کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات
National Conference on Computer Science and Engineering and Information Technology

امنیت و چالش‌های پیش روی فناوری اینترنت اشیاء

فرزانه قهرمانی کوشان[1*]، **رسول روستایی**[2]

[1] دانشجوی کارشناسی ارشد،گروه کامپیوتر،واحد ملایر،دانشگاه آزاد اسلامی، ملایر، ایران
Ghahremani.farzaneh@gmail.com
[2] عضوهیات علمی، گروه کامپیوتر،واحد ملایر،دانشگاه آزاد اسلامی، ملایر، ایران
Rassoulrostaei@yahoo.com

خلاصه

اینترنت اشیاء [1]فناوری پیشرفته‌ای است که در آن برای هر موجود قابلیت ارسال داده از طریق شبکه‌های ارتباطی اعم از اینترنت و یا اینترانت فراهم می‌شود .مهم‌ترین مزیت همه‌گیر شدن IOT، قابلیت اتصال انواع اشیا و وسایل به دنیای مجازی است به عبارت دیگرهرچیزی، از جمله اشیا بی‌جان، برای خود هویت دیجیتال داشته باشند و به کامپیوترها اجازه دهند آنها را سازماندهی و مدیریت کنند. اینترنت اشیاء نیازمند مکانیزم‌های محرمانگی، یکپارچگی، تصدیق هویت و کنترل دسترسی به صورت دقیق می‌باشد. اتصال میلیاردها شیء و ابزار به اینترنت به معنای افزایش آسیب‌پذیری‌های امنیتی بالقوه در دنیای مجازی است زیرا تا چند سال دیگر انواع لوازم‌خانگی،خودروها، درها و... هم به یکی از زیرمجموعه‌های صنعت فناوری اطلاعات مبدل می‌شوند. امنیت و حریم خصوصی از عمده‌ترین مشکلات IOTهستندکه مسئولان باید اقدامات لازم را برای رفع آنها بکار گیرند.در این مقاله مرور کوتاهی بر چالشهای پیش رو این فناوری خواهیم داشت سپس معماری امنیت ، و نیازمندی های امنیت را ارائه می کنیم .

کلیدواژه‌ها: اینترنت اشیا، چالش های پیش رو ، امنیت ،حریم خصوصی

National Conference
15/9 /2016
Kome elmavaran danesh
R.S. Institute
Article Code: 11015

[1] Internet of thing (IoT)

مقدمه

اصطلاح " اینترنت اشیا (IOT) "اولین بار توسط کوین اشتون در سال ۱۹۹۹ مطرح گردید. او جهانی را توصیف کرد که در آن هر چیزی، برای خود هویت دیجیتال داشته باشد و به کامپیوترها اجازه دهند آنها را سازمان‌دهی و مدیریت کنند. تعریفی که اتحادیه بین‌المللی مخابرات از "اینترنت اشیا" دارد بدین صورت می‌باشد: در هر زمان، هر مکان، برای هر کسی، ما اتصالی برای هر چیزی خواهیم داشت.IOT هنوز دیدگاه جدیدی است و در جامعه جا نیافتاده است. این روند قرار است جمع آوری، پروسه کردن، ذخیره سازی و توضیع اطلاعات را از حالت سنتی در آورده و به فرم نهایی مدرن خود برساند. به همین دلیل بسیاری از روش های سنتی امنیت IT در آینده کار برد نخواهند داشت و ما باید خود را برای این فصل جدید اول از لحاظ دیدگاهی و به زودی از نظر امنیت فیزیکی آماده نماییم .در آینده ای نزدیک حجمی وسیع از اطلاعات توسط وسایل متصل و سیستم های مدیریتی دریافت و ارسال خواهد شد. پیش بینی میشود که با ورود به عصر IOTحجم اطلاعات ورودی و خروجی شبکه ها چندین برابر خواهد شد و اطلاعات غیر منتظره جدیدی به این حجم نیز اضافه خواهد شد.در دنیای اینترنت اشیا، بسیاری از اشیا اطراف ما (شامل حسگرها و محرک‌ها بر اساس پروتکل‌های استاندارد ارتباطی، به یک شبکه‌ی جهانی متصل خواهندبود و داده‌های دریافت‌شده را میان بسترهای گوناگون به اشتراک خواهندگذاشت تا به هدف واحدی دست یابند. اصلی‌ترین نقطه‌ی قوت ایده‌ی IOT تأثیرات قابل توجه آن بر جنبه‌های مختلف زندگی روزمره هم‌چون خانه‌های هوشمند، حمل‌ونقل هوشمند، شهرهای هوشمند و سلامت الکترونیک است.در نظر داشته باشید که اطلاعات مرتب در حال حرکت و جابجایی است و با ورود IOTروش این جابجایی از حالت فعلی بسیار متفاوت خواهد بود. امنیت داشتن در حالت IOTو اتصال همه چیز به هم کاملاً از روند های فعلی متفاوت خواهد بود. ما باید به نقاط اتصالی و ارتباطی انتقال اطلاعات ما بین تمامی وسایل و ابر و شبکه ها بپردازیم و ایمنی را در آنجا بوجود آوریم. این مسئله در واقع به "فعل و انفعال، تعامل یا "Interaction به عنوان کلید کار اشاره میکند .با داشتن IOTمی توان پیش بینی کرد که مجرمان سایبری در مرحله اول به نقاط بوجود آمدن و انتقال اطلاعات، مراکز ارسال دستورات، نقاط و gateway های شبکه حمله خواهند نمود و محافظت را نیز باید برای این چالش ها فراهم نمود.

چالشهای اینترنت اشیاء

چندین مانع سبب کاهش سرعت توسعه IOT هستند موانع اصلی عبارتند از:

۱-امنیت برای اینترنت اشیاء

اینترنت اشیاء در حال تبدیل شدن به یک عنصر کلیدی از اینترنت آینده و یک زیرساخت حیاتی ملی و بین المللی می باشد .با این شرایط، تامین امنیت کافی برای زیرساخت های اینترنت اشیاء، اهمیت روزافزونی پیدا می کند .امنیت در "اینترنت اشیا" را باید در تمامی سطوح کاملا بررسی کرد .امنیت باید به صورت ابتدا تا انتها در نظر گرفته شود: امنیت در رمزگذاری داده‌ها در دستگاه‌ها، امنیت در رمزگذاری داده‌ها در مسیر انتقال (شبکه(، امنیت برای داده جمع‌آوری شده توسط سنسورها، امنیت در جمع‌آوری داده از طریق شبکه و امنیت داده‌های ذخیره شده روی پایگاه‌های داده و امنیت در سرویس مورد ارائه.

امنیت شبکه و اطلاعات با مؤلفه های شناسایی، محرمانگی، یکپارچگی و انکارناپذیری سنجیده می‌شوند. اینترنت اشیاء 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 اشیاء می‌توان پیش بینی کرد که مجرمان سایبری در مرحله اول به نقاط به وجود آمدن و انتقال اطلاعات، مراکز ارسال دستورات، نقاط ومدخل‌های[۲] 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 (Zou,Suo Wan, 2012).

به گزارش RCR Wireless News، تحلیلگران معتقدند ایجاد یک شبکه IoT مانند ساختن خانه‌ای با میلیون‌ها در و پنجره است، و همه آن چه که یک تبهکار یا سارق نیاز دارد این است که ببیند کدام یک از این در و پنجره‌ها باز مانده و به حال خود رها شده است.

پیشرفت ها در برخی حوزه ها برای ایجاد اینترنت اشیاء امن، مورد نیاز است تاIOTرادربرابراین مقاصد مختصمانه محافظت کندکه شامل موارد زیراست :

- حملات DOS / DDOS در حال حاضر به خوبی برای اینترنت فعلی قابل درک است .لیکن اینترنت اشیاء نیز مستعد ابتلا به چنین حملاتی است .تکنیک های خاص و سازوکارهایی برای حصول اطمینان از عدم غیرفعال سازی یا واژگونی زیرساخت های حمل و نقلی ،انرژی و شهری مورد نیاز است.
- تشخیص کلی حملات ، بازیابی ومقاومت برای مقابله با تهدیدات خاص IOT

- آگاهی از وضعیت سایبری ابزارها یا تکنیک ها که نیاز به توسعه دارندتا زیرساخت های مبتنی بر IOT نظارت، مدیریت و بررسی شوند .پیشرفت های مورد نیازبرای توانمندسازی اپراتور مطابق با حفاظت از IOT در طول چرخه عمر سیستم وکمک به اپراتورها، در اتخاذ مناسب ترین اعمال حفاظتی در طی حملات از جمله موارد مهم ومورد توجه است.
- اینترنت اشیاء نیاز به انواع کنترل دسترسی ها، طرح های حسابداری مربوط به حمایت از مجوزو استفاده از مدل های مختلف مورد نیاز کاربران، دارد .ناهمگونی و تنوع دستگاه ها یا درگاه های مورد نیازکنترل دسترسی،به طرح های سبک جدیدی برای توسعه نیاز خواهند داشت

- اینترنت اشیاء نیاز دا ردتا به طور مجازی همه سبک های عملیاتی را توسط خودش و بدون وابستگی به کنترل انسانی ،هدایت نماید.تکنیک های جدیدی مثل یادگیری ماشین ،برای هدایت به سوی IOT خودمدیریتی موردنیازاست.

۲-حفظ حریم خصوصی برای اینترنت اشیاء

دلایل متعددی برای به خطر افتادن اطلاعات موجود در IoT وجود دارد .این دلایل شامل موارد زیر است:

1-حملات لایه فیزیکی: یک هکر میتواند اطلاعات درون دستگاههای IoT را استخراج یا حذف کند و یا تغییر دهد، چرا که این دستگاهها در اکثر اوقات در محیط رها میشوند.

2-حمله به اطلاعات بیسیم: مهاجم ممکن است بتواند قبل از رسیدن اطلاعات به گیرنده، آن را بدست آورد.در این زمینه موضوعات مطالعاتی مختلف و متعددی از نظر امنیتی وجود دارد و یک چالش بزرگ محسوب میشود.

[2] gateway

۳- توان دفاعی پایین: بیشتر دستگاههای IoT امکان پذیرش بسته های امنیتی را به دلایلی مثل توان مصرفی، قدرت پردازشی، هزینه و صرفه جویی های دیگر، ندارند.

حریم خصوصی یک مقوله مهم در کشورهای متمدن است .حریم خصوصی یعنی فراهم آورنده اطلاعات(یا یک کاربر)تنها توسط مشاهده استفاده از سیستم وی قابل تشخیص باشد(و حداقل، تشخیص او باید بسیار سخت باشد.)

جمع آوری، هدایت و Mining اطلاعات در سیستمهای IoT به گونه دیگری صورت می گیرد و دلیل این امر، وجوداه حل های مختلف در سیستم های IoT است(مثل سیستم کنترل منابع خانه .)بنابراین برای تضمین حریم خصوصی اطلاعات شخصی، باید از سه موضوع اصلی زیر اطمینان حاصل کنیم.

1-چه کسی اطلاعات شخصی را جمعآوری میکند.

2-این اطلاعات چگونه جمعآوری میشوند.

۳-زمان فرایند جمع آوری چه قدر است.

ضمن اینکه باید تضمین شود که اطلاعات شخصی جمع آوری شده توسط افراد مجاز استفاده و در سرورهای مجازذخیره می شود .همچنین هر فرد باید بداند که چه اطلاعاتی از حریم خصوصی او در اختیار افراد مجاز قرار میگیردو تمام این فرایند با آگاهی، اجازه و رضایت وی انجام شود.

۳- اتکای بیش از اندازه بر فناوری

دیگر اشکالاتی وجود دارد که به طور مداوم در ارتباط با فناوری رخ میدهد، مخصوصا وقتی پای اینترنت هم در میان باشد . مشکل اینترنت اشیا، اتکای بیش از اندازه بر فناوری است. با پیشرفت زمان، نسل کنونی با دسترسی آسان به اینترنت و فناوری رشد یافته است. هرچند، تکیه بر اینترنت و گرفتن تصمیم بر مبنای اطلاعاتی که در آن وجود دارد، می‌تواند دردسر بیافریند، زیرا هیچ سیستمی بی‌اشکال نیست. همیشه بسته به میزان استفاده، اتکای انفرادی بر اطلاعات فراهم‌شده در صورت سقوط سیستم می‌تواند زیان‌بار باشد. هرچه بیشتر به اینترنت اعتماد کنیم و بیشتر به آن وابسته باشیم، درصورت خرابی، می‌تواند منجر به مصیبت بزرگتری شود .

۴-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.

۵-گسترش IPv6

در فوریه ۲۰۱۰ آدرس های IPv4 رو به اتمام بود. در حالی که تاثیر خاصی بر روی عموم مردم نداشت ، این وضعیت پتانسیل کاهش سرعت توسعه IOT را داشت زیرا میلیاردها سنسورها نیاز به آدرس IP های خاص خود دارند .علاوه بر این، IPv6 ، به

دلیل پیکربندی خودکار قابلیت ها و ویژگی های امنیتی ، موجب بهبود مدیریت آن شود اما این مورد برای سنسورها تعریف نگردیده بود .

۶- پروتکل های کم توان

دستگاه‌های بسیاری در سناریوهای "اینترنت اشیا" وجود دارند. چنین دستگاه‌هایی باید از نظر مشخصه‌های خاموشی، خاموشی کامل، دریافت، انتقال اطلاعات و وضعیت ترکیبی، در میان دیگر دستگاه‌ها متمایز باشند. علاوه بر این، از نظر در دسترس بودن خدمات، هر لایه ارتباطی با چالش دیگری در مورد میزان توان مصرفی مورد نیاز مواجه است. به‌عنوان‌مثال پیدا کردن یک دستگاه با پروتکل مناسب که به توان مصرفی کمتری نیاز داشته باشد در عین حال از در دسترس بودن خدمات در لایه MACنیز اطمینان داشته باشد، مشکل است.

۷-انرژی سنسور

برای رسیدن به پتانسیل کامل IOT ، نیاز به خودکفایی سنسورها داریم.تصور کنید که احتیاج به تعویض باتری در میلیاردها دستگاه های مستقر در سراسر این سیاره و حتی درفضا داشته باشیم. بدیهی است، این غیرممکن است. یک راه برای تامین انرژی مورد نیاز سنسور ، استفاده از برق عناصر زیست محیطی مانند ارتعاش، نور، و جریان هواست.

در ۲۴۱ امین نشست ملی و نمایشگاه انجمن شیمی آمریکادر ۱۹ مارس ۲۰۱۱، دانشمندان اعلام کردند که یک تراشه نانو تجار ی طراحی کرده اند ، که این چیپ تجاری با استفاده از حرکات بدن (مانند حرکت انگشتان) باعث تولیدالکتریسیته می شود. این توسعه [نانو] نشان دهنده یک نقطه عطف به سمت تولید لوازم الکتریکی قابل حمل است که می تواند توسط حرکات بدن بدون استفاده از باتری و یا پیگیری رسانه های الکتریکی موجب تغییر زندگی در آینده است. پتانسیل تنها توسط تصورات فرد محدود میشود. " زونگ لین وانگ "

۸. استانداردها

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. به‌منظور استانداردسازی باید طیف گسترده‌ای از موضوعات مانند لایه ارتباطات و پشته پروتکل، شامل لایه‌های فیزیکی (PHY) و کنترل دسترسی به رسانه(MAC) ، رابط‌های دستگاه، رابط تجمیع داده‌ها و رابط درگاه را در نظر داشت. با وجود اینکه پیشرفت های زیادی در زمینه استاندارد IoT صورت گرفته است اما به پیشرفتهای بیشتری درباره مسائل امنیتی، حریم خصوصی، معماری، و ارتباطات. IEEE نیاز داریم . یکی ازساختارهایی است که برای حل این چالش از بسته های IPv6 برای مسیر دهی در انوع مختلف شبکه ها استفاده می کند.

۹-ارتباط اشیا(مشکل با رابط های چندگانه)

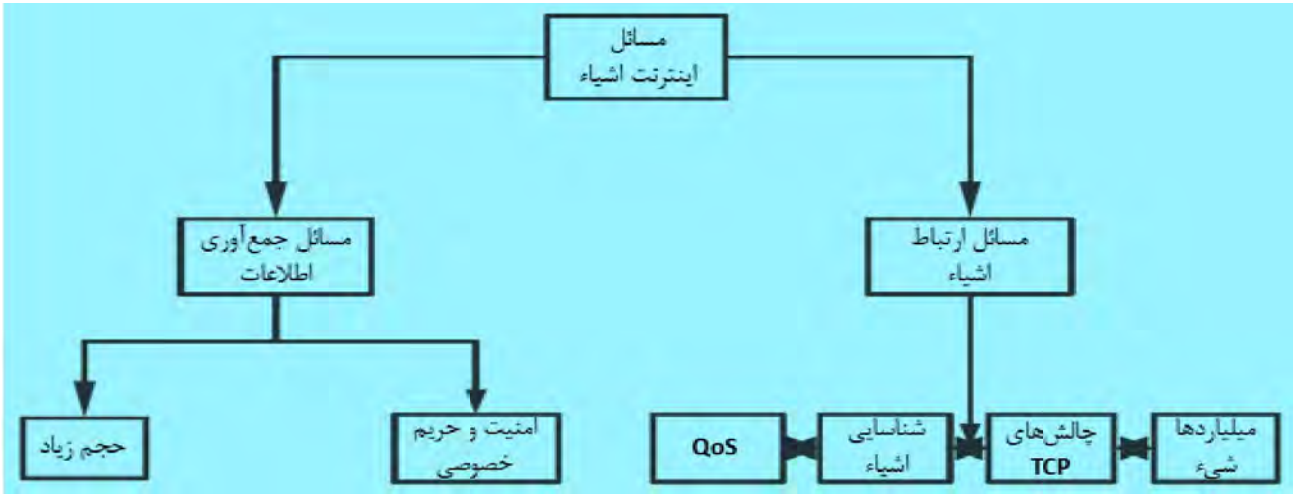
یکی دیگر از مشکلات این است که تعداد زیادی از دستگاه های متصل در اطراف وجود دارد که به صورت جداگانه هوشمند و مفید هستند، اما به عنوان یک "تیم "کار نمی کند. به این دلیل است که شما نمی توانید مجموعه ای از دستگاه های IOT را از یک محل واحد کنترل کنید و داده های آنها را همگام سازی نمایید. برای مثال اگر شما یک ماشین هوشمند، یک ردیاب تناسب اندام و یک ترموستات هوشمند داشته باشید، مجبور خواهید بود سه نرم افزار مختلف تلفن همراه برای هر یک از این ها

داشته باشید. شما نمی توانید یک قانون برای تنظیم درجه حرارت در اتاق با توجه به داده ردیاب تناسب اندام راه اندازی کنید .اگرچه در این زمینه پیشرفت هایی وجود دارد و چند شرکت عمده، مانند اتحادیه AllSeen و کنسرسیوم اتصال باز، در حال کار برای ایجاد یک استاندارد باز هستند که اجازه همکاری بین اکثر دستگاه های IOTرا خواهد داد.

۱۰-فقدان شغل :

اتصال هرچه بیشتر دستگاه‌ها به اینترنت منجر به فقدان شغل می‌شود .کنترل و هدایت دستگاه به صورت خودکار به وسیله اینترنت، تاثیری مخرب بر دورنمای استخدام کارگرهایی که تحصیلات کمتری دارند، خواهد داشت؛ زیرا دستگاه‌ها نه تنها می‌توانند با یکدیگر ارتباط برقرار کنند، بلکه اطلاعات را به صاحبان کارخانه‌ها منتقل می‌کنند. ما در حال حاضر هم شاهد هستیم که شغل ها تحت تاثیر ماشین‌های اتوماتیک قرار گرفته‌اند، مثل استفاده از خودپردازها..

دسته بندی دیگری از چالشهای اصلی اینترنت اشیا



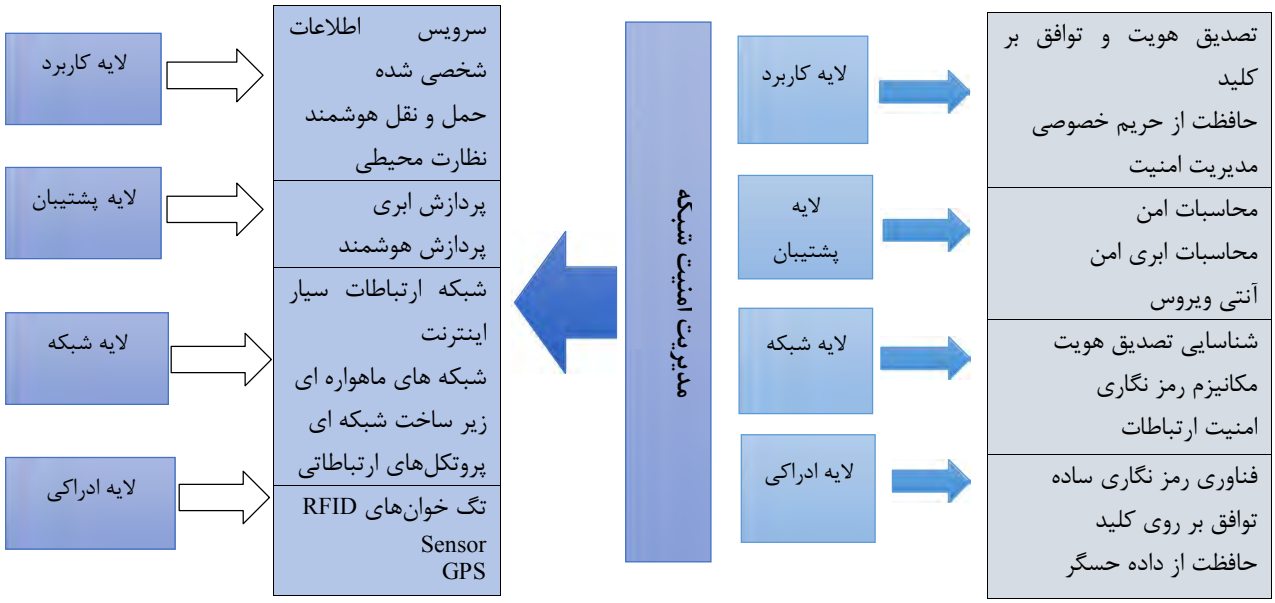
شکل ۱- دسته بندی چالشهای IOT

بررسی‌های سایت Computingدرحالی است ۳۹ درصد از مدیران ارشد دنیای فناوری اطلاعات نگرانی از نحوه ایمن‌سازی داده‌ها را چالش اصلی عرصه IOTمی‌دانند. ۳۴ درصد هم عدم شفافیت درزمینه درک هدف از استفاده از IOTو مزایای آن را نام‌برده‌اند.نگرانی در مورد به خطر افتادن حریم شخصی و نظارت‌ها و جاسوسی‌های دولتی و همین‌طور جمع‌آوری اطلاعات کاربران هم توسط ۲۷ درصد از پاسخ‌دهندگان مطرح‌شده است. ۲۵ درصد هم به مشکل عدم وجود استانداردهای فراگیر اشاره‌کرده‌اند و ۲۴ درصد پاسخ‌دهندگان مشکل نبود مهارت یا عدم استفاده از فناوری مناسب را مطرح کرده‌اند.

دیگر چالش‌های استفاده از IOTکه موردتوجه متخصصان قرارگرفته عبارت‌اند از عدم پذیرش به علت نگرانی‌های مربوط به حریم شخصی، نحوه مدیریت داده‌ها، مشکلات مربوط به زیرساخت‌ها، فقدان منابع و ضعف ارتباطات است.

معماری امن در اینترنت اشیاء

یکی از مکانیزم‌های ایجاد امنیت در اینترنت اشیاء بهره گیری از معماری مناسب می‌باشد. معماری اینترنت اشیاء دارای چهار سطح است. در شکل ۲ 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.



شکل۲- معماری امنیتیIoT و نیازمندی‌های امنیتی در هر لایه(Gubbi,2013)

نتیجه گیری

IOT نشان دهنده تکامل اینترنت در آینده می باشد با اینکه میدانیم انسانها می توانند به کمک این فناوری داده های خام را به اطلاعات، وسپس اطلاعات را به دانش و و در نهایت دانش را به خبرگی تبدیل نماید ،IOTاین پتانسیل را دارد تا دنیایی را که می شناسیم بهتر نماییم.اینترنت شیوه‌ی زندگی مردم را تغییر داده‌است و تعاملات میان انسان‌ها از دنیای واقعی به فضای مجازی گسترش یافته‌است. در این میان، IOTابعاد جدیدی در این فرآیند ایجاد کرده‌است و ارتباطات میان اشیا با دیدگاهِ «در هرزمان، هرمکان و با هروسیله» را امکان‌پذیر می‌سازد. با توجه به این‌که IOTجزئی از اینترنت آینده خواهدبود از این پس خود داده‌ها و اطلاعات باید نقطه‌ی تمرکز راهکارهای ارتباطی و شبکه‌بندی باشد. (فارغ از اینکه فرستنده یا گیرنده‌ی اطلاعات چه‌کسی است) از این‌رو، اخیراً مبحثی با عنوان شبکه‌های مبتنی بر اطلاعات مورد توجه بسیاری از پژوهشگران قرار گرفته‌است. مشخص است که در میان تمام چالش‌های موجود، چالش تأمین امنیت و حفظ حریم خصوصی افراد باید به دقت مطالعه شود و راهکارهایی ویژه‌ی IOT ارائه شود.هرچندIoTدروازه بزرگ و مهمی برای ورود به دنیایی با قابلیت‌های بیشتر برای بشر باز کرده،

در عین حال تهدیداتی بزرگ‌تر از همیشه را نیز متوجه زندگی ما کرده است. در این میان، اولین قدم برای فرار از این تهدیدات این است که هر فرد و نهادی، انفرادی خود را مسئول صیانت و حفاظت از همه اطلاعات بداند. همچنین نکته‌ای که بارها و بارها از سوی متخصصان امنیتی به آن اشاره شده، یعنی اقدامات پیشگیرانه و استفاده از عقل سلیم در برقراری ارتباطات مهم‌ترین نکته برای خنثی کردن این تهدیدات است.

منابع

1. Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 3, pp. 648-651). IEEE.
2. Alur R., Berger E., Drobnis A. W., Fix L., Fu K., Hager G. D. Zorn B. (2015). *System Computing Challenges in the Internet of Things*: A white paper prepared for the Computing Community Consortium committee of the Computing Research Association
3. Ren .L,(2015) IoT Security: Problems, Challenges and Solutions http://www.snia.org/sites/default/files/DSS-Summit-2015/presentations/Liwei Ren_Iot_Security_Problems_Challenges_revision.pdf
4. E Borgia, DG Gomes, B Lagesse, R Lea,D Puccinelli(2016)Special issue on "Internet of Things: Research challenges and Solutions" Computer Communications, Computer Communications Volumes 89–90, 1 September 2016, Pages 1–4 ,Internet of Things\: Research challenges and Solutions
5. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

۶. مفرح, حمید، ۱۳۹۳، بررسی فناوری ها، کاربردها و چالش های اینترنت اشیا و نگاهی به آینده ی آن، اولین همایش ملی فناوری و مدیریت دانش با محوریت اقتصاد مقاومتی، تربت حیدریه، دانشگاه تربت حیدریه

۷. شفیع پورمطلق, زهرا؛ امیرهوشنگ تاجفر و محمد قیصری، ۱۳۹۳، چالش های امنیتی رایانش ابری در فناوری اینترنتی از اشیاء، اولین کنفرانس ملی چالش های مدیریت فناوری اطلاعات در سازمان ها و صنایع، تهران، دانشگاه پیام نور،

۸. محمدحسام تدین ،نسرین تاج ،عاطفه ترکمن ۱۳۹۴،شناسایی مراکز تحقیقاتی،چالشها وراه حل ها در امنیت اینترنت اشیا،پژوهشگاه فناوری اطلاعات و ارتباطات