بررسی و تحلیل استراتژی های استقرار سیستم تشخیص نفوذ در شبکه های اینترنت اشیا

علیرضا مقصودیان

کارشناسی‌ارشد مهندسی فناوری اطلاعات گرایش تجارت الکترونیکی

چکیده

هدف از مقاله حاضر بررسی استراتژی های استقرار سیستم تشخیص نفوذ در شبکه های اینترنت اشیا می باشد با گسترش روزافزون اینترنت، شاهد حضور گسترده آن در تمامی حوزه های زندگی افراد هستیم. در شبکه های اینترنت اشیاء، سیستم تشخیص نفوذ می تواند در مسیریاب مرزی، در یک یا چند میزبان اختصاصی یا در هر شی فیزیکی قرار بگیرد. مزیت قرار گرفتن سیستم تشخیص نفوذ در مسیریاب مرزی تشخیص حملات نفوذی از اینترنت بر روی اشیا موجود در دامنه فیزیکی است. با این حال یک سیستم تشخیص نفوذ در مسیریاب ممکن است سربار ارتباطی بین گره های LLN و مسیریاب مرزی ایجاد کند. قرار گرفتن سیستم تشخیص نفوذ در گره های LLN ممکن است سربار ارتباطی وابسته به نظارت شبکه را کاهش دهد، ولی منابع پردازشی، ذخیره سازی و انرژی بیشتری از گره ها نیاز دارد.توزیع عامل های تشخیص نفوذ در میان برخی از گره های اختصاصی نیز ممکن است یک راه حل برای نظارت کمتر ترافیک و حجم پردازشی بیشتر باشد. با این حال تنها راه حل نیاز به سازماندهی شبکه به مناطق مختلف دارد که این مورد ممکن است خود به یک چالش تبدیل شود.

.

کلیدواژه: استراتژی ،استقرار سیستم، تشخیص نفوذ ، شبکه ، اینترنت اشیا

بیان مسئله

در سال های اخیر، محققان معماری های مختلفی را برای اینترنت اشیاء نشان دادهاند(سین و همکاران، ۲۰۱۱؛ خان و همکاران، ۲۰۱۲؛ هان و همکاران، ۲۰۱۳) که به شدت به مراحل جمع آوری ، انتقال، پردازش، مدیریت و بهره برداری وابسته هستند. اگرچه روش های ارائه شده در برخی جنبه های تفاوت دارند ولی تمام این روش ها در سه دامنه گسترده سناریوهای اینترنت اشیا سازماندهی می کنند که این دامنه ها شامل دامنه های فیزیکی، شبکه و کاربردی . دامنه فیزیکی مربوط به جمع آوری است و شامل وسایلی است که محیط فیزیکی را حس کرده و در آن فعالیت می کنند و اغلب یک LLN را تشکیل می دهند. دامنه شبکه که بر مرحله انتقال متکی است راه حل ها و پروتکل های متداول شبکه را برای انتقال داده ها از محیط فیزیکی به برنامه های کاربردی و کاربران در کنار هم گردآوری می کند. یک مسیریاب مرزی لازم است که بین دامنه های شبکه شبکه و فیزیکی قرار بگیرد تا پروتکل های LLN موجود در لایه فیزیکی را با پروتکل های متداول در دامنه شبکه ادغام و یکپارچه نماید. در نهایت، دامنه کاربردی شامل واسط هایی است که به کاربران اجازه می دهد تا به اشیاء موجود در دامنه فیزیکی رسیدگی کنند.

عبارت اینترنت اشیا اگر به شکل معنایی تعریف شود، می توان گفت به اشیای متصل به هم در سطح جهانی اشاره دارد که هر کدام از با یک شناسه منحصر به فرد شناخته می شود و با استفاده از پروتکل های استاندارد با هم ارتباط می گیرند. این تعریف تعداد بسیار زیادی از گره های متصل ناهمگن را شامل می شود (آتزوری و همکاران[1]، ۲۰۱۰). در مورد اینترنت اشیا به سختی بتوان تعریف دقیق که همه جوانب آنرا در نظر گرفته باشد، ارائه داد اما با نگاهی به گذشته می توان دید که اولین تعریف برای این اصطلاح توسط آقای کوین اشتون ارائه شده است. در مقاله ایاشتون[2](۲۰۰۹)، تعریف اصطلاح را به این شکل آورده است:« اگر رایانه هایی در دسترس داشتیم که توانایی داشتند بدون هیچ کمکی از سوی ما داده ها را خود جمع آوری کنند و به عبارتی همه چیز را درباره همه چیز می دانستند، می توانستیم رد همه چیز را بگیریم و کمیت آنها را اندازه گیری کنیم در این صورت وقت و انرژی کمتری اتلاف می شد. با این کار می توانستیم بدانیم، چه چیز، چه موقع نیاز به تعمیر، تعویض یا راه اندازی دارد. به عبارت دیگر با اینترنت اشیا جهان فیزیکی که در آن زندگی می کنیم به یک سیستم اطلاعاتی بزرگ تبدیل می شود.» با تو جه به این تعریف هدف از ایجاد چنین شبکه ای را اطلاع پیدا کردن از وضعیت همه چیز در هر زمان دانست. بر اساس گفته های گوبی و همکارانش[3] (۲۰۱۳)، اشیا به عوامل فعالی در فرآیندهای اطلاعاتی، کسب و کار و اجتماعی گفته می شود که توانایی ارتباط و تعامل با یکدیگر و محیط اطرافشان را دارند.

تشخیص نفوذ یک روش دفاعی قابل توجه برای دفاع از سیستم ها و شبکه های رایانه ای است. طبق روش های مختلف تشخیص، تشخیص نفوذ در درجه اول به سیستم های تشخیص نفوذ مبتنی بر امضا و مبتنی بر ناهنجاری تقسیم می شو د. در حال حاضر، استفاده از سیستم تشخیص نفوذ هوشمند به عنوان یک راه حل موثر برای امنیت شبکه و محافظت در برابر تهدیدات خارجی مشاهده می شو د. با این حال، سیستم تشخیص نفوذ موجود معمولا در هنگام حملات جدید میزان تشخیص کمتری دارد و هنگام کار با داده های حسابرسی، سربار بالایی دارد و بنابراین روش های یادگیری ماشین که به طور گسترده ای در تشخیص نفوذ استفاده شده است.

اینترنت اشیا برای نخستین بار در سال ۱۹۹۹ توسط کوین اشتون مورد استفاده قرار گرفت و جهانی را توصیف کرد که در آن هر چیزی، از جمله اشیا بی‌جان، برای خود هویت دیجیتال داشته باشند و به کامپیوترها اجازه دهند آن‌ها را سازمان‌دهی و مدیریت کنند. در آینده نه چندان دور بسیاری از کاربردهای اینترنت اشیا در خانه‌های هوشمند، کارخانه‌های هوشمند ، مزارع هوشمند، ادارات هوشمند، سیستم حمل‌ونقل هوشمند، بیمارستان‌های هوشمند، دانشگاه‌های هوشمند و غیره به وسیله فناوری اطلاعات به یکدیگر متصل و به کار گرفته خواهد شد(بائر، ام و جی. والوسکی[4]، ۲۰۱۳).

---

[1] Atzori et al
[2] Ashton
[3] Gubbi et al
[4] Bauer, M. and J.W. Walewski

در حال حاضر اینترنت اشیا (IoT) یک پارادایم مردمی است که جهانی را در نظر می‌گیرد که در آن انواع اشیاء فیزیکی، به اینترنت متصل می‌شوند و قادر به برقراری ارتباط با یکدیگر و همکاری برای دستیابی به اهداف مشترک هستند. این امر فراتر از ارتباطات ماشین به ماشین(M2M) است، زیرا تمامی داده‌های سنسورها یا دستگاه‌های ارسال‌کننده از طریق یک واسط اینترنت یا اینترانت به سرورها ارسال می‌شود و گیرنده‌ها(داشبوردها یا نرم‌افزارهای کاربردی) داده‌های مورد نیاز را از سرورها دریافت می‌کنند. در ارتباط ماشین به ماشین دستگاه‌ها به صورت یک به یک با یکدیگر ارتباط دارند و عملا داده‌های بسیار ما بین دستگاه‌ها تبادل نمی‌شود و محلی برای ذخیره داده‌ها وجود ندارد(دی کونینک، ای.، و همکاران[5]، ۲۰۱۵).

سه استراتژی ممکن است برای قرا رگفتن سیستم های تشخیص نفوذ باشد که به اختصار شرح داده می شوند:

قرار گرفتن سیستم تشخیص نفوذ به صورت توزیع شده

در این استراتژی سیستم های تشخیص نفوذ در هر شی فیزیکی در LLN (شبکه های کم توان و با اتلاف زیاد)قرار داده می شوند. سیستم تشخیص نفوذ در مستقر شده در هر گره باید بهینه باشد چراکه این گره ها منابع محدودی دارند. در این روش گره ها ممکن است مسئولیت نظارت همسایگان خود را نیز برعهده داشته باشند. اوو و همکاران(۲۰۱۴) روش تشخیص زودهنگام را پیشنهاد کرده اند که هدف اصلی آنها کاهش تعداد انطباق های مورد نیاز برای تشخیص حمله است. آنها رویکرد خود را با الگوریتم Wu-Manber مقایسه کرده اند که یکی از سریع ترین الگوریتم های انطباق الگو است.

قرار گرفتن سیستم تشخیص نفوذ به صورت متمرکز

در این استراتژی سیستم تشخیص نفوذ در یک جز متمرکز قرار می گیرد. به عنوان مثال در یک مسیریاب مرزی یا یک میزبان اختصاصی مستقر می شود. تمام داده هایی که گره های LLN جمع آوری می کنند، از طریق مسیریاب مرزی به اینترنت انتقال می دهند و همچنین تمام درخواست های کاربران اینترنتی نیز از طریق مسیریاب مرزی به گره های LLN ارسال می شود. بنابراین سیستم تشخیص نفوذ قرار گرفته در یک مسیریاب مرزی می تواند به تحلیل تمام ترافیک مبادله شده بین LLN و اینترنت بپردازد(رضا و همکاران، ۲۰۱۳؛ خان و فروغی، ۲۰۰۹).سیستم تشخیص متمرکز ممکن است با نظارت گره ها در حین یک حمله مشکل داشته باشد، حمله ای که بخشی از شبکه را در معرض خطر قرار می دهد.

قرار گرفتن سیستم تشخیص نفوذ به صورت ترکیبی

قرار گرفتن سیستم تشخیص نفوذ به صورت ترکیبی در واقع مفاهیم قرار گرفتن به صورت متمرکز و توزیع شده را ترکیب می کند تا از مزایای آنها بهره برده و از نقاط ضعف آنها پیشگیری کند. اولین رویکرد برای قرار گرفتن ترکیبی،شبکه را به خوشه ها یا مناطقی تقسیم کرده و سازماندهی می کند و فقط گره اصلی هر خوشه یک نمونه از سیستم تشخیص نفوذ را میزبانی می نماید. سپس این گره مسئولیت نظارت به دیگر گره های عضو خوشه خودش می شود. در این رویکرد تنها گره های انتخاب شده ای که اغلب گره های قوی تری هستند، نمونه های سیستم تشخیص نفوذ را میزبانی می کنند. از این رو قرار گرفتن سیستم های تشخیص نفوذ به صورت ترکیبی ممکن است برای مصارف منابع بیشتری نسبت به قرار گرفتن سیستم تشخیص نفوذ ها به صورت توزیع شده طراحی شده باشند. در رویکرد دوم، برای قرار گرفتن ترکیبی، ماژول های سیستم تشخیص نفوذ هم در مسریاب مرزی و هم در دیگر گره های شبکه قرار می گیرند. تفاوت اصلی این رویکرد با رویکرد اول، حضور یک جزء مرکزی است. ماژول های سیستم تشخیص نفوذ در مسیریاب مرزی مسئول انجام وظایفی هستند که ظرفیت منابع بیشتری را می طلبند در حالی که ماژول های سیستم تشخیص نفوذ در گره های معمولی اغلب به صورت سبک و کم حجم می باشند.

روش های تشخیص نفوذ

رویکردهای مبتنی بر امضا

در این رویکرد سیستم های تشخیص نفوذوقتی حملات را تشخیص می دهند که رفتار سیستم یا شبکه با امضای حمله ای مطابق داشته باشد که این امضاها در پایگاه داده های داخلی سیستم تشخیص نفوذ ذخیره شده اند. اگر هر گونه فعالیت سیستم یا شبکه با

[5] De Coninck, E., et al

امضاها یا الگوهای ذخیره شده مطابق داشته باشد، آنگاه هشداری فعال خواهد شد. این روش تهدیدات شناخته شده بسیار دقیق و موثر هستند. از معایب این روش آن است که حملات جدید را نمی توانند شناسایی کنند(لیو و همکاران، ۲۰۱۳).

رویکرد مبتنی بر ناهنجاری ها

در این رویکرد، فعالیت های هر سیستم را در هر لحظه با پروفایل رفتار عادی سیستم مقایسه می کنند و هرگاه انحرافی از رفتار عادی را بیابد که از آستانه فراتر رفته است آنگاه سیستم تشخیص نفوذ هشداری را تولید می نماید. این رویکرد برای تشخیص حملات جدید کارآمد است به ویژه حملاتی که مرتبط با سواستفاده از منابع هستند. محققان برای ایجاد نمایه ای از رفتار عادی معمولاً از روش های آماری یا الگوریتم های یادگیری ماشین استفاده می کنند. از معایب این روش آن است که هر گونه مشاهده ای که با یک رفتار عادی مطابق نداشته باشد، به عنوان یک نفوذ در نظر گرفته می شود و یادگیری کل حوزه رفتار عادی سیستم کار ساده ای نیست(چن و میتچل، ۲۰۱۴؛ دبار، ۲۰۰۲؛ میل و اسکارفون، ۲۰۰۷).

رویکردهای مبتنی بر مشخصه

مشخصه در واقع مجموعه ای از قوانین و آستانه ها است که رفتار مورد انتظار را برای اجزای شبکه از قبیل گره ها، پروتکل ها و جداول مسیریابی تعریف می کنند. رویکردهای مبتنی بر مشخصه نفوذهایی را تشخیص می دهند که در آنها رفتارهای اجزای شبکه از مشخصه های تعریف شده انحراف یافته و یا تغییر داشته باشند. بنابراین این رویکرد اهداف مشابهی را با رویکرد مبتنی بر ناهنجاری دارد. تفاوت این دو روش در این است که در روش مبتنی بر مشخصه، یک انسان متخصص باید به صورت دستی قوانین هر مشخصه را تعریف کند(آمارا و همکاران، ۲۰۱۴؛ بوتون، ۲۰۱۴).

رویکردهای ترکیبی

رویکردهای ترکیبی از مفاهیم تشخیص مبتنی بر امضا، مشخصه و ناهنجاری استفاده می کنند تا مزایای این روش ها را حداکثر رسانده و تاثیر معایب آنها را به حداقل برسانند. هدف از این نوع سیستم ارائه یک توزان بین هزینه ها ذخیره سازی در روش مبتنی بر امضا و هزینه محاسباتی در روش مبتنی بر ناهنجاری است و این رویکرد می تواند به طیف وسیع تری از حملات با یک سیستم تشخیص نفوذ تنها رسیدگی کند(پتر و کرملینگ، ۲۰۱۴).

یکی از شایع‌ترین حملات، حمله انکار سرویس(DOS) و در حالت خطرناک‌تر حملات انکار سرویس توزیع‌شده(DDOS) است. این حملات به صورت نزولی در حال رشد است. تعداد حملات انکار سرویس توزیع‌شده در سال ۲۰۱۵ در سه ماه اول سال ۳۴ درصد نسبت به سال گذشته افزایش پیدا کرده است و حملات به بیش از ۵ گیگابایت بر ثانیه رشد پیدا کرده است. حمله به سرورهای بسیاری از وب‌سایت‌های مهم نظیر توییتر، آمازون، نیویورک‌تایمز بسیاری از کارشناسان و متخصصان را بیش از پیش متوجه پتانسیل انجام این حملات کرده است(منسفیلد–دوین، اس[6]، ۲۰۱۵).

رشد اخیر اینترنت اشیاء (IoT) موجب افزایش حملات DDoS مبتنی بر اینترنت اشیاء شده است پتانسیل حملات DDoS با ظهور اینترنت اشیا (IoT) افزایش یافته است. تولیدکنندگان دستگاه‌های اینترنت اشیا علاقه‌مند به کاهش هزینه‌ها با نادیده گرفتن مقررات امنیتی هستند که موجب آسیب گسترده و مانع رشد اینترنت اشیا می‌شود. افزایش حملات DDoS مبتنی بر اینترنت اشیا، که در سال‌های اخیر شاهد آن هستیم، احتمالاً ادامه خواهد یافت تا زمانی که تولیدکنندگان IoT مسئولیت‌پذیری و مکانیسم های امنیتی را در دستگاه‌های خود قرار دهند. تا این زمان، اینترنت اشیا توانایی تبدیل شدن به محیطی برای حملات سایبری آینده را دارد و همین دلیل چالش‌ها بزرگی را ایجاد خواهد کرد(مک درموت و همکاران[7]، ۲۰۱۸).

[6] Mansfield-Devine, S
[7] McDermott

سیستم تشخیص نفوذ

سیستم تشخیص نفوذ[8] یک سیستم دفاعی است که فعالیت‌های خصمانه در یک شبکه کامپیوتری را پیدا میکند .به عبارت دیگر مهمترین مسئله در این سیستم ها این است که اغلب فعالیت‌هایی که ممکن است امنیت سیستم را به خطر بیندازد و یا کارهایی که منجر به شروع یک خرابکاری در سیستم بشود را تشخیص میدهد مانند: شناسایی اولیه اطلاعات سیستم‌ها و یا فاز جمع‌آوری داده که منجر به آسیب رساندن به سیستم میشود، مانند: عملیات اسکن پورت‌های سیستم. یک ویژگی مهم سیستم‌های تشخیص نفوذ توانایی آنها در نمایش فعالیتهای غیرفرمال در شبکه میباشد مانند تلاش کاربران برای ورود به محیط‌های غیرمجاز و اعلام خطر به مدیر سایت(اس. ویمالا و همکاران[9]، ۲۰۱۹).

علاوه بر آن یک سیستم تشخیص نفوذ این توانایی را دارد که بتواند حملاتی که از داخل یک سازمان و یا خارج از سازمان به داخل آن میشود را تشخیص دهد. برای درک بهتر دستگاه‌های تشخیص نفوذ باید گفت که برخلاف لغات و اصطلاحات بکار رفته در تعاریف بالا هر چیزی را نمیتوان در این دسته‌بندی قرارداد. به‌صورت منحصربه‌فرد ابزارهای زیر یک سیستم تشخیص نفوذ نمیباشد(هایدر و همکاران[10]، ۲۰۱۵).

ابزارهایی که برای نگهداری گزارش روزانه یک سیستم بکار میرود به‌عنوان‌مثال تشخیص انواع آسیب‌پذیری‌هایی که منجر به ازکارافتادن سیستم میشود. این ابزارها سیستم‌های مانیتور ترافیک شبکه میباشند.

ابزارهایی که برای تشخیص آسیبپذیری‌های مربوط به باگ و عیب سیستم‌های عامل و سرویس‌های شبکه بکار میروند برای مثال : Cyber Cop Scanner

ابزارهایی که برای تشخیص نرم افزارهای مخرب مانند ویروس ها، اسب های تروجان، کرم ها و بمب‌های منطقی طراحی شده‌اند. اگرچه این موارد بسیار شبیه ویژگی‌های سیستم‌های تشخیص نفوذ میباشند یا به‌عبارت‌دیگر می‌توانند زمینه را برای یک نفوذ آماده کنند(همان).

دسته‌بندی حملات

به‌طورکلی حملات را میتوان به چهار دسته زیر تقسیم‌بندی کرد:

وارسی[11]:

در این نوع از حملات شخص مهاجم برای جمع‌آوری اطلاعات و یا یافتن نقاط آسیب‌پذیر سیستم شروع به جمع‌آوری اطلاعات از سیستم یا شبکه میکند.

حمله از کار انداختن سرویس[12]:

در این حمله مهاجم آنقدر منابع سیستم را با استفاده از ابزارهایی که دارد مشغول میکند که سیستم سرویس دهنده به دلیل اتمام منابع قادر به پاسخگویی به سرویس ها نمیباشد.

حمله کاربر به ریشه[13]:

در این حمله مهاجم قصد دارد با دستیابی به نام کاربری یک کاربر مجاز در سیستم، نقاط آسیب پذیر را کشف کند.

---

[8] Intrusion Detection System
[9] S.Vimala et al
[10] Haider et al
[11] Probing
[12] Denial of Service
[13] User to Root

حمله کنترل از راه دور[14]:

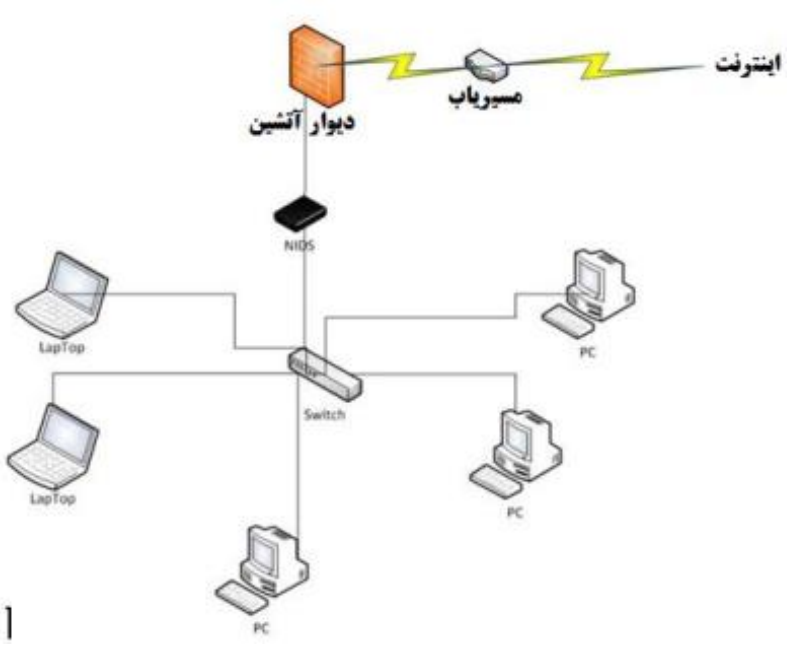
در این حمله مهاجم از راه دور و از طریق شبکه بسته هایی را به سیستم های موردنظر ارسال میکند تا بتواند نقاط آسیب‌پذیر سیستم را کشف کند(آنیرودا و همکاران[15]، ۲۰۱۷).

انواع دسته بندی سیستم های تشخیص نفوذ

سیستم‌های تشخیص نفوذ را میتوان از جهات مختلف دسته بندی کرد.

سیستم تشخیص نفوذ مبتنی بر شبکه[16]

در این سیستمها که اختصارا(NIDS) نامیده میشود، برخلاف حالت قبل به بررسی حملات روی شبکه می پردازد. طبق شکل ۲-۳علاوه بر بررسی بسته های رسیده به کارت شبکه خود به اطلاعات در حال نقل و انتقال در کل شبکه نیز میپردازد. (مثلا بسته های عبوری از روتر را موردبررسی قرار میدهد) اگر ترافیک شبکه رمز شده باشد، NIDS نمیتواند برخی از حملات را تشخیص دهد این نوع از سیستمهای تشخیص نفوذ کارایی بالایی برای تشخیص حملات DOS دارند.



شکل ۲-۳: NIDSها باید در جایی قرار داشته باشند که ترافیک کل شبکه را مورد بررسی قرار دهند(ادواردو و همکاران ، ۲۰۱۷)

مدل ترکیبی

بدیهی است بهترین حالت وقتی است که ترکیبی از دو حالت قبل یعنیNIDS وHIDS برای تشخیص حملات در شبکه داشته باشید

[14] Remote to Local
[15] Anirudha et al
[16] Network-based Intrusion Detection System

تشخیص نفوذ در اینترنت اشیا

در سالهای اخیر ، همزمان با توسعه اینترنت اشیا، سخت افزار هوشمند و واقعیت مجازی، روش تشخیص نفوذ تحت اینترنت اشیا به روندی در توسعه فناوری اطلاعات تبدیل شده است. با این حال، تحقیقات در مورد چنین مشکلی هنوز در مراحل ابتدایی است. از آنجا که می توان اینترنت اشیا را به عنوان یک شبکه ناهمگن گسترده تصور کرد، بیشتر کارهای موجود شروع به مطالعه اجزای اینترنت اشیا برای یافتن یک روش تشخیص مناسب نفوذ کرده است(فوو و همکاران[17]، ۲۰۱۷)

به دلیل محدودیت منابع موجود در IoT ، بسیاری از مکانیزمهای امنیتی برای محافظت از شبکه های اینترنت اشیا به سختی قابل اجرا هستند. سیستم تشخیص نفوذIDS ،یک تکنیک کارآمد است که میتواند برای شناسایی مهاجمان در هنگام خرابی رمزنگاری مورد استفاده قرار گیرد و میتواند برای تقویت امنیت شبکه های اینترنت اشیا استفاده شود. از آنجا که میتوان اینترنت اشیا را به عنوان یک شبکه ناهمگن گسترده تصور کرد، بیشتر کارهای موجود، شروع به مطالعه اجزای اینترنت اشیا برای یافتن یک روش تشخیص نفوذ مناسب کرده است. محققان از تئوری بازی، روش تشخیص نفوذ ترکیبی و غیره استفاده کردهاند. در این پایاننامه یک روش تشخیص نفوذ ترکیبی با استفاده روش تحلیل مولفه های اصلی و نایو بیز پیشنهاد شده است. با روش پیشنهادی می توان حملات احتمالی اینترنت اشیا را به خوبی شناسایی کرد.

پیشینه پژوهش

ایلکه هودو و همکاران در سال ۲۰۱۶ یک تجزیه و تحلیل با استفاده از شبکه عصبی مصنوعی (ANN) برای مقابله با تهدیدات در محیط اینترنت اشیا ارائه داده اند . این روش مبتنی بر شبکه عصبی برای تشخیص نفوذ در شبکه IoT برای شناسایی حملات DDoS ارائه شده است. تشخیص بر اساس طبقهبندی الگوهای طبیعی و تهدید است. مدل ANN بر روی شبکهٔ IoT شبیهسازی شده با دقت بیش از ۹۹٪ تأیید شد. آنها توانستند با موفقیت انواع مختلف حملات را شناسایی کند و عملکرد خوبی را از لحاظ نرخهای واقعی و غلط مثبت نشان دادند. اما این روش در شناسایی حملات جدید با حجم بسیار بالا مفید و کارامد نیست و با افزایش حجم اطلاعات کارایی سیستم به شدت کاهش مییابد.

تاماوتسو و کاوامورا در سال ۲۰۱۷ یک ماژول شناسایی رویداد برای حملات انکار سرویس توزیع (DDoS) در اینترنت اشیا (IoT) را پیشنهاد کرده اند. این ماژول شناسایی رویداد، میتواند در دستگاههای IoT جاسازی شود. ماژول پیشنهادی بر رفتار سیستم تحت حملات DDoSتمرکز میکند و با استفاده از اطلاعاتی که از NTP در سرویس هماهنگ زمان استفاده میشود، حملات را تشخیص میدهد. مزیت این ماژول نسبت به آنهایی که در حال حاضر، وجود دارند در این است که هیچ گونه تجهیزات گران قیمت اضافی (نظیر سرور نظارت) و تعمیرات دورهای شامل دانش فنی نیاز ندارد و این ماژول به تنگنا تبدیل نمیشود. نتایج آزمایشهای صورت گرفته نشان میدهد که ماژول پیشنهادی مقادیر فراخوانی و دقت بالا و نشان دهنده مفید بودن آن در تشخیص رویداد زمان واقعی در IoT است.

محمد بهنساوی و همکاران در سال ۲۰۱۶ الگوریتمهای رمزنگاری متقارن و غیر متقارن مورد بررسی قرار داده اند. پیادهسازی ASIC از این نوع الگوریتم انتخاب شده است. یک مقایسه کامل سختافزاری ASIC را برای برخی از الگوریتمهای امنیتی مورد استفاده در برنامههای IoT ارائه میدهد. در این مطالعه، مقایسهای انواع مختلفی از مهمترین مشخصاتی که محدودیتهای اصلی برنامههای کاربردی IOT هستند مانند مصرف انرژی، فرکانس، توان، محدوده و ایمنی علیه حملات مورد بررسی قرارگرفته است. پیادهسازی ASIC در مقایسه باAES ، ۳ DESو Two fish دارای مصرف انرژی و سطح تراشه مناسب است. از این رو، آنها را برای برنامههای IoT فوقالعاده کم مصرف توصیه میکند که بیشتر در کاربردهای پزشکی استفاده می شوند.

ادلیسون مارکوس دا سیلو کاردوسو در سال ۲۰۱۸ یک سیستم جهت تشخیص حملات DDoS که قادر به شناسایی ترافیک مخرب در زمان واقعی در محیطهای IOT با استفاده از قوانین CEP را پیشنهاد کرده است. معماری سیستم پیشنهادی مبتنی بر محاسبات لبه است. سیستم پیشنهادی باعث توسعه یک سیستم تشخیص نفوذ بر اساس مکانیزم پردازش رویداد، جهت تشخیص نفوذ در محیط IoT است.

[17] Fu et al

نتایج تجربی نشان می‌دهد که سیستم پیشنهادی عملکرد مناسبی دارد. نتایج بدست آمده نشان می‌دهد که مکانیزم CEP برای برنامه‌های کاربردی و سر ویس‌هایی که نیاز به پردازش داده‌های بزرگ دارند، مناسب است و به عنوان یک ابزار مفید برای شناسایی نفوذ در محیطهای IoT مناسب است.

شریفیان و همکاران(۱۳۹۹)[] در پژوهشی با عنوان« بهبود تشخیص نفوذ در شبکه با شناسایی ویژگی‌های مؤثر بر پایهٔ الگوریتم‌های تکاملی و دسته‌بند ماشین بردار پشتیبان» یک روش جدید برای انتخاب ویژگی‌های مؤثر در تشخیص نفوذ در شبکه، مبتنی بر الگوریتم تخمین توزیع ارائه دادند که از درخت وابستگی احتمالاتی برای شناسایی تعاملات بین ویژگی‌ها استفاده می‌کند. به‌منظور ارزیابی عملکرد این الگوریتم از مجموعه دادهٔ NSL-KDD استفاده شده است که در آن، بسته‌ها به پنج دستهٔ نرمال و نفوذهای نوعDOS ، U2R، R2Lو Prob تقسیم شده‌اند. عملکرد الگوریتم ارائه‌شده به تنهایی و به‌صورت ترکیبی با سایر الگوریتم‌های انتخاب ویژگی، مانند انتخاب پیشرو، انتخاب پسرو و الگوریتم ژنتیک، مقایسه و تأثیر پارامترهای الگوریتم، مانند اندازهٔ جمعیت بر میزان دقت تشخیص نفوذ بررسی شده است. براساس نتایج حاصل از این تحلیل و نیز ترکیب نتایج بررسی میزان دقت درون دسته‌ای حاصل از به‌کارگیری الگوریتم‌های انتخاب ویژگی متفاوت، زیرمجموعه‌ای از ویژگی‌های مؤثر در تشخیص نفوذ شناسایی شده است.

منیری و شاکری(۱۳۹۷)[] در پژوهشی با عنوان « بهبود کارایی در سیستم های تشخیص نفوذ با بهره بردن از علم اعتماد» با کمک گرفتن از علم اعتماد و استفاده از الگوریتم های مختلف طبقه بندی نشان دادند استفاده همزمان از الگوریتم های یادگیری عمیق و جنگل تصادفی به عنوان طبقه بند می تواند باعث بالا رفتن دقت و صحت انجام کار در سیستم های تشخیص نفوذ می شود.

نیک بخش(۱۳۹۵)[] در پژوهشی با عنوان « روشی ترکیبی جهت بهبود کارایی در سیستم تشخیص نفوذ مبتنی بر الگوریتم های تکامل تفاضلی و درخت تصمیم فازی» شی ترکیبی بر مبنای درخت تصمیم فازی والگوریتم تکامل تفاضلی جهت تشخیص نفوذ ارائه داد. نتایج تحقیق نشان داد که دقت روش پیشنهادی در مقایسه با سایر روش ها بهتر و بیشتر است.

عباسی و غیوری ثالث(۱۳۹۴)[] در پژوهشی با عنوان « بهبود کارایی سیستم های تشخیص نفوذ با بکار گیری داده کاوی و یادگیری ماشین» بااستفاده ازتکنیک های داده کاوی و یادگیری ماشین مدلهای مختلفی جهت بهبود کارایی سیستم های تشخیص نفوذ ارائه دادند. نتایج آنها نشان داد که مدلهای ترکیبی میتوانند حداکثر نرخ تشخیص نفوذرا باکاهش اخطارهای اشتباه به همراه شناسایی حملات جدید ارایه نمایند.

پیرزمان و کرمی اصل(۱۳۹۴)[] در پژوهشی با عنوان « ارائه روشی نوین جهت بهبود دقت تشخیص نفوذ در شبکهها با استفاده ازالگوریتمهای فازی و تکاملی» با استفاده از قوانین فازی الگوریتم کلونی مورچگان، نفوذ در سیستم را تشخیص دادند. مدل ارائه شده دارای ۲ لایه میباشد که در لایه ا ول قوانین فازی اولیه اتسخراج شده در لایه دوم توسط الگوریتم کلونی مورچگان قوانین اضافی هرس شده و مابقی باهم ترکیب میشوند و قوانین کاراتر به وجود آمده است درنهایت مدل پیشنهادی برروی مجموعه داده های NSL KDD اجرا شده و نتایج آن موردبحث و تحلیل قرار گرفته است.

چیکامکورتی و دیرو [۱۰]، در بررسی با عنوان طرح شناسایی حمله های توزیع شده با استفاده از روش های یادگیری عمقی برای اینترنت اشیا بیان کرده‌اند امنیت اینترنتی یکی از مهم ترین موضوعات برای تمام بخش های فضای اینترنتی می باشد زیرا تعداد حمله های امنیتی به مرور زمان در حال افزایش می باشد. اکنون کاملا مشخص شده است که تعداد حمله های روز صفر در حال افزایش می باشد زیرا پروتکل های مختلفی در فضای اینترنتی افزوده شده اند که عموما از اینترنت اشیا (IoT) سرچشمه می گیرند. بیشتر این حمله ها، نمونه هایی کوچک از حمله های اینترنتی است که از پیش شناخته شده اند. این موضوع نشان می دهد که حتی مکانیزم های پیشرفته مانند سیستم های یادگیری ماشینی متداول، در زمینه ی شناسایی این جهش های کوچک در نوع حمله ها در مرور زمان، با مشکل رو به رو هستند. در طرف دیگر، موفقیت روش یادگیری عمیق (DL) در زمینه های مختلف با داده های گسترده، موجب شده است که فعالان در زمینه ی فضای اینترنتی به این روش ها علاقه مند بشوند. استفاده از DL بسیار کاربردی بوده است زیرا این روش‌ها موجب بهبود CPU و ابعاد الگوریتم های شبکه های عصبی می شوند. استفاده از DL برای شناسایی حمله در فضای اینترنتی، می تواند یکی از روش های قوی برای شناسایی جهش های کوچک و یا حمله های جدید باشد زیرا این روش ها توانایی استخراج ویژگی بسیار قوی ای

دارند. ظرفیت های خود آموزی و فشردگی در معماری شبکه‌های یادگیری عمیق، مهم ترین مکانیزم های کشف الگوهای پنهان از داده های تمرینی می باشد تا این شبکه ها بتوانند حمله های اینترنتی را نسبت به جریان عادی ترافیک، تفکیک کنند. هدف این تحقیق استفاده از یک روش جدید یادگیری عمیق برای زمینه های امنیت اینترنتی بوده است تا بتوان حمله های اینترنتی در شبکه های اجتماعی اینترنت اشیا را شناسایی کرد. عملکرد این مدل یادگیری عمیق با روش های یادگیری متداول ماشینی مقایسه شده و توانایی آن ها برای شناسایی توزیع شده ی حمله ها در مقایسه با سیستم های شناسایی مرکزی، ارزیابی شده است. آزمایش ها نشان می‌دهد که سیستم توزیع شده ی شناسایی حمله که ارائه شده است، نسبت به سیستم های شناسایی مرکزی با استفاده از مدل های یادگیری عمیق، عملکرد بهتری دارند. همچنین در این بررسی نشان داده شده است که مدل های یادگیری عمیق نسبت به دیگر روش های غیر عمقی، عملکرد بهتری دارد.

در بررسی هو[۱۱]، روی تحلیل آماری فایل های قابل اجرا مطالعه انجام شده است و بر پایه بیزین و ماشین بردار پشتیبان و درخت تصمیم برپایهngram مقایسه صورت گرفته است که کار رده بندی گروهی را روی windowsapicall انجام می دهد و از فایل های‌قابل اجرا استخراج می گردد.

درمطالعه ژانگ [۱۲]، الگوریتم های انتخاب ویژگی را برای بدست آوردن مجموعه های ویژگی از فایل های pe بکار رفته است واز شبکه های عصبی مصنوعی برای تشخیص بد افزارهای جدید و ناشناس استفاده شده است.درسالهای اخیر تلاشهای تحقیقاتی محدودی برای تشخیص بد افزار با استفاده از یادگیری ژرف صورت‌گرفته است. نمودارهای پیش کنترلی را برای ارایه نمونه های بد افزاراستخراج کرد و از مدل، احتمالات‌پیچیده برای مقایسه شباهت ها بین نمونه های بد افزاراستفاده شده است.

در بررسی لی و همکاران[۱۳] یک روش تشخیص حملات مخرب ترکیبی براساس خودرمزگذار و شبکه عصبی عمیق بلیف‌پیشنهاد شده است که در آن خودرمزگذار برای کاهش بعد پذیری داده استفاده می‌شود و مورد دیگر برای تشخیص کد آسیب رسان است یعنی خودرمزگذار در دو نقش در شبکه ایفای نقش می کند. این پژوهش براساس یک مجموعه نمونه بزرگ و واقعی از مرکز امنیتی comodo cloud استفاده شده است تا یک ساختار پیچیده فراگیری را با مدلsaes جهت آموزش ویژگی های اصلی بد افزار ونهایتا تشخیص بد افزار ناشناس استفاده شود.

سوناوان و همکاران(۲۰۱۰)[] برای تشخیص نفوذ مبتنی بر سوء استفاده ، دو روش بر پایه شبکه عصبی ارائه داده اند. نخستین روش، استفاده از شبکه عصبی با داده های کمتر و استفاده از شبکه عصبی با همه ویژگی های پایگاه داده است. بر طبق نتایج به بدست آمده ، بکارگیری ویژگی های کمتر در پایگاه **KDDCUP99** پارامترهای زمان و حافظه لازم برای تشخیص نفوذ را بهبود می بخشد.

نسخ و همکاران(۲۰۱۶) [] یک سیستم کشف نفوذ با استفاده از الگوریتم آنالیز اجزای اصلی برای کاهش تعداد ویژگی ها به منظور پایین آوردن پیچیدگی سیستم و استفاده از ماشین بردار پشتیبان برای دسته بندی کردن نمونه ها معرفی شده است. سیستم پیشنهادی ، سرعت پردازش کشف نفوذ را بالا برد و فضای حافظه لازم را به مراتب کاهش داده است.

شکوه سلجوقی و میروزیری(۲۰۱۹)[] در پژوهشی با عنوان بهبود کارایی سیستم تشخیص نفوذ با استفاده از شبکه‌های عصبی و الگوریتم بهینه‌سازی ازدحام ذرات؛ پیش‌پردازش بر روی مجموعه داده**KDD - CUP** ۹۹، **NSL - KDD**و **CIDD** برای انتخاب زیرمجموعه‌ای از ویژگی‌ها، کاهش ابعاد و سپس نرمال کردن داده‌ها انجام داده اند. ترکیبی از الگوریتم بهینه‌سازی ازدحام ذرات و الگوریتم های شبکه عصبی برای تشخیص حملات نفوذ استفاده می‌شوند که می‌تواند حملات را به طور موثر طبقه‌بندی کرده و تعداد آژیر کاذب را کاهش داده و میزان تشخیص را بهبود بخشد. نتایج **Obtained** نشان می‌دهد که روش پیشنهادی صحت و کارایی بالاتری را با الگوریتم‌های دیگر برای تشخیص کلاس‌های مختلف حملات فراهم می‌کند.

کونگیان خو و همکاران در سال ۲۰۱۸ برای بهبود عملکرد سیستم های تشخیص نفوذ شبکه(IDS) ، تئوری یادگیری عمیق را جهت تشخیص نفوذ و یک مدل شبکه عمیق با قابلیت استخراج خودکار را پیشنهاد داده است. ویژگی‌های نفوذ مربوط به زمان را در نظر گرفته است و یک سیستم تشخیص نفوذ جدید ارائه داده است که شامل یک شبکه عصبی بازگشتی (RNN) با واحدهای مکرر گسسته (GRU)، یکپارچه‌سازی چند لایه (MLP) و ماژول softmax است. آنها در آزمایش‌های مقایسه‌ای نشان داده‌اند که GRU به عنوان یک واحد حافظه برای سیستم تشخیص نفوذ از LSTM مناسب تر است. همچنین در نتایج خود نشان داده‌اند که با استفاده از GRU دو طرفه می‌تواند بهترین عملکرد را در مقایسه با روش‌های اخیر به دست آورد.

چانلانگ ین و همکاران در سال ۲۰۱۷ به بررسی نحوه مدل‌سازی یک سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق پرداخته‌اند و یک روش یادگیری عمیق برای تشخیص نفوذ با استفاده از شبکه‌های عصبی مکرر (RNN-IDS) پیشنهاد کرده‌اند. علاوه بر این، عملکرد مدل در کلاس‌های دوتایی و چند کلاس و تعداد نورون ها و تأثیرات مختلف یادگیری بر عملکرد مدل پیشنهادی را مورد مطالعه قرار داده‌اند. آنها روش کار خود را با شبکه عصبی مصنوعی، جنگل تصادفی، ماشین بردار پشتیبانی و سایر روش‌های یادگیری ماشین که توسط محققان قبلی ارائه شده است مقایسه کرده‌اند. نتایج تجربی آنها نشان می‌دهد که مدل پیشنهادی (RNN-IDS)برای مدل‌سازی، یک مدل طبقه‌بندی با دقت بالا و مناسب است و عملکرد آن بهتر از روش های طبقه‌بندی یادگیری ماشین سنتی است. انها معتقد بودند که مدل پیشنهادی(RNN-IDS)صحت تشخیص نفوذ را بهبود می‌بخشد و یک روش تحقیق جدید برای تشخیص نفوذ فراهم می‌کند.

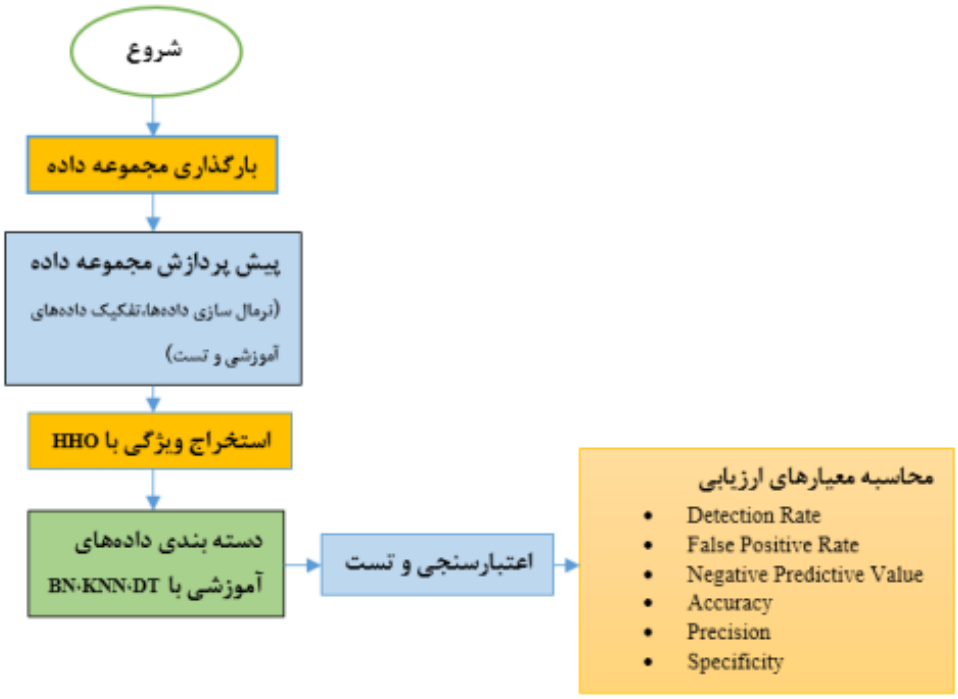
سوهایب هنیف و همکاران در سال ۲۰۱۹ روشی برای تشخیص نفوذ در اینترنت اشیا با استفاده از شبکه های عصبی مصنوعی روی مجموعه داده UNSW-۱۵ ارائه داده اند. دستگاه های اینترنت اشیا با حمله های سایبر زیادی به علت قدرت کم، نیازهای محاسباتی کم و محیط کنترل شده مواجه هستند. پیاده سازی یک سیستم شناسایی حملات خیلی سخت می باشد. در این مقاله یک شبکه عصبی مصنوعی برای تشخیص حملات برای اینترنت اشیا برای حل موضوع های احراز هویت پیشنهاد شده است. شبکه های عصبی مصنوعی شامل لایه های ورودی، خروجی و پنهان هستند. تکنیک پیشنهادی توانا به تشخیص حمله ها به طور موثر می باشد و یک دقت میانگین ۸۴ درصد با ۸ درصد نرخ مثبت اشتباه را ارائه می دهد.

روش پژوهش

این پژوهش از نوع کاربردی است. از روش کاربردی با استفاده از نتایج تحقیقات بنیادی به منظور بهبود و به کمال رساندن رفتارها، روش ها، ابزارها، وسایل، تولیدات، ساختارها و الگوهای مورد استفادهء جوامع انسانی انجام می شود . ابتدا به مطالعه مقالات معتبر در مجلات بین المللی مانند Elsevier، IEEE، ACM و Springer پرداخته شده است از مجموعه داده ۱۹۹۹ KDD Cup استفاده خواهد شد که اکثر محققین دیگر در حوزه تشخیص نفوذ استفاده می کنن با استفاده از نرم افزار پایتون پیاده سازی انجام شده و سپس ارزیابی روی مجموعه داده صورت می گیرد و نتایج کار با روشهای دیگر ارزیابی می شود.

معیار های ارزیابی

۱. Accuracy
۲. F۱measure
۳. Precision
٤. Recall



شکل ۳-۱: فلوچارت مراحل کار

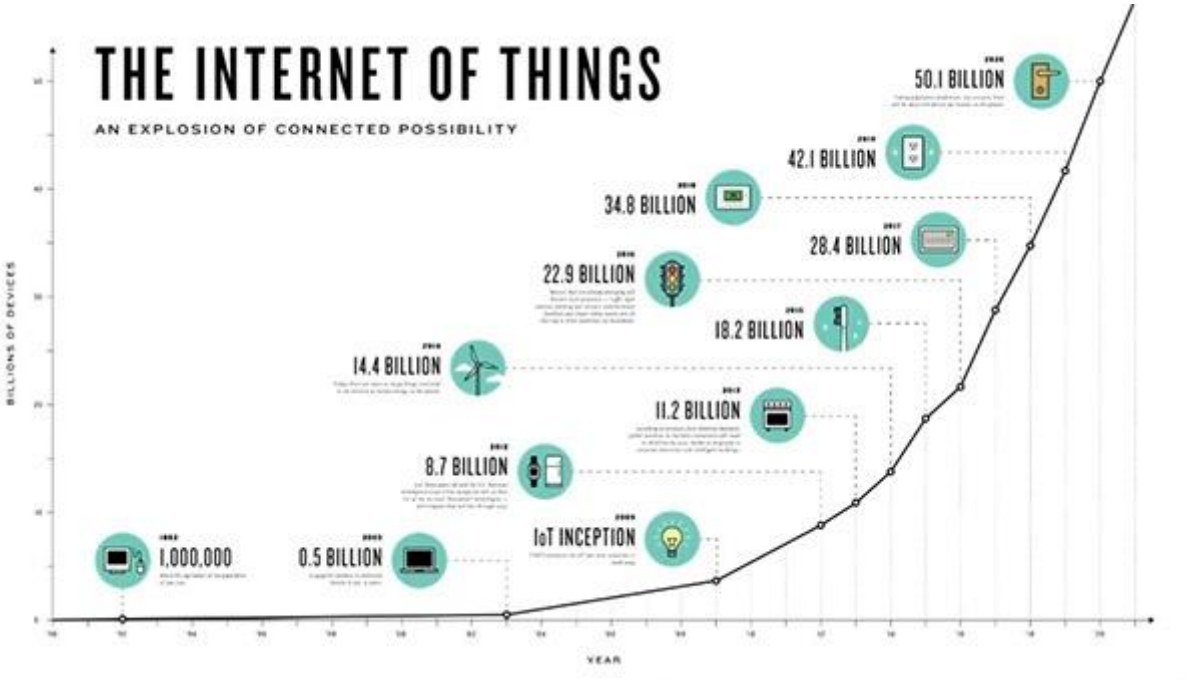
بحث و مبانی نظری

اینترنت اشیا یا IoT یک شبکه در حال رشد از اشیا است که در صنایع مختلفی از آن استفاده می شود . دامنه کاربرد اینترنت اشیا بسیار گسترده می باشد و از ماشین های صنعتی گرفته تا کالاهای مصرفی را می تواند شامل شود. با اتصال دستگاه های مختلف و جدید به اینترنت و تولید داده توسط حسگرهای تعبیه شده درون این نوع دستگاه ها، شاهد تولید حجم بسیار بالائی از داده خواهیم بود. تحلیل این حجم از داده های عظیم نیازمند یک رویکرد جدید است .

حجم ، سرعت و تنوع اشیا تولید کننده داده بگونه ای است که می توان داده تولید شده را در زمره داده های عظیم در نظر گرفت که تحلیل صحیح آن مستلزم وجود زیرساخت های مناسب است . با یک نگاه اجمالی به اعداد و ارقام ، به ابعاد گسترده این فناوری بیشتر آگاه می شویم و می بایست در انتظار خبرهای بسیار بیشتری از این فناوری در آینده ای نه چندان دور بود . پیش بینی شده است تا سال ۲۰۱۹ ، بیش از ۳۵ میلیارد شی به اینترنت متصل می شوند که اکثریت آنها اشیایی هستند که در گذشته شرایط اتصال به شبکه را نداشتند . ترموستات ها ، ساعت ها ، دستگاه های فروش خودکار، اتومبیل ها ، روبات ها ، ماشین آلات سنگین و ... نمونه هایی از نورسیده هایی می باشند که برای اتصال به اینترنت لحظه شماری می کنند . هم اینک دستگاه های محدودی (کامپیوترهای شخصی ، تبلت ها ، لب تاپ ها ، تلفن های هوشمند و ...) امتیاز اتصال به اینترنت و بهره گیری از پتانسیل های این شبکه را در اختیار دارند که با گسترش اینترنت اشیا ، می بایست در انتظار یک تحول بزرگ بود .تحولی که می تواند منشاء بروز تحولات بسیار گسترده تری در سایر عرصه های حیات بشری باشد . به عنوان نمونه پیش بینی شده است تا سال ۲۰۲۰ ، بیش از ۴۰ هزار اگزا بایت داده توسط حسگرهای تعبیه شده درون اشیا فیزیکی متصل به اینترنت تولید می گردد.این حجم اطلاعات بیش از ۹۰ ٪ داده ئی است که تاکنون در دنیا تولید شده است .

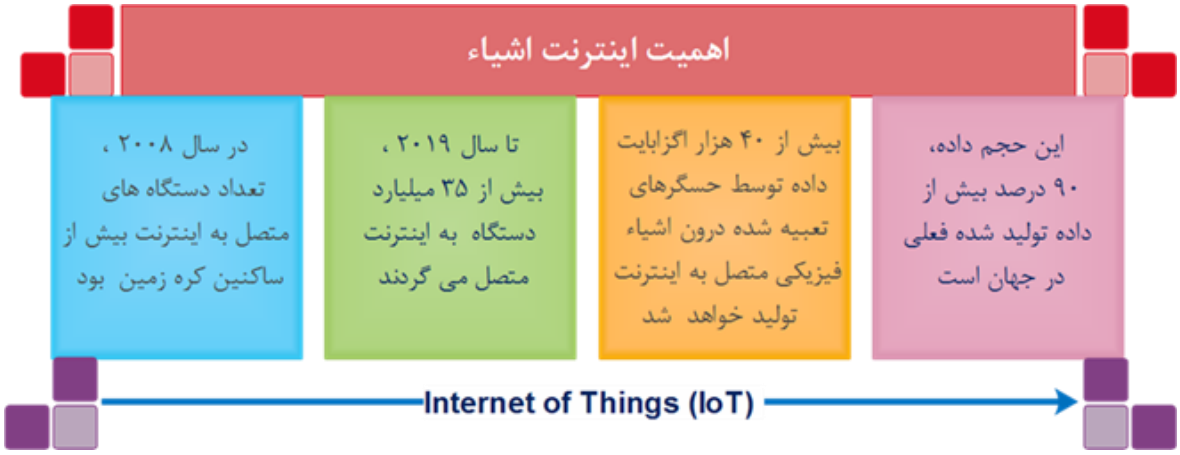
حجم گسترده داده‌های تولیدشده توسط اینترنت اشیا، یکی از بزرگ‌ترین موانع استقرار این فناوری در سازمان‌ها است؛ به‌عبارت‌دیگر سازمان‌ها باید بدانند با حجم انبوهی از اطلاعاتی که جمع‌آوری می‌شود، چه‌کاری باید انجام دهند. مایک ردینگ مدیرعامل Accenture Technology Labs دراین‌باره می‌گوید: «رسانه‌های اجتماعی، حس‌گرها و دستگاه‌های نهفته (تعبیه‌شده)، توانایی

جمع‌آوری اطلاعات در زمینه‌هایی که تاکنون کشف نشده‌اند را گسترش می‌دهند». همان‌گونه که در شکل ۱ می‌بینید، رشد انفجاری استفاده از اینترنت، همراه با اسمارت‌فون‌ها و برنامه‌های اجتماعی و ارتباطات ماشین به ماشین، در کلان داده‌ها انقلابی به وجود آورده است. در سال ۲۰۱۳ مؤسسه IDC تخمین زد که اندازه داده‌های دیجیتال در جهان به رقم ۴.۴ زتابایت رسیده است (۴.۴ تریلیون گیگابایت)؛ این رقم در سال ۲۰۲۰ رشد ده برابری خواهد داشت و به رقم ۴۴ زتابایت خواهد رسید (شکل ۱).



شکل(۴-۱) رشد انفجاری استفاده از اینترنت اشیا در کلان داده‌ها، انقلابی پدید آورده است.

شکل ۲ ، برخی شاخص های مهم اینترنت و حجم داده با در نظر گرفتن اینترنت اشیا را نشان می دهد.



شکل (۴-۲) برخی شاخص های مهم اینترنت و حجم داده با لحاظ کردن اینترنت اشیا

امنیت اینترنت اشیا و تمرکز بر روی هر یک از سطوح هفت گانه و همچنین مبادله داده بین سطوح ، مستلزم صرف زمان بسیار زیادی است . در این مطلب صرفا به این نکته مهم اشاره می گردد که سنجش امنیت می‌بایست :

- ایمن سازی هر دستگاه و یا سیستم را انجام دهد .
- امنیت را برای تمامی فرآیندها در هر یک از سطوح ارایه نماید
- ایمن سازی انتقال داده و تعامل بین هر سطح را تامین نماید .

شکل ۱ ، جایگاه امنیت در مدل مرجع اینترنت اشیا را نشان می دهد .امنیت می بایست بر تمامی مدل حاکم باشد .

شکل (۵-۱) امنیت در اینترنت اشیا

در دهه گذشته، اینترنت اشیا در مرکز توجهات و تحقیقات قرار داشته است. امنیت و محرمانه بودن، مسائل مهمی برای کاربردهای IOT بوده و همچنان با چالش های بزرگی مواجه است. به منظور تسهیل این حوزه از موارد ظهورکرده، ما به طور خلاصه به بررسی روش تحقیق IOT پرداخته و به مقوله امنیت توجه می کنیم. با استفاده از تحلیل عمیق معماری امنیت و ویژگی های آن، نیازمندی های امنیت ارائه شده اند. بر مبنای این تحقیقات، ما وضعیت تحقیقات در تکنولوژی های اساسی را شامل مکانیزم رمز نگاری، مخابرات امن، حفاظت از داده سنسور و الگوریتم های رمزنگاری را بحث کرده و به طور خلاصه، نمای کلی چالش ها را بیان می کنیم.

به منظور برآورده کردن مسئله امنیت، IOT با چالش های بیشتری مواجه است. دلایل زیر برای این موضوع وجود دارد:

۱) IOT از طریق اینترنت سنتی، شبکه موبایل و شبکه سنسور و ... توسعه داده می شود

۲) بسیاری از اشیا به این نوع از اینترنت متصل می شوند

۳) این اشیا با یکدیگر ارتباط برقرار می کنند. در نتیجه، یک مشکل امنیتی و حریم خصوصی جدید، بروز می‌کند. توجهات بیشتری برای قابلیت اعتماد، تشخیص و تلفیق داده در IOT باید انجام بگیرد.

در این سطح، هوش محیطی و کنترل مستقل، بخشی از مفهوم اصلی IOT نمی باشد. با توسعه روش های پیشرفته شبکه و کنترل چند عاملی و محاسبات ابری، انتقالی بین مفاهیم IOT و کنترل مستقل در تحقیقات M2M جهت تولید یک سیر تکاملی در M2M در

شکل CPS ایجاد شده است. CPS به طور کلی بر روی هوشمند سازی تعامل ها، برنامه های تعاملی، کنترل بلادرنگ توزیع شده، بهینه سازی سطح مقطع، بهینه سازی حوزه سطحی و ... تمرکز دارد. در نتیجه، برخی از تکنولوژی ها و روش های جدید، باید جهت برآورده کردن نیازمندی های بیشتر بر حسب قابلیت اطمینان، امنیت و حریم خصوصی، توسعه داده شود. دنیای دیجیتال، با داده های شخصی و اشتراکی و ثبت شده توسط افراد اشباع شده است و نگرانی‌هایی را در زمینه امنیت و حفاظت از اطلاعات افراد و دولت‌ها فراهم کرده است. مشکلات ناشی شده از انتقال و پردازش داده های ناخواسته، موجب نگرانی‌های کاربران و مسائل قانونی شده است.

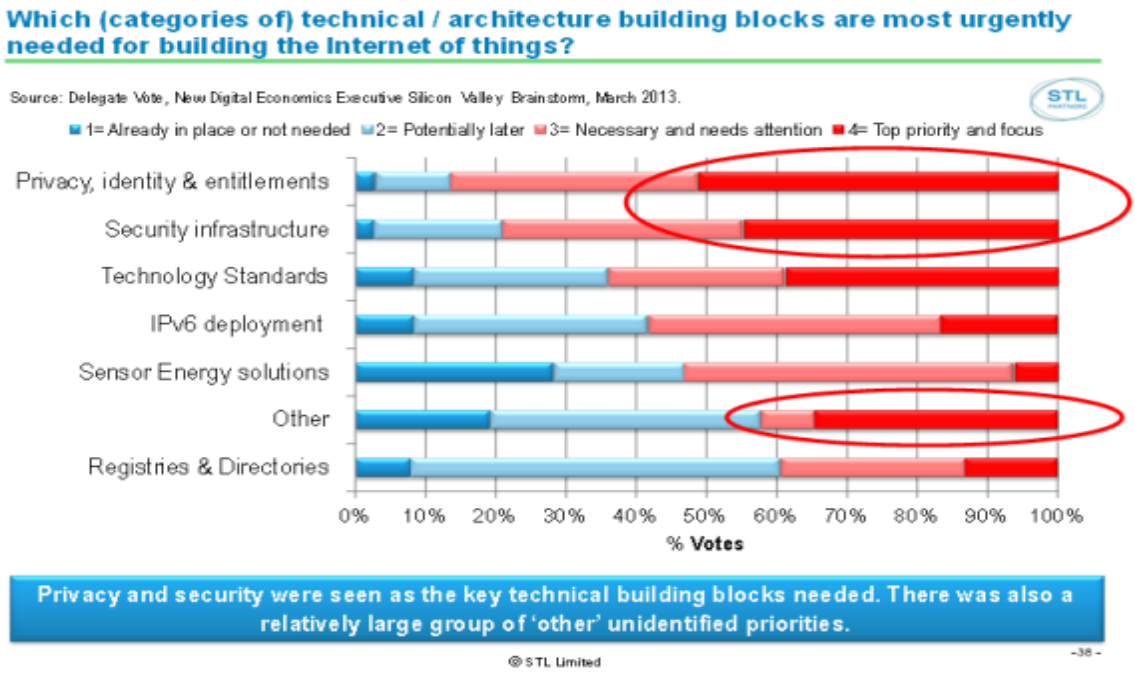
با رشد سریع کاربردهای IoT ، مفاهیم امنیتی مورد توجه قرار می‌گیرند و نگرانی‌هایی در زمینه محرمانگی و ناتوانی مردم در کنترل زندگی شخصیشان شکل می‌گیرد. اگر فعالیت روزانه افراد نظارت شده و آن‌ها تولید کننده خروجی‌های اطلاعاتی باشند، فعالیت‌های سیاسی، اقتصادی و اجتماعی تحت تأثیر قرار می‌گیرند. در صورت نقض امنیت، رخداد حمله و اختلال در عملکرد ، مزایای IoT کمرنگ می‌شود. در آینده ای نزدیک حجمی وسیع از اطلاعات توسط وسایل متصل و سیستم‌های مدیریتی دریافت و ارسال خواهد شد. در نظر داشته باشید که اطلاعات مرتب در حال حرکت و جابجایی است و با ورود اینترنت اشیا رویکرد این جابجایی بسیار متفاوت از حالت فعلی خواهد شد. امنیت اینترنت اشیا به واسطه اتصال همه دستگاه‌ها به یکدیگر کاملاً متفاوت از روند های فعلی خواهد بود. ما باید به نقاط اتصالی و ارتباطی انتقال اطلاعات ما بین تمامی وسایل و ابر و شبکه‌ها توجه کرده و ایمنی را در آنجا به وجود آوریم .

مرکز امنیتی Sopho به عنوان یکی از بزرگ‌ترین بانک‌های پشتیبانی از محصولات امنیتی، به پیش‌بینی تهدیدات امنیتی سال ۲۰۱۵ دست زده است. به اعتقاد Sopho در سال ۲۰۱۵ سوءاستفاده از آسیب‌پذیری‌های نرم‌افزاری کاهش خواهد یافت. با توجه به کاهش تعداد آسیب‌پذیری‌های نرم‌افزاری، معدودی آسیب‌پذیری‌ها به شدت مورد استفاده قرار خواهند گرفت. اینترنت اشیا، بزرگ‌ترین نگرانی امنیتی سال ۲۰۱۵ به نظر می‌رسد. این فناوری نوپا، در بدو تولد خود به شدت به موضوع امنیت توجه نشان داده است. شرکت‌های گوگل، سامسونگ، سونی و دیگر غول‌های فناوری که به نوعی در رشد یافتن این فناوری نقش داشته‌اند، رعایت ایمنی را یکی از اصول اولیه کار قرار داده‌اند اما به اعتقاد کارشناسان، اینترنت اشیا بعد از عبور از مرحله "ایمن نمایشی" به مرحله "خطرناک در حال کار" خواهد رسید و بی‌شک، برخورد واقعی با بد افزار نویسان، شرایط را به گونه دیگری تغییر خواهد داد.

امنیت شبکه و اطلاعات با مؤلفه های شناسایی، محرمانگی، یکپارچگی و انکارناپذیری سنجیده می‌شوند. اینترنت اشیا در حوزه اقتصاد جهانی و در خدمات پزشکی، مراقبت‌های بهداشتی، حمل و نقل هوشمند و بسیاری دیگر از حوزه‌ها به کار گرفته می‌شود، لذا نیازمندی‌های امنیتی در آن از اهمیت بالایی برخوردارند. با داشتن اینترنت اشیا می‌توان پیش بینی کرد که مجرمان سایبری در مرحله اول به نقاط به وجود آمدن و انتقال اطلاعات، مراکز ارسال دستورات، نقاط و مدخل‌های[18] شبکه حمله خواهند نمود و محافظت را باید برای این نقاط فراهم نمود. ناهمگونی پروتکل‌ها و دستگاه‌ها، توسعه سرویس‌های امنیتی با تحمل خطای بالا را به فعالیتی دشوار تبدیل می‌کند.

اینترنت اشیا با چالش‌های زیادی رو به رو است. از نظر مقیاس پذیری برنامه های کاربردی IoT به تعداد زیادی از دستگاه‌ها نیاز دارد که پیاده سازی آن‌ها به دلیل محدودیت‌های زمان، حافظه و پردازش مشکل است. به عنوان مثال محاسبه تغییرات روزانه دمایی در محدوده یک کشور به دستگاه های زیادی نیازمند است و مدیریت بر داده های زیادی را می‌طلبد. در شکل ۲ نیازمندی‌های امنیتی ضروری برای اینترنت اشیا نمایش داده شده است. همان طور که مشاهده می‌کنید محرمانگی و امنیت به عنوان بلوک‌های سازنده فنی کلیدی مورد نیاز می‌باشند.

[18] - *gateway*



شکل (۵-۲) نیازمندیهای امنیتی IoT

IOT به عنوان یک موضوع تحقیقاتی فعال و جدید، حوزه های مختلفی از مشکلات را باید حل کند، در لایه های مختلف معماری و از جنبه های مختلف امنیت اطلاعات، زیر بخش های زیر چالش های مشترکی را برای امنیت اینترنت اشیا تحلیل و خلاصه می کند.

الف) ساختار معماری

در مرجع ۱۰، IOT در طول کل بازه زمانی، پایدار باقی می ماند و مکانیزم امنیت در هر لایه منطقی نمی تواند سیستم دفاع کامل را پیاده سازی کند، در نتیجه، این موضوع یک چالش بوده و حوزه های تحقیقاتی فراوانی جهت ایجاد ساختار امن با ترکیب کنترل و اطلاعات، مورد نیاز است.

ب) مدیریت اساسی

از آنجا که مدیریت اساسی، پایه مهمی از مکانیزم امن می باشد، این موضوع همواره یک موضوع تحقیقاتی داغ می باشد. این مورد همچنان مشکل ترین جنبه امنیت رمزنگاری است. در حال حاضر، محققان راه حل ایده آل برای این موضوع را پیدا نکرده اند. الگوریتم رمزنگاری سبک یا عملکرد بالاتر گره سنسور، همچنان اعمال نشده است. در نتیجه، شبکه سنسور مقیاس بزرگ همواره به صورت قابل اجرا باقی می ماند. مسائل امنیت شبکه بیشتر مورد توجه قرار گرفته و تبدیل به یک نکته مهم شده و مشکلاتی را در حوزه تحقیقات محیط شبکه ایجاد می کند.

ج) قوانین و مقررات امنیت:

در حال حاضر، قانون و مقررات امنیت، همچنان در مرکز توجهات قرار ندارد و هیچ استاندارد تکنولوژی ای در مورد IOT وجود ندارد. IOT مربوط به اطلاعات امن ملی، اسرار تجاری و حریم شخصی افراد می باشد. در نتیجه، کشور ما نیاز به دیدگاه قانونی جهت توسعه IOT است. مقررات و قوانین به صورت بلا انکاری مورد نیاز است. در این جنبه، ما راه زیادی تا انجام این مسئله داریم.

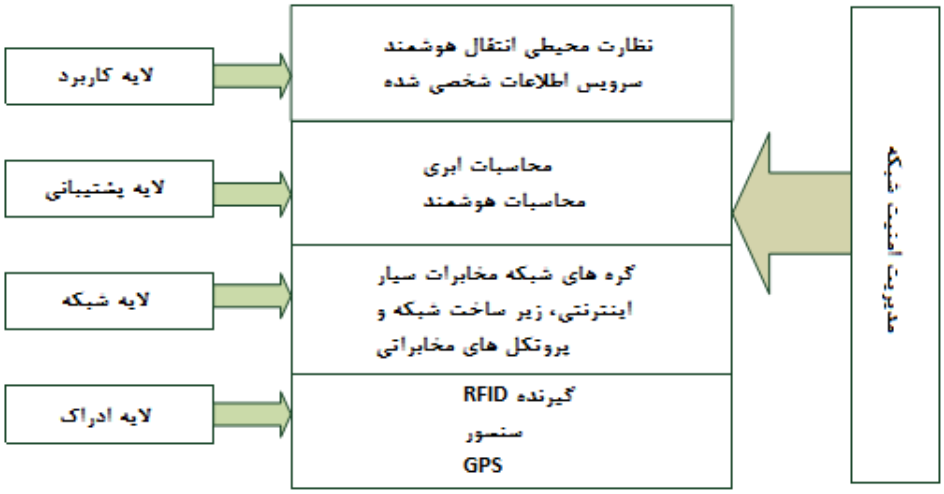
د) نیازمندی ها برای کاربردهای نوظهور

با توسعه WSNها، تشخیص فرکانس رادیویی(RFID)، تکنولوژی محاسبات فراگیرنده، تکنولوژی مخابرات شبکه، و تئوری کنترل بلادرنگ توزیع شده، CPS، یک شکل بروز پیدا کرده از IOT تبدیل به واقعیت شده است. در این سیستم، امنیت بالا برای تضمین عملکرد سیستم مورد نیاز است.

همانطور که اشاره شده، چالش های امنیت برای IOT برآورده شده است. ایجاد ساختارهای شبه امن نیز بسیار ضروری می باشد. مدیریت اساسی در یک شبکه سنسور مقیاس بزرگ واقعی نیز همواره از مسائل چالشی بوده و مقررات و قوانین این حوزه که مربوط به IOT استف نیز جزو موضوعات چالشی می باشد.

معماری امن

به طور کلی، IOT می تواند به چهار سطح کلی تقسیم شود. شکل ۳، معماری سطح اشیا را نشان می دهد.



شکل (۵-۳) معماری اشیا

اساسی ترین پایه، لایه ادراک یا لایه تشخیص می باشد که تمامی اطلاعات را از طریق تجهیزات فیزیکی جمع آوری کرده و دنیای فیزیکی را شناسایی می کند، این اطلاعات شامل خصوصیات اشیا، شرایط محیطی و ... می باشد و تجهیزات فیزیکی شامل خواننده RFID، تمامی انواع سنسورها، GPS و دیگر تجهیزات می باشد. مولفه اساسی در این لایه، سنسورها برای دریافت و بیان دنیای واقعی در دنیای دیجیتال است.

سطح دوم، لایه شبکه است. لایه شبکه مسئول ارسال اطلاعات از لایه ادراک، پردازش اولیه اطلاعات، دسته بندی و بسپارش[۱۹] می باشد. در این لایه، ارسال اطلاعات مبتنی بر چندین شبکه پایه بوده که شامل اینترنت، شبک مخابرات سیار، گره های ماهواره ای، شبکه بیسیم، ساختار شبکه بوده و پروتکل های مخابراتینیز جهت تبادل اطلاعات بین تجهیزات ضروری است.

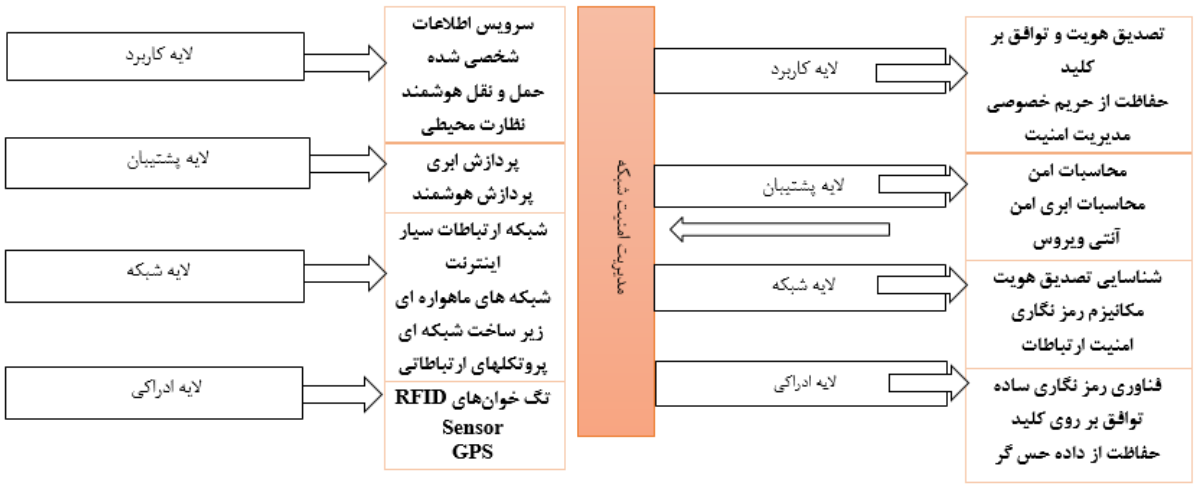
سطح سوم، لایه پشتیبانی است. لایه پشتیبانی یک بستر پشتیبانی قابل اطمینان را برای لایه برنامه کاربردی، تنظیم می کند، در این بستر پشتیبانی، تمامی توان محاسباتی هوشند از طریق شبکه اتصال و محاسبات ابری، سازمان دهی می شود. این لایه نقش یک لایه ترکیب کاربردها را ایفا می کند.

لایه برنامه کاربردی و مدیریت یک نقش اساسی در هر سطح بالا را ایفا می کند. آنگاه، ویژگی های امنیت را تحلیل خواهیم کرد.

[19] *polymerization*

معماری امن در اینترنت اشیا

یکی از مکانیزم‌های ایجاد امنیت در اینترنت اشیا بهره گیری از معماری مناسب می‌باشد. معماری اینترنت اشیا دارای چهار سطح است. در شکل ۴ چهار سطح IoT ، در سمت چپ و در سمت راست نیازمندی‌های امنیتی هر لایه، برای آشنایی با لایه های معماری این فناوری و مکانیزم‌های هر لایه نمایش داده شده است. بحث پیرامون نحوه عملکرد این ۴ لایه و سیستم امنیتی آن‌ها مبحث جداگانه ای را می‌خواهد که در این نوشتار نمی‌گنجد.



شکل (۵-۴) معماری امنیتیIoT و نیازمندیهای امنیتی در هر لایه

۳-۴-۵- ویژگی های امنیت

الف) لایه ادراک: عموماً گره های ادراکی کوچکتر از توان محاسباتی و ظرفیت ذخیره سازی است زیرا آنها ساده بوده و توان مصرفی کمتری دارند. در نتیجه، قادر به اعمال فرکانس مخابراتی مورد نظر و الگوریتم رمزنگاری اصلی عمومی جهت محافظت امن نمی باشند. و لذا ایجاد یک سیستم محافظت امن، بسیار مشکل است. در همین حال، حملاتی از شبکه های خارجی مانند عدم دسترس به شبکه نیز مسایل امنیتی جدیدی را ایجاد می کند. از طرف دیگر، داده سنسور همچنان نیازمند محافظت برای تلفیق، تشخیص و قابلیت اعتماد است.

ب) لایه شبکه: اگرچه شبکه مرکزی دارای قابلیت محافظت امن کامل است، اما حملات انسانی و حملات ساختگی، همچنان وجود دارد، ضمناً، ایمیل های ناخواسته و ویروس های کامپیوتری نیز نمی توانند صرفنظر شوند، حجم زیادی از ارسال داده سبب ایجاد ازدحام می شود. در نتیجه، مکانیزم امنیت در این سطح، در IOT بسیارحائز اهمیت است.

ج) لایه پشتیبانی: وظیفه انجام پردازش داده سنگین و تصمیم گیری هوشمند رفتار شبکه در این لایه را بر عهده دارد، پردازش هوشمند برای اطلاعات جعلی محدود می باشد زیار چالشی جهت بهبود قابلیت تشخیص اطلاعات ناخواسته و جعلی وجود دارد.

د) لایه برنامه) در این سطح، امنیت برای محیط برنامه مختلف، متفاوت بوده و اشتراک گذاری داده به صورت یکی از مشخصه های لایه برنامه های کاربردی می باشد که سبب ایجاد مشکلاتی در حریم خصوصی داده، کنترل دسترسی و افشاء اطلاعات می شود.

نیازمندی های امنیت

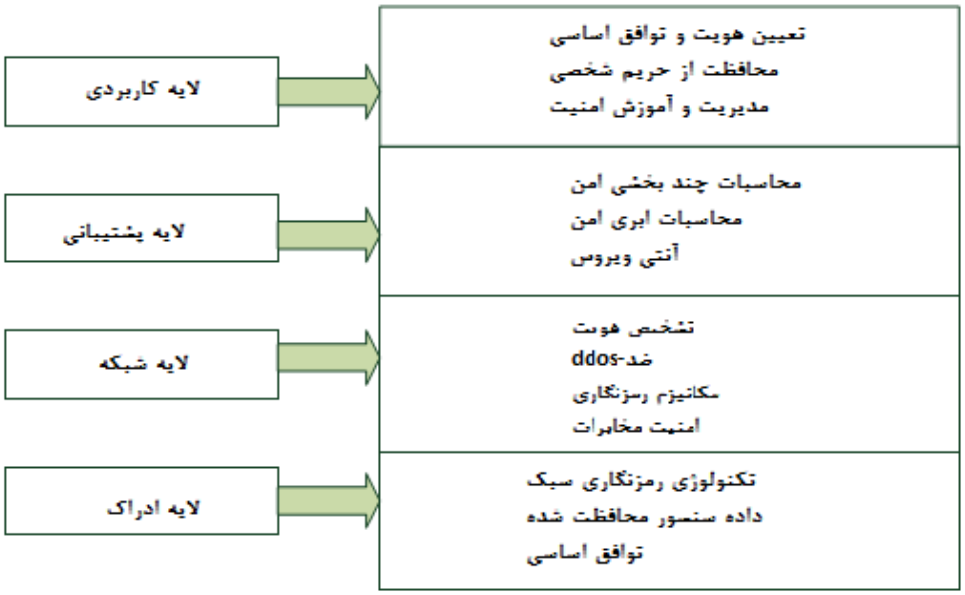
با توجه به تحلیل بالا، می توانیم نیازمندی های امنیت را برای هر سطح به صورت زیر و مطابق شکل ۵ نشان دهیم.

الف) لایه ادراک: در ابتدا، تایید گره جهت جلوگیری از دسترسی گره غیرقانونی لازم است. ثانیاً، جهت محافظت از قابلیت اطمینان ارسال داده بین گره ها، رمز گذاری داده کاملاً مورد نیاز است. و قبل از رمزنگاری داده، توافق اساسی، فرآیند مهمی می باشد. هرچه اندازه گیری های امن قوی تر باشد، مصرف منابع کمتر خواهد بود، به منظور حل این مشکل، تکنولوژی های رمزنگاری های سبک، مهم شده که شامل الگوریتم رمزنگاری سبک و پروتکل رمزنگاری سبک می باشد. در این زمان، تلفیق و تشخیص داده سنسور به صورت یک موضوع تحقیقاتی درآمده و لذا ما در بخش بعدی به تفصیل در این مورد صحبت می کنیم.

ب) لایه شبکه: در این لایه، اعمال مکانیزم های امنیت مخابراتی موجود، دشوار است. تشخیص مشخصات، مکانیزمی جهت جلوگیری از گره های غیر قانونی بوده و و حالتی از مکانیزم امن می باشد، قابلیت اعتماد و تمامیت، از اهمیت یکسانی برخوردار هستند، در نتیجهف لازم است که داده را به صورت مکانیزم قابل اعتماد و به درستی ثبت کنیم. حملات عدم دسترسی به سرویس توزیع شده(DDOS)، یک روش حمله معول در شبکه بوده و به طور مشخص در بسیاری از کاربردهای اینترنت اشیا استفاده می شود. در نتیجه جهت جلوگیری از حملات DdoS برای گره آسیب پذیر نیز مسئله دیگری جهت حل در این لایه می باشد.

ج) لایه پشتیبانی) لایه پشتیبانی نیازمند معماری امن کاربردی زیادی مانند محاسبات ابری و محاسبات چند بخشی امن می باشد، تقریباً تمامی الگوریتم های رمزنگاری قوی و پروتکل های رمزنگاری، از سیستم های امنیتی و آنتی ویروس ها، قوی تر هستند.

د) لایه برنامه کاربردی) به منظور حل کردن مسئله امنیت در لایه برنامه، ما به دو جنبه نیاز داریم. یکی تشخیص و دیگری توفق اساسی در شبکه ناهمگن می باشد، مورد دیگر محافظت حریم خصوصی افراد است. بعلاوه، یادگیری و مدیریت، در امنیت اطلاعات، علی الخصوص مدیریت رمز عبور، بسیار حائز اهمیت است.



شکل (۵-۵) نیازمندی های امنیت در هر سطح

حالت تحقیقاتی تکنولوژی های اساسی

حال، ما به حالت تحقیق برای نیازمندی های امن در بخش ۲ توجه می کنیم و توضیحات بیشتری در مورد مکانیزم رمزنگاری، امنیت ارتباطات، حفاظت از داده سنسور و الگوریتم رمزنگاری در زیر بخش های زیر، ارائه می کنیم.

مکانیزم رمز گذاری

در لایه شبکه سنتی، ما از روش رمز گذاری مرحله به مرحله استفاده می کنیم، در این روش، اطلاعات در فرآیند ارسال رمزنگاری می شود اما لازم است که پیام اصلی در هر گره از طریق عملیات رمزگذاری و رمز برداری حفظ می شود. ضمناً، در لایه برنامه های کاربردی سنتی، مکانیزم رمزگذاری به صورت رمزگذاری انتها به انتها می باشد، به این صورت که اطلاعات تنها برای ارسال کنندگان و دریافت کنندگان صریح بوده و در فرآیند ارسال و گره های فوروارد، همواره رمزنگاری انجام میگیرد.

درIOT ، لایه شبکه و لایه برنامه کاربردی به صورت بسیار نزدیک به یکدیگر متصل می شوند که در نتیجه باید از روش های انتها به انتها و اتصال نزدیک استفاده شود، می توانیم تنها لینک هایی که نیاز به محافظت دارد را محافظت می کند، زیرا در لایه شبکه، می توانیم آن را به تمامی تجارت ها اعمال کنیم که سبب ایجاد پیاده سازی امن برنامه های کاربردی مختلف می شود. در این روش، مکانیزم امنیت در برنامه های تجاری واضح بوده که سبب راحتی کاربر نهایی می شود. در این روش، این حالت سبب ایجاد ویژگی هایی در حالت by-hop مانند تاخیر اندک، بازدهی بالا، هزینه پایین، و ... می باشد. با این حال، به سبب عملیات رمزگشایی در گره ارسال، استفاده از روش by-hop در هر گره می تواند به پیام اصلی رمز منجر شده که در نتیجه سبب ایجاد قابلیت اعتبار بالا در گره های ارسال می شود.

با استفاده از رمزنگاری انتها به انتها، می توانیم مقررات امنیتی مختلفی را براساس نوع تجارت انتخاب کنیم، در نتیجه، می تواند محافظت امنیت سطح بالایی را در نیازمندی های امنیت تجارت، ایجاد کند. با این حال، رمزنگاری انتها به انتها نمی تواند آدرس مقصد را رمزنگاری کند زیرا هر گره تعیین می کند که چگونه پیام به براساس آدرس مقئد ارسال کند که نتایج آن نمی تواند از منبع و مقصد در پیام ارسال شده مخفی بماند و حملات ناخواسته ای را ایجاد کند.

با توجه به تحلیل بالا، می توانیم نتیجه گیری کنیم که: زمانی که نیازمندی امنیت در برخی از تجارت ها، خیلی بالا نیست، می توانیم محافظت رمزنگاری by-hop را اتخاد کنیم: زمانی که تجارت ما نیاز به امنیت بالا دارد، آنگاه رمزنگاری انتها به انتها، اولین انتخاب می باشد. در نتیجه، با توجه به نیازمندی های مختلف، می توانیم از مکانیزم های رمزنگاری جایگزین استفاده کنیم.

در حال حاضر، IOT در فاز اولیه خود در حال توسعه است، و تحقیقات در مکانیزم امنیت، نکته توجه نشده در این حوزه است، در نتیجه، ما راه زیادی برای تحقیقات خود در این حوزه داریم.

۲-۵-۵- امنیت مخابرات

در ابتدا، در پروتکل های مخابراتی، برخی از راه حل ها ایجاد شده است، این راه حل ها می تواند تمامیت، تشخیص و قابلیت اطمینان را برای مخابرات TLS/SSL یا IPSec فراهم کند. TLS/SSl به منظور رمزنگاری لینک در لایه انتقال طراحی شده است. این مورد می تواند تمامیت، تشخیص و قابلیت اعتماد را در هر لایه تامین کند. و نیاز برای امنیت نیز ناشی از این مورد بوده اما متاسفانه به طور گسترده استفاده نشده است.

مکانیزم های امنیت مخابره نیز به ندرت در کاربردهای امروزی اعمال شده است. از انجا که تجهیزات IOT کوچک، توان پردازشی اندکی دارند، این حالت منجر به مخابره امنی که غالباً ضعیف می باشد، می شود. در همین حال در IOT، شبکه مرکزی نیز همواره به صورت فعلی با اینترنت نسل آتی می باشد، اغلب اطلاعات از طریق اینترنت ارسال می شود. در نتیجه، DdoS نیز همچنان وجود داشته و یک مشکل بسیار بزرگ می باشد. این محدودیت ها و حملات DdoS سبب از بین رفتن قابلیت دسترسی در شبکه های مخابراتی می شود. زمانی که حملات DdoS سازمان یافته یا مقیاس بزرگ به وقوع می پیوندد، نحوخ بازیابی این مشکلات قابل توجه می شود، در نتیجه، لازم است توجه بیشتری به تحقیقات جهت پیشگیری و مکانیزم های بازیابی خطرات، انجام دهیم.

۳-۵-۵- حفاظت از داده سنسور

دقیقاً مشابه به مواردی که در بخش ۲ گفته شد، تمامیت و صحت داده سنسور تبدیل به یک موضوع تحقیقاتی شده و قابلیت اعتماد داده سنسور یک خواسته پایین تر بوده زیرا زمانیکه یک حمله کننده بتواند سنسور خود را به صورت فیزیکی در نزدیکی سنسور اصلی قرار دهد، می تواند مقادیر مشابهی را دریافت کند. در نتیجه، در خود سنسور، نیاز به قابلیت اعتمادنسبتاً اندک است.

موضوع تحقیقاتی دیگر در سنسورها بحث حریم خصوصی است، و حریم خصوصی نیز یک موضوع حائز اهیمت است. لازم است که مکانیزمی را جهت حافظت از حریم خصوصی افراد و شایاء در دنیای واقعی ارائه کنیم. در اغلب زمان ها، افراد اغلب از سنسورها در زندگی خود بیخبر هستند، در نتیجه لازم است مقرراتی وضع شود که امنیت افراد را تامین کند.

۴-۵-۵- الگوریتم های رمزنگاری

الگوریتم های رمزنگاری مناسب و قابل اطمینان و معروفی در پروتکل های امنیت اینترنت مطابق جدول ۱ ارائه شده است.

جدول (۵-۱) الگوریتم های رمزنگاری

الگوریتم	هدف
استاندارد رمزگذاری پیشرفته	قابلیت اعتماد
Rivest shamir adelman (RSA یا رمزنگاری منحنی بیضوی	انتقال امضا دیجیتال
Diffie-hellman (DH)	تطبیق اساسی
SHA-1/SHA-256	تمامیت

عموماً، الگوریتم رمزنگاری متقارن به منظور رمزگذاری داده برای قابلیت اعتماد مانند استاندارد رمزگذاری پیشرفته(AES) استفاده می شود؛ الگوریتم غیر متقارن نیز به منظور استفاده در کاربردهای امضا دیجیتال و انتقال مهم استفاده می شود. تطبیق ECC نیز کاهش یافته و ممکن است در کاربردهای اخیر، مورد استقبال قرار بگیرد.

به منظور به کارگیری این الگوریتم های رمزنگاری، منابع در دسترس مانند سرعت پردازنده و حافظه، مورد نیاز است. در نتیجه، نحوه اعمال این روش های رمزنگاری در IOT واضح نیست، لازم است تلاش های بیشتری در جهت انجام تحقیقات به منظور تایید این موضوع که الگوریتم ها می توانند به خوبی با استفاده از حافظه های محدود و پردازنده های سرعت پایین در IOT استفاده شوند، پیاده سازی شود.

نتیجه گیری و کارهای آینده

مدل های توزیع شده دارای عملکرد بهتر نسبت به مدل متمرکز است. همچنین با تعداد گره های افزایش یافته در شبکه توزیع شده سیستم های مه، دقت کل می تشخیص از 96 درصد به بیش از 99 درصد افزایش یافته است. و یادگیری عمیق از یادگیری ماشین های کلاسیک برای هر دو نوع باینری و چند کلاس بهتراست. این نشان می‌دهد که توزیع توابع شناسایی حمله درگره های مه کارگریک مکانیزم کلیدی برای شناسایی حمله در سیستم های IoT اجتماعی مانند شهر هوشمند است که نیاز به شناسایی زمان واقعی دارد .افزایش دقت در طرح توزیع شده می تواند به دلیل اشتراک پارامترهای یادگیری مشترک باشد که اجتناب از اضافه کردن پارامترهای مدلی را نادیده می گیرد و از این رو به تطابق با یکدیگر کم می کند. از سوی دیگر، دقت مدل عمیق بیشتر از مد کم عمق است. نتایج نشان می دهد که میزان هشدار اشتباه مدل عمیق، 1,85٪ بسیار کمتر از مد ل یادگیری ماشین (6,57٪) است.

عملکرد آموزش عمیق بهتر ازمدل یادگیری ماشین برای هر کلاس حمله است. به عنوان مثال، فراخواند عمیق 99,27٪ است، در حالی که مدل سنتی برای یک طبقه بندی باینری از 97,51٪ استفاده می کند. به طور مشابه، متوسط فراخوان DM٪5.96 است در حالی که SM به طور متوسط شمارش امتیاز 93,66٪ در چند طبقه بندی به ثمر رسانده است. با این حال یادگیری عمیق زمان یادگیری بیشتری نسبت به الگوریتم های آموزش سنتی ماشین طو ل می کشد، در حالی که نرخ تشخیص از هر دو الگوریتم به طور قابل توجهی یکسان است. انتظار می رود که شبکه های عمیق به دلیل اندازه پارامترهای ممورد اسمتفاده در یادگیری زمان بیشتری را

صرف آموزش کنند. مراحل اصلی برای سیستم های تشخیص حمله متمرکز شدن بر سرعت تشخیص بیشتر از سرعت یادگیری است. به این ترتیب، این نشان می دهد که یادگیری عمیق، پتانسیل بزرگی برای تغییر جهت امنیت سایبری به شمار می رود، زیرا تشخیص حمله در محیط های توزیع شده مانند سیستم های IoT / Fog می تواند نتیجه ای مثبت رانشان دهد.

ما یک سیستم تشخیص حمله شبکه IoT / Fog مبتنی بر یادگیر ی توزیع شده را پیشنهاد دادیم. آزمایش موفقیت پذیرفتن شدن هوش مصنوعی را به امنیت سایبری نشان داده است و سیستم تشخیص نفوذ و حمله در معماری توزیع شده برنامه های کاربردی IOT مانند شهرهای هوشمند را طراحی و اجرا کرده است. فرآیند ارزیابی دقت، میزان تشخیص، میزان هشداراشتباه، و غیره به عنوان معیارهای عملکرد برای نشان دادن اثربخشی مدل های عمیق در مدل های کم عمق مورد استفاده قرار گرفته است. این آزمایش نشان داده است که تشخیص حمله توزیع شده می تواند حملات سایبری(در اینترنت اشیا) را بهتر از الگوریتمهای متمرکز تشخیص دهد به این دلیل به اشتراک گذاری پارامترها می تواند مانع از حداقل موانع محلی در آموزش شود.همچنین نشان داده شده اسمتکه مدل عمیق ما از سنتی فراتر رفته است. سیستم های یادگیری ماشین مانند softmax برای طبقه بندی داده های شبکه به شکل نرمال/ حمله در هنگام ارزیابی در داده های آزمون غیر قابل مشاهده است .پیشنهاد ما برای کار آینده این اسمت که IDS آموزش داده شده عمیق را برای مجموعه داده های دیگر و الگوریتم های مختلف سنتی یادگیری ماشین مانند SVM، درخت های تصمیم گیری و دیگر شبکه های عصبی مقایسه شود. علاوه بر این، اطلاعات بارگیری شبکه، به عنوانی الگوی مه، برای تمایز برای شناسایی نفوذ مورد بررسی قرار خواهدگرفت.

منابع فارسی

[۱] اینترنت اشیا ، قابل مشاهده در وب سایت http://avav.ir ، تاریخ مشاهده ۱۳۹۵/۰۴/۶

[۲]خدمتگزار،حمیدرضا؛ بررسی نقش اینترنت اشیا در سیستم‌های مدیریت دانش (مورد مطالعه: مدیریت عملکرد کارکنان شهرداری یزد)، مدیریت فناوری اطلاعات » پاییز ۱۳۹۴ – شماره ۲۴ علمی–پژوهشی/ISC (۲۰ صفحه – از ۵۵۳ تا ۵۷۲)

[۴] «چهار فناوری جدید که اتوماسیون صنعتی را در آینده نزدیک تحت تأثیر قرار خواهد داد». ایران اتوماسیون، ۲۱ اسفند ۱۳۹۴

[۵] ریچارد رایسمن و فرانچسکا موریس. «Internet of Things: The Legal Issues CIOs Should Consider». وال‌استریت‌ژورنال، ۲۰ آوریل ۲۰۱۵.

[۶] معرفی خدمات و کاربردهای فراگیر اینترنت اشیا، وبگاه پژوهشگاه ارتباطات و فناوری اطلاعات

[۷]زرین صدف محمد ، اینترنت اشیا؛ آشنایی با یک مفهوم ناآشنا،وبگاه دیجی کالا مگ https://mag.digikala.com ، تاریخ مشاهده ۱۳۹۵/۰۴/۶.

[۸] کوین اشتون، دو تعریف از اینترنت اشیا، ماهنامه پیوست، شماره ۴، صفحه ۸۶

[۹] فرازمند عاطفه ، احمدی سروش ؛اینترنت اشیا IOT و کاربرد های آن،اولین همایش ملی کامپیوتر، فناوری اطلاعات و ارتباطات اسلامی ایران

[۱۰] کریمی حسن ؛از سیر تا پیاز؛ تمام چیزهایی که باید در مورد اینترنت اشیا (Internet of Things) بدانید،وبگاه فارنت (اخبار دنیای صفرو یک) http://farnet.ir/، تاریخ مشاهده ۱۳۹۵/۰۴/۶.

[۱۱] فرازمند, عاطفه و سروش احمدی، ۱۳۹۴، اینترنت اشیا IOT و کاربرد های آن، اولین همایش ملی کامپیوتر، فناوری اطلاعات و ارتباطات اسلامی ایران، قم، مرکز مطالعات و تحقیقات اسلامی سروش حکمت مرتضوی، http://www.civilica.com/Paper-ICCONF01-ICCONF01_113.html

[۱۲] قیصری, محمد؛ ساره حسینی و داود وحدت، ۱۳۹۲، نقش فناوری نوین اینترنتی از اشیا در حوزه مصرف انرژی خانه های هوشمند، همایش ملی معماری پایدار و توسعه شهری، بوکان، شرکت سازه کویر، http://www.civilica.com/Paper-SAUD01-SAUD01_750.html

[۱۶] ترکمانی, سعید و سیدحسین شاهرخی، ۱۳۹۴، چالش ها وتهدیدهای اینترنت اشیا، کنفرانس بین المللی پژوهش های کاربردی در فناوری اطلاعات، کامپیوتر و مخابرات، تربت حیدریه، شرکت مخابرات خراسان رضوی، http://www.civilica.com/Paper-ITCC01-ITCC01_107.html

[۱۷] فشارکی اصفهانی, امیرحسین و ریحانه خورسند مطلق اصفهانی، ۱۳۹۴، بررسی چالش ها، طبقه بندی و مقایسه سیستم عامل هایی برای اینترنت اشیا، اولین کنفرانس ملی ایده های نو در مهندسی کامپیوتر، شهرکرد، دانشگاه آزاد اسلامی واحد شهرکرد، http://www.civilica.com/Paper-NICE01-NICE01_016.html

منابع انگلیسی

1. Bil Dry and Hazim Dahir. People, Processes, Services, and Things:Using Services Innovation to Enable the Internet of Everything. Business Expert Press, LLC, 2015
2. [1]. 2013. [Online]. Available: http://www.gartner.com/newsroom/id/2636073.
3. [2]. S. Li, L. D. Xu and S. Zhao, "The internet of things: a survey," 2014 springer
4. [3]. D. Giusto, A. Iera, G. Morabito and L. Atzori, The Internet of Things, Springer, 2010
5. [4]. D. Miorandi, S. Sicari, F. D. Pellegrini and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, 2012.
6. [5]. L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, 2010 elsevier
7. [6]. Ji Eun Kim, George Boulos, John Yackovich, Tassilo Barth,
8. Christian Beckel and Daniel Mosse, "Seamless Integration of Heterogeneous Devices and Access Control in Smart Homes," 2012 IEEE.
9. [7].P. Baronti, P. Pillai and V. W. Chook, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," *Computer Communications*, vol. 30, no.
10. 7,2007 Elsevier
11. [8]. J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami,
12. "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, 2013
13. [9]. Whitmore.A and Agarwal.A, "The Internet of Things—A survey of topics and trends," vol. 17, no. 2, 2014 Springer
14. [10]. R. Khan, S. U. Khan and R. Zaheer, "Future Internet: The
15. Internet of Things Architecture,Possible Applications and Key Challenges," 2012.
16.
17. [1] International Telecommunication Union (5002 .)The Internet of Things .Internet Report 5002 .
18. Available at http//:www.itu.int/osg/spu/publications/ internetofthings.
19. [5] van Kranenburg, R (500 .)The Internet of Things :A critique of ambient technology and the all
20. seeing network of RFID, Network Notebooks 05, Institute of Network Cultures, Amsterdam, 500 .
21. [3] Open Source Sensing Initiative (5010 .) Home page http//:opensourcesensing.org. Accessed 5 April
22. 5010.
23. [4] Guinard, D., Baecker, O., & Michahelles, F(.5002 .)Supporting a Mobile Lost and Found
24. Community .In Proceedings of the 10th International Conference on Human-Computer Interaction with Mobile Devices and Services (pp .۴۰ -۴۱۰ .)New York.
25.
26. 1.Bassi, A. and Bauer, M. and Fiedler, M. and Kramp, T. and van Kranenburg, R. and Lange, S. and Meissner, S. (2013), “Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model,” Springer Berlin Heidelberg, pp. 163-211.

27. 2.Ruan, D.X. and Wu, D. and Wu, X.B. (2012), "The Internet of things technology in logistics application: Stages, trend and drive modes", Management of Technology (ISMOT), 2012 International Symposium, Hangzhou, IEEE, pp. 452-455.
28. 3.hang, Y. and Sun, S. (2013), "Real-time Data Driven Monitoring and Optimization Method for IoT – based Sensible Production Process, Networking", Sensing and Control (ICNSC), 2013 10th IEEE International Conference, pp. 486-490.
29. 4.Yuqiang, C. and Jianlan, G. and Xuanzi, H. (2010), "The research of Internet of things" supporting technologies which face the logistics industry, Computational Intelligence and Security (CIS) International Conference, pp. 659663.
30. 5.Tsai, C.W. and Lai, C.F. and Chiang, M.C.and Yang, L.T. (2014), "Data Mining for Internet of Things: A Survey. Communications Surveys & Tutorials", IEEE 16 (1), pp. 77-97.
31. 6. Timpanaro, J.P. and Chrisment, I. and Festor, O. (2011), "Monitoring the I2P network". Research Report RR – 7844.
32. 7Digital Age (New in Paper)", 1st ed, Princeton University Press, pp. 3–15.. Mayer-Schonberger, V. (2011), "Failing to Forget the Drunken Pirate, in: Delete: the Virtue of Forgetting in the
33. www.cisco.com
34. www.iotwf.com
35. http://Particle.io
36. http://docs.particle.io
37. http://www.anandtech.com/show/8541/mediatek-labs-and-linkit-platform-launch-targetingiot-and-wearables
38. http://www.engadget.com/2014/12/09/intel-iotplatform/?utm_source=Feed_Classic_Full&utm_medium=feed&utm_campaign=Engadget&?nci d=rss_full&utm_reader=feedly
39. http://www.androidauthority.com/what-is-the-internet-of-things-592491/
40. http://techcrunch.com/2015/01/14/mesh-indiegogo-sony/
41. http://www.theverge.com/2015/5/28/8677119/google-project-brillo-iot-google-io-2015
42. http://www.theverge.com/2015/5/20/8628905/huawei-internet-of-things-operating-systemlite-os
43. http://www.engadget.com/2015/05/12/samsung-artik-iot/?ncid=rss_truncated

Intrusion detection system deployment strategies in Internet of Things networks

Alireza Maqsoodian

Abstract

With the ever-increasing expansion of the Internet, we see its widespread presence in all areas of people's lives. In Internet of Things networks, the intrusion detection system can be located in a border router, in one or more dedicated hosts, or in any physical object. The advantage of placing the intrusion detection system in the border router is to detect intrusion attacks from the Internet on objects in the physical domain. However, an intrusion detection system in the router may cause communication overhead between the LLN nodes and the border router. Placing the intrusion detection system in LLN nodes may reduce the communication overhead related to network monitoring, but it requires more processing, storage and energy resources from the nodes (Walgreen et al., 2013). Distribution of intrusion detection agents among Some dedicated nodes may also be a solution for less traffic monitoring and more processing volume. However, the only solution requires organizing the network into different regions, which may become a challenge in itself.

The purpose of this article is to investigate the deployment strategies of the intrusion detection system in Internet of Things networks.

Keywords: Internet of Things, system deployment, penetration in the Internet of Things