پنجمین کنفرانس ملی فناوری های نوین در مهندسی برق و کامپیوتر
۳۰ شهریور ماه ۱۴۰۱ - اصفهان
ISC پایگاه استنادی علوم جهان اسلام ۰۱۲۲۰-۹۰۱۳۵

تجزیه و تحلیل داده‌های امنیتی شبکه با قابلیت تنظیم و مقیاس‌پذیری در اینترنت اشیاء

فرهاد پوررضا ، کارشناس ارشد فناوری های نرم افزاری ، موسسه آموزش عالی سراج
pourreza@seraj.ac.ir

چکیده

در سال‌های اخیر، گرایش نسبتا زیادی به رویکردهای مربوط به مسائل امنیتی در زیرساخت اینترنت اشیا و برنامه‌های کاربردی که از یادگیری ماشین و تکنیک‌های یادگیری عمیق استفاده می‌کنند وجود دارد. پیش نیاز چنین رویکردهایی توسعه زیرساخت های مقیاس پذیر برای جمع آوری و پردازش مجموعه داده های مرتبط با امنیت از سیستم ها و دستگاه هایی است که از اینترنت اشیاء استفاده می کنند. در این مقاله راهکارهایی برای جمع‌آوری داده مقیاس‌پذیر و قابل تنظیم برای امنیت اینترنت اشیا مبتنی بر داده را معرفی خواهیم کرد که شامل مجموعه داده‌هایی از عناصر مختلف سیستم‌های اینترنت اشیا، از جمله دستگاه‌ها ، اشیاء هوشمند و بسترهای مجازی اینترنت اشیا خواهد بود. مقیاس‌پذیری زیرساختی شناخته شده است که از ادغام فناوری‌های پیشرفته برای جمع‌آوری، پخش و ذخیره‌سازی داده‌ها در مقیاس بزرگ ناشی می‌شود، در حالی که قابلیت پیکربندی آن به یک رویکرد توسعه یافته برای مدل‌سازی داده‌های امنیتی از انواع سیستم‌ها و دستگاه‌های اینرنت اشیاء متکی است. این رویکرد، نمونه‌سازی و استقرار سیستم‌های جمع‌آوری داده‌های امنیتی را بر روی زیرساخت های پیچیده اینترنت اشیا امکان‌پذیر می‌سازد، که بستری برای استفاده از الگوریتم‌های تحلیلی امنیتی موثر برای شناسایی تهدیدها، آسیب‌پذیری‌ها و الگوهای حمله می باشد.

کلمات کلیدی : اینترنت اشیاء ، امنیت داده ها ، مدل سازی داده ها ، هوش مصنوعی ، یادگیری ماشین

۱- مقدمه

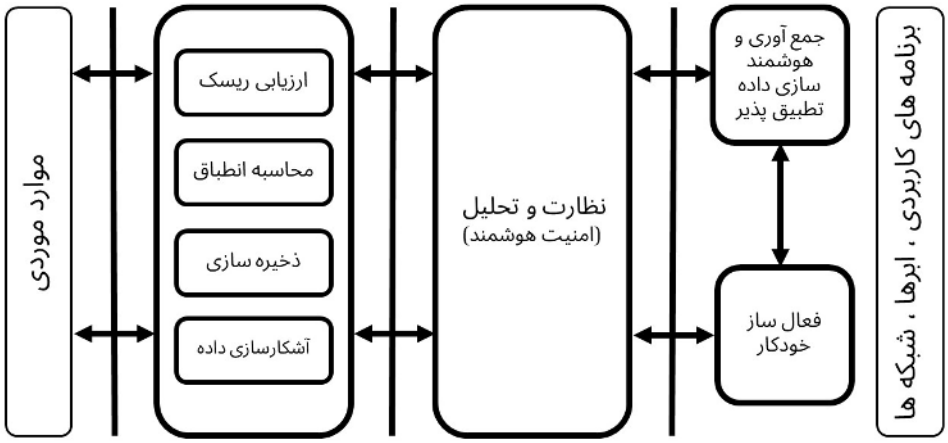
در سال‌های اخیر جهان شاهد گسترش اینترنت اشیاء بوده که عمدتاً ناشی از افزایش تعداد دستگاه‌های متصل به اینترنت است که در حال حاضر به چندین میلیارد می‌رسد [۱]. این تمایل به شبکه سازی با افزایش پیچیدگی سیستم های اینترنت اشیاء همراه بوده است. به دلیل افزایش مقیاس شبکه ها و ظهور اشیاء هوشمندی که رفتار نیمه مستقلی از خود نشان می دهند (مانند پهپادها، ربات ها و وسایل نقلیه هدایت خودکار) در این چشم انداز، توسعه دهندگان اینترنت اشیا با چالش های امنیتی فزاینده ای از جمله آسیب پذیری های بیشتر و حملات امنیتی مواجه می شوند که در مورد دوم نیازمند رویکردهای جدید و هوشمندتری برای امنیت اینترنت اشیا است، به ویژه رویکردهایی که قادر به مقابله با حملات پیچیده، غیرقابل پیش‌بینی و گاه نامتقارن در مقیاس هستند [۲]. در جستجوی رویکردهای جدید که بتواند با این پیچیدگی کنار بیاید، جامعه امنیتی اینترنت اشیا اخیراً به انواع یادگیری ماشینی [۳] و هوش مصنوعی [۴] روی آورده است. چنین رویکردهایی اخیراً برای انواع خاصی از زیرساخت‌های اینترنت

اشیا مانند شبکه‌های حسگر بی‌سیم [۵] و شبکه‌های هوشمند [۶] و برای انواع خاصی از حملات مانند شناسایی بدافزار [۷] و تشخیص نفوذ [۸] توسعه یافته‌اند. علاوه بر این، راهبردهای یادگیری متفاوتی از جمله یادگیری عمیق [۳] و یادگیری تقویتی [۹] به کار گرفته شده است. استفاده از یادگیری ماشین و رویکردهای یادگیری عمیق برای شناسایی، تجزیه و تحلیل و در برخی موارد پیش‌بینی حملات امنیتی مفهوم جدیدی نیست. رویکردهای مشابهی از نزدیک به دو دهه پیش در این چالش ظاهر شده است [۱۰]، [۱۱]. با این حال، تکامل فعلی فناوری‌های محاسباتی و ذخیره‌سازی افق‌های جدیدی را در استفاده از تکنیک‌های یادگیری ماشین و هوش مصنوعی برای امنیت اینترنت اشیا باز می‌کند. استفاده از تکنیک‌های داده کاوی (مانند یادگیری ماشین) برای نظارت و تحلیل امنیتی کاملاً با معماری‌های اصلی اینترنت اشیا، از جمله مدل‌های معماری مرجع مرتبط، همسو است. کلید پیاده‌سازی موفقیت‌آمیز چنین چرخه ای که در راستای معماری‌های فوق‌الذکر است، مشخصا یک زیرساخت مقیاس‌پذیر، قابل تنظیم و پاسخ‌گو برای جمع‌آوری و ذخیره داده‌های امنیتی مورد تجزیه و تحلیل است. با توجه به حجم بسیار زیاد، تنوع و سرعت بالقوه بالای داده‌های امنیتی، چنین زیرساخت جمع‌آوری داده‌ها باید الزاماتی مشابه آنچه برای سیستم‌های ابرداده ای بیان می‌شوند را برآورده کند. در این مقاله ما یک زیرساخت مبتنی بر ابرداده را برای جمع‌آوری، ذخیره، مدیریت و تجزیه و تحلیل داده‌های امنیتی از سیستم‌های اینرنت اشیاء را معرفی می‌کنیم. این زیرساخت به بررسی چالش‌های مقیاس‌پذیری که در بالا اشاره شد می پردازد این در حالی است که به‌منظور پشتیبانی از نظارت امنیتی برای سیستم‌های مختلف اینترنت اشیا، به‌صورت انعطاف‌پذیر قابل تنظیم خواهد بود و جنبه های زمینه ای اطلاعاتی و امنیتی را در بر می گیرد. به عنوان مثال، مقدار و نرخ داده های جمع آوری شده ممکن است به شاخص های امنیتی خاصی بستگی داشته باشد. زیرساخت جمع‌آوری داده‌های ارائه‌شده بخشی از یک سیستم نظارت، تحلیل و فعال‌سازی امنیت اینترنت اشیا گسترده‌تر است که در محدوده پروژه افق های امنیتی اینترنت اشیاء اجرا می‌شود که هدف آن ارائه خدمات امنیتی برای هدف قرار دادن سیستم‌های اینترنت اشیاء است ، بنابراین، قبل از ارائه معماری دقیق زیرساخت جمع‌آوری داده، آن را در زمینه گسترده‌تر پروژه امنیت اینترنت اشیاء قرار می‌دهیم. بسترمجازی کلی این سیستم ابزاری را برای نظارت امنیتی سرتاسر یک سیستم اینترنت اشیا، از جمله حفاظت از تمام بلوک‌های عملکردی و نقاط پایانی را فراهم می‌کند. برای این منظور، تجزیه و تحلیل های پیچیده ای در این سیستم ادغام شده که ابزاری را برای شناسایی و پیش بینی حملات به دستگاه های متصل به اینترنت، از جمله اشیاء هوشمند با رفتار پویاست. ساختار بقیه مقاله به شرح زیر است: بخش دوم بستر کلی برای نظارت بر امنیت سیستم های پیچیده اینترنت اشیا معرفی می کند و در بخش سوم جزئیاتی در مورد زیرساخت های جمع آوری داده های بستر ، از جمله بلوک های سازنده اصلی آن و اصول ساختاری پشت آن ها را ارائه خواهد کرد.

۲ - معماری مبتنی بر داده در اینترنت اشیاء

بستر مجازی اینترنت اشیاء ، امنیت داده ها را بر اساس الگوی اشیاء امن به عنوان سرویس ارائه می دهد. عملکرد این بستر با استفاده از تکنیک‌های تجزیه و تحلیل داده‌های مرتبط با امنیت که از تعدادی مؤلفه اینترنت اشیا جمع‌آوری شده هدایت می‌شود که ممکن است از دستگاه‌های ساده تا ساختارهای پیچیده اینترنت اشیا را شامل شده و چندین بستر مجازی و حوزه مدیریتی را دربرگیرد . این بستر مجازی داده‌های سیستم‌ها و دستگاه‌های موجود در اینترنت اشیاء را به منظور ارائه خدمات ارزیابی ریسک و حسابرسی انطباقی، همراه با طیف وسیعی از اتوماسیون امنیتی (به عنوان مثال، هشدارها) و خدمات تجسمی (مانند ارائه اطلاعات امنیتی در داشبورد) تجزیه و تحلیل می‌کند[13].

بستر مجازی امنیتی به طور منطقی به عنوان یک سیستم نظارت و اجرای امنیتی چند لایه ساختار یافته است. شکل ۱ نمای کلی سطح بالایی از لایه های مختلف این بستر مجازی را ارائه می دهد که شامل بخش های زیر خواهند بود:



شکل ۱ : نمونه ای از معماری سیستم نظارتی ساختاری

۱ – ۲ لایه سیستم شامل برنامه های کاربردی، ابرها و شبکه ها

این لایه شامل عناصر مختلف سیستم های اینترنت اشیا است که می توانند به عنوان منابع اطلاعات امنیتی عمل کنند. عناصر ممکن است در بسترهای مختلف اینترنت اشیا مستقرشده و دامنه های مدیریتی متعددی را در بر گیرند.

۲–۲ لایه جمع آوری ، نظارت، هوشمند و فعال سازی داده ها

این لایه وظیفه تعامل با میدان با دو رویکرد دارد: جمع آوری داده های مربوط به امنیت از عناصر ذکر شده در بالا از طریق کاوشگرهای مختلف و هدایت وظایف اتوماسیون و فعال سازی مرتبط با امنیت مانند پیکربندی ویژگی های امنیتی سیستم های اینترنت اشیا.

۲–۳ لایه نظارت و تحلیل بر داده و خدمات امنیتی

این لایه داده های جمع آوری شده را به منظور شناسایی رویدادها و شاخص های مرتبط با امنیت در قالب حوادث، تهدیدات و حملات تجزیه و تحلیل می کند. این لایه به عنوان لایه هوشمندی شناخته می شود، زیرا جایی است که استدلال هایی مبتنی بر هوش مصنوعی در زمینه امنیتی با استفاده از تکنیک های تجزیه و تحلیل داده ها انجام می شود. همچنین این لایه شامل خدمات امنیتی است که توسط بسترمجازی امن ارائه می شود، از جمله این خدمات میتوان ارزیابی ریسک ، خدمات بررسی های انطباقی و خدمات پشتیبانی از توسعه دهنده را نام برد. این لایه خدمات دیگری را نیز پیاده سازی می کند که مبتنی بر نتایج پردازش داده های لایه های امنیتی هستند، مانند خدمات هشدار و آشکارسازی داده ها .

۲–۴ لایه کاربرد و موارد موردی

این بخش از لایه خدمات امنیتی به منظور ارائه عملکردهای امنیتی برای برنامه های خاص اینترنت اشیاء استفاده می کند. در این سطح، برنامه های مختلف اینترنت اشیا از خدمات امنیتی (مثلا ارزیابی ریسک) به منظور افزایش امنیت و انعطاف پذیری سایبری خود استفاده می کنند. معماری این بستر ایجاب می‌کند که زیربخش ها در لایه‌های مختلف از طریق واسط هایی که تعریف شده‌اند، تعامل داشته باشند تا زیربخش های لایه‌های بالایی از خدمات لایه‌های پایین‌تر استفاده کنند.واسط لایه‌های امنیتی این

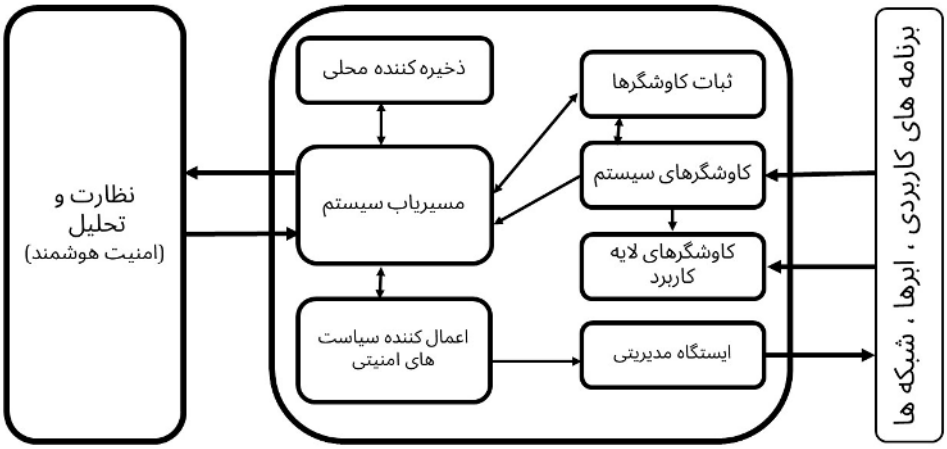
بستر مجازی بصورت سیستم های باز هستند (مانند نرم افزارهای بازمتن) ، یعنی توسط اشخاص ثالث قابل دسترسی هستند، نه اینکه فقط به صورت داخلی برای سایر زیربخش های بستر مجازی قابل مشاهده باشند.

۳- زیرساخت هایی برای جمع آوری داده ها

در این بخش زیرساخت های جمع آوری ، فعال سازی داده ها و همچنین اجزای اطلاعاتی آن را ارائه خواهیم کرد.

۱ – ۳ جمع‌آوری و فعال‌سازی داده‌ها

شکل ۲ ساختار لایه جمع‌آوری و فعال‌سازی داده‌های بسترمجازی امنیتی را با زیربخش های اصلی آن و تعاملات با سایر لایه‌های این بستریعنی سیستم‌های میدانی و لایه اطلاعات امنیتی را نشان می دهد.



شکل۲ : معماری لایه جمع‌آوری و فعال‌ساز بسترمجازی با زیربخش های اصلی و تعاملات سطح بالا

۳-۱-۱ کاوشگرهای سطح سیستم

اجزایی هستند که به منظور جمع‌آوری داده‌های مرتبط با امنیت از سیستم‌های اینترنت اشیا، مانند ترافیک شبکه روی یک میزبان یا دستگاه، استفاده از پردازنده و حافظه آن، وضعیت هر یک از زیر ماژول‌ها و رابط‌ها، تلاش‌های دسترسی از راه دور به آن و غیرهاستفاده می شوند. از نظر فیزیکی، در مواردی که دستگاه نیازهای محاسباتی و انرژی کاوشگر را برآورده می‌کند، یک کاوشگر می‌تواند در داخل سیستم یا دستگاه اینترنت اشیا قرار گیرد. با این حال، از دیدگاه سیستمی یک کاوشگر سیستم توسط مالک دستگاه با همکاری ارائه‌دهنده خدمات بستر مجازی امنیتی مستقر و مدیریت می‌شود.

۳-۱-۲ کاوشگرهای لایه کاربرد

این کاوشگرها به منظور جمع‌آوری داده‌های امنیتی مرتبط با رفتار سطح برنامه، مانند داده‌های مربوط به الگوهای حرکتی بازوی ربات یا حرکت یک ماشین مستقل متصل به اینترنت، در سیستم اینترنت اشیا مستقر می‌شوند. در بسیاری از موارد، نظارت و تجزیه و تحلیل رفتار سطح برنامه برای درک حوادث امنیتی مهم است. این امر به ویژه برای برنامه‌های اینترنت اشیا که شامل اشیاء هوشمند است (به عنوان مثال، اشیاء با رفتار نیمه مستقل) مهم است، زیرا نحوه رفتار این اشیا ممکن است نشان‌دهنده ناهنجاری‌ها باشد، به‌ویژه زمانی که رفتارها از عملکرد عادی منحرف می‌شوند. کاوشگرهای سطح کاربرد به طور جداگانه ازکاوشگرهای سطح سیستم ارائه می شوند زیرا از نظر فنی و همچنین تجاری تفاوت هایی دارند.

۳-۱-۳ ثبات کاوشگرها

کاتالوگی است که تمامی کاوشگرهای سیستم در آن ثبت می شوند. این ثبت تضمین می‌کند که سیستم نظارتی پویا است و ابزاری برای کنترل قابل اعتماد بودن مجموعه داده‌ها فراهم می‌کند، ثبت داده ها می تواند به صورت خودکار نیز انجام شود.

۳-۱-۴ مسیریاب سیستم

این بخش وظیفه انتقال داده های امنیتی از کاوشگرها به گیرندگان (یا همان مصرف کنندگان) داده های امنیتی شبکه را بر عهده دارد. برای این منظور هم با بخش ثبات برای کشف و دسترسی به کاوشگرهای موجود و هم با مؤلفه‌های مصرف‌کننده داده (یعنی برنامه‌های امنیتی) که دارای مجوزهای مناسب برای دسترسی و پردازش این داده‌ها هستند، تعامل دارد. این بخش معمولاً از طریق یک میان افزار جریان با کارایی بالا پیاده سازی می شود.

۵ -۱-۳ اعمال کننده سیاست های امنیتی

این زیربخش سیاست های امنیتی در نظر گرفته شده برای سیستم را اجرا می کند که با استفاده از تجزیه و تحلیل داده های جمع آوری شده از لایه جمع آوری و فعال سازی داده ها یا لایه اطلاعات امنیتی هدایت می شوند. تصمیم هایی که این لایه می گیرد معمولا بر دونوع هستند بخش اول تصمیمات پیکربندی جمع آوری داده که برای کاوشگرها تعیین می شوندو بخش دوم عملکردهای فعال سازی و اتوماسیون امنیتی.این بخش نقش مهمی در ویژگی‌های هوشمندی و تطبیقی فرآیند جمع‌آوری داده ایفا می‌کند، زیرا عملکردهایی را برای تغییر پیکربندی و عملکرد مجموعه داده‌ها در راستای زمینه امنیتی فراهم می‌کند[14]. نمونه هایی از عملکرد این بخش شامل بستن یک درگاه (پورت) ، غیرفعال کردن یا فعال کردن برخی از عملکردهای اجزای اینترنت اشیا و غیره است.

۱-۳-۶ ایستگاه مدیریتی

این بخش ابزاری برای تعامل با سیستم‌ها و دستگاه‌های شبکه به منظور پیاده‌سازی عملکردهای اتوماسیون و فعال‌سازی مرتبط با امنیت فراهم می‌کنند. استقرار عوامل مدیریتی مشابه کاوشگرها است، با این حال تفاوت هایی در عملکرد و ویژگی های عملیاتی آنها وجود دارد که ما را بر آن داشت تا آنها را از کاوشگرها ها متمایز کنیم.

۱-۳-۷ ابزارهای مدیریت و پیکربندی

این بخش ابزاری برای مدیریت و پیکره بندی عناصر ذکر شده در بالا فراهم می کند. به طور خلاصه پیکربندی کاوشگرها و ثبت عوامل مدیریت و عملکرد آنها را تامین می کند. کاوشگرها را می‌توان از نظر ویژگی‌های استقرار (به عنوان مثال، محل سکونت)، نرخ تحویل داده‌ها، ورود به سیستم و فیلتر کردن داده‌ها، پیکربندی کرد، به همین ترتیب، رجیستری کاوشگرهای اینترنت اشیا را می توان بر اساس کاوشگرهایی که در آن ثبت شده و ویژگی های آنها پیکربندی کرد[15].

۱-۳-۸ ذخیره‌ساز های محلی

ذخیره‌سازی محلی به بخش هایی اشاره دارد که برای پایدار سازی داده هایی که از کاوشگرها سرچشمه می‌گیرد استفاده می شوند. این بخش به‌عنوان «لبه» یا «محلی» شناخته می‌شود، زیرا وظیفه آن ذخیره داده های محلی بوده و از اطلاعات ذخیره‌شده در سطح ابر متمایز می‌شود. ذخیره‌سازی محلی داده‌های امنیتی می‌تواند اطلاعات امنیتی مبتنی بر تجزیه و تحلیل لبه و هوشمندی لبه‌ها را به عنوان ابزاری برای شناسایی و کاهش رویدادها در بازه‌های زمانی کوتاه/دقیق تسهیل کند.

۲ -۳ هوشمند سازی داده ها

هوشمند سازی داده ها معمولا عملکردهای امنیتی برای پیش بینی مشکلات شبکه بر اساس تکنیک های تجزیه و تحلیل داده را فراهم می کند. مؤلفه اطلاعات داده با داده‌های امنیتی که از کاوشگرهای مستقر جمع‌آوری شده است تغذیه شده و هشدارها، اعلان‌ها و دستورالعمل‌هایی را که برای هدایت ماژول اجرایی برای اعمال اقدامات لازم به سیستم اینترنت اشیا استفاده می‌شوند، دریافت می‌کند[16].این بخش شامل دوبخش استخراج الگو و موتورالگوهاست. مولفه استخراج الگو تجزیه و تحلیل آماری را بر روی

داده‌های امنیتی جمع‌آوری‌شده گذشته انجام می‌دهد و سعی می‌کند قوانینی را کشف کند که بر روابط بین آنها حاکم است، بخش دوم قوانین کشف شده را روی داده های امنیتی که از کاوشگرهای اینترنت اشیا جمع آوری شده را اعمال می کند. هر زمان که مقدمات یک الگو برآورده شود، نتیجه آن فعال می شود، پیامد آن ممکن است اعلام یک هشدار ،اطلاع به بخش مدیریتی، یا ارسال دستورالعملی برای بخشی از سیستم باشد.

۴- نتیجه

امروزه یادگیری ماشین و یادگیری عمیق به طور فزاینده ای برای ایمن سازی سیستم های اینترنت اشیاء به کار گرفته می شوند. این رویکردها مستلزم جمع‌آوری و مدیریت حجم بالایی از داده‌های امنیتی برای آموزش و ساختن سیستم‌های یادگیری تحت نظارت و بدون نظارت است که باید کارآمد و قادر به انطباق با زمینه‌های امنیتی مختلف و زیرساخت های شبکه باشند، بنابراین ساخت زیرساخت‌های مقیاس‌پذیربا قابلیت توسعه یک طراحی خوب برای جمع‌آوری داده‌های امنیتی از تمام عناصر مختلف که شامل سیستم‌های غیرمعمول از جمله دستگاه‌ها و زیرساخت‌های محاسبات ابری خواهند بود چالش بسیار است. این مقاله چالش های ایجاد چنین زیرساخت هایی را بررسی کرده و راه حل هایی ارائه برای آن ارائه می کند. راه حل های ارائه شده در این نوشتار قابل تنظیم، مقیاس پذیر و هوشمند هستند و از زیرساخت های ابرداده ای موجود استفاده می کنند. این مقاله برخی از اصول کلی برای طراحی زیرساخت جمع آوری داده های امنیتی را هم مورد بحث قرار داده است.

مراجع

[1] J. Soldatos et al., "*OpenIoT: Open Source Internet-of-Things in the Cloud*", In: Podnar Žarko I., Pripužić K., Serrano M. (eds.) Interoperability and Open-Source Solutions for the Internet of Things. Lecture Notes in Computer Science, vol. 9001. Springer, Cham, Mar. 2015.

[2] Aikaterini Roukounaki, "*Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data*",Global Internet of Things Summit (GIoTS). 22 July 2019

[3] U. Jayasinghe, G. M. Lee, T. Um and Q. Shi, "*Machine Learning based Trust Computational Model for IoT Services*", in IEEE Transactions on Sustainable Computing, May 2018.

[4] L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu, "*IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?*", in IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41–49, Sept. 2018.

[5] M. Abu Alsheikh, S. Lin, D. Niyato, H. P. Tan, "*Machine learning in wireless sensor networks: Algorithms strategies and applications*", IEEE Comm. Surveys Tutorials, vol. 16, no. 4, pp. 1996–2018, Apr. 2014.

[6] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, H. V. Poor, "*Machine learning methods for attack detection in the smart grid*", IEEE Trans. Neural Networks and Learning Syst., vol. 27, no. 8, pp. 1773–1786, Mar. 2015.

[7] F. A. Narudin, A. Feizollah, N. B. Anuar, A. Gani, "*Evaluation of machine learning classifiers for mobile malware detection*", Soft Computing., vol. 20, no. 1, pp. 343–357, Jan. 2016.

[8] Ma, Tao, et al., "*A Hybrid Spectral Clustering and Deep Neural Network Ensemble Algorithm for Intrusion Detection in Sensor Networks*". Sensors 16.10 (2016): 1701.

[9] M. A. Aref, S. K. Jayaweera, S. Machuzak, "*Multi-agent reinforcement learning based cognitive anti-jamming*", Proc. IEEE Wireless Communication and Networking Conf., pp. 1–6, Mar. 2017.

[10] Kruegel, C., Mutz, D., Robertson, W., Valeur. F., "*Bayesian event classification for intrusion detection*". Proc. 19th Annual Computer Security Applications Conference pp. 14–23, (2003).

[11] Sinclair, C., Pierce, L., Matzner, S., "*An application of machine learning to network intrusion detection*". Proc. 15th Annual Computer Security Applications (1999) 371–377.

[12] Z. Ma, A. Hudic, A. Shaaban and S. Plosz, "*Security Viewpoint in a Reference Architecture Model for Cyber-Physical Production Systems*", 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, 2017, pp. 153–159. doi: 10.1109/EuroSPW.2017.65.

[13] K. Schweichhart, "*Reference Architectural Model Industrie 4.0 - An Introduction*", April 2016, Deutsche Telekom,

[14] S. Schrecker, H. Soroush, J. Molina, "*Industrial Internet of Things Volume G4: Security Framework*", IIC Security Framework, IIC:PUB:G4:V1.0:PB:20160926, 2016.

[15] S Lin, M. Crawford (SAP) and S. Mellor (eds.), "*The Industrial Internet of Things: Volume G1: Reference Architecture*", Industrial Internet Consortium Reference Architecture, IIC:PUB:G1:V1.80:20170131, 2017.
[16] Ken Bever, "*The OpenO&M Information Service Bus and Common Interoperability Registry*", October 2009.