توسعه فناوری اینترنت اشیاء و امنیت

علی سخنور

دانشجوی ارشد هوش مصنوعی , دانشگاه آزاد اسلامی واحد تهران غرب

Sokhanvar_ali۱۳۶۰@yahoo.com

چکیده

در دهه گذشته، اینترنت اشیاء 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.

کلمات کلیدی : اینترنت اشیاء، امنیت، حریم خصوصی، قابلیت اعتماد، چالش ها, معماری امن

۱- مقدمه

اینترنت اشیاء[۱] یکی از فناوری‌های نوین در عصر کنونی است. اما حوزه های کاربردی آن هنوز به طور کامل مورد تحلیل و بررسی قرار نگرفته است. پس از فراگیر شدن کاربرد اینترنت اشیاء، موضوع امنیت و محرمانگی آن توجه زیادی را به سمت خود جلب کرده و به موضوعی بحث بر انگیز در این حوزه مبدل شده است. حفاظت از IoT فعالیتی پیچیده و مشکل است. اینترنت اشیاء نیازمند مکانیزم‌های محرمانگی، یکپارچگی، تصدیق هویت و کنترل دسترسی به صورت دقیق می‌باشد. اینترنت کنونی در حال حاضر به طور مداوم به علت مشکلات فنی ، قانونی و انسانی تحت حملات متعددی قرار می‌گیرد. اینترنت اشیاء نوآوری آینده در زمینه تکنولوژی‌های بی سیم محسوب می‌شود. این پدیده، صدها چالش‌های امنیتی جدید به وجود خواهد آورد که باید به تفصیل مورد بررسی قرار گیرند. چالش دیگری که در این حوزه مطرح می‌شود این مسئله است که اینترنت اشیاء باعث افزایش و تعمیق شکاف دیجیتال می‌شود. در این نوشتار مرور کوتاهی بر مباحث امنیتی پیش رو این فناوری و تأثیراین فناوری بر شکاف دیجیتالی خواهیم داشت.

۲- اینترنت اشیاء

اینترنت، کامپیوترها را در سراسر جهان به هم متصل می‌کند و از طریق شبکه جهان گستر[۲] یک پلات فرم جهانی برای ذخیره سازی، اشتراک منابع و ارائه خدمات ایجاد می‌کند. در سال‌های اخیر

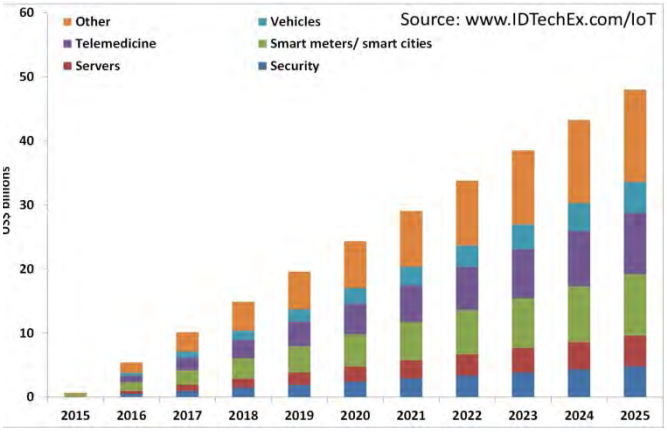
[۱]-Internet of thing(IoT)

[۲]-World Wide Web

پیشرفت‌ها در زمینه فناوری اطلاعات باعث سرعت بخشیدن به توسعه جهان مجازی شده است. از طرفی تکنولوژی‌های مبتنی بر وب متعددی مانند وب معنایی، پردازش شبکه ای، پردازش سرویس گرا و محاسبات ابری دنیای شبکه ای را نه تنها به یک پلات فرم تحقیقاتی/ خدماتی ، بلکه به یک فضای همکاری و ارتباطات جهانی با جوامع ، انجمن‌ها و سازمان‌های مجازی مختلف تبدیل کرده است[۱].

بسیاری دانشمندان بر این باورند که توسعه محاسبات پوشیدنی و تعبیه شده انقلاب آینده در فناوری‌های دیجیتال را رقم خواهند زد، و افزایش سلامت، بهره‌وری، امنیت، راحتی و طیف گسترده ای از اطلاعات مفید برای افراد و سازمان‌ها را در پی خواهد داشت.از طرفی چالش‌هایی در حیطه محرمانگی شخصی، پیچیدگی تکنولوژی و ایجاد شکاف دیجیتال مطرح خواهند شد. طبق گزارشات مرکز تحقیقاتی پو[۱] در ماه می سال ۲۰۱۴ ، اینترنت اشیاء تا سال ۲۰۲۵ رشد قابل توجهی خواهد داشت[۳].

با این که فعالیت در حوزه‌ی فناوری اینترنت اشیاء از اوایل دهه ۹۰ میلادی آغاز شد، اما اصطلاح "اینترنت اشیاء" را کوین اشتون در سال ۱۹۹۹ ارائه کرد. اینترنتِ اشیاء مفهومی جدید در دنیای فناوری اطلاعات و ارتباطات است. به صورت خلاصه اینترنت اشیاء فناوری مدرنی است که در آن برای هر موجودی (انسان، حیوان و یا اشیاء) قابلیت ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترانت ، فراهم می‌گردد. طبق گفته گارتنر بیش از ۵۰ درصد اتصالات اینترنت بین IoT ها می‌باشد، که در سال ۲۰۱۱ تعداد آن‌ها بیش از ۱۵ بیلیون تخمین زده شد و پیش بینی می‌شود تا سال ۲۰۲۰ به ۳۰ بیلیون دستگاه برسد [۲].هم چنین مطابق شکل ۱ ارزش بازار نودهای آدرس دهیIoT از کمتر از ۱ بیلیون دلار در سال ۲۰۱۵ به ۴۸ بیلیون دلار در سال۲۰۲۵ می‌رسد[۳].



شکل ۱- ارزش تجاری IoT(Courtesy: IDTechEx,۲۰۱۴)

فناوری‌های تعبیه شده از قبیل شناسایی خودکار رادیویی[۲]، فناوری‌های ارتباطات بی سیم، شبکه های حسگر، شبکه تجهیزات تعبیه شده ، و شبکه محرک (SEA-شبکه) فناوری اینترنت اشیاء را شکل می‌دهد. وب اشیاء[۳] بر اساس اینترنت اشیاء ایجاد شده است. WoT بر اساس تکنولوژی‌هایی نظیر پروتکل‌های اینترنتی، فناوری‌های سنسور و تلفن‌های هوشمند و فناوری RFID کار می‌کند. بر اساس پیشرفت‌های سریع در ارتباطات سیار ، شبکه های حسگر بی سیم و RFID ، مکانیزم‌های مختلف IoT می‌توانند با یکدیگر در هر مکان، هر زمان و به هر شکل یکپارچه شوند. [۵]

فرآیند ارسال داده‌ها در فناوری اینترنت اشیاء بدین ترتیب است که به سوژه‌ی مورد نظر یک شناسه‌ی یکتا و یک پروتکل اینترنتی[۴]تعلق می‌گیرد که داده‌های لازم را برای پایگاه داده‌ی مربوطه ارسال می‌کند. داده‌هایی که توسط ابزارهای مختلف از قبیل گوشی‌های تلفن همراه و انواع رایانه‌ها و تبلت‌ها قابل مشاهده خواهند بود. فرآیند ارسال داده‌ها در فناوری اینترنت اشیاء نیازی به تعامل «انسان با انسان» یا «انسان با رایانه» نخواهد داشت و داده‌ها به صورت اتوماتیک و بر اساس تنظیمات انجام شده و در زمان‌های مشخص (معمولاً به صورت دائم و لحظه‌ای) ارسال می‌گردند.

۱-Pew research center

۲ -RFID
۳ -Web of things
٤ - IP

در حال حاضر کاربرد های فناوری‌های مختلف اینترنت / وب و اینترنت اشیاء مانند وب ۲، وب ۳، جهان هوشمند، محاسبات سبز و ... به ادغام جهان اجتماعی، فیزیکی و مجازی سرعت می‌بخشد. می‌توان پیش بینی کرد که جهان سایبری تشکیل شده از کامپیوترها، با جهان اجتماعی تشکیل شده از افراد و جهان فیزیکی متشکل از اشیاء در آینده تلفیق خواهد شد. به بیان دیگر ابر جهان[۱] از IoT/WoT تشکیل شده است و تأثیر عمیقی بر زندگی و کار افراد ایجاد می‌کند [۷]

اینترنت اشیا به ما فرصت‌ها و چالش‌های جدیدی ارائه می‌دهد و اگر این فناوری درست به کار برده شود، برای کار و زندگی آینده تحولی عظیم و نوبه وجود خواهد آورد.

۳- مشکلات و دغدغه های امنیتی اینترنت اشیاء

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 دولت ها فراهم کرده است. مشکلات ناشی شده از انتقال و پردازش داده های ناخواسته ، موجب نگرانی های 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 شخصی شان 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 اشیاء رویکرد این جابجایی بسیار متفاوت از حالت فعلی خواهد شد. امنیت اینترنت اشیاء به واسطه اتصال همه دستگاه ها 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 [۶]

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 اشیاء، 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 یک اصول اولیه کار قرار داده‌اند اما به اعتقاد کارشناسان، اینترنت اشیاء بعد از عبور از مرحله"ایمن نمایشی"به مرحله"خطرناک درحال کار"خواهد رسید و بی‌شک ، برخورد واقعی با بدافزار نویسان ، شرایط را به گونه دیگری تغییرخواهد داد [۶]

امنیت شبکه و اطلاعات با مؤلفه های شناسایی، محرمانگی، یکپارچگی و انکارن اپذیری 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 و مدخل‌های[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 [۴]

اینترنت اشیاء 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 اشیاء نمایش داده شده است. همان طور که مشاهده می‌کنید محرمانگی و امنیت به عنوان بلوک‌های سازنده فنی کلیدی مورد نیاز می‌باشند.

---

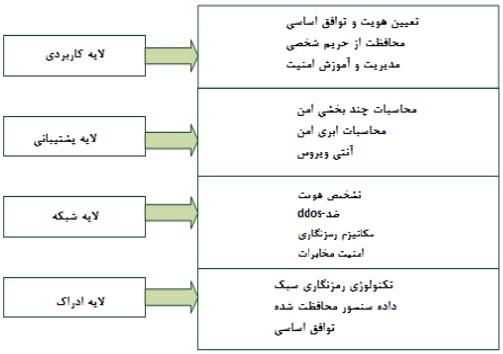
۱ -hyper world

۲- gateway

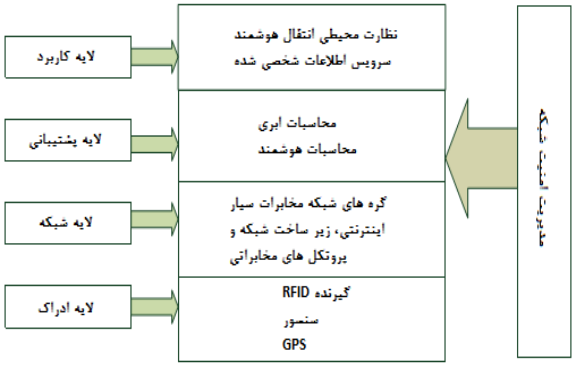
شکل۲. نیازمندی‌های امنیتی IoT [۴]

۴- 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 ۳ چهار سطح IoT، در سمت چپ و در سمت راست نیازمندی‌های امنیتی هر لایه،برای آشنایی با لایه های معماری این فناوریو 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 نوشتارنمی‌گنجد.



شکل۳- معماری امنیتیIoT



شکل ۴- نیازمندی‌های امنیتی در هر لایه[۵]

۵- اینترنت اشیاء و تشدید شکاف دیجیتال

از دیگر دغدغه های مطرح در اینترنت اشیاء ، افزایش شکاف دیجیتال می‌باشد. افرادی که به شبکه دیجیتالی متصل نیستند یا تمایلی به اتصال به این شبکه را ندارند در صورت فراگیر شدن اینترنت اشیاء از بسیاری خدمات محروم خواهند شد. دانشمندان زیادی به توزیع نابرابر امکانات اشاره کرده و متذکر شدند احتمال شکل گیری شکاف اجتماعی بین افرادی که منابع لازم برای پرداخت هزینه تجهیزات ، مهارت و سواد اطلاعاتی برای کار در محیط‌های با فناوری پیچیده را ندارند، وجود دارد. این مسئله نه تنها به تفاوت دسترسی به فناوری‌ها بین اقشار مختلف جامعه بلکه به تفاوت‌های فرهنگی، جغرافیایی، ساختار اجتماعی اشاره دارد. اینترنت اشیاء مزایای زیادی برای افراد در کشورهای توسعه یافته ، ایجاد خواهد کرد. هم چنین تأثیر به سزایی بر روی صنایع همگانی مانند آب و برق و انرژی خواهد داشت. شایان ذکر استاین فناوری به کشورهای در حال توسعه با نگرش‌های توسعه ای کوتاه مدت کمک کمتری خواهد کرد[۷].

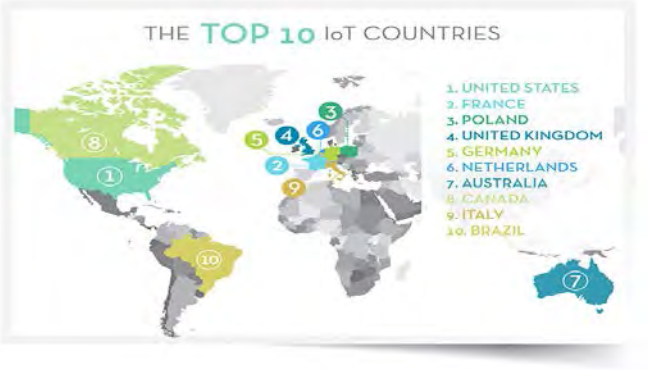
باید توجه داشت که امروزه با وجود قطع اتصال رایانه و دستگاه‌ها به اینترنت نمی‌توان از حفظ امنیت و حریم شخصی مطمئن بود و همین نگرانی در سطوحی بالاتر در مورد دیگر وسایل قابل اتصال به اینترنت وجود خواهد داشت. البته افرادی هم که به استفاده از اینترنت اشیاء علاقه دارند، ممکن است کاربرد آن را به خصوص در محیط‌های کاری غیرانسانی بدانند. امروزه از وسایل الکترونیک پوشیدنی برای کنترل کارمندان در محیط‌های کاری استفاده می‌شود. در آینده انجام این کار با پیشرفت فناوری به مراتب آسان‌تر بوده و موجب نقض حریم شخصی افراد و تبدیل آن‌ها از نظر کارفرمایان به اعداد خواهد شد. بنابراین ممکن است تا سال ۲۰۲۵ یعنی زمان همه‌گیر شدن اینترنت اشیاء دیگر اثری از حریم شخصی باقی نماند و انسان‌ها روح خود را از دست

بدهند و این دغدغه باعث می‌شود پذیرش این فناوری توسط برخی افراد و سازمان‌ها دیرتر صورت پذیرد.

دو نوع شکاف از عدم توسعه IoT ناشی می‌شود که به منزله دو روی یک سکه هستند. از یک طرف مانند دیگر فناوری‌های اطلاعاتی و ارتباطاتی شکاف دیجیتال به تفاوت در ویژگی‌های جمعیت شناختی نظیر(سن، درآمد، جنسیت، تحصیلات و ...) و دسترسی به ICT درون یا بین کشورها اشاره دارد و شکاف دیگری که با عنوان شکاف دانشی از آن یاد می‌کنیم از نداشتن مهارت و قدرت برای استفاده از تراکنش‌های خودکار داده و مدیریت این تراکنش‌ها بین اشیاء و فعالیت‌هایIoT اشاره دارد.کسانی که خود را با روند توسعه فناوری‌های جدید وفق ندهند با خطر از دست دادن دانش و مهارت‌های خود روبرو می‌شوند.

شکاف دیجیتالی به عنوان یکی از چالش‌های توسعه IoT محسوب می‌شود. هر چند این فناوری تا حدی بر افراد تحمیل می‌شود (مثال خوبی در این زمینه، جابه‌جایی‌های هوشمند، مانند شهرهای هوشمند ، حمل و نقل هوشمند، سلامت الکترونیک، کارخانجات هوشمند می‌باشد)، دسترسی و توزیع فناوریIoT با توجه به منطقه جغرافیایی متفاوت خواهد بود و در الگوهای کاری، فعالیت‌های سیاسی و مدنی و فعالیت‌های روزانه نفوذ خواهد کرد. از طرفی با توجه به نفوذ IoT در تمامی ابعاد زندگی تهدید افراد توسط بد افزارها مورد توجه قرار می‌گیرد. با وجود این که رشد شبکه های اجتماعی، نوعی شکوفایی دموکراسی در جامعه دانش محور به شمار می‌رفت، IoT نمونه ای دیگر از کنترل و ناتوانی افراد بر حفاظت از حریم خصوصی‌شان محسوب می‌شود و فضای تولید دانش اشتراکی و خلاقیت توسط IoT محدود می‌شود. بعلاوه کنترل توزیع شده IoT مواردی در زمینه پاسخگویی و مسئولیت پذیری به وجود می‌آورد، جایی که ردیابی مبدأ و مقصد داده و تراکنش‌های آن‌ها امکان پذیر می‌شود و این نیز نمونه ای از شکاف دانشی ناشی شده از IoT می‌باشد.

همان طور که در شکل ۴ نشان داده شده است ده کشور برتر در فناوری IoT بیشتر کشورهای توسعه یافته هستند و می‌توان نتیجه گرفت گسترشIoT در کشورهای توسعه یافته بیشتر از کشورهای در حال توسعه بوده و همین موضوع باعث افزایش شکاف دیجیتال بین این کشورها می‌شود.



شکل ۵- ده کشور برتر در استفاده از IoT[۳]

پیچیدگی این فناوری باعث می‌شود بسیاری افراد نتوانند از آن بهره گیرند. طبق گزارش‌ها، کشورهای توسعه یافته هنوز نتوانسته‌اند استفاده از این فناوری را کاملاً مقرون به صرفه کنند. هم چنین بسیاری کشورها استفاده از IoT را در محیط کار به دلیل نقض امنیت، غیر انسانی قلمداد می‌کنند.

از طرفی با وجود رشد اینترنت و کامپیوتر هنوز نسبت کمی از جمعیت به این فناوری دسترسی دارند و از مزایای آن استفاده می‌کنند. هر چند ویژگی IoT دسترسی همیشگی به آن است، هنوز همه مردم به آن دسترسی نداشته و این سؤال مطرح می‌شود که افرادی از این فناوری محرومند چه مزایایی را از دستمی‌دهند؟ چه تضمینی وجود دارد که زندگی افرادی که داوطلبانه یا غیر داوطلبانه از این فناوری استفاده می‌کنند، دچار آسیب نمی‌شود؟

۶- نتیجه گیری

اینترنت اشیاء به جای کاهش شکاف دیجیتال ممکن است حتی آن را تعمیق کند. بسیاری از افراد ممکن است نتوانند یا نخواهند از این سبک زندگی نوین استقبال کنند و آن را به دلایل اقتصادی، سیاسی، مالی، امنیتی، مذهبی و فرهنگی در تعارض با آنچه مطلوب می‌پندارند، بدانند. حال اگر بنگاه‌های بزرگ اقتصادی و دولت‌ها تصمیم بگیرند به سمت استفاده از اینترنت اشیاء حرکت کنند و عده‌ای از شهروندان تمایلی به این امر نداشته باشند، شکاف‌ها و اختلافات اجتماعی تشدید خواهد شد. چون با نصب دستگاه‌ها و سیستم‌های جدید فناوری مبتنی بر اینترنت اشیاء، به عقاید و دیدگاه‌های این افراد بی‌توجهی خواهد شد. مجبور کردن مردم به خرید لوازم خانگی قابل اتصال به اینترنت و طراحی آن‌ها به گونه‌ای که عدم استفاده از چنین قابلیت‌هایی مشکلاتی ایجاد کند نیز، از جمله دغدغه های این فناوری بوده است.

پیچیدگی جهان مبتنی بر اینترنت اشیاء و تبعات امنیتی آن ممکن است بسیاری از افراد یا کشورها را به عدم استفاده از دستاوردهای این پدیده ترغیب کند. کاربرد فناوری‌های یاد شده به نفع بسیاری از کشورهای در حال توسعه است، اما ممکن است این کشورها به دلایل دیگری از جمله هزینه‌های سنگین قادر به استفاده از آن نباشند و تمامی این موارد باعث تعمیق شکاف دیجیتال می‌شود. از طرفی دغدغه های امنیتی پیش روی این فناوری باید به دقت مورد بررسی قرار گیرند و سیاست‌های مناسب برای مقابله با این تهدیدات و ترغیب افراد، دولت‌ها و کشورها جهت تمایل به استفاده از این فناوری، اتخاذ گردند. تردیدی وجود ندارد که اینترنت اشیاء در کنار مزایایش، مشکلاتی هم دارد و صاحب نظران و سیاست‌گذاران باید از هم اکنون در اندیشه مقابله با چالش‌های آن باشند.

تقدیر تشکر:

با تشکر از استاد عزیز جناب آقای دکتر مقسمی و حمایت های ایشان که اینجانب را در جهت پیش برد هر چه بهتر این مقاله راهنمایی کردند .

۷- منابع :

[۱] Bruce D. Weinberg , George R. Milne , Yana G. Andonova b, Business Horizons (۲۰۱۵)

Fatima M. Hajjat ", Internet of Things: Convenience vs. privacy
and secrecy"
[۲] Journal of Computer and Communications, ۲۰۱۵, ۳, ۱٦٤-۱۷۳,Published Online May ۲۰۱۵ in SciRes.
http://www.scirp.org/journal/jcc,http://dx.doi.org/۱۰.٤۲۳٦/jcc.۲۰۱۵.۳۵۰۲۱, Received January ۲۰۱۵,
Internet of Things (IoT): A Literature Review
[۳] International Workshop on Big Data and Data Mining Challenges on IoT and Pervasive Systems (BigD۲M ۲۰۱۵)" New Security Architecture for IoT Network"
[٤] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, Moussa Ayyash ,
COMST.۲۰۱۵.۲٤٤٤۰۹۵, IEEE Communications Surveys & Tutorials"Internet of Things: A Survey on Enabling Technologies, Protocols and Applications"
[۵] Feng Chen,, Pan Deng, JiafuWan, Daqiang Zhang,Athanasios V. Vasilakos,۵ and Xiaohui Rong ",Received January ۲۰۱۵; Accepted ۱ March ۲۰۱۵Data Mining for the Internet of Things:Literature Review and Challenges"
[٦] Future Generation Computer Systems ۲۹ (۲۰۱۳) , Internet of Things (IoT): A vision, architectural elements, and future directions