نظر را با توجه به ارضا ی الزامات امنیتی و حفظ حریم خصوصی ایجاد می کنند .

۶ - مجوز سیستم یا کنترل های مشترک را براساس این تشخیص که ریسک برا ی عملیات و دارایی های سازمانی ، افراد، سایر سازمان ها و کشور قابل قبول است، بررسی کنید .

۷ - سیستم و کنترلهای مرتبط را به طور مداوم نظارت کنید تا شامل ارزیابی اثربخشی کنترل، مستندساز ی تغییرات در سیستم و محیط عملیات، انجام ارزیابیهای ریسک و تجزیه و تحلیل تأثیرات، و گزارش وضعیت امنیت و حریم خصوصی سیستم باشد.

فصل سوم

خلاصه :

روش های یادگیری ماشینی به میزان گسترده ای برای توسعه یک سیستم آشکار سازی نفوذ (IDS) برای آشکار سازی و دسته بندی حمله های سایبری در سطح شبکه و سطح میزبان به صورت بموقع و خودکار، مورد استفاده قرار می گیرند. اما، چالش های بسیاری بوجود آمده اند، زیرا حمله های بدخواهانه دائماً در حال تغییر هستند و در حجم بسیار بزرگی در حال رخ دادن هستند که در نتیجه، یک راهکار مقیاس پذیر را ملزم کرده اند. مجموعه داده های بدافزارهای مختلفی برای عموم به صورت مجانی فراهم شده تا پژوهش های بیشتری توسط جامعه ایمنی سایبری انجام شود. اما، هیچ مطالعه ای تاکنون تحلیل تفصیلی عملکرد الگوریتم های یادگیری ماشینی مختلف بر مجموعه داده های مختلف مهیا برای مردم، را نشان نداده است. بخاطر ماهیت پویای بدافزار با روش های حمله دائماً در حال تغییر، مجموعه داده های بد افزار ارائه شده برای عموم، به صورت نظام مند باید آپدیت و معیارگذاری شوند. حملات امنیت سایبری به طور تصاعدی در حال افزایش است و مکانیسم های شناسایی موجود را ناکافی می سازد و نیاز به طراحی مدل ها ورویکردهای پیش بینی مرتبط تر را افزایش می دهد. اخیراً، رویکردهای یادگیری ماشین و به ویژه تکنیک های یادگیری عمیق، به دلیل عملکرد بالای بی نظیرشان در چندین زمینه مبتنی بر پیش بینی، مورد توجه بسیاری از محققان قرار گرفته اند. به ویژه، یک LSTMجدید (حافظه کوتاه مدت طولانی)، RNNشبکه عصبی مکرر پیشنهادمی کند. و مدل های مبتنی بر (MLP پرسپترون چند لایه) با دقت طراحی شده اند تا نوع حمله را پیش بینی کنند.

معرفی :

حملات سایبری که تهدیدی فراگیر برای سازمان ها، شرکت ها، دولت ها و کشورهاهستند، در حال افزایش هستند. باافزایش تصاعدی حملات سایبری، طراحی یک مکانیسم پیش بینی که بتواندرفتارها و حملات مخرب را قبل از وقوع پیش بینی کند به یک ضرورت تبدیل می شود، اگرچه تلاش های تحقیقاتی در زمینه تشخیص حمله به بلوغ خوبی رسیده است، اما هنوز یک منطقه تحقیقاتی چالش برانگیز و بازاست. در واقع، تاکنون هیچ ابزار کارآمد و مطمئنی وجود ندارد که بتواند انواع مختلف حملات سایبری را با دقت قابل قبولی پیش بینی کند. یادگیری عمیق زیرمجموعهای از یادگیری ماشین بوده و از ساختار شبکه های عصبی برای تقلید در تصمیم گیری حل یک مسئله مشابه مغز انسان استفاده میکند، و همانکار یادگیری ماشین را انجام میدهد، ولی قابلیتهای متفاوتی در آن هوش مصنوعی یادگریی ماشی یادگیری عمیق بازسازی رفتار هوشندانه انسان توسط ماشی aامکان آمو زش خودکار یک سیستم زیرجممومعه یادگریی ماشی که در آن روش ها و الگوریتمها شبکه عصبی برای آموزش مدلها شبکه های عصبی MLPشبکه ها عصبی یکی از روشهای یادگریی عمیق است.. در مقایسه یادگی ری ماشین با یادگیری عمیق اینگونه میتوان

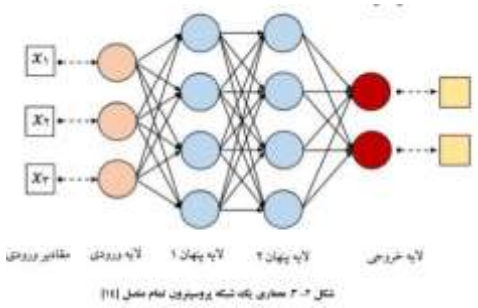
بیان کرد، در حالیکه یادگیری عمیق به طور خودکار ویژگیها را از ساختار داده ها استخراج میکند، این عمل توسط یادگیری ماشین باید به صورت دستی انجام گیرد.

LSTM(RNN) :

شبکه‌ی عصبی LSTM یا حافظه‌ی کوتاه‌مدت طولانی (Long-Short Term Memory) نوعی خاص از شبکه عصبی بازگشتی (RNN / Recurrent Neural Network) محسوب می‌شود. پس برای اینکه بتوانیم نحوه‌ی کار شبکه‌ی LSTM را درک کنیم لازم است با شبکه‌ی عصبی RNN آشنا شیم. در این مطلب به‌صورت مختصر درباره‌ی شبکه‌ی RNN صحبت کرده‌ایم و سپس به شبکه‌ی عصبی حافظه‌ی کوتاه‌مدت طولانی و نحوه‌ی کارش پرداخته‌ایم.

شبکه‌ی عصبی RNN نوعی شبکه عصبی است که حافظه‌ی داخلی دارد؛ به‌عبارت دیگر، این شبکه یک شبکه‌ی عصبی معمولی است که در ساختارش حلقه‌ای دارد که ازطریق آن در هر گام (Step) خروجی گام قبلی، به‌همراه ورودی جدید، به شبکه وارد می‌شود. این حلقه به شبکه کمک می‌کند تا اطلاعات قبلی را در کنار اطلاعات جدید داشته باشد و بتواند براساس این اطلاعات خروجی مدنظر را به ما بدهد. این ویژگی شبکه‌ی RNNاین امکان را می‌دهد که بتوانیم با داده‌های ترتیبی(Sequential Data) ، مانند متن، صدا و غیره، کار کند. حال به خاطر اینکه شبکه‌ی عصبی RNN در مسائلی که نیاز باشد حافظه‌ی بلندمدت داشته باشد نمی‌تواند خیلی‌خوب عمل کند هممیم عامل باعث شد تا lstm بوجود آید.

شبکه های پروسپترون چندلایه شبکه های پروسپترون چند لایه که باعنوان شبکه های پیشخور عمیق نیز یاد میشود دو یا چند نرون میتوانند باهم در قالب یک لایه ترکیب شوند و یک شبکه خود میتواند از چند لایه تشکل شده باشد در شبکه های پروسپترون هر نرون در هر لایه به تمام نرونها لایه بعدی متصل است و به اصطلاح اتصال در این شبکه ها به صورت تمام متصل است .در این شبکه ها با رفتن به هر لایه دیگر، جمع وزندار مجموعه نرونهای لایه قبلی محاسبه شده و پس از اعمال تابع فعالساز غیرخطی به لایه دیگر منتقل میشوند تا در نهایت به لایه خروجی برسند.



کارهای مرتبط :

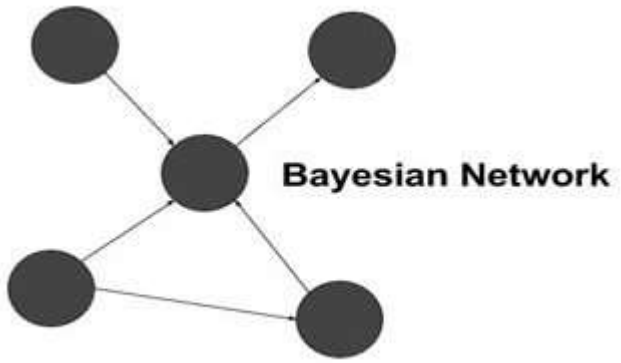
پیش بینی حملات سایبری در مقایسه با تشخیص حملات سایبری کمتر مورد توجه جامعه تحقیقاتی قرار گرفته است. میانگین متحرک یکپارچه خودرگرسیون مدل های مارکوف ، شبکه های بیضی و مدل های یادگیری، و به طور خاص مدل های یادگیری عمیق، که موفقیت خود را در مدیریت ناهمگن ثابت کرده اند . وداده های پیچیده، و توسط بسیاری از آثار در پیش بینی حملات سایبری موردتوجه قرار گرفته اند :

بخش‌های اساسی مدل HMM عبارت‌اند از:

- حالت‌های پنهان
- نمادها (یا حالت‌ها)ی مشاهده
- توزیع احتمال انتقال از حالت ابتدایی به حالت پنهان ابتدایی
- توزیع احتمال انتقال به حالت نهایی (این مورد در مدل در نظر گرفته نمی‌شود، زیرا در حالت عمومی همه‌ی احتمالات برابر با ۱ هستند).
- توزیع احتمال انتقال حالت
- توزیع احتمال تولید حالت

شبکه های بیزی :

شبکه بیزی یک گراف خطی است که در آن هر لبه مربوط به یک وابستگی مشروط است و هر گره مربوط به یک متغیر تصادفی منحصر به فرد است. به طور کل اگر یک لبه (A,B) در نمودار وجود داشته باشد به معنی وجود متغیر تصادفی A و B است، این به آن معنا است که P(A|B) یک عامل در احتمال شرطی است. بنابراین نیاز است برای نتیجه گیری P(B|A) را برای تمام مقادیر به دست آوریم. شبکه بیزی ار محاسبات احتمالی استفاده می کند. هدف این شبکه نشان دادن وابستگی های مشروط در گراف ها با استفاده از لبه ها است. به عبارت دیگر با استفاده از روابط مشخص شده توسط شبکه بیزی ما قادر هستیم تا یک توزیع احتمالی مشترک با استفاده از استقلال مشروط را بدست آوریم.



براساس اطلاعات تهدید، نویسندگان یک سیستم پیش بینی حمله شبکه را با هدف پیش بینی رفتار متجاوزان در پاسخ به (APT تهدید پایدار پیشرفته) پیشنهاد کردند. با این حال، روش پیشنهادی تنها بر APTمتمرکز است و بنابراین نمی تواند انواع دیگر حملات را پیش بینی کند.

APT :

تهدید مداوم پیشرفته (APT) نوعی حمله سایبری تحت شبکه است که یک شخص احراز هویت نشده می تواند برای مدت زمان زیادی به صورت ناشناس به شبکه دسترسی پیدا کند. هدف حملات APT صرفاً ضربه زدن به سازمان و یا اعمال خراب کارانه نیست، بلکه هدف در این گونه حملات سازمانی هایی که اطلاعات مفیدی در اختیار دارند (مانند سازمان دفاع، صنایع تولیدی و مالی و ...) است. برخلاف حملات رایج که در آن، حمله کننده تلاش می کند تا به سرعت وارد شده، اطلاعات را گرفته و سیستم را ترک کند تا سیستم های تشخیص نفوذ شانس کمتری برای یافتن این گونه حملات داشته باشند؛ در این حملات هدف ورود و خروج سریع نبوده و معمولاً این گونه حملات، مانا یا Persistent هستند. بدین منظور حمله کننده باید دائماً کدهای فایل مخرب را بازنویسی نماید و تکنیک های پنهان سازی پیچیده ای را استفاده نماید به همین دلیل به آنها Advanced گفته می شود.
فناوری اینترنتی APT توسط حمله کنندگان در بسیاری از کشورها به عنوان وسیله ای برای جمع آوری اطلاعات از فرد، گروه و افراد مشخص استفاده می شود. گفته می شود که برخی از گروه های درگیر در APTتوسط منابع متعدد دولتی به طور مستقیم یا غیرمستقیم حمایت می شوند.

حملات APT به گونه ای طراحی شده اند که اقدامات امنیتی موجود در هدف را دور بزنند و به سازمان هدف نفوذ کنند. اجرای یک حمله APT نیاز به ترکیبی از دانش های پیشرفته در مورد زیرساخت های سازمان، سیاست ها و رویه های امنیتی و استفاده از تاکتیک های پیچیده دارد. تقریباً تمام حملات APT از چرخه زیر پیروی می کنند:

پیش زمینه :

یادگیری عمیق از شبکه های عصبی مصنوعی که در سال ۱۹۴۳ توسط فیزیولوژیست عصبی وارن مک کالوچ و یک ریاضیدان جوان والتر پیتس اختراع شد، سرچشمه گرفت. این یک مدل محاسباتی است که برخی از خصوصیات را با مغز حیوانات به اشتراک می گذارد که در آن بسیاری از واحدهای ساده (به نام نورون ها) بدون واحد کنترل متمرکز به موازات کار میکنند. وزن بین نورون ها ذخیره اطلاعات طولانی مدت در شبکه های عصبی است. به روز رسانی وزن ها، راه اصلی یادگیری اطلاعات جدید توسط شبکه عصبی است

پرسپترون چندلایه MLP یک شبکه عصبی مصنوعی پیشخورANN است که از یک لایه ورودی و یک خروجی تشکیل شده است.

شبکه های عصبی سنتی فرض می کنند که ورودی و خروجی مستقل از یکدیگرهستند. با این حال، این فرض برای برخی از کاربردها مانند تشخیص گفتار و متن صادق نیست. برای مقابله با این موضوع، شبکه عصبی بازگشتی RNN برای در نظر گرفتن اطلاعات متوالی طراحی شده است RNN.نوعی شبکه عصبی است که از گذشته و حال درس می گیرد RNN .می تواند اطلاعات زمانی تعبیه شده در توالی های ورودی را مدیریت کند.

معماری مدل ها :

لایه ورودی که در آن شبکه را با داده های قابل مشاهده تغذیه می کنیم فرآیند پیش بینی بر اساس دو متغیر قابلم شاهده (مدل پایه) یا سه متغیر قابل مشاهده (مدل نگاه به عقب) خواهد بود. هر یک از این متغیرها با یک گره در لایه ورودی نمایشداده می شوند.

•اولین لایه پنهان یکی از این موارد را نشان می دهد : یک لایه منظم متراکم یا (۲) یک لایه RNN یا (۳) یک لایه .LSTM در این کار، اگر یک لایه LSTMاعمال شود، مدل حاصل را "مدل" LSTM می نامند. علاوه براین، بسته به پیکربندی ورودی، مدل "مدل پایه" LSTM یا "مدل LSTMنگاه به عقب" نامیده می شود. همین اصطلاح در مورد استفاده از یک لایه RNN نیز صدق می کند. اگر یک لایه متراکم منظم اعمال شود، مدل ها در آن مورد «مدل پایه» MLP و «مدل MLPنگاه به عقب» نامیده می شوند، زیرا توپولوژی به سادگی یک پرسپترون چند لایه (معروف به) MLP می شود.

دومین لایه پنهان یک لایه حذفی است. لایه حذف لایه ای است که درآن چندین گره به صورت تصادفی در طول آموزش غیرفعال می شوند.این تکنیک منظم سازی به طور گسترده ای برای جلوگیری از مسائل بیش از حد برازش و سپس بهبود عملکرد مدل در داده های دیده نشده استفاده می شود.

سومین لایه پنهان یک لایه متراکم است. این یک لایه منظم متشکل ازنورون های ساده است که همه به طور کامل به لایه قبلی متصل هستند.به عبارت دیگر، هر گره در آن لایه یک ورودی برای تمام گره های موجود در لایه قبلی دریافت می کند.

لایه خروجی لایه ای است که در آن تصمیم طبقه بندی گرفته می شود.همچنین یک لایه متراکم است زیرا کاملاً به لایه قبلی متصل است.در واقع در این لایه هر کلاس با یک گره نمایش داده می شود .برای طبقه بندی، کلاس مناسب.

نتایج و بحث

تمام معیارهای ارائه شده در این بخش نشان دهنده F-Measuresهستند. یادآوری می کنیم که F-Measuresمیانگین هارمونیک یادآوری و دقت است. یادآوری، دقت و اندازه گیری F در فرمول های زیر یادآوری می شودکه در آن:

- .است:تعداد نمونه هایی که در یک کلاس طبقه بندی شده و در واقع به آن‌کلاس تعلق دارند True Positive مخفف TP
- .تعدادنمونه هایی که در یک کلاس طبقه بندی شده اند و در واقع به آن کلاس‌تعلق ندارند :False Positive برای FP
- .تعدادنمونه هایی که به یک کلاس تعلق دارند اما در کلاس دیگری طبقه بندی‌می شوند :False Negative برای FN

$$\text{به‌خاطر آوردن} = \frac{TP}{FN+TP}$$

$$\text{دقت،درستی} = \frac{TP}{FP+TP}$$

$$\text{اف-اندازه گرفتن} = \frac{2*\text{به خاطر آوردن*یادآوری}}{\text{دقیق+دقت، درستی}}$$

دربخش مدل سازی، دو ورودی پیکربندی Model Back Looking- Basic Model و همچنین سه نوع توپولوژی RNN ، MLPوLSTM ارائه شد. از این رو، در مجموع شش مدل استخراج شده است. این مدل هابه شرح زیر است: مدل پایهMLP ، مدل نگاه به عقبMLP ، مدل پایه RNN، مدل نگاه به عقب RNN، مدل پایه LSTM و مدل نگاه به عقب .LSTM

فصل چهارم

معرفی :

راه کار های تجزیه و تحلیل امنیت، داده ها را از منابع متعددی جمع می کند که شامل داده های مربوط به نقاط پایانی و رفتار کاربر، برنامه های تجاری، گزارش وقایع سیستم عامل، فایروال ها، روترها، آنتی ویروس ها، اطلاعات تهدید خارجی و موارد دیگر است. ترکیب و همبستگی این داده ها به سازمان ها یک مجموعه داده اصلی برای کار می دهد و به متخصصان امنیتی این امکان را می دهد تا الگوریتم های مناسب را به کار گیرند و جستجوی سریع را برای شناسایی شاخص های اولیه حمله انجام دهند. علاوه بر این، از فن آوری های یادگیری ماشین نیز می توان برای انجام تهدید و تجزیه و تحلیل داده ها در زمان واقعی استفاده کرد.

امنیت سایبری یک نگرانی عمده برای تعداد زیادی از سازمان ها، موسسات، شرکت ها و افراد در سراسرجهان است. بیشترشبکه ها به طور گسترده از طریق اینترنت به یکدیگر متصل هستند و وسیله ای برای به اشتراک گذاری داده ها، اطلاعات، اطلاعات، نرم افزار و سخت افزار فراهم می کنند. اگرچه، به اشتراک گذاری منابع ارزشمند برای افزایش کارایی عملیاتی، الگوی شبکه های کامپیوتری را مشخص کرده است، اما منبعی یکپارچه برای انتشار آسان بدافزارها ایجاد کرده است و از این طریق، تشدید حملات سایبری در فضای سایبری رواج یافته است. این گسترش در چشم انداز تهدید، عاملی از قدرت فزاینده نیروی سایبری است که به تدریج در کنترل همه عملکردهای خانگی، تجاری و صنعتی است.

محافظت در برابر حملات سایبری به هر دو رویکرد فعال و واکنشی نیاز دارد. این رویکردها، که می توانندبه عنوان فعال و غیرفعال نیز توصیف شوند، در زمینه استفاده مرتبط هستند.

به طور کلی، تشخیص و پیش بینی حمله را می توان با استفاده از یادگیری ماشین و الگوریتم های تکاملی،و همچنین تکنیک های آماری و قوانین مرتبط به دست آورد.

رویکردهای تشخیص حمله سایبری :

تشخیص حملات سایبری یک تکنیک رایج کاهش حملات است. این شامل پاسخ دادن به یک اتصال غیرعادی برای گزارش وجود یک الگوی حمله یا نمایه در یک شبکه است. یکی از رویکردهای اصلی برای شناسایی حملات سایبری، تشخیص نفوذ است.

سیستم های تشخیص نفوذ :

سیستم تشخیص نفوذ یا IDS سیستمی است که وظیفه‌ی آن رصد ترافیک شبکه جهت شناسایی فعالیت مشکوک یا ترافیک غیرعادی است. سیستم‌های IDS با نظارت و تجزیه‌وتحلیل دائمی ترافیک شبکه اقدام به شناسایی و گزارش فعالیت‌های مشکوک و مخرب می‌کنند. گذشته از این، برخی از انواع سیستم تشخیص نفوذ به‌طور خودکار قادر به انجام اقداماتی جهت مقابله با تهدید شناسایی‌شده نیز هستند.

سیستم‌های IDS به دو نوع کلی تقسیم می‌شوند: سیستم تشخیص نفوذ مبتنی بر شبکه، و سیستم تشخیص نفوذ مبتنی برهاست یا همان میزبان. تفاوت این دو نوع در محل استقرار سیستم است. سیستم تشخیص نفوذ مبتنی بر شبکه در شبکه مستقر می‌شود و سیستم تشخیص نفوذ مبتنی برهاست بر روی رایانه کلاینت نصب می‌گردد.

لزوم استفاده از سیستم های تشخیص نفوذ:

سیستم های تشخیص نفوذ برای بسیاری از سازمانها ، ازدفاتر کوچک تا شرکت های چند ملیتی ، ضروری هستند. برخی از فواید این سیستم ها عبارتند از:

کارایی بیشتر در تشخیص نفوذ ، در مقایسه با سیستم های دستی -منبع دانش کاملی از حمالت -توانایی رسیدگی به حجم زیادی از اطالعات -توانایی هشدار نسبتا بالدرنگ که باعث کاهش خسارت می شود - دادن پاسخ های خودکار ، مانند قطع ارتباط کاربر ، فعال سازی حساب کاربر ، اعمال مجموعه دستر های خودکار و غیره -توانایی گزارش دهی.

روش های تشخیص نفوذ روشهای تشخیص مورداستفاده درسیستم های تشخیص نفوذبه دودسته تقسیم می شوند :۱ - روش تشخیص رفتار غیر عادی 2-روش تشخیص سوءاستفاده یا تشخیص مبتنی بر امضا

رویکرد یادگیری ماشین

تکنیک های یادگیری ماشینی در زمان های اخیر در شناسایی حملات سایبری رایج شده اند .یادگیری ماشین به ویژه برای تجزیه و تحلیل داده ها و پیش بینی نتیجه رویدادهای خاص بر اساس ورودیهای نمونه

موجود، که برای ساختن یک مدل مناسب برای تصمیم گیری درست استفاده می شود،کارآمد است. وظایف اصلی الگوریتم های یادگیری ماشینی طبقه بندی و پیش بینی وجود یاعدم وجود یک نمونه آموخته شده با استفاده از داده های آموزشی است. استفاده از یادگیری ماشین یدر سناریوی فعلی تشخیص حملات سایبری به بهبود فرآیند تشخیص با درجه بالایی از دقت کمک کرده است.

تکنیک های یادگیری ماشین:

یادگیری نظارت شده جنبه ای از تشخیص الگو است که از مجموعه ای از نمونه های برچسب گذاری شده به عنوان داده های آموزشی با خروجی دلخواه متناظر استفاده می کند. با نمونه های برچسب گذاری شده، یک مدل پیش بینی در مرحله آموزش برای طبقه بندی مجموعه داده های جدیدمشتق می شود. این امر با تغذیه نمونه های برچسب گذاری شده در یک الگوریتم یادگیری ماشین خاص به دست می آید.

مثل : KNN و ماشین بردار پشتیبان (SVM).

تکنیک تشخیص صفحات وب مخرب ترکیبی به صورت سلسله مراتبی ماژول های تشخیص سوءاستفاده و ناهنجاری را با هم ترکیب می کند به طوری که در اولین مرحله، هر صفحه وب توسط ماژول تشخیص سوء استفاده تجزیه و تحلیل می شود. سپس این ماژول از الگوریتم درخت تصمیم برای شناسایی صفحات وب مخرب با تطبیق ویژگی های این صفحات با الگوهای شناخته شده صفحات وب استفاده می کند.

این رویکرد با ترکیب روش های تشخیص سوء استفاده و ناهنجاری، که مکمل یکدیگر در فرآیند شناسایی نمونه های شناخته شده و ناشناخته صفحات وب مخرب هستند، نرخ تشخیص بهبود یافته٪۹۸.۸ را ایجاد کرد. در حالی که این روش قادر به دستیابی به نرخ تشخیص ٪۹۸.۸ بود، نرخ مثبتکاذب ٪۳۰.۵ را تولید کرد که یک اشکال عمده رویکرد پیشنهادی است.

KNN: Knnمخفف عبارت k nearest neighbors است و برای تخمین خروجی داده جدید(تست) از k تا نزدیک‌ترین همسایه ی نمونه تست در داده های آموزش کمک می‌گیرد.

همانطور که می‌دانیم، الگوریتمهای یادگیری ماشین نیاز به پروسه آموزش دارند، تا با کمک داده آموزش یک دانشی را بدست بیاورند و بعدا بتوانند طبق این دانش، خروجیِ داده جدید را تخمین بزنند.

SVM: این الگوریتم میتونه برای طبقه بندی های خطی یا غیر خطی، رگرسیون و حتی شناسایی داده های پرت هم استفاده بشه SVM .یکی از محبوب ترین مدل های ماشین لرنینگ هست و یادگیری این الگوریتم برای علاقه مندان ماشین لرنینگ ضروری هست SVM .ها بطور خاص مناسب طبقه بندی دیتاست های با اندازه کوچیک یا متوسط هستند.

برخی از محدودیت های شناسایی شده در این رویکرد شامل ناتوانی CANN در شناسایی حملات کاربربه ریشه U2R و ریشه به محلی R2Iاست. این ممکن است با استفاده از یک نمایش ویژگی مبتنیبر فاصله یک بعدی برای آموزش و آزمایش مدلی که در نهایت کلاس های مختلف حملات را شناسایی می کند، بی ارتباط نباشد. در انجام این کار، فرض می شود که فضای ویژگی نمی تواند به طورکامل الگوهای حملات U2Rو r2Iرا نشان دهد.

مراحل این رویکرد شامل پیش پردازش داده ها، خوشه بندیMeans-k ، آموزش و طبقه بندی است.عادی سازی یا پیش پردازش به صورت خطی داده ها را بر اساس مجموعه ویژگی های حداقل وحداکثر تبدیل می کند. این فرآیند بلافاصله توسط خوشه بندی مجموعه داده از پیش پردازش شده با استفاده از الگوریتم خوشه بندی .Means-k داده ها با تخصیص مشابه ترین داده ها به یک خوشه خاص در مجموعه داده های آزمایشی و آموزشی خوشه بندی می شوند.

رویکردیادگیری بدون نظارت

یادگیری بدون نظارت با کشف الگوها در یک مجموعه داده بدون برچسب استفاده می شود که به عنوان داده های آموزشی به منظور اتخاذ تصمیمات طبقه بندی درست در مجموعه ای از نمونه های جدیداستفاده می شود. این معمولاً شامل استفاده از خوشه ها برای شناسایی کلاس هایی است که نمونه هابه آن ها تعلق دارند.

استفاده از یادگیری بدون نظارت در این رویکرد یک تکنیک موثر برای طبقه بندی نمونه های جدید بااستفاده از آستانه برای تعریف حمله و داده های عادی در زمان ساخت مدل فراهم می کند. در این مرحله،بر اساس این واقعیت که اتصالات عادی در شبکه های ناهمگن متفاوت است، می توان یک اشکال قابل توجه رویکرد را به وضوح شناسایی کرد، و به این ترتیب پروفایل های ساختمانی با رفتار عادی می توانند به طور قابل توجهی بدتر شوند. این انحراف قابل توجه در الگوهای رفتاری و ویژگی هاییک شبکه نسبت به شبکه های دیگر می تواند منجر به یک مدل ناکارآمد شود، که همواره به معیار خوبی از تنظیم و بهینه سازی پارامتر برای مطابقت با الزامات یک محیط شبکه خاص نیاز دارد.

یادگیری بدون ناظر (Unsupervised Learning) که به‌عنوان یادگیری ماشین بدون ناظر (Unsupervised Machine Learning)نیز شناخته می‌شود از الگوریتم‌های یادگیری ماشین برای تجزیه‌وتحلیل و خوشه‌بندی مجموعه‌ی داده‌های بدون برچسب (Unlabeled) استفاده می‌کند. این الگوریتم‌ها، بدون نیاز به دخالت انسان، الگوهای پنهان یا گروه‌های مختلف موجود در داده‌ها را کشف می‌کنند.

مزایای استفاده از یادگیری بدون ناظر

مزایای استفاده از یادگیری بدون موارد را می‌توان به‌صورت کلی این‌طور برشمرد:

- یادگیری ماشین بدون ناظر همه نوع الگوی ناشناخته را در داده‌ها پیدا می‌کند؛
- روش‌های بدون ناظر به ما در یافتن ویژگی‌هایی که می‌توانند برای دسته‌بندی داده‌ها مفید باشند کمک می‌کند؛
- یادگیری بدون ناظر در لحظه و به‌صورت بی‌درنگ (Real-time) انجام می‌شود؛ بنابراین تمامی داده‌های ورودی در حین یادگیری تجزیه‌وتحلیل و برچسب‌گذاری می‌شوند؛
- یافتن داده‌های بدون برچسب راحت‌تر از داده‌های برچسب‌دار است که به مداخله‌ی انسانی نیاز دارند.

معایب استفاده از یادگیری بدون ناظر

به‌صورت کلی معایب استفاده از یادگیری بدون ناظر از این قرار است:

- نمی‌توان اطلاعات زیادی درباره‌ی نحوه‌ی مرتب‌سازی داده و طبقه‌بندی آن‌ها در خروجی به دست آورد؛ زیرا یافتن الگوهای پنهان در داده و برچسب‌گذاری آن‌ها با ماشین انجام می‌شود؛
- دقت خروجی یادگیری بدون ناظر کم است؛ زیرا کار برچسب‌گذاری داده را خود ماشین، به‌تنهایی، انجام می‌دهد و دخالت انسانی در آن وجود ندارد؛

- هیچ دانش قبلی در روش یادگیری ماشین بدون ناظر وجود ندارد؛ علاوه‌براین، تعداد کلاس‌ها نیز مشخص نیست. این امر به ناتوانی در تعیین نتایج حاصل از تجزیه‌وتحلیل می‌انجامد.

رویکردیادگیری نیمه نظارتی

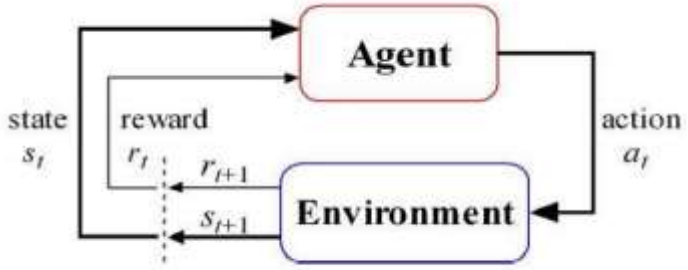
یاگیری نیمه‌نظارتی به انگلیسیSemi-supervised learning :دسته‌ای از روش‌های یادگیری ماشین است که در آن از داده‌های بدون برچسب و داده‌های برچسب‌دار به صورت هم‌زمان برای بهبود دقت یادگیری استفاده می‌شود. کاربردها تشخیص گفتار پردازش زبان طبیعی نظارت ویدئویی پیشگویی ساختار سه بعدی پروتئین فیلتر کردن هرزنامه ها انواع روش ها روش های Inductive پیشگویی برچسب نمونه هایی که تاکنون مشاهده نشده اند؛ امتحان کلاسی روش های Transductive پیشگویی بر چسب نمونه هایی که در مجموعه آموزش بکار رفته اند؛ امتحان take-home مزایا سادگی عدم وابستگی به مدل دسته بندی اشکال تقویت اشتباه در مراحل یادگیری حساس به Outlier روش‌های یادگیری نیمه‌نظارتی را در یک دسته‌بندی کلی به دسته‌های زیر می‌توان تقسیم کرد. روش‌های مولد در روش‌های مولد ابتدا یک مدل پارامتری برای تابع توزیع نقاط (مثلا توزیع گاوسی) انتخاب می‌شود که آن را با نشان می‌دهیم که در آن مدل است. سپس از روی داده‌های برچسب‌دار تخمین زده می‌شود. احتمال وقوع نقاط با توجه به تابع توزیع هر دسته، بر حسب پارامترهای مدل، به صورت تحلیلی محاسبه می‌شود. سپس با اعمال قانون بیز می‌توان تابع توزیع برچسب در هر نقطه را محاسبه کرد. در روش‌های مولد معمولاً هدف بیشینه کردن این احتمال وقوع یا به طور معادل بیشینه کردن راست‌نمایی آن‌ها نسبت به پارامترهای مدل است. از روش‌های مختلفی می‌توان برای بهینه‌کردن پارامترهای مدل نسبت به میزان راست‌نمایی استفاده کرد. در مقابل روش‌های مولد، روش‌هایی که به طور مستقیم به یادگیری می‌پردازند یا روش‌های تمایزی هستند. توجیهات نظری وجود دارد که نشان می‌دهد که روش‌های مولد نیاز به داده‌های بیشتری نسبت به روش‌های تمایزی جهت یادگیری دارند. همچنین در عمل روش‌های تمایزی موفق‌تر نشان داده‌اند. بنابراین تحقیقات روی روش‌های مولد کم‌رنگ بوده است. روش‌های مبتنی بر فرض جداسازی کم‌چگالی همانطور که گفته شد، فرض خوشه با فرض جداسازی کم چگالی معادل است. با توجه به این نکته می‌توان عبارت‌های منظم‌سازی تعریف کرد که وجود مرز طبقه‌بندی در نقاط پرچگالی را جریمه می‌کنند. به این ترتیب الگوریتم‌های زیادی برای یادگیری نیمه‌نظارتی مطرح می‌شوند. معروف‌ترین الگوریتم در این دسته از روش‌ها، الگوریتم TSVM است، که در سال ۱۹۹۸ توسط وپنیک ارائه شد. وپنیک از مفهوم ابعاد VC و قاعده‌یSRM ، برای طراحی یک مسئله بهینه‌سازی مشابه مسئله‌ی بهینه‌سازی SVM بهره گرفته است. مسئله‌ی بهینه‌سازیTSVM ،

مسئله‌ای پیچیده است و تاکنون الگوریتمی کارا برای یافتن جواب بهینه‌ی عمومی آن ارائه نشده است. روش‌های دیگری هم در حوزه‌ی استفاده صرف از فرض خوشه استفاده شده‌اند که شامل می‌شوند. همه‌ی این روش‌ها در دو خاصیت مشترکند، یکی اینکه برای طبقه‌بندی طراحی شده‌اند و اینکه طراحی آن‌ها حول مفهوم مرز جداساز و اندازه مرز بوده است. روش‌های مبتنی بر گراف این روش‌ها در صورتی مؤثر هستند که فرض همواری نیمه‌نظارتی و فرض خمینه در حالت ضعیف، هم‌زمان برقرار باشد. برای استفاده از فرض خمینه به طور صریح، باید ساختار خمینه به نحوی بیان شود. یکی از راه‌های بیان کردن ساختار خمینه در فضای با بعد بالا، استفاده از گراف‌های همسایگی است. در گراف همسایگی، رئوس همان نقاط هستند و میان نقاط نزدیک به هم روی خمینه یال با وزن متناسب قرار داده می‌شود. در روش‌های نیمه‌نظارتی مبتنی بر گراف ابتدا گراف همسایگی روی نقاط ساخته می‌شود، سپس از روشی برای تعیین برچسب نقاط بدون برچسب استفاده می‌شود. به عبارت دیگر، هر الگوریتم نیمه‌نظارتی مبتنی بر گراف شامل گام‌های کلی زیر است: ۱. پیش‌پردازش داده‌ها، که شامل استخراج ویژگی‌ها، کاهش بعد، حذف نویز و موارد دیگر می‌باشد. ۲. ایجاد گراف همسایگی مناسب روی نقاط که معمولاً لازمه‌ی آن محاسبه‌ی فاصله‌ی بین نقاط است. ۳. استنتاج برچسب نقاط بدون برچسب با یکی از روش‌های استنتاج برچسب.

رویکردیادگیری تقویتی :

یادگیری تقویتی یک رویکرد یادگیری ماشینی است که به یک عامل نرم افزاری مانند گره حسگر اجازه می دهد تا با تعامل با محیط خود یاد بگیرد ،

الشیخ و همکاران، معتقد است که یادگیری تقویتی در زمینه تشخیص الگوی مهم است زیرا به عوامل نرم افزار اجازه می دهد تا تجربیاتی را از تعاملات خود با محیط ایجاد کنند تا بهترین اقدامات را برای پاداش های طولانی مدت انجام دهند. به طورمشابه، اشاره کرد که عوامل یادگیری تقویتی پیام ها را در یک محیط ناشناخته اولیه ارسال میکنند و از اطلاعات به دست آمده برای تعریف مجدد سیاست های اقدام برای به حداکثر رساندن پاداش خود استفاده می کنند .در، الگوریتم های تقویتی مورد بحث قرار گرفته است. نویسندگان معتقدند که یادگیری تقویتی برای حل مسائل متوالی، که می تواند به عنوان فرآیندهای تصمیم مارکوف (MDPs) مدل سازیشود، و به همین دلیل برای تفسیر مسائل کنترل یادگیری مناسب است. تفسیر این مسائل معمولاً توسط الگوریتم های یادگیری نظارت شده دشوار است. یک مسئله یادگیری تقویتی معمولی در شکل ۲ نشان داده شده است.



شکل2. مدلی از مسئله یادگیری تقویتی [16]

یادگیری تقویتی یک رویکرد یادگیری ماشینی است که به یک عامل نرم افزاری مانند گره حسگر اجازه می دهد تا با تعامل با محیط خود یاد بگیرد.

برای ارزیابی عملکرد، سلسله مراتب خوشه بندی تطبیقی کم انرژی LEACH با شبیه ساز NS ۲-شبیه سازیشد تا دقت تشخیص و دفاع رویکرد را نشان دهد. معماری رویکرد به سوراخ سینک و ایستگاه پایه اجازه می دهد تا در فرآیند انتخاب مناسب ترین استراتژی برای شناسایی و پاسخ به یک حمله خود به خود، سازگار شوند. برای شناسایی حملات آینده، IDPSبه طور منظم پارامترهای یادگیری خود را با استفاده از یادگیری Q فازی در فرآیندی که به عنوان خودآموزی مداوم حملات گذشته توصیف می شود، اصلاح می کند. با توجه به این رویکرد که فقط حملات سیل DDoS را در نظرمی گیرد، ممکن است تعیین اثربخشی آن در برابر سایر اشکال حملات دشوار باشد. در نتیجه، این مدل نیاز به یک بهبود کل نگر دارد تا بر قابلیت های تصمیم گیری افزایش یافته، به ویژه با توجه به کوتاه کردن حملات جدید، تأثیر بگذارد.

یادگیری تقویتی یکی از روش‌های یادگیری ماشین است که در آن، عامل یادگیری پس از ارزیابی هر اقدام، باز خوردی به صورت پاداش و یا جریمه دریافت می‌کند. درگذشته، این روش اغلب در بازی‌ها (از جمله بازی‌های آتاری و ماریو) به‌کار گرفته می‌شد و عملکرد آن در سطح انسان و حتی گاهی فراتر از توانایی ما بود. اما در سال‌های اخیر، این الگوریتم‌های یادگیری تقویتی درنتیجه ادغام با شبکه‌های عصبی تکامل پیدا کرده و حال قادر است اعمال پیچیده‌تری از جمله حل کردن مسائل را نیز انجام دهد.

امروزه، یادگیری تقویتی با عملکردهای فرابشری، بویژه در دنیای بازی‌های کامپیوتری، که از خود نشان داده‌است، تبدیل به یکی از موضوعات به روز و برجسته هوش مصنوعی شده است. در همین راستا در این مقاله، به سازوکار و مفاهیم اصلی یادگیری تقویتی در هوش مصنوعی، الگوریتم‌ها و مواردی جهت آموزش و پیاده‌سازی آن اشاره می‌گردد. همچنین یادگیری تقویتی عمیق که تلفیقی از یادگیری تقویتی و شبکه‌های عصبی عمیق می‌باشد، نیز مورد بررسی قرار خواهد گرفت.

رویکردهای پیش بینی حمله سایبری:

پیش بینی حمله سایبری شامل پیش بینی احتمال حمله به یک محیط شبکه کنترل شده و پویا است.با توجه به هدف اصلی پیش بینی حملات سایبری (تهاجم) افزایش قابلیت های امنیتی سیستمهای دفاعی در فضای سایبری است ، برای پیش بینی حمله چند مرحله ای در دیدگاهی دیگر، الگوریتمDBSCAN ، اگرچه در برابر نویز و نقاط پرت مقاوم است، اما مستعد توصیف گرهای ضعیف و همچنین حساسیت بالا به تنظیمات پارامتر ورودیاست.

عبارت DBSCAN مخفف Density Based Spatial of Application with Noise هست . این الگوریتم تو سال ۱۹۹۶ توسط آقای Martin Ester اختراع شد. کلا این الگوریتم دو تا پارامتر مهم داره. یکی minPoints و یکی هم.Epsilon . پارامتر Epsilon نشون دهنده شعاع دایره ایه که دور هر نقطه برای تعیین چگالی اون به کار میره و همینطور minPoints حداقل تعداد داده‌ای رو نشون میده که باید تو دایره یه نقطه باشن تا اون نقطه هسته (Core) به حساب بیاد.

پیش بینی حملات را با استفاده از اپیزودهای بحرانی که یک پنجره اپیزود را فرا می گیرند،مدل می کند و در نتیجه برای ساخت درخت حمله استفاده می شود. ساخت یک درخت حمله در مدل سازی سناریوهای حمله در رویکرد آنها شامل تشخیص و پیش بینی حملات چند مرحله ای دقت ۹۵ درصدی را در هر دو مورد ایجاد کرد.

ساخت درخت های حمله می تواند برای یادگیری و استفاده ساده باشد و همچنین می تواند خروجی واضحی تولیدکند. درختان حمله را می توان برای مدل سازی فرآیند تصمیم گیری مهاجم استفاده کرد. این کار با ساختن درختی انجام می شود که به عنوان گره ریشه هدف مهاجم را داشته باشد در حالی که گره های برگ مسیرهای مختلفی را نشان می دهند که از طریق آنها می توان چنین هدفی را محقق کرد.

رویکردهای پیشگیری از حملات سایبری:

پیشگیری از حملات یک فعالیت پیشگیرانه است که تهدیدات احتمالی را در یک شبکه به سرعت شناسایی کرده و به آنها پاسخ می دهد. پیشگیری در روند کاهش حملات سایبری بسیار مهم است .اکثرروش های تشخیص واکنشی هستند و تنها پس از وارد شدن آسیب زیاد به ناحیه ضربه اعمال میشوند. چندین سیستم پیشگیری از نفوذ IPS به عنوان وسیله ای برای بهبود امنیت فضای سایبرییپیشنهاد شده است.

پیشگیری از حمله، در این مورد، با بررسی بسته های ورودی که با استفاده از Jpcap در حالت غیرقانونی گرفته شده اند، انجام می شود. هنگامی که بسته ها بررسی می شوند و پرچم SYN در بسته تنظیم می شود

و به همان آدرس مقصد در یک جریان پیوسته از ترافیک شبکه اشاره می کند، سیستمیک حمله سیل SYN را فرض می کند. اطلاعات حمله شناسایی شده در فایل log ذخیره می شودو اقدامات بعدی برای رها کردن بسته با اجرای دستور (iptables لینوکس) یاfilter-net ویندوز انجام می شود.

یکی از فراری ترین انواع حملات در فضای سایبری، حملات سیل انکارسرویس توزیع شده DDoS است که از بات نت ها (که در غیر این صورت ارتش حمله نامیده میشود) برای اختلال در خدمات ارائه شده برای کاربران واقعی یک سیستم یا شبکه استفاده می کند.بات نت ها معمولاً برای پر کردن تعداد زیادی از رایانه ها، گاهی اوقات در مقیاس جهانی با بسته های مخرب از طریق اینترنت، با بهره برداری از حفره های امنیتی که آسیب پذیری ها در این رایانه هانیز نامیده می شوند، مستقر می شوند.

بات نت ها :

بات نت مخفف چیست؟ botnet تشکیل شده از دو واژه Ro(bot) و (Net)work به معنای روبات و شبکه است که در اصطلاح رایج به شبکه‌ای گسترده از روبات‌ها اشاره دارد. فردی که مسئولیت هدایت این شبکه را بر عهده می‌گیرد به‌نام بات اصلی (botMaster) شناخته می‌شود که بیشتر منابع از اصطلاح بات مستر برای توصیف آن استفاده می‌کنند.

بات نت (BotNet) شبکه‌ای از تجهیزات الکترونیکی هوشمند است که توسط هکرها به بدافزارهایی آلوده شده‌اند و هکرها کنترل کاملی روی عملکرد این سامانه‌ها دارند. این سامانه‌ها می‌توانند کامپیوترهای شخصی، سرورها، تجهیزات سیار و حتا دوربین‌های آی‌پی باشند. بات نت‌ها می‌توانند از سخت‌افزار سامانه‌های قربانیان برای استخراج بیت‌کوین و سایر ارزهای دیجیتال استفاده کنند. از مهم‌ترین تاثیرات مخرب بات نت‌ها می‌توان به حمله به وب‌سایت‌ها، سرقت اطلاعات شخصی، ارسال هرزنامه‌ها، انتشار تبلیغات جعلی، بارگذاری بدافزار یا برنامه‌های مخرب روی دستگاه‌های مختلف و حمله به زیرساخت‌های بزرگ اشاره کرد.

باافزایش نیازهای امنیتی سازمان ها، راه حل های قوی تری برای حفاظت از فضای عظیم منابع موردنیاز است. یکی از جنبه های دستیابی به یک راه حل امنیتی پایدار، داشتن یک محصول یا رویکردمقرون به صرفه، قابل سفارشی سازی و مقیاس پذیر است. این تمرکز در رویکرد زمان واقعی پیشنهادی آنها برای شناسایی و جلوگیری از حملات است .این رویکرد، که بر اساس چارچوب مهندسی نرم افزار توسعه یافته است - تجزیه و تحلیل نیاز، طراحی،پیاده سازی و آزمایش، خروپف را در حالت درون خطی پیکربندی می کند تا به جلوگیری از نفوذدست یابد. پیکربندی خروپف در حالت درون خطی به IPS اجازه می دهد تا حسگرهای خود را درگرفتن و رها کردن بسته های مشکوک، که احتمالاً دارای بار حمله هستند، مستقر

کند. بسته های رهاشده در نهایت با Splunk ثبت می شوند. با وجود این، ناتوانی سیستم های تشخیص نفوذ و پیشگیری مبتنی بر امضا مانند Snort در شناسایی حملات ناشناخته از جمله عملکرد ضعیف آن با ترافیک سنگین شبکه یک اشکال بزرگ برای این رویکرد است .

فصل پنجم

نتیجه گیری:

امنیت مصونیت از تعرض ، تجاوز بر اساس حیطه ای است که پیرامون آن طرح می شود. فضای سایبری به مانند فضای حقیقی و ژئوپلوتیکی دارای تهدیدها و آسیب پذیری هایی است که انسان در بر خورد با آن شرایطی را برای مصونیت در یک چرخه دائمی شکل می دهد.فضای سایبر هم از آن جهت که مبانی انسان شناختی فضای تولید تکنولوژی و محتوی را در بر گرفته مخاطراتی را متوجه انسان و جامعه اسلامی می نماید. بنابر این پدافند غیر عامل به مجموعه اقداماتی اطلاق می گردد که مستلزم به کارگیری جنگ افزار نبوده و با اجرای آن می توان از وارد شدن خسارات مالی به تجهیزات و تاسیسات حیاتی و حساس نظامی و غیر نظامی و تلفات انسانی جلوگیری نموده و با میزان این خسارات و تلفات را به حداقل ممکن کاهش داد. اهمیت پدافند غیر عامل دفاع غیر عامل در واقع مجموعه تمهیدات ، اقدامات و طرح هایی است که با استفاده از ابزار ، شرایط و حتی المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت گیرد چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب دیده را با کمترین هزینه فراهم می سازد. در حقیقت طرح های پدافند غیر عامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می گردند با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح هایی فراهم می گردد ضروری است این قبیل تمهیدات در متن طراحی ها لحاظ گردند. به کارگیری تمهیدات و ملا حظات پدافند غیر عامل علاوه بر کاهش شدید هزینه ها کارآیی دفاعی طرح ها، اهداف و پروژه ها را در زمان تهاجم دشمن بسیار افز ایش خواهد داد

منابع :

۱ -مروری بر ارزیابی ریسک با استفاده از پیش بینی ریسک تکنیک در شبکه پردیس (نورخوشاینی آونگ،۱ گانتان L/A نارایانا سامی،۲ نور حفیظه حسن، -
(http://www.warse.org/IJATCSE/static/pdf/file/ijatcse3891.32020.pdf

۲ - پیش بینی حمله امنیت سایبری: رویکرد یادگیری عمیق(Ouissem Ben Fredjانستیتوی عالی علوم کاربردی و فناوری دسوس، دانشگاه سوس، تونس-علاءالدین محوب گروه سیستم اطلاعات مدیریت و مدیریت تولید، دانشکده بازرگانی و اقتصاد، - معزکریچن دانشکدهCSIT، دانشگاه البهاء، عربستان سعودی،آزمایشگاهReDCAD ، دانشگاه سفکس، تونس -)

۳ – بررسی رویکردهای امنیت سایبری برای تشخیص، پیش بینی و پیشگیری از حملات (آی ایبور موسسه آلن تورینگ – فلورانس آلابا اولادجی دانشگاه لاگوس-اولوسوجی اوکونویه دانشگاه لاگوس)

۴ – پیش بینی حملات سایبری با استفاده از عموم دادههای موجود(جورج اونوه دانشگاه ایالتی بووی بووی،مریلند)

۵ - پیش بینی حمله سایبری بر اساس سیستم های تشخیص نفوذ شبکه برای تکنیک های همبستگی هشدار: یک نظرسنجی(هاشم آلبشیر۲،۱مهیزه مد سراج،۱*، عزت مبارکعلی،۲ عمر السیر تایفور،۲ سید صالح،۳ مصعب حمدان،۴ سلیمان خان،۵ آنازیدا زینل۱ وسامیر کامرودین۲)

۶ - استراتژی امنیت سایبری پدیدآورنده (ها) : انوشا، سهیل؛ نیکجو، مهنوش؛ کولیوند، روح اله

۷ - امنیت سایبری(صحرائی محمد صالح)

۸ – امنیت داده در رایانش ابری(احمدالبوگمی- مدینی ع.السافی- رابرتوالترز، گری ویلز)

۹ -ازامنیت اطلاعات تا امنیت سایبری(روسووفون سولمز*، یوهان ون نیکرک - دانشکده فناوری اطلاعات و ارتباطات، دانشگاه متروپولیتن نلسون ماندلا، پورت الیزابت ،۶۰۳۱ آفریقای جنوبی)

۱۰ - مروری بر امنیت سایبری؛

درس هایی برای جمهوری اسلامی ایران (فصلنامه علمی ـ پژوهشی مطالعات انقلاب اسلامی)