



چالشهای پیش روی اینترنت اشیاء

مهدی ازبک زایی

دانشجوی کارشناسی ارشد علوم محاسبات، دانشگاه استافورد شایر، انگلستان

mehdiozbak@gmail.com

چکیده

اینترنت اشیاء یکی از نوآوریهای جدیدی است که با توسعه شبکه های بی سیم و استفاده از وسایل هوشمند در حال گسترش می باشد و همانند هر فن آوری در تاریخچه جوامع انسانی با چالشها و مشکلات فراوانی روبرو است و لزوم شناسایی این مشکلات جهت استفاده بهتر از آن ضروری می باشد در این تحقیق سعی گردیده تا پس از معرفی اینترنت اشیاء به شناسایی مشکلات موجود در رابطه با آن پرداخته شود.

کلمات کلیدی: اینترنت اشیاء، چالش، شبکه بی سیم.



Internet of things challenges

Mahdi Ozbak Zaei

Master student in Computing Science, Staffordshire University, UK

Email:mehdiozbak@gmail.com

Abstract

The Internet of things is one of the newest technology that expanding by developing wireless network and using smart devices as every technology in human history face with new problems and challenges that is necessary to identify challenges for better using internet of things ,in this research tried after describing internet of things introduced problems related to that.

Key words: internet of things, challenges, wireless network.

۱. مقدمه

یکی از فن آوریهای نو ظهور که با توسعه شبکه های بی سیم و ابداع وسایل هوشمند جدید به زندگی روزانه انسانها ورود پیدا نموده، اینترنت اشیا^۱ می باشد که روند توسعه آن با سرعت زیادی در حال انجام می باشد. پیش بینی می گردد که تا سال ۲۰۲۰ تعداد ۲۱۲ میلیارد شیء^۲ تولید و مورد استفاده قرار گیرد (PISHVA, 2016). عبارت اینترنت اشیا در سال ۱۹۹۹ توسط کوین اشتون عرضه گردید و از آن زمان روند توسعه شبکه های بی سیم نظیر زاگی^۳، بلوتوث^۴، وای فای^۵ و... زمینه استفاده از وسایلی با توانایی ارتباط با اینترنت را فراهم نموده است تا مصرف کنندگان و شرکت ها به ابداع و استفاده از وسایلی با توانایی فرستادن اطلاعات در جهت تحلیل و راحتی بیشتر مصرف کنندگان اقدام نمایند، واژه هوشمند به تمام امکانات و وسایلی اطلاق می گردد که توانایی بهبود شرایط محیطی را بدون دخالت انسان برای مصرف کنندگان فراهم نمایند، خانه هوشمند، کارخانه هوشمند و در حالت کلی شهر هوشمند که تمام زیرساختهای آن به نوعی با اینترنت در ارتباط بوده و شهروندان قادر خواهند بود تا تمام نیازهای خود را با استفاده از اطلاعاتی که توسط سنسورهای نصب شده در جاهای مختلف فرستاده و در فضای رایانشی^۶ تحلیل گردیده اند برطرف نمایند. این فضای ترسیم شده که درگیر مستقیم با اشخاص و حریم خصوصی آنها دارد چالشهای فراوانی را ایجاد می نماید که لزوم پژوهشهای گسترده در جنبه های مختلف را می طلبد. کشورها از لحاظ موقعیت و درآمدهای حاصله و زیرساختهای موجود و ساختار جمعیتی و گروه بندی به کشورهای توسعه یافته و در حال توسعه تقسیم می شوند و مطمئنا چالشهای بیشتری برای اینترنت اشیا در این کشورها می توان متصور شد، در بخش های مختلف پس از معرفی اینترنت اشیا به مشکلات و چالشهای پیشرو به طور مشروح پرداخته و تحلیل می گردند.

۲. معرفی اینترنت اشیا

واژه اینترنت اشیا برای اولین بار در سال ۱۹۹۹ توسط کوین اشتون مورد استفاده قرار گرفت و از آن زمان سیر پیشرفت و توسعه آن صعودی بوده است، اینترنت اشیا را می توان شبکه ای از اشیا فیزیکی تعبیه شده با قطعات الکترونیکی، نرم افزار، سنسورها و اتصالات دانست که با تبادل اطلاعات مابین تولید کننده، اپراتور و یا دستگاههای دیگر قادر به ارائه ارزش و خدمات بیشتر می باشند، هر عضوی از اینترنت اشیا به تنهایی توسط سیستم تعبیه شده در آن قابل شناسایی است و قادر به تعامل با زیرساخت اینترنت موجود هستند، تبادل داده ها در اینترنت اشیا نیازی به حضور انسان نداشته و داده ها به صورت اتوماتیک و بر اساس تنظیمات انجام شده و در زمانهای مشخص به صورت دائم و یا لحظه ای ارسال می گردند، چنین توصیفی از اینترنت اشیا مرهون توسعه فن آوریهای بی سیم و سامانه های میکرو الکترونیک می باشد (ازبک زایی، ۱۳۹۵).

اشیا در این تکنولوژی به هر دستگاهی که دارای سنسور^۷ جهت تبادل اطلاعات است خطاب می شود، سنسورهای دما، ترافیک، تشخیص حرکت و تشخیص گازها نمونه ای از سنسورهایی است که به عنوان شیء در اینترنت اشیا بکار گرفته می شوند، تمامی این سنسورها اطلاعاتی را به دستگاه مقصد می فرستند تا بر اساس این اطلاعات تصمیماتی اتخاذ کنند (ازبک زایی، ۱۳۹۵). بزرگترین فایده اینترنت اشیا این است که به ما امکان می دهد تا با دنیای آنالوگ پیرامون خود (ماشین ها، مردم، حیوانات، گیاهان، و چیزهای دیگر) به زبان دیجیتال با تمام فواید ارتباطات دیجیتال سخن بگوییم (Kellmerit, 2013)، گرایشهای کلیدی که منجر به توسعه هر چه بیشتر این تکنولوژی شدند عبارتند از:

1-internet of things 2-thing 3-zigbee 4-bluetooth 5-WiFi 6-computing 7-sensor

۱-۲ کوچک سازی: بر اساس قانون مور و همچنین بهینه سازی در مدیریت انرژی الکترونیکی، دستگاههای کوچکتر و قدرتمندتر شدند.

۲-۲ قیمت: هزینه مولفه ها و شبکه های الکترونیکی نیز بر اساس قانون مور به صورت مداوم کاهش پیدا کرده است.

۲-۳ سیم زدایی: هر روزه چیزهای بیشتری به صورت بی سیم قابل استفاده می شوند و این بدان معنی است که آن ها می توانند در هر جایی قرار گیرند. حضور فراگیر و در حال رشد تلفن همراه و شبکه های وای فای دلیل اصلی این امر است.

معمولا زمانی که پیش نیازهای تکنولوژی فراهم باشد بکارگیری آن به سرعت اتفاق می افتد، استفاده از تلفن های همراه هوشمند مثال خوبی از این شرایط می باشد (Kellmerit, 2013). همانند اینترنت که پروتکل های ارتباطی از شبکه کامپیوترها پشتیبانی می کند در اینترنت اشیاء نیز استانداردهای متفاوتی از لایه های مختلف آن پشتیبانی می کند تا ارتباط موثرتر و ایمن تری بین اجزاء آن برقرار گردد. CoAp^۱ نمونه ای از اینگونه پروتکل هاست همچنین نرم افزارهای مختلفی جهت توسعه و کنترل ارتباط برخی از اجزاء اصلی آن تهیه گردیده است (Bani Yassein, 2016). تنوع در استانداردها و نرم افزارها در میان تولید کنندگان و شرکت ها خود یکی از چالشهای^۲ اینترنت اشیاء می باشد که در بخش های بعدی بیشتر توضیح می دهیم.

۳. معماری اینترنت اشیاء

معماری و اجزاء اینترنت اشیاء بر اساس چندین مدل معرفی گردیده و لایه های مختلفی برای اجزاء آن تعریف شده است، مدل های مختلف به ترتیب در سه، چهار، پنج و هفت لایه آن را تقسیم و هر لایه با اجزاء خاص ترسیم شده، مدل با لایه هفتگانه توسط شرکت سیسکو در سال ۲۰۱۴ معرفی شده است (Mohsen Nia, 2016)، اما آنچه بیشتر محققان در دنیا به آن اشاره نموده اند مدل چهارگانه است که به عنوان مبنا از آن استفاده نموده اند، در این مدل چهار لایه وجود دارد.

۱- لایه حسی^۳ (ادراکی): این لایه شامل انواع متفاوتی از سنسورها و حس گرها می باشد که وظیفه تعامل با محیط اطراف بعهدده آن است و اطلاعات بصورت خام دریافت می شود، میلیاردها سنسور و حسگر در این لایه نصب خواهند شد، انواع مختلفی از سنسور با کاربردهای متفاوت تولید شده که از ابزار پوشیدنی تا حس گرهای حرارتی نصب شده در داخل و بیرون منازل را شامل و به تعداد آنها روزانه افزوده می شود (اختری، ۱۳۹۴). این سنسورها بصورت وایرلس با همدیگر در ارتباط هستند و اطلاعات را منتقل می نمایند، این سنسورها فاقد حافظه می باشند و قابل برنامه ریزی نمی باشند که مشکلات امنیتی خاصی را ایجاد می نماید.

۲- لایه شبکه^۴: این لایه شامل تمام دستگاهها و ابزارهایی است که وظیفه تامین شبکه اتصالات حس گرها و سنسورها را بعهدده دارند، دروازه های ورودی، روترها نمونه ای از این ابزارها می باشند، شبکه های مخابراتی متفاوتی این وظیفه را انجام می دهند، شبکه های وای فای، بلوتوث، ال تی ای، جی اس ام نمونه هایی از اینگونه شبکه ها می باشند که از طریق دروازه های ورودی اطلاعات را از حس گرها دریافت و به لایه های بالاتر انتقال می دهند، دروازه های ورودی با داشتن محدودیت در حافظه و انرژی مصرفی فاقد توانایی و نصب سیستم های عامل و دیواره های آتش^۵ در جهت حفاظت از حمله های سایبری^۶ بوده و دارای مشکلات امنیتی خاصی می باشند (اختری، ۱۳۹۴).

1-Constrained Application Protocol 2-challeng 3-Perception Layer 4-Network Layer 5-Fire Wall 6-Cyber Attacks

۳- لایه میان پوششی^۱: این لایه شامل دریافت اطلاعات از لایه شبکه و پردازش و ذخیره اطلاعات می باشد، سرورها و رایانش ابری نمونه ای از ابزارهای این لایه می باشند، با توجه به قابلیت خوب نصب نرم افزارهای ویژه حفاظتی و سیستم عامل های متفاوت کاربر پسند این لایه مشکلات امنیتی کمتری داشته (اختری، ۱۳۹۴).

۴- لایه کاربردی^۲: این لایه وظیفه ارتباط با کاربر و یا کاربران را که طیف وسیعی را شامل می شوند و در واقع مصرف کننده گان اطلاعات پردازش شده لایه میان پوششی هستند را شامل می شود، برنامه های متفاوتی که در گوشی های هوشمند، تبلت ها، کامپیوترها برای کنترل اشیاء همانند لامپهای هوشمند بر اساس سیستم های عامل متفاوت مثل اندروید، ویندوز، مک اینتاش جهت ارتباط با اشیاء تهیه گردیده نمونه هایی از اینگونه برنامه ها می باشند که وظیفه ارتباط

کاربر را با اطلاعات پردازش شده در سرورها و فضای رایانش ابری بر عهده دارند(اختری،۱۳۹۴)، این لایه دامنه کاربرد اینترنت اشیا را در محیط های متفاوت تعیین می نماید حوزه هایی همچون حمل و نقل، سلامت، خانه های هوشمند، ساخت و ساز، نفت و گاز... پس از معرفی مختصر لایه های اینترنت اشیا به مبحث چالشهای آن می پردازیم.

۴. چالشهای پیشروی اینترنت اشیا

همانگونه که با ورود فن آوریهای جدید در میان جوامع بشری همواره مسائل و مشکلات خاصی همراه با فواید بیشتر آنها ایجاد شده، اینترنت اشیا نیز نمونه ای دیگری از این فن آوریهای خلاقانه عصر اطلاعات می باشد که با ورودش مشکلات و مسائل خویش را بهمراه آورده است. محققین مختلف در سراسر جهان در حال رصد کردن این موضوع هستند و در کارهای تحقیقی آنها به این موضوعات پرداخته شده است. متأسفانه مسائل حل نشده اینترنت و فضای مجازی و شبکه ها که اینترنت اشیا وارث آنهاست بصورت خودکار وارد این فن آوری شده است، این مشکلات در نقاط مختلف کره زمین و متفاوت و در برخی نقاط پر رنگ تر می باشد، اما مهمترین چالشهای پیشرو در بیشتر نقاط فارق از توسعه یافتگی و عدم توسعه یافتگی موارد زیر می باشد.

۴-۱ چالشهای امنیتی^۱: از مهمترین مشکلاتی که متأسفانه در محیط اینترنت به صورت کامل حل نگردیده است مسئله امنیت داده ها و اطلاعات مبادله شده میان لایه های متفاوت اینترنت اشیا می باشد، هک^۲ نمودن یخچال هوشمند جهت استفاده از ای میل های شخصی از مواردی است که بدلیل ضعف در سیستم امنیتی اینگونه اشیا رخ داده است (صنعت جو، ۱۳۹۴)، مطمئناً هیچ کسی دوست ندارد که اطلاعات محرمانه پزشکی او که از طریق وسایل پوشیدنی به بیمارستان و پزشک معالج منتقل می گردد توسط هکرها به سرقت رود. دسترسی غیر مجاز به داده ها^۳، نسخه برداری اطلاعات^۴، استراق سمع کردن^۵، حقه زدن^۶، پارازیت RF، حمله سیبل^۷ و... نمونه هایی از حملات احتمالی توسط سارقین و خرابکاران اینترنت اشیا می باشند (Mohsen Nia, 2016)، همچنین تنوع در استانداردها و نرم افزارهای به کار رفته در اینترنت اشیا خود باعث کاهش ضریب ایمنی شده و امکان نفوذ و سرقت حمله کنندگان سایبری از اطلاعات شخصی و سازمانی ذخیره شده و یا مبادله ای بین گره های شبکه بی سیم را فراهم می نماید.

1-security challenges 2-hack 3-Unauthorized Access to the Tags 4-Tag Cloning 5-Eavesdropping 6-Spoofing 7-Sybil Attack

۴-۲ حریم خصوصی^۱: یکی از مهمترین دغدغه های اصلی در اینترنت اشیا حفظ حریم خصوصی می باشد، بکارگیری ابزارها و اشیا متفاوت می تواند به حریم خصوصی افراد لطمه وارد نماید، دوربین های هوشمند، انتقال صدا، سنسورهای حرکتی بعنوان نمونه لامپ های نوری هوشمند با قابلیت تشخیص حرکت می توانند ساعات خروج و ورود به منازل را ذخیره و به سادگی توسط سارقین اطلاعات مورد سوء استفاده قرار گیرد (Byfield, 2016)، در کشورهای مختلف با بهبود پروتکل های امنیتی سعی در بهبود حریم خصوصی نموده اند.

۴-۳ ذخیره اطلاعات: با گسترش اینترنت اشیا و ایجاد داده های فراوان یکی از مهمترین چالشهای پیش رو ذخیره نمودن این اطلاعات می باشد، سرورها و مراکز داده ها وظیفه ذخیره حجم عظیم اطلاعات را خواهند داشت (Byfield, 2016).

۴-۴ دفع زباله های الکترونیکی: از مهمترین چالش های پیشرو که همه محصولات الکترونیکی را شامل می شود پس ماندهای میلیارد ها سنسور، باتریها کوچک، قطعات پلاستیکی و مدارهای الکترونیکی معیوب و آسیب دیده می باشند که می توانند آسیب های جدی به محیط زیست وارد نمایند (Byfield, 2016).



۴-۵ تقاضای انرژی: استفاده از میلیاردها سنسور و دروازه های ورودی و سرورهای ذخیره و پردازش اطلاعات نیازمند مصرف انرژی الکتریکی فراوانی می باشد و افزایش تقاضا برای تولید الکتریسیته بیشتر خود می تواند آسیبهای زیست محیطی بیشتری همانند گرمایش جهانی را تشدید نماید (Byfield,2016).

۴-۶ چالش های مالی: این مسئله بیشتر در کشورهای در حال توسعه مطرح می باشد که نیازمند سرمایه گذاری برای ایجاد اینترنت اشیا و خرید تجهیزات سخت افزاری و نرم افزاری مورد نیاز می باشد (Byfield,2016).



نتیجه گیری

منافع محتمل اینترنت اشیاء و کمک به بهبود زندگی انسانها راه را برای توسعه اینترنت اشیاء فراهم می نماید و چالشهای پیشرو بمرور کمتر خواهند شد و یا در مسیر مناسب با کمترین آسیبهای فردی و اجتماعی و محیط زیستی قرار خواهد گرفت اما تا آن زمان نیاز به شناسایی بیشتر و مطالعه دقیق تری در تمام سطوح اینترنت اشیاء داشته تا راههای نفوذ و سوء استفاده سارقین و یا گروههای خاص از اطلاعات خصوصی ذخیره شده جلوگیری بعمل آید و همچنین متخصصین با بکارگیری الگوریتم های پیچیده در تبادل اطلاعات در سطوح مختلف اینترنت اشیاء به ایمن نمودن آن کمک نمایند و تولید کنندگان حس گرها و باتریهایشان با بکارگیری مواد کمتر مضر و بادوام تر از ایجاد میلیونها تن پس ماندهای غیر قابل بازیافت جلوگیری بعمل آورند تا بتوان از مزایای اینترنت اشیاء بدون نگرانی استفاده نمود.

مراجع

ازبک زایی م، ۱۳۹۵. اینترنت اشیا و هوشمند سازی شهری، اولین کنفرانس و نمایشگاه مدیریت و فن آوری اطلاعات و ارتباطات، تهران.

اختری م، ۱۳۹۴. تجزیه و تحلیل نگرانی های امنیتی در اینترنت اشیا، اولین کنفرانس حسابداری و مدیریت در هزاره سوم، رشت.

صنعت جو م، ۱۳۹۴. حمله سایبری به یخچال برای دسترسی به اطلاعات جی میل، ماهنامه شبکه، شماره ۱۷۳

1-privacy

Kellmerit D, Obodovski D, September 2013. The Silent Intelligence: The Internet of Things, Published September 20th 2013 by Dnd Ventures LLC.

PISHVA D, 2016. Internet of Thing: Security and Privacy Issues and Possible Solution, ICACT Transactions on Advanced Communications Technology (TACT) Vol. 5, Issue 2, March 2016.

Bani Yassein M, Shatnawi MQ and Al-zoubi D, 2016. Application Layer Protocols for the Internet of Things: A survey, Engineering & MIS (ICEMIS), International Conference on.

Mohsen Nia A, K. Jha N, 2016. A Comprehensive Study of Security of Internet-of-Things, IEEE Transactions on Emerging Topics in Computing, Volume: PP, Issue: 99.

Byfield B, June 2016. The Internet of Things: 7 Challenges.