

تحلیل چالش‌های فراروی توسعه فناوری اینترنت اشیا: تهدیدات امنیتی و شکاف دیجیتالی

سال اول | شماره ۷ | مهر ۹۴

ماهنامه

نوشتار کوتاه

ساناز شفیعی

دانشگاه تربیت مدرس، تهران، ایران

HP



تحلیل چالش‌های فراروی توسعه فناوری اینترنت اشیا:

تهدیدات امنیتی و شکاف دیجیتالی

ساناز شفیعی

دانشگاه تربیت مدرس، تهران، ایران

Sanaz.shafiee@modares.ac.ir

۱ مقدمه

بسیاری دانشمندان بر این باورند که توسعه محاسبات تعبیه شده انقلاب آینده در فناوری‌های دیجیتال را رقم خواهند زد، و افزایش سلامت، بهره‌وری، امنیت، راحتی و طیف گسترده‌ای 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. اینترنت اشیا^۱ یکی از فناوری‌های نوین در عصر کنونی است. اما حوزه‌های کاربردی آن هنوز به طور کامل مورد تحلیل و بررسی قرار نگرفته است. 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 نو به وجود خواهد آورد (Roman, Najera, 2011). اینترنت اشیا مزایای زیادی برای افراد در کشورهای توسعه یافته، ایجاد خواهد کرد. هم چنین تأثیر به‌سزایی بر روی صنایع همگانی مانند آب و برق و انرژی خواهد داشت. (SY, 2015) پس از فراگیر شدن کاربرد اینترنت اشیا، موضوع امنیت و محرمانگی آن توجه زیادی را به سمت خود جلب کرده و به موضوعی بحث برانگیز در این حوزه مبدل شده است. حفاظت از IoT فعالیتی پیچیده و مشکل است. اینترنت اشیا 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 اشیا نوآوری آینده در زمینه تکنولوژی‌های بی‌سیم محسوب می‌شود (Anderson, 2014). 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 اشیا باعث افزایش و تعمیق شکاف دیجیتال می‌شود. در این نوشتار مرور کوتاهی بر مباحث امنیتی پیش رو این فناوری و تأثیر این فناوری بر شکاف دیجیتالی خواهیم داشت. بدین منظور ابتدا به معرفی فناوری اینترنت اشیا و مفاهیم مرتبط با آن، سپس به بررسی نیازمندی‌های امنیتی این حوزه می‌پردازیم و یک مدل معماری امن ارائه می‌شود، در

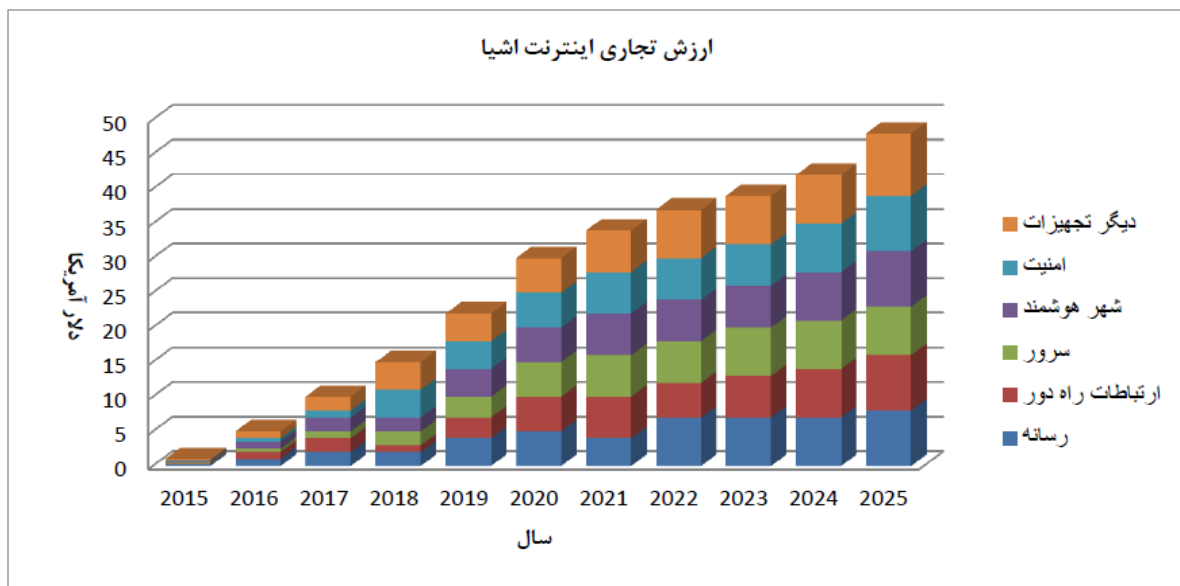
^۱ - Internet of thing (IoT)



آخر درباره تاثیر این فناوری بر شکاف دیجیتال بحث خواهد شد.

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 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 (Zhong, 2013). طبق گزارشات مرکز تحقیقاتی پو ۳ در ماه می سال ۲۰۱۴، اینترنت اشیاء تا سال ۲۰۲۵ رشد قابل توجهی خواهد داشت (Anderson et al, 2014). 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. اینترنت 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 بلیون تخمین زده شد و پیش بینی می‌شود تا سال ۲۰۲۰ به ۳۰ بلیون دستگاہ برسد (Abomhara, 2014). هم چنین مطابق شکل ۱ ارزش بازار نودهای آدرس دهی IoT از کمتر از ۱ بلیون دلار در سال ۲۰۱۵ به ۴۸ بلیون دلار در سال ۲۰۲۵ می‌رسد (Courtesy IDTechEx, 2014).



شکل ۱- ارزش تجاری IoT (Courtesy: IDTechEx, 2014)

فناوری‌های تعبیه شده از قبیل شناسایی خودکار رادیویی^۴، فناوری‌های ارتباطات بی سیم، شبکه‌های حسگر، شبکه تجهیزات تعبیه

² -World Wide Web

^۳ -Pew research center

^۴ -RFID

شده، و شبکه محرک اینترنت اشیا را شکل می‌دهد. وب اشیا^۵ بر اساس اینترنت اشیا 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، شبکه‌های حسگر بی سیم و RFID، مکانیزم‌های مختلف IoT می‌توانند با یکدیگر در هر مکان، هر زمان و به هر شکل یکپارچه شوند (Bandyopadhyay, 2011). فرآیند ارسال داده‌ها در فناوری اینترنت اشیا بدین ترتیب است که به سوژه‌ی مورد نظر یک شناسه‌ی یکتا و یک پروتکل اینترنتی^۶ 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 اشیا 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 ارسال می‌گردند. در حال حاضر کاربرد های فناوری‌های مختلف اینترنت / وب و اینترنت اشیا 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 اشیا در آینده تلفیق خواهد شد. به بیان دیگر ابر جهان^۷ از IoT/WOT تشکیل شده است و تأثیر عمیقی بر زندگی و کار افراد ایجاد می‌کند (Khoo, 2010).

۳ مشکلات و دغدغه‌های امنیتی اینترنت اشیا

دنیای دیجیتال، با داده‌های 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 داده‌های ناخواسته، موجب نگرانی‌های کاربران و مسائل قانونی شده است (Whitmore, Agarwa, 2014). 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 آینده‌ای 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 (Gang, Zeyong, 2011).

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 «ایمن‌نمایی» به مرحله «خطرناک» در حال کار خواهد رسید و بی‌شک، برخورد واقعی با بد افزار نویسان، شرایط را به گونه دیگری تغییر خواهد داد (Lyne, 2014). اینترنت

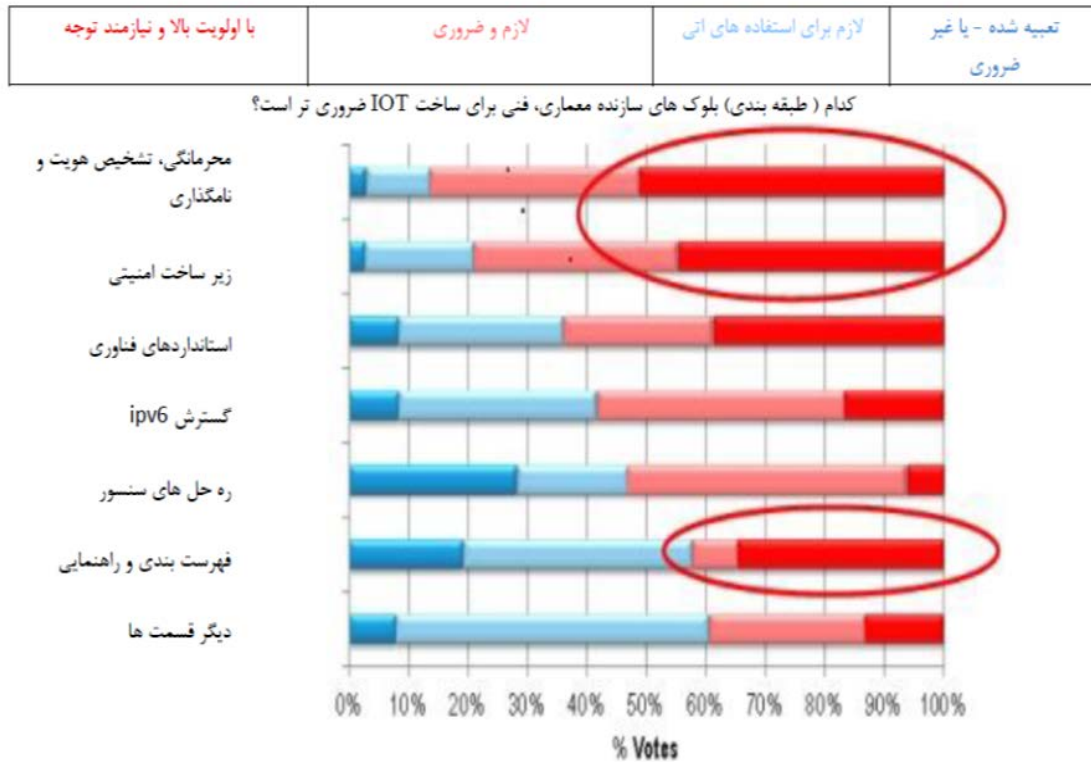
۵ -Web of things

6 - IP

۷ -hyper world



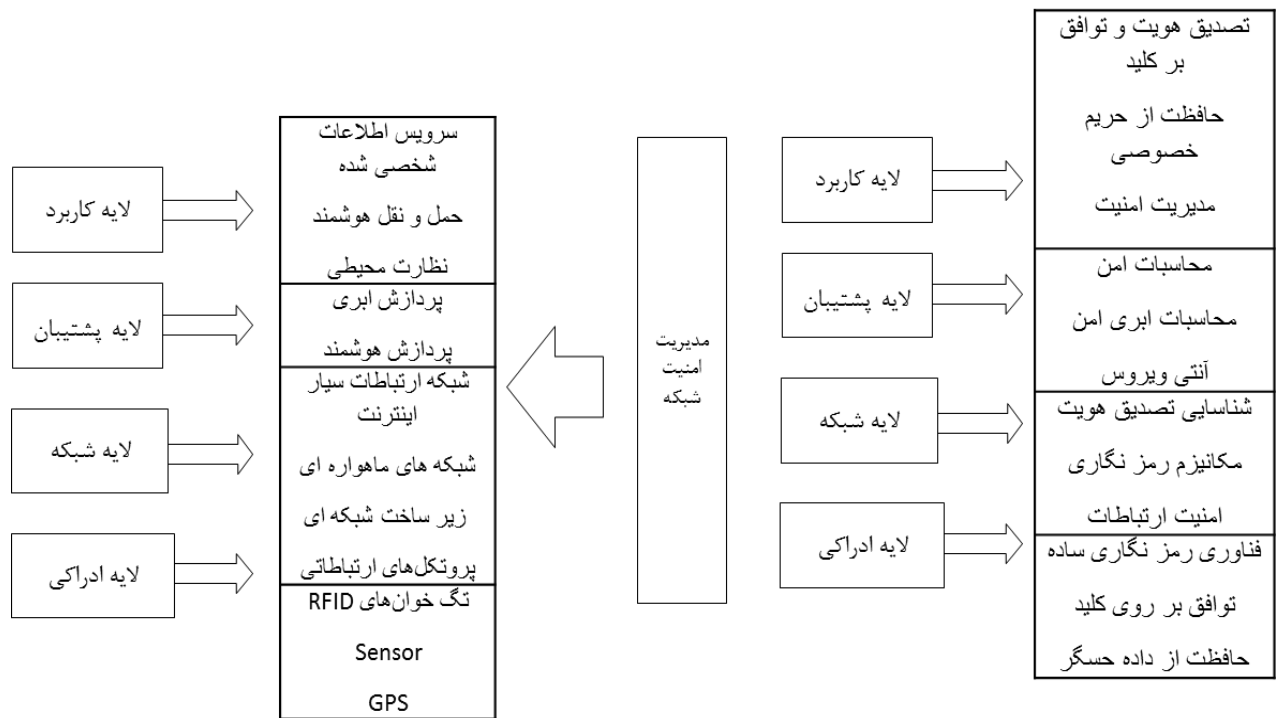
اشیاء با چالش‌های زیادی رو به رو است. از نظر مقیاس پذیری برنامه‌های کاربردی IoT به تعداد زیادی از دستگاه‌ها نیاز دارد که پیاده‌سازی آن‌ها به دلیل محدودیت‌های زمان، حافظه و پردازش مشکل است. به عنوان مثال محاسبه تغییرات روزانه دمایی در محدوده یک کشور به دستگاه‌های زیادی نیازمند است و مدیریت بر داده‌های زیادی را می‌طلبد (Silicon Valley brainstorm, 2013). در شکل ۲ نیازمندی‌های امنیتی ضروری برای اینترنت اشیا نمایش داده شده است. همان‌طور که مشاهده می‌کنید محرمانگی و امنیت به عنوان بلوک‌های سازنده فنی کلیدی مورد نیاز می‌باشند.



شکل ۲. نیازمندی‌های امنیتی IoT (Silicon Valley brainstorm, 2013)

۳.۱ معماری امن در اینترنت اشیا

امنیت شبکه و اطلاعات با مؤلفه‌های 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 شبکه حمله خواهند نمود و محافظت را باید برای این نقاط فراهم نمود. (Zou, Suo, Wan, 2012). با توجه به نفوذ فناوری اینترنت اشیا در تمامی ابعاد زندگی و تهدید افراد توسط بد افزارها، استفاده از یک معماری امن برای مقابله با این قبیل تهدیدات مورد توجه قرار می‌گیرد. یکی از مکانیزم‌های ایجاد امنیت در اینترنت اشیا بهره‌گیری از معماری مناسب می‌باشد. معماری اینترنت اشیا دارای چهار سطح (لایه ادراکی، لایه پشتیبان، لایه شبکه و لایه کاربرد) است. در شکل ۳ چهار سطح IOT، در سمت چپ و در سمت راست نیازمندی‌های امنیتی هر لایه به صورت جداگانه، نمایش داده شده است (Gubbi, 2013). بحث پیرامون نحوه عملکرد این ۴ لایه و سیستم امنیتی آن‌ها مبحث جداگانه‌ای را می‌خواهد که در این نوشتار نمی‌گنجد.



شکل ۳- معماری امنیتی IoT و نیازمندی‌های امنیتی در هر لایه (Gubbi,2013)

۴ اینترنت اشیا و تشدید شکاف دیجیتال

از جمله دغدغه های مطرح در اینترنت اشیا، 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 اشیا 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. شایان ذکر است این فناوری به کشورهای در حال توسعه با نگرش‌های توسعه ای کوتاه مدت کمک کمتری خواهد کرد (SY,2015). 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 اشیا 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 اشیا دیگر اثری از حریم شخصی باقی نماند و انسان‌ها روح خود را از دست بدهند و این باعث می‌شود پذیرش این فناوری توسط برخی افراد و سازمان‌ها دیرتر صورت پذیرد (IDTechEx,2014).

دو نوع شکاف از عدم توسعه IoT ناشی می‌شود که به منزله دو روی یک سکه هستند. از یک طرف مانند دیگر فناوری‌ها، شکاف دیجیتال به تفاوت در ویژگی‌های جمعیت شناختی نظیر (سن، 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 اشیا و فعالیت‌های IoT 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 می‌باشد)، دسترسی و توزیع فناوری IOT با توجه به منطقه جغرافیایی متفاوت خواهد بود و در الگوهای کاری، فعالیت‌های سیاسی و مدنی و فعالیت‌های روزانه نفوذ خواهد کرد. با وجود این که رشد شبکه‌های اجتماعی، نوعی شکوفایی دموکراسی در جامعه دانش محور به شمار می‌رفت، IOT نمونه‌ای 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 نمونه‌ای از شکاف دانشی ناشی شده از IOT می‌باشد (Anderson, 2014). طبق آمار شکل ۴، ده کشور برتر در فناوری IOT بیشتر کشورهای توسعه یافته هستند و می‌توان نتیجه گرفت گسترش IOT در کشورهای توسعه یافته بیشتر از کشورهای در حال توسعه بوده و همین موضوع باعث افزایش شکاف دیجیتال بین این کشورها می‌شود.



| | |
|----|---------------------|
| ۱ | ایالات متحده امریکا |
| ۲ | فرانسه |
| ۳ | لهستان |
| ۴ | بریتانیا |
| ۵ | آلمان |
| ۶ | هلند |
| ۷ | استرالیا |
| ۸ | کانادا |
| ۹ | ایتالیا |
| ۱۰ | برزیل |

شکل ۴- ده کشور برتر در استفاده از IOT (Thingspeak, 2014)

۵ 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 دغدغه‌های 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 دغدغه‌های 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 صاحب‌نظران و سیاست‌گذاران باید از هم اکنون در اندیشه مقابله با چالش‌های آن

باشند.

بعلاوه با رویکردی انتقادی می‌توان استدلال کرد که پیچیدگی این فناوری باعث می‌شود بسیاری افراد نتوانند از آن بهره‌گیرند. طبق گزارش‌ها و نظر دیگر متخصصین در این حوزه، کشورهای توسعه یافته هنوز نتوانسته‌اند استفاده از این فناوری را کاملاً مقرون به صرفه کنند. هم‌چنین بسیاری کشورها استفاده از IoT را در محیط کار به دلیل نقض امنیت، غیر انسانی قلمداد می‌کنند (Abomhara, 2011). از طرفی با وجود رشد اینترنت و کامپیوتر هنوز نسبت کمی از جمعیت به این فناوری دسترسی دارند و از مزایای آن استفاده می‌کنند (SY, 2015). 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 دست می‌دهند؟ چه تضمینی وجود دارد که زندگی افرادی که داوطلبانه یا غیر داوطلبانه از این فناوری استفاده می‌کنند، دچار آسیب نمی‌شود؟

۶ مراجع

Anderson, Janna. et al. (2014). The internet of thing will thrive by 2025, Pew Research Center.

Abomhara, M., & Koien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. In Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on (pp. 1-8). IEEE.

Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1), 49-69.

IDTechEx. (2014). Internet of Things (IoT): Business Opportunities 2015-2025, www.IDTechEx.com/research.

Gang, G., Zeyong, L., & Jun, J. (2011). Internet of things security analysis. In Internet Technology and Applications (iTAP), 2011 International Conference on (pp. 1-4). IEEE.

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.

Khoo, B. (2010). RFID - from tracking to the Internet of Things: A review of developments. *Proceedings of the IEEE/ ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*

Silicon Vally. (2013). New Digital Economics Executive Brainstorm and Innovation Forum, , San Francisco.

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.

SY, P. (2015). Defending Privacy e Dark Side of IoT, Automating Cryptography.



Whitmore, A., Agarwal, A., & Da Xu, L. (2014). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, 1-14.

Zhong, N., Ma, J. H., Huang, R. H., Liu, J. M., Yao, Y. Y., Zhang, Y. X., & Chen, J. H. (2013). Research challenges and perspectives on Wisdom Web of Things (W2T). *The Journal of Supercomputing*, 64(3), 862-882.

لینک مقالات دیگری از « ساناز شفیعی »

در سایت نوشتار کوتاه www.scoder.ir

آمادگی الکترونیک ضرورت توسعه جامعه دانش بنیان

