ISSN: 2745-3673
http://www.Rcsj.ir

مجله علمی پژوهش در علوم رایانه (سال پنجم)
شماره ۱۸ / تابستان ۱۳۹۹ / ص ۸۱- ۷۴

مروری بر تامین امنیت اینترنت اشیا با استفاده از یادگیری ماشین

منا نجفی سرپیری[۱]، محمدرضا سلطان آقایی[۲]

[۱] گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان).

[۲] گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان).

نام نویسنده مسئول:
محمدرضا سلطان آقایی

تاریخ دریافت: ۱۳۹۹/۴/۱۲
تاریخ پذیرش: ۱۳۹۹/۶/۲۲

چکیده

با گسترش استفاده از اینترنت که کلیه نقاط جهان را به یکدیگر متصل نموده است، شبکه های اینترنت اشیا با اتصال دستگاه‌های مختلف به شدت مورد توجه قرار گرفتند. اینترنت اشیا یک شبکه از اشیا هستند که با حسگرها، نرم‌افزارها و سایر تکنولوژی ها و به هدف ارتباط و تبادل داده با سایر دستگاه‌ها بر روی بستر اینترنت است. اینترنت اشیا در همه حوزه‌های فنی، اجتماعی و اقتصادی تاثیر فزاینده‌ای دارد. افزایش روزافزون دستگاه‌های متصل به شبکه اینترنت اشیا باعث شد تا تهدیدات و خطرات احتمالی در این نوع شبکه ها بیش از هرچیز مورد توجه قرار گیرد. بسیاری از دستگاه‌های متصل در شبکه اینترنت اشیا اساسا ناامن هستند و در بستر اینترنت در معرض حملات مختلف قرار می‌گیرند که ممکن است منجر به آسیب-های جدی گردد. وجود خطرات و تهدیدات مختلف در فضای شبکه اینترنت اشیا باعث شد راه‌کارهای متنوعی جهت تامین امنیت این شبکه‌ها مانند حفاظت از داده‌ها، رمز نگاری، مخابرات امن، سنسور ها و الگوریتم های رمزنگاری ارائه گردد. یکی از حوزه‌هایی که می‌تواند در مبحث تامین اینترنت اشیا بسیار مورد توجه قرار گیرد استفاده از مفاهیم و الگوریتم‌های یادگیری ماشین است. توانایی یادگیری ماشین در تحلیل داده‌ها، طبقه بندی و کشف و شناسایی تهدیدات و حملات در شبکه های اینترنت اشیا، به عنوان یک لایه محافظتی در این شبکه‌ها هستند.در این مقاله برخی از تحقیقات انجام شده در خصوص راهکارهای تامین امنیت شبکه اینترنت اشیا با استفاده از الگوریتمها و مفاهیم یادگیری ماشین بررسی می‌گردد.

واژگان کلیدی: شبکه، اینترنت اشیا، امنیت شبکه، یادگیری ماشین، الگوریتم های یادگیری ماشین..

مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۱۸، تابستان ۱۳۹۹، ص ۸۱- ۷۴

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

اینترنت اشیا که به اختصار IOT [1] نامیده می‌شود، به عنوان یک شبکه توزیع شده و در عین حال پیوسته است که میتواند از طریق تکنولوژی اتصال بی سیم و یا از طریق سیم کشی منجر به برقراری یک ارتباط گردد. همچنین میتوان اینترنت اشیا را "شبکه ای از اشیاء فیزیکی یا دستگاه‌ها که دارای محاسبات محدود، ذخیره سازی و قابلیت‌های ارتباطی نامید که به وسایل الکترونیکی (مانند سنسورها و یا حسگرها)، نرم‌افزارها، اتصالات شبکه‌ای و داده‌های قابل انتقال"، تعریف کرد [۱].

کاربردهای اینترنت اشیا در زندگی روزمره انسانها به وفور دیده می‌شود. از نمونه استفاده از اینترنت اشیا در سطحی‌ترین حالت آن می‌توان به دستگاه‌های خانه هوشمند مانند لامپ، یخچال و گاز هوشمند، آداپتورهای هوشمند، کنتورهای هوشمند، سنسور دما، ردیاب دود و هزاران مورد دیگر اشاره نمود. کاربردهای اینترنت اشیا تنها به خانه هوشمند ختم نشده و در بسیاری از دستگاه‌های پیشرفته و تخصصی مانند شناسایی فرکانس رادیویی، دستگاه‌های RFID، ردیاب های ضربان قلب، شتاب سنج-ها، انواع سنسورها و غیره مورد استفاده قرار می‌گیرد [۲-۵].

اینترنت اشیا نه تنها در زندگی روزمره و فردی انسان‌ها حضور دارد بلکه در صنعت نیز شاهد استفاده از آن هستیم. مفهوم اصلی اینترنت اشیا در صنعت بهره گیری از اینترنت در سیستمهای کنترل صنعتی که به اختصار ICS [2] نامیده می‌شود، است. سیستمهای کنترل صنعتی به عنوان بخشی جدایی ناپذیر از زیرساخت های حیاتی بوده و برای مدت زمان طولانی جهت نظارت بر ماشین‌ها و فرآیندهای صنعتی مورد استفاده قرار گرفته اند. سیستمهای کنترل صنعتی وظیفه نظارت و تعامل در زمان واقعی با دستگاه ها، جمع آوری و تجزیه و تحلیل داده ها در زمان واقعی و همچنین ثبت کلیه وقایعی که در سیستم‌های صنعتی رخ می‌دهد، را بر عهده دارند. استفاده از فناوری اینترنت اشیا در این سیستم ها باعث تقویت هوش و امنیت شبکه در بهینه سازی و هدایت خودکار فرایندهای صنعتی می‌گردد [۶, ۷].

مقیاس عظیم شبکه های اینترنت اشیا چالش‌های جدیدی را به وجود می‌آورد که از نمونه این چالش‌ها میتوان به مدیریت دستگاه‌ها، حجم زیادی از داده، ذخیره سازی، ارتباطات، محاسبات و امنیت و حفظ حریم خصوصی، اشاره نمود [۸]. این چالش-ها نیاز به تحقیقات گسترده در مورد جنبه‌های مختلف استفاده از اینترنت اشیا را می‌طلبد. با وجود اهمیت کلیه چالش‌های موجود در استفاده از فناوری اینترنت اشیا، سنگ بنای تجاری سازی فناوری اینترنت اشیا بر روی امنیت و حفظ حریم در کنار جلب رضایت مشتری است. با وجودی که فناوری اینترنت اشیا منجر به امکان استفاده از فناوری‌هایی مانند شبکه‌های مبتنی بر نرم‌افزار، محاسبات ابری [3] و ... گردید، با این حال فضایی مناسب برای ایجاد مخاطرات و تهدیدها را در اختیار حمله‌کنندگان قرار می‌دهد [۹, ۱۰].

اینترنت اشیا یک تحول نوظهور در دنیای مدرن است و اگر چه ارزش‌های متعددی در زندگی افراد و صنعت ایجاد نموده-است اما نگرانی های امنیتی متعددی را نیز ایجاد کرده‌است. بسیاری از این چالش‌های امنیتی به دلیل جدید بودن بستر اینترنت اشیا هنوز ناشناخته بوده و به همین دلیل به یکی از مهمترین موضوعات مورد توجه محققان این حوزه تبدیل شده‌است و راهکارها و چارچوب‌های مختلفی در این خصوص ارائه شده است [۱۱]. از جمله این موارد میتوان به امنیت سخت‌افزاری، امنیت شبکه، حفاظت از ارتباطات، استفاده از تکنیکهای رمزنگاری و استفاده از راهکارهای مبتنی بر تحلیلهای امنیتی اشاره کرد [۱۲]. یکی از راهکارهایی که در حال حاضر به شدت مورد توجه محققان حوزه امنیت اینترنت اشیا قرار گرفته است استفاده از یادگیری ماشینی می‌باشد.

راه‌حلهای امنیتی مبتنی بر یادگیری ماشین در مقایسه با راهکارهای امنیتی سنتی اینترنت اشیا که عمدتا مبتنی بر کنترل و رمزگذاری هستند، جایگزین مناسبتری هستند. از دیدگاه تدافعی، راهکارهای سنتی نتوانسته‌اند امنیت شبکه های اینترنت اشیا را تامین کنند و به نظر می رسد استفاده از یک لایه اضافی از امنیت مبتنی بر یادگیری ماشین می تواند در تقویت

[1] Internet of Things
[2] Industrial Control Systems
[3] Cloud Computing

ISSN: 2745-3673
http://www.Rcsj.ir

امنیت این شبکه‌ها سودمند باشد [۱۳]. هدف این مقاله، بررسی راهکارهای ارائه شده در امنیت اینترنت اشیا بر مبنای استفاده از مفاهیم و الگوریتم های یادگیری ماشینی است.

امنیت در شبکه‌های اینترنت اشیا

اینترنت اشیاء سهولت استفاده از دستگاههای متصل به اینترنت و اتصال پایدار را که هر دو از فعالیتهای روزمره ما در فضای مجازی را پشتیبانی می کند. با اتصال دستگاههای بیشتر به اکوسیستم اینترنت اشیا، ریسکها و چالشهای امنیتی نیز بیشتر شده و احتمال وقوع حملات بیشتر می شود.

در حقیقت، با توجه به افزایش دستگاه‌های اینترنت اشیا که در محیط اینترنت اشیا با یکدیگر در ارتباط هستند، امکان حملات بسیار بیشتر است. ایمنی دستگاه های اینترنت اشیا در فضای سایبری یکی از چالشهای اساسی محسوب میشود [۱۴]. به عنوان مثال، با استفاده از ابزارهایی مانند موتور جستجو برای دستگاه های اینترنت اشیا ، میلیون ها دستگاه (به عنوان مثال، دوربین های امنیتی خانگی) با درگاه های مهم (به عنوان مثال، درگاه های ۱۴۳ برای پروتکل دسترسی به پیامهای اینترنتی یا ۴۴۵ برای خدمات راهنمای مایکروسافت) قابل کشف و دسترسی هستند [۱۵]. با توجه به اینکه بسیاری از کاربران دستگاه های اینترنت اشیا را بدون تغییر در اطلاعات ورود پیشفرض آن مورد استفاده قرار می دهند، شبکه اینترنت اشیا را به بستری برای نفوذ به شبکه و کاهش امنیت آن تبدیل می‌کنند. در حقیقت، با گسترش سریع استفاده از شبکه های اینترنت اشیا، پروتکل های ناامن مانند Telnet بار دیگر مورد استفاده قرار گرفته‌اند. علاوه بر این، بسیاری از این دستگاه ها در شبکه اینترنت اشیا با استفاده از شبکه های بی سیم کار می کنند که باعث می شوند این دستگاه ها در صورت عدم وجود راهکارهای مناسب امنیتی در خارج از محیط شبکه سیم کشی سنتی قابل دسترسی باشند.

نمونه های متعددی از حملات به شبکه های اینترنت اشیا وجود دارد که یکی از این موارد در [۱۶] مطرح شده است. در این مقاله به استخراج داده‌های مربوط به یک کازینو اشاره شده است که از طریق دستگاه کنترل دمای آکواریوم که به اینترنت متصل بوده است، انجام شده است. مهاجمان برای دسترسی به شبکه داخلی از این دستگاه استفاده کرده و چندین گیگابایت داده را منتقل کردند. پایگاه داده کازینو حاوی اطلاعات خصوصی در مورد ثروتمندترین مهمانان است.

اثرات نفوذ به دستگاههای اینترنت اشیا تنها افراد یا سازمانهایی که میزبان این دستگاه ها در شبکه های خود هستند را درگیر نمی کند. دستگاه های سازگار با اینترنت اشیا می توانند به عنوان بخشی از بات نت برای راه اندازی حملات محرومیت از سرویس[4] (DoS) در مقیاس بزرگ استفاده شوند [۱۷]. هزینه هایی که چنین حملاتی به سازمان ها و جامعه تحمیل می کنند، بسیار قابل ملاحظه است.

به دلیل دلایل متعددی تامین امنیت در شبکه های اینترنت اشیا دشوار و پرهزینه است [۱۸]. برای مثال، محیطی که دستگاه های اینترنت اشیا در آن مورد استفاده قرار می‌گیرند. امروزه بسیاری از دستگاه های اینترنت اشیا از اتصالات بی سیم استفاده می کنند که ممکن است در خارج از محیط شبکه داخلی آن منزل یا سازمان قابل دسترسی باشد. همچنین بروزرسانی میان‌افزارها و پچهای آسیب پذیر یکی دیگر از این دلایل است. در صورتی که به روز رسانی سیستم عامل و نرم‌افزارها به درستی انجام نشود دسترسی به شبکه اینترنت اشیا به راحتی ممکن است. یکی دیگر از این دلایل میتواند مربوط به فضای ذخیره سازی، اندازه و قدرت محاسباتی محدود دستگاه های شبکه اینترنت اشیا است. این محدودیت‌ها استفاده از کنترل‌های امنیتی که در سیستم های شبکه ای سنتی مستقر شده اند را، دشوار می کند. به همین دلایل و دلایل بسیار دیگری که وجود دارد، اهمیت به امنیت شبکه های اینترنت اشیا به یکی از مباحث روز دنیا تبدیل شده است [۱۹, ۲۰].

[4] Denial-of-Service

ISSN: 2745-3673
http://www.Rcsj.ir

یادگیری ماشینی

تهدیدات و ریسکهای موجود در شبکه های اینترنت اشیا باعث ایجاد انگیزه جهت استفاده از تکنیک های شناسایی و مسدود کردن حملات ترافیک در این شبکه ها با استفاده از یادگیری ماشین گردید. راه‌حلهای امنیتی مبتنی بر یادگیری ماشین گزینه های قابل قبولی برای جایگزینی با روشهای تامین امنیت سنتی که تمرکز آنها بر کنترل دسترسی و کدگذاری بوده است، می‌باشد [۱۳]. هرچند از دیدگاه مقابله با تهدیدات، این روشها محکوم به شکست بوده و وجود یک لایه اضافی از امنیت مبتنی بر یادگیری ماشین می تواند در تقویت امنیت سودمند باشد. روشهای یادگیری ماشین در یک دیدگاه کلی به سه دسته اصلی تقسیم شده است که عبارتند از: یادگیری نظارت شده، نظارت نشده و تقویتی، هرچند، دسته بندی های دیگری نیز وجود دارد [۱۳]. به عنوان مثال، با توجه به میزان در دسترس بودن داده های یک شبکه، این روشها میتوانند به دو دسته مبتنی بر شبکه و مبتنی بر میزبان تقسیم شوند. در [۱۵] محققان به ارائه دسته بندی ها و چگونگی ارتباط الگوریتمها و اثربخشی آنها در یادگیری ماشین اشاره نموده است. این دسته بندی ها در جدول ۱ ارائه شده است.

جدول ۱: خلاصه دسته بندی تکنیک های یادگیری ماشین [۱۵]

تکنیکهای یادگیری ماشین	روشهای یادگیری	الگوریتم های مرتبط	محدویتهای محاسبتی	نرخ از دست دادن دیتا
مبتنی بر شبکه	یادگیری نظارت شده	CNN و ADA	کم	زیاد
	نظارت نشده	DBSCAN	کم	زیاد
	تقویتی	DQN و SARSA	متوسط	زیاد
مبتنی بر میزبان	یادگیری نظارت شده	k-NN و SVM	زیاد	کم
	نظارت نشده	k-Means و GGMs	زیاد	کم
	تقویتی	Q-Learning	زیاد	متوسط

امنیت شبکه های اینترنت اشیا مبتنی بر یادگیری ماشین

همانطور که قبلا گفته شد، استفاده از قابلیتها و توانمندی‌های روشهای یادگیری ماشین منجر به بهبود امنیت در شبکه های اینترنت اشیا گردیده است. در این بخش از مقاله به مرور برخی راهکارهای امنیتی مبتنی بر یادگیری ماشین پرداخته می-شود.

یانگ و همکاران در [۲۱] به ارائه یک سیستم ایمنی برای یک مکانیسم کنترل دسترسی دو سطحی برای تامین امنیت داده های مراقبتهای بهداشتی بیماران پرداخته اند که برای هر دو شرایط عادی و اضطراری به صورت خود- سازگار عمل می کند. در کاربرد عادی، کارکنان مرکز بهداشتی با کلید های مخفی مناسب می توانند از به داده ها دسترسی داشته باشند. در شرایط اضطراری، سوابق پزشکی بیمار با استفاده از مکانیسم دسترسی شیشه- شکسته مبتنی بر رمز عبور قابل بازیابی است.

این مکانیسم کنترل دسترسی دارای ویژگی های چند وجهی مانند توانایی اشتراک گذاری داده های متقابل پلتفرم، رسیدگی به سناریوهای اضطراری و تعریف سیاست های اشتراکی مبتنی بر حقوق دسترسی است. علاوه بر این، این طرح همچنین از جابجایی هوشمند پشتیبانی می‌کند که در آن داده های اضافی برداشته می شود تا از فضای ذخیره سازی کمتر استفاده شود.

در مطالعه ای که نسا و همکارانش [۲۲] انجام داده اند، یک مکانیزم تشخیص برای داده های پرت و ناسالم در شبکه های اینترنت اشیا ارائه نموده اند. آنها از روش غیر پارامتری استفاده کرده اند که به دلیل اینکه این روشها نیازی به فضای ذخیره سازی بزرگی جهت نگهداری داده های ورودی ندارند، برای داده های شبکه اینترنت اشیا مناسب هستند. همچنین در این مطالعه از یادگیری نظارت شده مبتنی بر توالی استفاده نموده اند که برای تشخیص داده های پرت مناسب هستند. نتایج این تحقیق نشان داد که نرخ تشخیص در دیتابیس های مختلف ۹۹,۶۵٪ و ۹۸,۵۳٪ بوده است.

ISSN: 2745-3673
http://www.Rcsj.ir

در تحقیق که لی و همکارانش انجام داده اند [۲۳]، یک مکانیزم کنترل دسترسی به همراه یک روش جدید رمزگشایی کارآمد جهت ارائه کنترل دسترسی برای برنامه های اینترنت اشیا صنعتی ارائه شده است. نویسندگان در این تحقیق پیچیدگی محاسباتی را از گره های حسگر به سمت دروازه به جهت تامین کارایی برنامه ها منتقل کردند. همچنین رنامه ها. همچنین از بلاک چین برای تضمین کنترل دسترسی در اینترنت اشیا استفاده شده است.

در [۲۴] محققان به ارائه یک چارچوب مبتنی بر شبکه‌های عصبی ارائه نمودند که امکان تأیید هویت نودهای بی سیم در زمان واقعی را بر مبنای اثرات تغییر فرایند ذاتی بر خصوصیات RF فرستنده های بی سیم با استفاده از یادگیری ماشین در RX انجام می‌دهد. این مدل از چارچوب ارتباطی RF نامتقارن موجود استفاده میکند و نیازی به هیچ مدار اضافی جهت استخراج ویژگی ها ندارد. این ساز و کار کاملا شبیه عملکرد قسمت شنوایی مغز انسان است. طبق نظر محققان این چارچوب می تواند به عنوان یک ویژگی امنیتی مستقل یا به عنوان بخشی از یک سیستم احراز هویت سنتی چند فاکتوره مورد استفاده قرار گیرد.

لئو و لانگ در مقاله خود که در سال ۲۰۱۹ به چاپ رسید [۲۵] پژوهشی متفاوت در خصوص استفاده از یادگیری ماشین و یادگیری عمیق در حوزه سیتسمهای تشخیص نفوذ ارائه کردند. آنها در این مطالعه به ارائه یک طبقه بندی از سیستم‌های تشخیص نفوذ پرداختند که از اشیا داده به عنوان بعد اصلی جهت دسته بندی سیستم های تشخیص نفوذ مبتنی بر یادگیری ماشین و یادگیری عمیق استفاده می‌کند. این چارچوب طبقه بندی ابتدا مفهوم و دسته بندی سیستمهای تشخیص نفوذ را بررسی می‌کند، سپس الگوریتمهای یادگیری ماشین مورد استفاده در امنیت سایبری؛ معیارها و دیتاست‌های مرتبط را معرفی می‌کند. در مرحله بعد با استفاده از مرور ادبیات حوزه امنیت سایبری، سیستم طبقه بندی برای حل مشکلات کلیدی سیستمهای تشخیص نفوذ راهکارهایی مبتنی بر یادگیری ماشین معرفی می‌کند.

چاتری و همکارانش یک مکانیزم احراز هویت بر مبنای شبکه عصبی مصنوعی یا ANN برای شبکه های اینترنت اشیا ارائه نمودند [۲۴]. احراز هویت مبتنی بر تابع کپی ناپذیر فیزیکی میتواند در شبکه های اینترنت اشیا که ویژگی های فیزیکی فرستنده تحلیل میشوند، موثر باشد. محققان با استفاده از این ویژگی ها دقت کشف خطای سیستم خود را اندازه گیری کرده و نتیجه بررسی در ۴۸۰۰ فرستنده مشخص کرد که خطاهای کشف شده کمتر از ۰،۰۰۱ بوده و با افزایش تعداد فرستنده ها تا ۱۰۰۰۰ فرستنده، این میزان به میزان بسیار کمی و در حد ۰،۰۱ تغییر کرد. همچنین از دیدگاه بهره وری، فرستنده ها سرباری ایجاد نکردند در حالی که گیرنده ها به دو شبکه عصبی که میزان مصرف برق را ۳ تا ۵ درصد بیشتر میکند، احتیاج دارند.

در [۲۶] محققان عنوان کرده‌اند که استفاده از رفتارهای خاص شبکه‌های اینترنت اشیا (به عنوان مثال تعداد محدودی از نقاط پایانی و فاصله زمانی منظم بین پاکت‌ها) برای اطلاع از انتخاب ویژگی ها[5] و با استفاده از الگوریتم های یادگیری ماشین مانند شبکه‌های عصبی، می‌تواند منجر به تشخیص حملات محرومیت از سرویس توزیع شده (DDoS) با دقت بالا در ترافیک شبکه اینترنت اشیا شود. نتایج این تحقیق نشان می‌دهد که روترهای خانگی یا سایر میان‌افزارهای شبکه می‌توانند به طور خودکار منابع حملات محرومیت از سرویس توزیع شده در دستگاه‌های محلی اینترنت اشیا را با استفاده از الگوریتم‌های یادگیری ماشین با هزینه پایین و داده‌های ترافیکی که مبتنی بر جریان و پروتکل آگونیستی است، تشخیص دهند.

جانیس و آنتونی در [۲۷] به ارائه یک جهت تشخیص نفوذ مبتنی بر الگوریتمهای یادگیری ماشین پرداختند. آنها در این تکنیک از الگوریتم ژنتیک و ANN جهت تامین امنیت شبکه اینترنت اشیا استفاده کردند. آنها داده های دریافی از دستگاه های لبه را جمع آوری نموده و موارد غیرعادی آنها را بررسی نمودند. در طول تحقیقات ۹۹ درصد موارد از موارد غیرعادی پیش بینی شده بودند که مربوط به داده های آموزشی و مرتبط به دو نرون از ANN بودند.

در مقاله آراچیگه و همکارانش [۲۸] چارچوبی به نام PriModChain معرفی گردید که هدف آن حفظ محرمانگی و قابلیت اعتماد در داده های اینترنت اشیا صنعتی با استفاده از الگوریتم‌های ترکیبی یادگیری ماشین، بلاکچین و ... است. امکان-سنجی این چارچوب با معیارهای پنج‌گانه محرمانگی، امنیت، قابلیت اطمینان، ایمنی و بازیابی توسط شبیه سازی که با استفاده

[5] Feature Selection

ISSN: 2745-3673
http://www.Rcsj.ir

از پایتون و برنامه‌نویسی سوکت۶ بر روی یک کامپیوتر با کاربری عمومی، ارزیابی شد. همچنین برای تست این چارچوب از الگوریتم شبکه عصبی استفاده شد. PriModChian نتایج بسیار خوبی را بر مبنای پنج رکن قابل اعتماد تولید نموده و ثابت کرد که یک راه حل مناسب برای قابلیت اعتماد و حفظ محرمانگی در سیستمهای اینترنت اشیا صنعتی است.

نتیجه گیری

گسترش دسترسی به اینترنت و لزوم استفاده از شبکه ها اینترنت اشیا باعث شده است که دستگاه های متعددی از طریق این شبکه به اینترنت متصل می شوند. استفاده از اینترنت اشیا در زندگی روزمره انسانها و همچنین در صنعت نقش بسیار حیاتی و غیر قابل اجتنابی را بازی می‌کند. امروزه استفاده از اینترنت اشیا بسیار گسترده شده و همین امر منجر به ایجاد مخاطرات و تهدیدهای امنیتی بسیار گشته است. بسیاری از این دستگاه‌ها در شبکه اینترنت اشیا اساساً ناامن هستند و شبکه را در معرض انواع حملات قرار می‌دهند. از همین رو محققان به بررسی راهکارهای تامین امنیت در شبکه های اینترنت اشیا روی آورده و راهکارهای امنیتی متنوعی ارائه شد. در بین راه‌حل‌های موجود استفاده از مفاهیم یادگیری ماشین بیش از سایر روش‌ها مورد استقبال قرار گرفت زیرا این راهکارها جایگزین مناسبی برای روش‌های سنتی در حوزه امنیت هستند زیرا روش‌های سنتی عموما بر کنترل دسترسی و کدگذاری متمرکز هستند. محققان در این مقاله به بررسی برخی از مطالعات انجام شده در حوزه تامین امنیت شبکه اینترنت اشیا با استفاده از الگوریتم‌های یادگیری ماشین پرداخته‌اند.

[6] socket programming

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IOT frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8-27, 2018.
[2] N. M. Radwan, "A Study: The Future of the Internet of Things and its Home Applications," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 18, no. 1, 2020.
[3] S. Chowdhury, R. Jain, M. Thimmaiah, R. Prajwal, and K. Rakesh, "IOT based home automation and security systems: A literature survey," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 5, no. 2, 2019.
[4] H. Hosseinian, H. Damghani, L. Damghani, G. Nezam, and H. Hosseinian, "Home appliances energy management based on the IOT system," *International Journal of Nonlinear Analysis and Applications*, vol. 10, no. 1, pp. 167-175, 2019.
[5] S. P. Yadav, A. Kumbhare, and R. Parab, "Smart Home Application using Internet of Things," *perception*, vol. 6, no. 02, 2019.
[6] Z. Zhao *et al.*, "A novel framework of three-hierarchical offloading optimization for MEC in industrial IOT networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5424-5434, 2019.
[7] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015, pp. 1-6: IEEE.
[8] T. Perković, S. Damjanović, P. Šolić, L. Patrono, and J. J. Rodrigues, "Meeting Challenges in IOT: Sensing, Energy Efficiency, and the Implementation," in *Fourth International Congress on Information and Communication Technology*, 2020, pp. 419-430: Springer.
[9] K. D. Kumar, M. Sudhakara, and R. K. Poluru, "Towards the Integration of Blockchain and IOT for Security Challenges in IOT: A Review," in *Transforming Businesses With Bitcoin Mining and Blockchain Applications*: IGI Global, 2020, pp. 45-67.
[10] S. Stankovski, G. Ostojić, L. Tarjan, M. Stanojević, and M. Babić, "CHALLENGES OF IOT PAYMENTS IN SMART SERVICES," *Annals of DAAAM & Proceedings*, vol. 30, 2019.
[11] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, " IOT security: ongoing challenges and research opportunities," in *2014 IEEE 7th international conference on service-oriented computing and applications*, 2014, pp. 230-234: IEEE.
[12] K. Tabassum, A. Ibrahim, and S. A. El Rahman, "Security issues and challenges in IOT," in *2019 International Conference on Computer and Information Sciences (ICCIS)*, 2019, pp. 1-5: IEEE.
[13] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IOT security: current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, 2020.
[14] M. A. Khan and K. Salah, " IOT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018.
[15] S. Zeadally and M. Tsikerdekis, "Securing Internet of Things (IOT) with machine learning," *International Journal of Communication Systems*, vol. 33, no. 1, p. e4169, 2020.
[16] F. Mclay, "Privacy law: How to save face: Data and privacy safeguards," *Governance Directions*, vol. 70, no. 4, p. 202, 2018.
[17] M. T. Gardner, C. Beard, and D. Medhi, "Using SEIRS epidemic models for IOT botnets attacks," in *DRCN 2017-Design of Reliable Communication Networks; 13th International Conference*, 2017, pp. 1-8: VDE.
[18] L. Munoz Gonzalez and E. Lupu, "The secret of machine learning," 2018.
[19] L. E. Kane, J. J. Chen, R. Thomas, V. Liu, and M. Mckague, "Security and Performance in IOT: A Balancing Act," *IEEE Access*, vol. ,۸ pp. 121969-121986, 2020.
[20] P. Williams, P. Rojas, and M. Bayoumi, "Security Taxonomy in IOT–A Survey," in *2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2019, pp. 560-565: IEEE.

ISSN: 2745-3673
http://www.Rcsj.ir

[21] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IOT-based healthcare big data storage and self-adaptive access control system," *Information Sciences*, vol. 479, pp. 567-592, 2019.
[22] N. Nesa, T. Ghosh, and I. Banerjee, "Non-parametric sequence-based learning approach for outlier detection in IOT," *Future Generation Computer Systems*, vol. 82, pp. 412-421, 2018.
[23] F. Li, J. Hong, and A. A. Omala, "Efficient certificateless access control for industrial internet of things," *Future Generation Computer Systems* ,vol. 76, pp. 285-292, 2017.
[24] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IOT security through authentication of wireless nodes using in-situ machine learning," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388-398, 2018.
[25] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," *Applied Sciences*, vol. 9, no. 20, p. 4396, 2019.
[26] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," in *2018 IEEE Security and Privacy Workshops (SPW)*, 2018, pp. 29-35: IEEE.
[27] J. Canedo and A. Skjellum, "Using machine learning to secure IOT systems," in *2016 14th annual conference on privacy, security and trust (PST)*, 2016, pp. 219-222: IEEE.
[28] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "A trustworthy privacy preserving framework for machine learning in industrial IOT systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no ,۹ .pp. 6092-6102, 2020.