تاریخ دریافت:۱۳۹۷/۰۸/۰۱
تاریخ پذیرش:۱۳۹۸/۰۱/۰۶

فصلنامهٔ مطالعات حفاظت و امنیت انتظامی
فصلنامهٔ علمی- ترویجی
سال سیزدهم، شمارهٔ چهل و نهم، زمستان ۱۳۹۷

اینترنت اشیاء، بایدها و نبایدها

امیر پناهی[۱]

چکیده

زمینه و هدف: اینترنت اشیاء مفهومی جدید در دنیای فنّاوری اطلاعات و ارتباطات است. به صورت خلاصه اینترنت اشیاء فنّاوری مدرنی است که در آن برای هر موجودی قابلیت ارسال داده از طریق شبکه‌های ارتباطی فراهم می‌گردد. با توجه به اینکه در آینده نه‌چندان دور از اینترنت اشیا، در برنامه‌های کاربردی مانند مراقبت پزشکی (نظارت بر بیمار از راه دور، نظارت بر سالمندان)، شبکه هوشمند، اتوماسیون خانگی (امنیتی، گرمایشی، رعد و برق) و شهرهای هوشمند (پایش آلودگی، حوادث غیرمترقبه) استفاده خواهد شد، باید چهارچوب مناسب این سامانه‌ها طراحی شود. این قراردادها باید قابلیت اطمینان و امنیت بالایی داشته باشند تا بتوانند در مقابل نفوذ و حملات به سیستم‌ها مقاومت نمایند.

روش‌شناسی: این مقاله از نوع تحقیقات کاربردی است و اطلاعات آن به شیوهٔ اسنادی و کتابخانه‌ای جمع‌آوری شده است. در این مقاله سعی شده است بایدها و نبایدها در این حوزه نوظهور بررسی و بر اساس آن پیشنهادهایی ارائه گردد.

یافته‌ها و نتیجه‌گیری: اینترنت اشیا در واقع آیندهٔ اینترنت را نشان می‌دهد که تمام ابزارها و وسایل با هم در ارتباط هستند و می‌توانند درکی از محیط اطراف خود داشته و با دیگر وسایل و ابزار ارتباط برقرار نمایند. برای برقراری این ارتباط نیاز به قراردادهای ارتباط وجود دارد تا دستگاه‌ها بتوانند از طریق آن با اینترنت و دیگر دستگاه‌ها ارتباط داشته باشند از این رو بررسی جنبه‌های امنیتی این فنّاوری و میزان امنیت قراردادهای به کارگیری شده برای انجام احراز هویت یک نیاز ضروری برای کاربران مختلف این فنّاوری است؛ بنابراین، با توجه به مطالب یاد شده در این مقاله سعی شد چالش‌ها و مشکلات امنیتی این فنّاوری به دقت مورد بررسی قرار گیرد.

کلیدواژه‌ها: اهمیت محرمانگی، اینترنت اشیاء، پایش دسترسی، حریم خصوصی، شکاف اطلاعاتی.

---

۱ کارشناس ارشد امنیت اطلاعات (Panahiamir2020@gmail.com).

مقدمه

کوین اشتون، بنیانگذار و مدیر اجرایی مرکز آتو- آیدی[1] در ام آی تی[2]، نخستین فردی بود که واژهٔ اینترنت اشیاء را در سال ۱۹۹۹ در حوزهٔ مدیریت زنجیرهٔ تأمین مطرح کرد (http://www.rfidjournal.com) با وجود این، در دههٔ اخیر، این مفهوم به دلیل شبکه های «IoT» جدید از جمله سلامت بهداشتی الکترونیکی و انتقال اطلاعات و... تعمیم و گسترش پیدا کرده است (Sundmaeker, H; Guillemin, P; Friess, P; Woelfflé, S, 2010).

بر طبق مفهوم «ITU»، در طراحی «IoT» پایه، تمام اشیاء در سراسر دنیا قابل دسترس هستند. اشیاء تبدیل به رایانه نمی‌شوند؛ اما دارای قابلیت‌های محدود شده رایانه‌ای و ماهیت هوشمندتری هستند (ITU. The Internet of Things; ITU Report: Genf, Switzerland, 2005). اینترنت اشیاء شامل فنّاوری‌های متنوعی نظیر معماری، حسگر، شناسایی، رمزگذاری، انتقال و پردازش داده‌ها، شبکه، اکتشاف و غیره می‌شود.

منبع رشد و تکامل «IoT»، هم‌گرایی فنّاوری‌های بی‌سیم، پیشرفت‌های دستگاه‌های میکروالکترومکانیکی[3] و الکترونیک‌های دیجیتالی است که منجر به تولید دستگاه‌های بسیار کوچک با قابلیت حس‌کردن و محاسبه و ارتباط بدون سیم می‌شوند. در حیطهٔ «IoT»، تعامل بین انسان‌ها و ماشین‌ها بیش از پیش مدنظر قرار می‌گیرد، چرا که ماشین‌ها روز به روز هوشمندتر شده و می‌توانند وظایف انسانی بیشتری را انجام دهند. در این وضعیت، انسان‌ها باید به ماشین‌ها اطمینان داشته و احساس امنیت کنند. یک

---

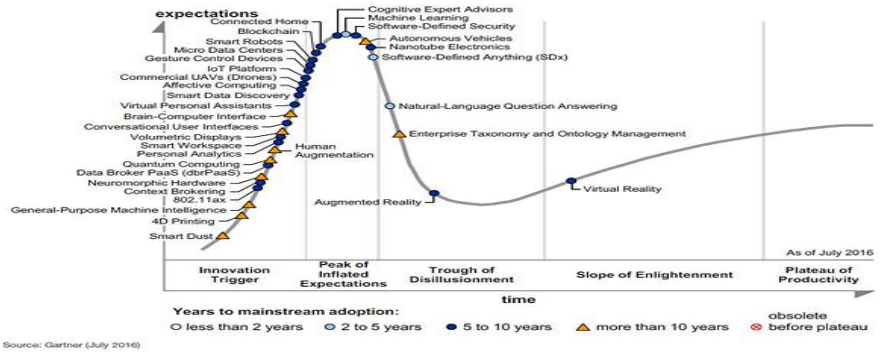
1 Auto-ID Center
2 MIT
3 MEMS

شیء ممکن است (دستگاهی پزشکی) برای تسهیل نظارت مستمر به روی بیمار در یک برنامهٔ مراقبت بهداشتی باشد و یا شیء به صورت یک شتاب‌سنج برای حرکت باشد که در محیط مزرعه‌ای به یک گاو متصل شده است.

(http://www.gartner.com/technology/research/hype-cycles).

طبق گفته گارتنر بیش از ۵۰ درصد اتصال های اینترنت بین «IoT»هاست که در سال ۲۰۱۱ تعداد آنها بیش از ۱۵ بیلیون تخمین زده شد و پیش‌بینی می‌شود تا سال ۲۰۲۰ به ۳۰ بیلیون دستگاه برسد (Abomhara , M, & Koien, G. M, 2014, pp. 1-8).

مطابق شکل ذیل ارزش بازار نودها آدرس‌دهی «IoT» از کمتر از ۱ بیلیون دلار در سال ۲۰۱۵ به ٤٨ بیلیون دلار در سال ۲۰۲۵ رسیده است (www.IDTechEx.com/research, 2014).



شکل۱- گزارش چرخهٔ هایپ[1] فنّاوری‌های در حال ظهور در سال ۲۰۱۷ توسط گارتنر

در حال حاضر مفاهیمی که شامل اینترنت اشیا می‌شود مانند شبکه‌های حسگر بی‌سیم[2]، ارتباطات ماشین به ماشین، ارتباطات بی‌سیم شخصی با توان پایین[3] و یا فنّاوری‌هایی مانند «RFID» است.

1 hype
2 WSN
3 LoWPAN

اینترنت اشیا در واقع آیندهٔ اینترنت را نشان می‌دهد که تمام ابزارها و وسایل با هم در ارتباط هستند و می‌توانند درکی از محیط اطراف خود داشته و با دیگر وسایل و ابزار ارتباط برقرار نمایند. برای برقراری این ارتباط نیاز به قراردادهای ارتباط وجود دارد تا دستگاه‌ها بتواند از طریق آن با اینترنت و دیگر دستگاه‌ها ارتباط داشته باشند.

برقراری این ارتباط با استفاده از قراردادهای ارتباطی اینترنتی موجود می‌تواند در زمینهٔ سنجش از راه دور هزینه‌بر باشد، زیرا قراردادهای اینترنت دارای برنامه‌هایی است که نیاز به منابع (پردازش، حافظه، انرژی و ...) زیادی داشته و به دلیل اینکه دستگاه‌های سنجش از راه دور دارای منابع محدودی به خصوص از لحاظ انرژی هستند نمی‌توانند کارایی لازم را داشته باشند.

با توجه به اینکه در آینده ای نه‌چندان دور از اینترنت اشیا، در برنامه‌های کاربردی مانند مراقبت پزشکی (نظارت بر بیمار از راه دور، نظارت بر سالمندان)، شبکهٔ هوشمند، اتوماسیون خانگی (امنیتی، گرمایشی، رعد و برق) و شهرهای هوشمند (پایش آلودگی، حوادث غیرمترقبه) استفاده خواهد شد باید قراردادهای مناسب این مجموعه‌ها طراحی شود همچنین این قراردادها باید قابلیت اطمینان و امنیت بالایی داشته باشند تا بتوانند در مقابل نفوذ و حمله ها به مجموعه‌ها مقاومت نمایند. قراردادهای موجود در این زمینه باید داری معیارهای مهمی مانند قابلیت اطمینان، بهره‌وری بالا، پشتیبانی از اینترنت و مصرف بهینهٔ انرژی باشند به علاوه این قراردادها از لحاظ امنیتی نیز باید در سطح بالایی قرار داشته باشند.

با رشد سریع کاربردهای «IoT»، مفاهیم امنیتی مورد توجه قرار می‌گیرند و نگرانی‌هایی در زمینهٔ محرمانگی و حریم خصوصی شکل می‌گیرد. اگر فعالیت روزانهٔ افراد نظارت شده و آنها تولیدکنندهٔ خروجی‌های اطلاعاتی باشند، فعالیت‌های سیاسی، اقتصادی و اجتماعی تحت تأثیر قرار می‌گیرند. در صورت نقض امنیت، وقوع حمله و اختلال در عملکرد، مزایای «IoT» کم‌رنگ می‌شود. در آینده‌ای نزدیک حجمی وسیع از اطلاعات توسط وسایل متصل و مجموعه‌های مدیریتی دریافت و ارسال خواهند شد.

در نظر داشته باشید که اطلاعات به صورت مرتب در حال حرکت و جابه‌جایی است و با ورود اینترنت اشیاء رویکرد این جابه‌جایی بسیار متفاوت از حالت فعلی خواهد شد. امنیت اینترنت اشیاء به‌واسطهٔ اتصال همهٔ دستگاه‌ها به یکدیگر به طور کامل متفاوت از روندهای معمول خواهد بود. ما باید به نقاط اتصال و ارتباط و انتقال اطلاعات بین تمامی وسایل و فضای ابر و شبکه‌ها توجه کرده و امنیت را در هر حال برقرار نماییم (Gang, G, Zeyong, L, & Jun, J. 2011، pp. 1-4).

به این ترتیب اینترنت اشیاء حتی با قابلیت‌های پیشرفتهٔ خود، در تبادل اطلاعات از نظر امنیت، مفهومی ناقص است؛ که در فاز اولیهٔ خود و قبل از توسعه به گستردگی از آن استقبال شده است. در این تحقیق ما در ارتباط با فنّاوری‌های مختلف، اتصال و تعامل که در اینترنت اشیاء، برای تبادل اطلاعات میان دستگاه‌ها استفاده می‌شود و می‌تواند حریم خصوصی کاربران را به نحوی تهدید کند را بررسی می‌کنیم.

با افزایش انواع حمله‌ها، به دلایلی مانند مسائل سیاسی، اقتصادی، اجتماعی و... همچنین استفادهٔ گسترده از فنّاوری اینترنت اشیاء در مشاغل و سازمان‌های مختلف و با در نظر گرفتن این موضوع که مشتریان اینترنت اشیاء هنوز به این فنّاوری اعتماد کامل ندارند (مسائل مربوط به حریم خصوصی)، بهبود و ارتقای امنیت در این مجموعه‌ها امری ضروری و صد البته اجتناب‌ناپذیر است.

مهم‌ترین ابزاری که برای تأمین امنیت این سامانه‌ها مورد استفاده قرار می‌گیرد قراردادهای به کار گرفته شده برای احراز هویت و حفظ حریم خصوصی است. به دلیل کم‌هزینه‌بودن و ارزان بودن تجهیزات به‌کار گرفته شده، در عمل امکان به‌کارگیری ابزارهای پیچیدهٔ رمزنگاری بر روی این قراردادها وجود ندارد. در نتیجه طراحان باید به کمک هوش و خلاقیت خود، قراردادهایی را طراحی کنند تا ضمن اینکه نیازهای امنیتی را تأمین کند، بار اضافی کمی را به مجموعه تحمیل نماید.

بنابراین، طراحی قراردادهایی که بتوانند نیازهای امنیتی مشتریان مانند حفظ حریم خصوصی، احراز اصالت و دسترس‌پذیری را تأمین کند و بهبود امنیت قراردادهای

موجود در اینترنت اشیاء از مهم‌ترین چالش‌های به‌کارگیری از این فنّاوری است که روز به روز در حال گسترش و توسعه است؛ بنابراین، محقق به دنبال پاسخ‌گویی به سؤال (اینترنت اشیاء، بایدها و نبایدهای آن کدام‌اند؟) است.

هدف اصلی: آشنایی با اینترنت اشیاء و چالش‌های به‌کارگیری آن

سؤال‌های تحقیق:

سؤال اصلی: اینترنت اشیاء، بایدها و نبایدهای آن کدام‌اند؟

سؤال‌های فرعی:

۱. روش‌های پیاده‌سازی اینترنت اشیاء کدام‌اند؟
۲. آیا قراردادهای به‌کارگیری شده در اینترنت اشیاء امن هستند؟
۳. چالش‌های امنیتی در حوزهٔ اینترنت اشیاء کدام‌اند؟
٤. آیا امکان امن‌سازی قراردادهای اینترنت اشیاء وجود دارد؟

مبانی نظری: امنیت و حریم خصوصی از مشکلات حیاتی پیشرفت فنّاوری است و برقراری امنیت شاید بزرگ‌ترین چالش در «IOT» باشد و به نظر می‌رسد هوشمندشدن بیشتر دستگاه‌ها به معنای ریسک بیشتر است؛ اگر با گسترش اینترنت اشیا هر شیء نوعی سیستم‌عامل و حافظه داشته باشد، این توان را دارد که مورد نفوذ قرار گرفته و در نتیجه اطلاعات کاربر به خارج منتقل شود و به اشتراک گذاشته شود به این ترتیب فرصت استراق‌سمع یا نفوذ در ارتباطات افزایش می‌یابد.

موضوع‌هایی که اینترنت اشیاء را با چالش اساسی مواجه می‌کند، شامل دوگانگی «امنیت در مقابل آزادی» و «راحتی در مقابل حفظ حریم شخصی» است.

مرکز امنیتی «سوفوس[1]» به عنوان یکی از شرکت‌های بزرگ پشتیبانی از محصولات امنیتی، اعلام نموده اینترنت اشیاء، بزرگ‌ترین نگرانی امنیتی سال ۲۰۱٦ به نظر می‌رسد. این فنّاوری نوپا، در بدو تولد خود به شدت به موضوع امنیت توجه نشان داده است. شرکت‌های گوگل، سامسونگ، سونی و دیگر غول‌های فنّاوری که به نوعی در

1 Sophos

رشدیافتن این فنّاوری نقش داشته‌اند، رعایت امنیت را یکی از اصول اولیه کار قرار داده‌اند؛ اما به اعتقاد کارشناسان، اینترنت اشیاء بعد از عبور از مرحلهٔ «امنیت نمایشی» به مرحلهٔ «خطرناک در حال کار» خواهد رسید و بی‌شک، روبه‌روشدن واقعی با نفوذگران و بدافزارنویسان، شرایط را به‌گونهٔ دیگری تغییر خواهد داد (Lyne,James. (2014),security threat train 2015,Sophos security Research Center,2014).

فنّاوری‌های مختلف اتصال و تعامل میان دستگاه‌ها در اینترنت اشیاء: تبادل خودکار اطلاعات بین دو مجموعه و یا دو دستگاه بدون هیچ‌گونه دخالت انسانی هدف اصلی اینترنت اشیاء است. این تبادل اطلاعات خودکار از طریق برخی فنّاوری‌های خاص صورت می‌گیرد که در ذیل به دو مورد از آنها اشاره می‌کنیم.

الف) شبکهٔ حسگر بی‌سیم: همان‌طور که در (I. F. Akyildiz, et al. 2002, pp. 114 - 102.) توصیف شده ترکیب‌بندی گره‌ها در شبکه‌های حسگر بی‌سیم مستقل از بسامد و پهنای باند ارتباط بی‌سیم صورت می‌گیرد. هر گره در شبکهٔ حسگر بی‌سیم به طور معمول از قسمت‌های ذیل تشکیل شده است:

- سنسور
- میکرو کنترولر
- حافظه
- رادیو فرستنده و گیرنده
- باتری

با توجه به دامنهٔ ارتباطات هر گره شبکهٔ حسگر بی‌سیم، چند هابِ اطلاعات را بین منبع و ایستگاه پایه بازپخش می‌کند. داده‌های مورد نیاز توسط سنسور بی‌سیم از طریق ارتباط میان گره‌های مختلف جمع آوری شده و سپس به گره سینک ارسال می‌شود. در اینجا شبکهٔ ارتباطی به صورت پویا و با استفاده از فرستنده و گیرنده‌های رادیویی

بی‌سیم به سهولت انتقال داده بین گره‌ها کمک می‌کنند. چند هاب داده‌های مورد درخواست گره‌های مختلف را به بارهای ترافیکی متنوع انتقال می‌دهند (G. Shen and B. Liu. 2011, pp.4-1).

ب) شناسایی بسامد رادیویی: «RFID» فنّاوری شناسایی از طریق امواج رادیویی، یک فنّاوری جدید است که برای شناسایی و احراز هویت اشیاء و موجودات زنده به کار گرفته می‌شود. به دلیل مزایای زیادی چون کم‌هزینه بودن، نیازنداشتن به تماس فیزیکی، سرعت و دقت بالا و انجام احراز اصالت در مقیاس وسیع، فنّاوری «RFID» مورد توجه سازمان‌ها و صنایع مختلف قرار گرفته و روز به روز به دامنهٔ کاربران آن افزوده می‌شود.

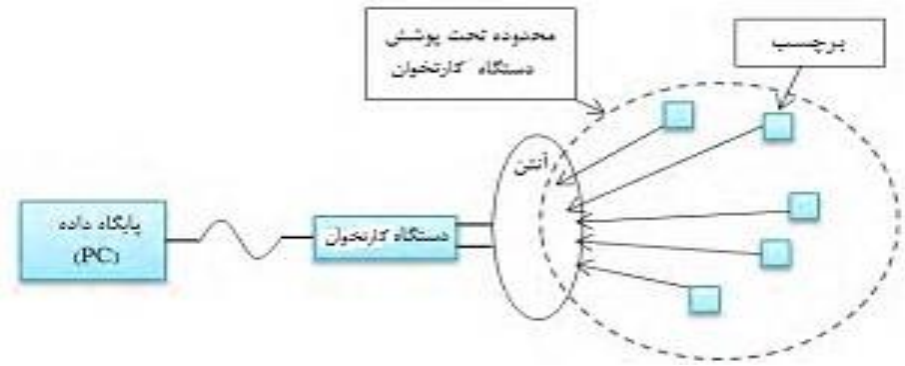
در اینترنت اشیاء فنّاوری «RFID» به طور عمده از برچسب در تعامل با یکدیگر به طور خودکار استفاده می‌کند. برچسب‌های «RFID» از امواج بسامد رادیویی برای برقراری ارتباط و تبادل اطلاعات بین یکدیگر بدون نیاز به اینکه در میدان دید مستقیم یکدیگر قرار گرفته یا با یکدیگر تماس فیزیکی داشته باشند استفاده می‌کند. یک «RFID» از سه جزء تشکیل شده است:

- برچسب[1]: بر روی شیء مورد نظر که قصد پایش حضور و یا جمع‌آوری اطلاعات در مورد آن را داریم نصب می‌گردد.
- کارتخوان[4]: وظیفهٔ ارتباط با برچسب به منظور دریافت اطلاعات را به عهده دارد. پس از آنکه این اطلاعات به کمک برچسب جمع‌آوری گردید، این اطلاعات به منظور پردازش در اختیار کارگزار (خدمات دهندهٔ نهایی) قرار می‌گیرد.

خدمات دهندهٔ نهایی: وظیفهٔ پردازش اطلاعات دریافتی به منظور کسب اطلاعات مفید و قابل درک برای مدیر مجموعه را به عهده دارد (S. Konomi and G. Roussos, 2007).

---

1 Tags



شکل ۲ – ساختار مجموعه‌های RFID

چالش‌های امنیتی، اهمیت محرمانگی و شکاف اطلاعاتی و ارتباطی در اینترنت اشیاء

چالش‌های امنیتی: امنیت اطلاعات با شاخص‌هایی از قبیل شناسایی، محرمانگی، یکپارچگی و انکارناپذیری سنجیده می‌شوند. اینترنت اشیاء در حوزهٔ اقتصاد جهانی و در خدمات پزشکی، مراقبت‌های بهداشتی، حمل و نقل هوشمند و بسیاری دیگر از حوزه‌ها به‌کار گرفته می‌شود؛ بنابراین، نیازمندی‌های امنیتی در آن از اهمیت بالایی برخوردارند. با داشتن اینترنت اشیاء می‌توان پیش‌بینی کرد که مجرمان سایبری در مرحلهٔ اول به نقاط انتشار و انتقال اطلاعات، مراکز ارسال داده‌ها، نقاط و زیرساخت‌های شبکه حمله خواهند نمود؛ بنابراین، امنیت را باید برای این نقاط فراهم نمود.

ناسازگاری قراردادها و دستگاه‌ها، توسعهٔ سازمان‌های امنیتی با تحمل خطای بالا را به فعالیتی دشوار تبدیل می‌کند (Suo, H, Wan, J, Zou, C, & Liu, J.2012).

با رشد سریع کاربردهای «IoT»، مفاهیم امنیتی مورد توجه قرار می‌گیرند و نگرانی‌هایی در زمینهٔ محرمانگی و حریم خصوصی شکل می‌دهد. اگر فعالیت روزانهٔ افراد نظارت شده و آنها تولیدکنندهٔ خروجی‌های اطلاعاتی باشند، فعالیت‌های سیاسی، اقتصادی و اجتماعی تحت تأثیر قرار می‌گیرند. در صورت نقض امنیت، انجام حمله و اختلال در عملکرد، مزایای «IoT» کم‌رنگ می‌شود. در آینده‌ای نزدیک حجمی وسیع از اطلاعات توسط وسایل متصل به هم دریافت و ارسال خواهد شد.

در نظر داشته باشید که اطلاعات مرتب در حال حرکت و جابه‌جایی است و با ورود اینترنت اشیاء رویکرد این جابه‌جایی بسیار متفاوت از حالت فعلی خواهد شد. امنیت اینترنت اشیاء به واسطهٔ اتصال همهٔ دستگاه‌ها به یکدیگر به طور کامل متفاوت از روندهای فعلی خواهد بود. ما باید به نقاط اتصالی و ارتباطی انتقال اطلاعات بین تمامی وسایل و ابر و شبکه‌ها توجه کرده و امنیت را در آنجا به وجود آوریم (Gang, G, Zeyong, L, & Jun, J. 2011, pp. 1-4).

اینترنت اشیاء با چالش‌های زیادی روبه‌روست. از نظر مقیاس‌پذیری 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 محاسبهٔ تغییرهای روزانهٔ دمایی در محدودهٔ یک کشور به دستگاه‌های زیادی نیازمند است و مدیریت بر داده‌های کلان را می‌طلبد.

الف) چالش‌های امنیتی در شبکهٔ حسگر بی‌سیم عملیات سرکوب‌گری در شبکهٔ حسگر بی‌سیم را می‌توان به سه دسته طبقه‌بندی کرد (J. Malhotra. 2015. 8, pp. 81-88):

- حمله به محرمانگی و احراز هویت
- حمله‌های خاموش بر یکپارچگی خدمات (جامعیت)
- حمله‌های در دسترس بودن شبکه (حمله‌های داس[1])

۱. حملهٔ داس در لایهٔ فیزیکی: لایهٔ فیزیکی یک شبکهٔ حسگر بی‌سیم وظایف تولید بسامد حامل، مدوالسیون، رمزگذاری و رمزگشایی، انتقال و دریافت اطلاعات را بر عهده دارد. این لایه از شبکهٔ حسگر بی‌سیم اغلب از طریق روش‌های ذیل مورد حمله قرار می‌گیرد:

- متراکم: در این نوع از حملهٔ داس کانال ارتباطی بین گره‌ها اشغال شده و از برقراری ارتباط بین آنها جلوگیری می‌شود.

---

1 DOS

- دست‌کاری گره: دست‌کاری گره به طور معمول با هدف استخراج اطلاعات حساس صورت می‌گیرد.

۲. حملهٔ داس در لایهٔ پیوند: لایهٔ پیوند وظیفهٔ نظارت بر جریان‌های مختلف شبکهٔ حسگر بی‌سیم و پایش خطا را بر عهده دارد، علاوه بر این لایهٔ پیوند قابلیت اطمینان نقطه به نقطه و نقطه به چند نقطه را تضمین می‌کند. حمله های داس قابل انجام در این لایه عبارت‌اند از (A. A. Alkhatib, 2012, pp. 35-22):

برخورد: این نوع از حملهٔ داس، زمانی رخ می‌دهد که دو گره به طور هم‌زمان اقدام به انتقال داده با بسامدی مشابه بر روی یک کانال انتقال می‌کنند. برخورد بسته‌های حاوی داده منجر به تغییرهای کوچک در نتایج بسته می‌شود و در نتیجه شناسایی بسته به علت دریافت نتیجهٔ ناسازگار باعث دور ریختن بستهٔ آسیب دیده و انتقال دوبارهٔ آن می‌شود (S. Ghildiyal, et al. 2015, pp.1163-2319).

- بی‌عدالتی: همان‌طور که در (S. Ghildiyal, et al. 2015, pp.1163-2319) توصیف شده، بی‌عدالتی یک حملهٔ تکرار برخورد پایه است همچنین می‌تواند به عنوان حملهٔ مبتنی بر فرسودگی در نظر گرفته شود. بدین معنا با انجام حمله‌های متعدد از نوع برخورد مانع انتقال اطلاعات از یک سمت ارتباط شده که در نتیجه موجب می‌گردد کاربر نتواند از خدمات مجموعه استفاده نماید.
- فرسودگی باطری: این نوع از حمله داس باعث شدآمد غیرمنتظرهٔ بالا در یک کانال و امکان دسترسی بسیار محدود به گره‌ها می‌شود. چنین اختلالی در کانال توسط تعداد زیادی از درخواست‌ها و انتقال در طول کانال ایجاد می‌شود.

۳. حملهٔ داس در لایهٔ شبکه: وظیفهٔ اصلی لایهٔ شبکه برای شبکه حسگر بی‌سیم مسیریابی است. حمله‌های خاص داس در حال وقوع در این لایه عبارت‌اند از:

- حقه‌بازی: در این نوع حمله با دست‌کاری در شدآمد و داده‌های مبادله شده بین دو طرف ارتباط، شدآمد به صورت دوباره و نادرست ارسال و هدایت می‌شود.

حملهٔ هِلو فِلود[1]: این حمله باعث شدآمد بالا در کانال توسط ارسال زیاد پیام‌های بی‌فایده است. در این حمله گرهِ مخرب، پیامی بی‌فایده ارسال می‌کند که پس از آن توسط مهاجم برای ایجاد شدآمد بالا بازپخش می‌شود (Y. Liu. 2012, pp. 41-33).

- حملهٔ خانگی: در حملهٔ خانگی جستجو در اطلاعات مبادله شده برای سرخوشه‌ها و گره‌هایی که کلیدهای ارتباطی را مدیریت می‌کنند صورت می‌گیرد که در صورت موفقیت توانایی تعطیل‌کردن کل شبکه را دارند.
- حمل و نقل انتخابی: همان‌طور که از نام آن مشخص است، در حملهٔ حمل و نقل انتخابی با توجه به نیاز و هدف مخرب، مهاجم چند گره انتخاب شده و این گره‌ها به جای تمام گره‌ها عمل ارسال داده را انجام می‌دهند.
- حملهٔ سایبیل[2]: در یک حملهٔ سایبیل، مهاجم یک گره را تکثیر و آن را با هویت چندگانه به گره‌های دیگر ارائه می‌دهد.
- حفره‌های کرم: این حملهٔ داس باعث جابه‌جایی بستهٔ داده از جایگاه اصلی خود در شبکه می‌شود. این جابه‌جایی بستهٔ داده از طریق تونل‌زنی بر روی یک لینک با تأخیر کم انجام می‌شود.

جاری‌شدن سیل‌آسای تأییدیه: تأییدیه‌ها در الگوریتم‌های مسیریابی شبکه‌های حسگر بی‌سیم استفاده می‌شوند. در حملهٔ جاری‌شدن سیل‌آسای تأییدیه، یک گره مخرب تأییدیه ارسال‌های اطلاعات نادرست را به گره‌های همجوار جعل می‌کند (D. G. Padmavathi and M. Shanmugapriya. 2009, pp. 68-60).

٤. حمله داس در لایه انتقال: این لایه در معماری شبکهٔ حسگر بی‌سیم قابلیت اطمینان در انتقال داده و جلوگیری از ازدحام ناشی از شدآمد بالا در مسیریاب را فراهم می‌کند. حمه‌های داسِ این لایه عبارت‌اند از:

- جاری‌شدن سیل: در اثر ازدحام نسنجیدهٔ کانال‌های ارتباطی از طریق رلهٔ پیام‌های غیرضروری و شدآمد بالا به وجود می‌آید.

---

1 Hello Flood
2 Sybil

- غیرهم‌زمانی: در حملهٔ غیرهم‌زمانی پیام‌های جعلی در یک و یا هر دو نقطهٔ انتهایی که درخواست ارسال مجدد برای اصلاح خطا صورت می‌گیرد ایجاد می‌گردد نتیجهٔ این حمله از دست‌رفتن انرژی در یک یا هر دو نقطهٔ انتهایی است.

۵. حملهٔ داس در لایهٔ کاربردی: لایهٔ کاربرد در شبکهٔ حسگر بی‌سیم مسئولیت مدیریت شدآمد را بر عهده دارد همچنین به عنوان ارائه دهندهٔ نرم‌افزار برای برنامه‌های مختلف که ترجمهٔ داده‌ها را به شکلی قابل فهم انجام می‌دهد کمک می‌کند (A. A. Alkhatib, 2012, pp. 35-22 –S. Ghildiyal, et al. 2015, pp.1163-2319) در این لایه یک حملهٔ داس مبتنی بر مسیر، با تحریک گره‌های حسگر برای ایجاد شدآمدی بزرگ در مسیر صورت می‌گیرد.

برخی از حمله‌های دیگرِ داس به شرح ذیل هستند (M. Saxena. 2007, pp. 115-125):

- سیاه چاله
- نقص گره
- پیام فساد
- براندازی گره
- گره قطع
- گره کاذب

برخی از مسائل امنیت و حریم خصوصی در شبکه‌های حسگر بی‌سیم عبارت‌اند از (K. Sharma, et al. 2010, pp. 44-31):

- محرمانگی اطلاعات
- یکپارچگی داده
- اعتبار داده‌ها
- همانگ‌سازی
- در دسترس‌بودن

- محلی‌سازی امن
- خود سازمان‌دهی
- انعطاف‌پذیری

شبکه‌های حسگر بی‌سیم را با توجه به تهدیدها به صورت ذیل نیز می‌توان طبقه‌بندی کرد:

- تهدیدهای داخلی در مقابل خارجی
- تهدیدهای فعال در مقابل غیرفعال

همچنین شبکه‌های حسگر بی‌سیم را با توجه به نوع حمله‌های صورت گرفته به صورت ذیل می‌توان طبقه‌بندی نمود:

- وقفه
- استراق‌سمع
- اصلاح شده (تغییر یافته)
- جعل

حمله‌های مربوط به شبکه‌های حسگر بی‌سیم را می‌توان به صورت ذیل نیز طبقه‌بندی نمود:

- حمله‌های مبتنی بر میزبان
- حمله‌های مبتنی بر شبکه

ب) چالش‌های امنیتی در اینترنت اشیاء مبتنی بر «RFID»: در چارچوب اینترنت اشیاء فنّاوری «RFID» برای تبادل خودکار اطلاعات بدون هیچ‌گونه دخالت کاربر استفاده می‌شود؛ اما وجود برخی از محدودیت‌ها نظیر ابعاد بسیار کوچک برچسب‌ها، قابلیت محاسباتی کم و حجم ذخیره‌سازی پایین باعث شده دستگاه‌های «RFID» در مقابل بسیاری از حمله‌های آسیب‌پذیر باشند که از جمله آنها می‌توان به استراق‌سمع، حملهٔ تکرار، حملهٔ فردی در میان و حملهٔ ممانعت از خدمات اشاره کرد (M. R. Thomas S. Heydt-Benjamin, Dan V. &Sohizadeh Abyaneh,2010 ،Bailey, Kevin Fu, Ari Juels, and Tom O'Hare. 2007).

بر اساس یک دسته‌بندی که در زمینهٔ تهدیدهای امنیتی قراردادهای «RFID» وجود دارد حمله‌هایی که بر روی یک قرارداد احراز اصالت انجام می‌شود به دو دسته تقسیم می‌شوند:

- حمله‌های غیرفعال[1]: حمله‌هایی که توجه مهاجم به شنود و استراق‌سمع پیام‌های ارسالی بین برچسب و کارتخوان معطوف بوده و او قادر به ایجاد تغییرهایی در پیام‌های ارسالی بین طرفین نبوده و نمی‌تواند در روند اجرای قرارداد تأثیرگذار باشد.
- حمله‌های فعال[2]: حمله‌هایی که در آنها مهاجم علاوه بر شنود و استراق‌سمع پیام‌های ارسالی بین برچسب و کارتخوان سعی دارد با ایجاد تغییرهایی هدفمند در روند اجرای قرارداد تأثیر بگذارد. از انواع این حمله‌ها می‌توان به حملهٔ جعل هویت[3]، حملهٔ پس‌رو[4] و حملهٔ پیش‌رو[5] اشاره نمود (Boyeon Song. 2010).
- در ادامهٔ این بخش به معرفی حمله های رایجی که بر روی دستگاه‌های «RFID» اعمال می‌شوند می‌پردازیم.

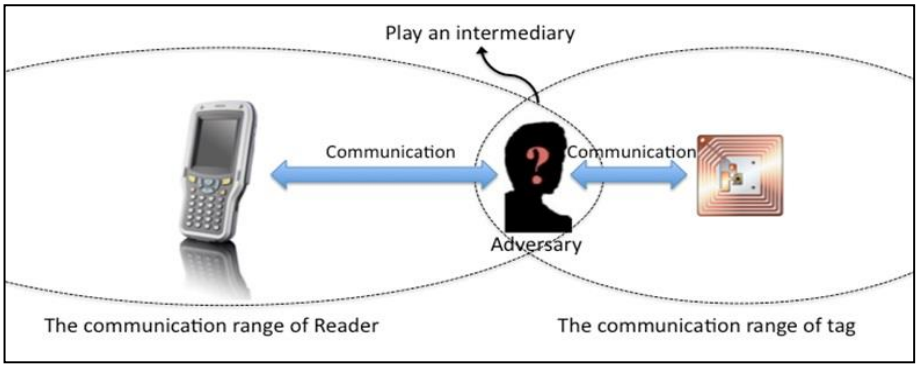
۱. حملهٔ شنود یا استراق‌سمع

- حملهٔ شنود یکی از تهدیدهای امنیتی رایج مرتبط با سامانه‌های «RFID» به‌شمار می‌آید که دلیل آن ماهیت ارتباط بی‌سیم بین برچسب و کارتخوان است. این حمله به تنهایی کارایی چندانی ندارد اما ترکیب آن با سایر حمله‌ها می‌تواند نتایج بهتری را برای مهاجمان در بر داشته باشد. از این رو این حمله مرحلهٔ آغازین حمله‌هایی مانند حملهٔ تکرار، حملهٔ جعل هویت و سایر حمله‌های مرتبط با این سامانه‌ها محسوب می‌شود.
- به طور کلی دو نوع حملهٔ استراق‌سمع در دستگاه‌های «RFID» وجود دارد.

---

1 Passive Attack
2 Active Attack
3 Impersonation Attack
4 Backward Attack
5 Forward Attack

- استراق‌سمع غیرفعال: این حمله به مشاهده یا ذخیرهٔ ارتباط بین یک برچسب و کارتخوان با یک موجودیت غیرمجاز مربوط می‌شود. این حمله ممکن است توسط شخص ثالثی‌که در محدودهٔ عملکردی سامانه قرار دارد انجام شود.
- استراق‌سمع فعال (اسکن‌کردن): در این حالت یک مهاجم سعی دارد بدون داشتن مجوز اطلاعات مبادله شده را بخواند. وقتی چنین حالتی در دستگاه «RFID» روی می‌دهد، مهاجم با استفاده از یک کارتخوان غیرمجاز به فعال‌کردن برچسب‌ها می‌پردازد. در این حالت مهاجم در محدودهٔ نشان داده شده در شکل ۳ فعالیت می‌کند.



شکل ۳- حملهٔ استراق‌سمع در «RFID»

۲. حملهٔ کشف کلید و شناسه: همان‌طور که اشاره شد حملهٔ شنود مقدمه‌ای برای سایر حمله‌ها محسوب می‌شود که حملهٔ کشف کلید و شناسه[1] یکی از این حمله‌هاست. در این حمله مهاجم با استفاده از اطلاعات شنود شدهٔ مربوط به یک یا چند نشست و با ترکیب آنها و یا به روش‌های دیگر کلیدهای محرمانه و برخی مقادیر نظیر شناسه منحصربه‌فرد را به‌دست آورد. جستجوی فراگیر کلید ساده‌ترین راه برای دست‌یابی به این هدف است و زمانی‌که طول پیام‌های ارسالی بین طرفین کوتاه باشد و یا ساختار قرارداد به گونه‌ای باشد که مهاجم بتواند با هوشمندی و ترکیبِ پیام‌ها این فضای جستجو را کاهش دهد، این حمله به شکل کارامدتری دنبال خواهد شد.

حملهٔ جعل هویت: در حملهٔ جعل مهاجم خود را به جای یکی از طرفین درگیر در

1 Key and ID recovery

ارتباط معرفی و سعی در فریب طرف دیگر دارد. او اطلاعات لازم را به طور معمول با استراق‌سمع پیام‌های چند نشست متوالی به‌دست می‌آورد. این حمله به دو صورت جعل هویت برچسب و جعل هویت کارتخوان انجام می‌گیرد. روالی که مهاجم در هر دو حالت دنبال می‌کند به طور معمول یکسان است. اگر مهاجم بتواند با ترکیب اطلاعات به‌دست آمده از یک یا چند نشست و یا به هر شکل دیگری به کلیدها و سایر مقادیر محرمانه برچسب یا کارتخوان دست یابد حملهٔ جعل شکل جدی به خود گرفته و این امکان را به مهاجم می‌دهد که در هر زمان که بخواهد بتواند با یک هویت جعلی به سامانه نفوذ و هدف‌های خود را دنبال کند. حالت دیگر این حمله زمانی است که مهاجم قادر به کشف کلید و مقادیر محرمانه نیست؛ اما او می‌تواند با ایجاد تغییرهایی در پیام‌های ارسال شده بین برچسب و کارتخوان در یک یا چند نشست با یک هویت جعلی و در نقش یک برچسب یا کارتخوان به مجموعه نفوذ کند؛ اما این حالت انعطاف‌پذیری کمتری دارد و شاید تنها برای یک یا چند دفعه احراز اصالت بتواند با هویت جعلی از خدمات سامانه بهره‌مند شود، زیرا اطلاعاتی را که پیشتر جمع‌آوری و تغییرهایی را که بر روی آنها انجام داده با عمل به‌روزرسانی که بین برچسب و کارتخوان صورت می‌گیرد دیگر کارامد نیست (KU, W. C, Chang S. T. Impersonation, pp.2165-2167,2005& Feldhofer, M, Dominikus, S, and Wolkerstorfer, J. Strong Authentication,2004).

حملهٔ تکرار: در حمله تکرار[1] مهاجم پس از شنود و جمع‌آوری اطلاعات یک یا چند نشست بین برچسب و کارتخوان سعی دارد با ترکیب و استفادهٔ مجدد از آنها و بدون دسترسی به کلید و مقادیر مشترک بین برچسب و کارتخوان و بی‌نیاز از ایجاد تغییرهای گسترده در پیام‌های ذخیره شده، خود را به عنوان یک هویت مجازی معرفی و وارد مجموعه گردد. حملهٔ تکرار یک حملهٔ برون‌خط[2] است بدین‌معنا که مهاجم می‌تواند از یک یا چند ارتباط بین طرفین به پیام معتبر برای حمله در مراحل بعدی

1 Relay attack
2 Off-line

دست یابد. یک راه‌کار بسیار مهم که باید همواره مورد توجه طراحان قراردادهای احراز اصالت به منظور مقابله با این حمله قرار گیـرد، تولیـد و اسـتفاده از مقـادیر تصـادفی و هم‌زمان انجام فرایند به‌روزرسانی مقادیر محرمانهٔ مشترک در پایـان هـر نشسـت اسـت (Hung-Min Sun and Wei-Chih Ting, August 2009, PP [1052-1062]).

۵. حملهٔ ممانعت از خدمات: حمله ممانعت از خدمات با قراردادن حجم زیـادی از برچسب‌های غیرمجاز در دامنهٔ یک کارتخوان یا مخدوش‌کردن تعدادی از برچسب‌ها و یا قطع یک ارتباط مانع از ارسال پیام‌ها می‌گردد و بـه عبـارتی مـانع از خـدمات‌رسـانی سامانه می‌شود. این حمله می‌تواند منجر به ناهم‌زمانی بین برچسب و کارتخوان شود.

٦. حملهٔ فردی در میان: در حملهٔ فردی در میان، مهاجم تلاش می‌کند با قرارگرفتن در میان ارتباط یـک برچسـب و کـارتخوان پیـام‌هـای مبادلـه شـده بـین آنهـا را بـرای دست‌یابی به هدف‌های خود حذف یا تغییر داده و یا پیام‌های مورد نظـر خـود را بـرای طرفین ارسال کند. مهاجم به‌گونه‌ای باید پیام‌ها را تغییر دهد که پس از ارسال، هیچ‌یـک از طرفین متوجه این فریبکاری نشوند و نتوانند به هویت جعلی مهاجم پی ببرنـد. ایـن حمله نیز مانند حملهٔ تکرار یک حملهٔ برون‌خط بوده و نتیجهٔ آن جعل هویت برچسب، کارتخوان و یا حملهٔ ردیابی برچسب است.

۷. حملهٔ بازپخشی: این حمله یک حالت خاص از حملهٔ فردی در میان اسـت و در آن مهاجم تلاش می‌کند در میان ارتباط یک برچسب و کـارتخوان مجـاز قـرار گیـرد و نقش یک واسط را برای طرفین بازی کند، به نحـوی کـه بـرای کـارتخوان نقـش یـک برچسب و برای برچسب در نقش کارتخوان ظاهر می‌شود.

این حمله از جهاتی مشابه حملهٔ تکرار و حملهٔ فردی در میان است. تفاوت اصلی با حملهٔ تکرار در این است که حملهٔ تکرار یک حملهٔ برون‌خط است و حملهٔ بازپخشـی[1] حمله‌ای برخط[2] است. حملهٔ بازپخشی بر خلاف حملهٔ فردی در میان، پیام‌های ارسـالی

1 Man in the middle attack
2 On-line

از طرفین را بدون آنکه بخواهد تغییری در آنها ایجاد کند دریافت و سپس باز ارسال می‌کند؛ اما در حملهٔ فردی در میان مهاجم با قرارگرفتن در میان ارتباط برچسب و کارتخوان پیام‌های مبادله شده را حذف یا تغییر داده و یا پیام‌های مورد نظر خود را تولید و برای برچسب یا کارتخوان ارسال می‌کند (حبیبی، ۱۳۹۰).

۸. حملهٔ ردیابی: حملهٔ ردیابی از مهم‌ترین تهدیدهای امنیتی است که می‌تواند سلامت یک دستگاه «RFID» را خدشه‌دار کند و نتیجه آن نقض حریم خصوصی برچسب‌ها و مالکان آنهاست. عمل ردیابی در سامانه‌های «RFID» به دنبال‌کردن مسیر حرکت افراد و اشخاصی اطلاق می‌شود که حامل یک برچسب هستند. اگر مهاجم در مکان‌های مختلف و دور از چشم کاربران کارتخوان‌هایی را نصب و در ارتباط با برچسبی خاص و ترکیب پیام‌های دریافتی آن به یک مقدار ثابتی دست یابد می‌تواند آن برچسب را از سایر برچسب‌ها متمایز و مسیر حرکت آن را ردیابی کند. برای جلوگیری از این حمله بسیاری از قراردادها از یک فرایند به‌روزرسانی در دل خود استفاده می‌کنند تا پس از انجام یک نشست موفق مقادیر محرمانه مانند شناسه‌ها و کلیدها به‌روزرسانی شوند.

حملهٔ ناهم‌زمانی: راه‌حلی که برای مقابله با حملهٔ ردیابی پیشنهاد شد گرچه تا حد قابل‌توجهی امنیت داده‌ها و موقعیت مکانی کاربران را از دید مهاجمان مخفی نگه‌داشت اما قراردادها را از جنبه‌های دیگری آسیب‌پذیر نمود. همان‌طور که اشاره شد برای مقابله با حملهٔ ردیابی در بسیاری از قراردادها برچسب و کارتخوان پس از هر نشستِ موفقِ مقادیرِ محرمانهٔ خود را به‌روزرسانی می‌کنند که با این کار اطلاعاتی که مهاجمان از نشست‌های مختلف با هدف ورود به حریم خصوصی کاربران در اختیار دارند کارایی لازم را ندارد؛ اما اگر برچسب و کارتخوان به هر دلیل نتوانند کلیدها و سایر مقادیر محرمانهٔ خود را به‌روزرسانی کنند و یا مقادیر متفاوتی را به‌روزرسانی کنند در نشست‌های آینده به دلیل ناهمگام‌بودن برچسب و کارتخوان احراز اصالت با موفقیت انجام نخواهد شد و برچسب هدف از سامانه حذف می‌شود (Nasour Bagheri, Masoumeh Safkhani et.al: Report 2012/702).

اهمیت محرمانگی (حریم خصوصی): حریم خصوصی یعنی اطمینـان از اینکـه تنهـا موجودیت‌های مجاز به اطلاعاتِ محرمانه دسترسی دارند یا به عبارت دیگر اطمینـان از اینکه تمامی اطلاعات در طول همهٔ ارتباطات به صورت امن منتقل شوند.

در اینترنت اشیاء، واژهٔ حریم خصوصی این چنین بیان شده است: (حق هر چیز، بـه طور معمول یک فرد) برای فعالیت در حریم خودش و تعیین گسترهٔ تعامل او با محـیط اطرافش است به طوری که در صورت تمایل اطلاعاتی در خصوص خودش در اختیـار دیگران قرار می‌دهد. به طور معمول در اینترنت اشیاء، دستگاه‌های متصل به هـم محـیط اطراف را به وسیلهٔ حس‌گرها حس کرده، سپس اطلاعات و رویدادهای جمع‌آوری شده را به سرور ارسال می‌کنند، این اطلاعات منطق برنامهٔ کاربردی را شکل می‌دهند. ارسـال اطلاعات به وسیلهٔ خطوط ارتباطی بی‌سیم یا ثابت انجام می‌شود. حفظ حریم خصوصی در دستگاه‌ها امری لازم است، در ذخیـره‌سـازی، انتقـال اطلاعـات و پـردازش داده‌هـا، ممکن است اطلاعات حساس کاربران افشا شود؛ بنابراین، حفاظت از حریم خصوصـی و داده‌های کاربران، یکی از چالش‌های مهم است که در اینترنت اشیاء باید مـورد توجـه قـرار گیـرد (P M.Madhura et al, April - May 2015, Page 2069 – 2074).

بعضی از مسائل امنیتی در اینترنت اشـیاء در حـال حاضـر بـرای رلـه (بـاز ارسـال) اطلاعات از یک دستگاه به دستگاه دیگر به وجود می‌آیند.

برخی از مسائل امنیتی چالش برانگیز ناشی از فنّاوری ارتباطـات بـه شـرح ذیـل اسـت: اهمیت محرمانگی در دسـتگاه‌هـا: دسترسـی یـا دسـت‌کـاری غیرمجـاز در سـخت‌افـزار و نرم‌افزار مربوط به دستگاه‌ها ممکن است باعث نشت اطلاعـات حسـاس شـود. بـه عنـوان نمونه، یک نفوذگر می‌تواند با برنامه‌ریزی مجدد دوربین مداربسته، کاری کند که عـلاوه بـر ارسال داده‌ها به سرور مجاز، یک نسخه از داده‌ها نیز برای وی ارسال شود؛ بنـابراین، بـرای دستگاه‌هایی که اطلاعات حسـاس را جمـع‌آوری مـی‌کننـد، اسـتحکام و نفـوذناپـذیری از ویژگی‌های مهم آنها به حساب می‌آید. برای اطمینـان از امنیـت اینترنـت اشـیاء، اسـتفاده از

فنّاوری محاسبات قابل اعتماد، از جمله اعتبار سنجی هویت دستگاه، نمونه های مقاوم در برابر نفوذ و استفاده از فضاهای امن، می‌تواند مفید واقع شود. به منظور فراهم‌آوردن حریم خصوصی در دستگاه‌ها، با مشکلات زیادی مواجه هستیم که یکی از آنها محرمانگی نشانی دستگاه، یعنی مخفی ماندن موقعیت دستگاه و مالک آن است، به عبارت دیگر به معنای حفاظت در مقابل شناسایی دقیق ماهیت دستگاه و حفاظت از اطلاعات شخصی در برابر سرقت و یا مفقودشدن دستگاه و مقاومت در برابر حمله های کانال جانبی است. محرمانگی موقعیت مکانی در شبکه‌های بی‌سیم با استفاده از الگوریتم چند مسیریابی تصادفی بین حسگرهای بی سیم به‌وجود می‌آید. برای حفاظت از اطلاعات شخصی و هویتی در زمانی که دستگاه گم شده یا به سرقت می‌رود، از روش رمز پاسخ سریع استفاده می شود برای غیرقابل شناسایی کردن دستگاه در حمله های کانال جانبی، استفاده از روش‌هایی نظیر افزودن تصادفی دستگاه‌ها به شبکه، ایجاد اختلال، داشتن چندین پردازندهٔ هم‌زمان و استفاده از مقادیر کور در محاسبات راه‌گشا خواهد بود (P .(M.Madhura et al, April - May 2015, Page 2069 – 2074

اهمیت محرمانگی در خلال ارتباطات: برای اطمینان از محرمانه بودن اطلاعات حین انتقال داده ها، عمومی ترین روش رمزگذاری است. در رمزگذاری، داده های خاصی به بسته‌های ارسالی افزوده می‌شوند که باعث می‌شود این بسته‌ها قابل ردیابی باشند مانند دنباله ای از اعداد، شاخص پارامتر امنیت و...، این اعداد برای تجزیه و تحلیل شبکه و ارتباط بسته ها با هم استفاده می شوند. استفاده از قرارداد ارتباط امن روش مناسبی برای ایجاد محرمانگی حین انتقال است. به منظور کاهش آسیب‌پذیری در طول انتقال داده‌ها، می‌توان از جایگزین کردن نام های مستعار در رمزگذاری استفاده کرد به صورتی که شناسایی دستگاه یا کاربری که اطلاعات را ارسال یا دریافت می کند امکان‌پذیر نباشد. یکی از مثال‌های نام آشنا، استفاده از هویت مشترک سیار و موقت است. برای از بین بردن احتمال افشای اطلاعات ناشی از انتقال داده‌ها، دستگاه‌ها فقط در صورت نیاز باید ارتباط برقرار کنند (P .(M.Madhura et al, April - May 2015, Page 2069 – 2074

تشدید شکاف اطلاعاتی ارتباطی: از دیگر چالش‌های مطرح در اینترنت اشیاء، افزایش شکاف اطلاعاتی است. افرادی که به شبکهٔ دیجیتالی متصل نیستند یا تمایلی به اتصال به این شبکه را ندارند در صورت فراگیرشدن اینترنت اشیاء از بسیاری خدمات محروم خواهند شد. محققان زیادی به توزیع نابرابر امکانات اشاره کرده و یادآور شدند احتمال ایجاد شکاف اجتماعی وجود دارد بین افرادی که منابع لازم برای پرداخت هزینهٔ تجهیزات، مهارت و کسب دانش برای کار در محیط‌هایی با فنّاوری پیچیده را ندارند. این مسئله نه‌تنها به تفاوت دسترسی به فنّاوری‌ها بین اقشار مختلف جامعه بلکه به تفاوت‌های فرهنگی، جغرافیایی و ساختار اجتماعی اشاره دارد. اینترنت اشیاء مزایای زیادی برای افراد در کشورهای توسعه‌یافته، ایجاد خواهد کرد. همچنین تأثیر بسزایی بر روی صنایع همگانی مانند آب و برق و انرژی خواهد داشت. ولی در طرف مقابل این فنّاوری به کشورهای در حال توسعه با نگرش‌های توسعه‌ای کوتاه‌مدت کمک کمتری خواهد کرد (SY, P. 2015).

امروزه با وجود قطع اتصال رایانه و دستگاه‌ها به اینترنت نمی‌توان از حفظ محرمانگی و حریم خصوصی مطمئن بود و همین نگرانی در سطوحی بالاتر در مورد دیگر وسایل قابل اتصال به اینترنت وجود خواهد داشت. امروزه از وسایل الکترونیکِ پوشیدنی برای پایش کارمندان در محیط‌های کاری استفاده می‌شود. در آینده انجام این کار با پیشرفت فنّاوری 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 همه‌گیرشدن اینترنت اشیاء دیگر اثری از حریم خصوصی باقی نماند و انسان‌ها روح خود را از دست بدهند و این دغدغه باعث گردد پذیرش این فنّاوری توسط برخی افراد و سازمان‌ها با تأخیر بیشتر صورت پذیرد.

توسعه نیافتن «IoT» منجر به ایجاد دو نوع شکاف می‌گردد که به منزلهٔ دو روی یک سکه هستند. از یک طرف مانند دیگر فنّاوری‌های اطلاعاتی و ارتباطی، شکاف اطلاعاتی به تفاوت در ویژگی‌های جمعیت‌شناختی نظیر (سن، درامد، 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 خودکارِ داده و مدیریت این تراکنش‌ها بین اشیاء و فعالیت‌های «IoT» اشاره دارد. کسانی که خود را با روند توسعهٔ فنّاوری‌های جدید وفق ندهند با خطر از دست‌دادن دانش و مهارت‌های خود روبه‌رو می‌شوند.

شکاف اطلاعاتی به عنوان یکی از چالش‌های توسعهٔ «IoT» محسوب می‌شود. هر چند این فنّاوری تا حدی بر افراد تحمیل می‌شود (مثال خوبی در این زمینه، جابه‌جایی‌های هوشمند، مانند شهرهای هوشمند، حمل و نقل هوشمند، سلامت الکترونیک، کارخانجات هوشمند است)، دسترسی و توزیع فنّاوری «IoT» با توجه به منطقهٔ جغرافیایی متفاوت خواهد بود و در فعالیت‌های کاری، سیاسی و اقتصادی و فعالیت‌های روزانه نفوذ خواهد کرد. از طرفی با توجه به نفوذ «IoT» در تمامی ابعاد زندگی تهدید افراد توسط بدافزارها مورد توجه قرار می‌گیرد.

با وجود اینکه رشد شبکه‌های اجتماعی، نوعی شکوفایی مردم‌سالارانه در جامعهٔ دانش‌محور به شمار می‌رفت، «IoT» نمونه‌ای دیگر از پایش و ناتوانی افراد بر حفاظت از حریم خصوصی‌شان محسوب می‌شود و فضای تولید دانش اشتراکی و خلاقیت توسط «IoT» محدود می‌شود. به‌علاوه پایش توزیع شده «IoT» مواردی در زمینهٔ پاسخ‌گویی و مسئولیت‌پذیری به‌وجود می‌آورد، جایی که ردیابی مبدأ و مقصد داده‌ها و تراکنش‌های آنها امکان‌پذیر می‌شود و این نیز نمونه‌ای از شکاف دانشیِ ناشی شده از «IoT» است. همان‌طور که ده کشور برتر در فنّاوری «IoT» بیشتر کشورهای توسعه‌یافته هستند، می‌توان نتیجه گرفت گسترش «IoT» در کشورهای توسعه‌یافته بیشتر از کشورهای در حال توسعه بوده و همین موضوع باعث افزایش شکاف اطلاعاتی بین این کشورها می‌شود (SY, P. 2015). پیچیدگی این فنّاوری باعث می‌شود بسیاری افراد نتوانند از آن بهره گیرند. طبق گزارش‌ها، کشورهای توسعه‌یافته هنوز نتوانسته‌اند استفاده از این فنّاوری را به طور کامل مقرون به صرفه کنند. همچنین

بسیاری کشورها استفاده از «IoT» را در محیط کار بـه دلیـل نقـص امنیـت، غیرانسـانی قلمداد می‌کنند.

بحث و نتیجه‌گیری

اینترنت اشیا در واقع آیندهٔ اینترنت را نشان می‌دهد که تمام ابزارها و وسایل بـا هـم در ارتباط هستند و می‌توانند درکی از محیط اطراف خود داشته و با دیگر وسایل و ابزار ارتباط برقرار نمایند. برای برقراری این ارتباط نیاز به قراردادهای ارتباط وجـود دارد تـا دستگاه‌ها بتواند از طریق آن با اینترنت و دیگر دستگاه‌ها ارتباط داشته باشـند از ایـن رو بررسی جنبه‌های امنیتی این فنّاوری و میزان امنیت قراردادهای به کـارگیری شـده بـرای انجام احراز هویت یک نیاز ضروری برای کاربران مختلف این فنّاوری است.

مهم‌ترین ابزاری که برای تأمین امنیت این سامانه‌هـا مـورد اسـتفاده قـرار مـی‌گیـرد قراردادهای به‌کارگرفته شده برای احراز هویت و حفظ حریم خصوصی است؛ بنابراین، طراحی قراردادهایی که بتوانند نیازهای امنیتی کـاربران ماننـد حفـظ حـریم خصوصـی، احـراز اصـالت و دسـترس‌پـذیری را در اینترنـت اشـیاء تـأمین کنـد و بهبـود امنیـت قراردادهای موجود از چالش‌های مهم به‌کارگیری از این فنّاوری اسـت کـه روز بـه روز در حال گسترش و توسعه است.

بنابراین، با توجه به مطالب یاد شده در این مقاله سعی شـد چـالش‌هـا و مشـکلات امنیتی این فنّاوری به دقت مورد بررسی قرار گیرد.

همان‌طور که بررسی شد روش‌های اتصال و تعامل میان دستگاه‌ها در اینترنت اشـیاء دچار ضعف‌های زیادی است که برای حفظ حریم خصوصی و رسیدن به یـک الگـوی کسب و کار با قابل اطمینان و امن باید برطرف گردند تا بتوان از مزایای زیـادی کـه در اینترنت اشیاء وجود دارد بهره‌مند شد.

اینترنت اشیاء به جای کاهش شکاف اطلاعاتی و ارتباطی ممکـن اسـت حتـی آن را تعمیق کند. بسیاری از افراد ممکن است نتوانند یا نخواهند از این سـبک زنـدگیِ نـوین استقبال کنند و آن را به دلایل اقتصادی، سیاسی، مـالی، امنیتـی، مـذهبی و فرهنگـی 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. این شکاف اطلاعاتی و ارتباطی ایجاد شده در کنار چالش‌های امنیتی که به مرور زمان در مسیر این فنّاوری قرار می‌گیرد می‌تواند مانعی بزرگ در رسیدن اینترنت اشیاء به جایگاه واقعی خود باشد، استقبال نداشتن عمومی و بی‌اعتمادی به محرمانگی اطلاعات و ارتباطات بزرگ‌ترین مشکل برای توسعهٔ اینترنت اشیاء خواهد بود.

مگر اینکه به مقوله امنیت بیش از پیش اهمیت داده شود و این موضوع نیز با پیشرفت همراه باشد، هم‌زمان با سرمایه‌گذاری بر مسئله امنیت و محرمانگی می‌توان با کمک روش‌های سخت‌افزاری و نرم‌افزاری (طراحی رابط کاربری آسان، سخت‌افزارهای بدون پیچیدگی) شکاف ایجاد شده بین کاربران و این فنّاوری نوین را کاهش داد و با اعتمادسازی باعث رشد سریع و در نتیجه مقبولیت بیشتر اینترنت اشیاء در بین کاربران شد.

اینترنت اشیا در کنار همهٔ مزایایش، مشکلاتی هم دارد که صاحب‌نظران و سیاست‌گذاران باید از هم اکنون در اندیشهٔ مقابله با چالش‌های آن باشند. ما در این مقاله به بررسی برخی از چالش‌ها و مشکلات امنیتی موجود در اینترنت اشیاء پرداختیم، ولی جای بحث‌های فراوانی در این حوزه باقی است.

پیشنهادها

۱. سرمایه‌گذاری بر مسئله امنیت و محرمانگی در حوزهٔ اینترنت اشیاء
۲. ارتقای امنیت قراردادهای امنیتی موجود یا ارائه قراردادهای امنیتی جدید به‌ویژه در موضوع احراز هویت و محرمانگی داده‌های مبادله شده
۳. استفاده از زیرساخت‌های امن و مطمئن مانند «RFID»، شبکهٔ حسگر بی‌سیم، بلاک‌چین و... به منظور پیاده‌سازی بستر ارتباطی اینترنت اشیاء

٤. سهولت دسترسی و ایجاد رابط کاربری آسان به منظور تشویق و ترغیب عموم مردم برای استفاده از این فنّاوری نوظهور
٥. کاهش هزینهٔ سخت‌افزار و توسعهٔ نرم‌افزارهای موجود به منظور فراگیرشدن فنّاوری اینترنت اشیاء

منابع

A. A. Alkhatib. (2012).MAC layer overview for wireless sensor networks, in International Journal oF Computer Networks and Communication Systems, vol 4, pp. 35-22.

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.

Boyeon Song. RFID Authentication Protocols using Symmetric Cryptography. PhD thesis, Royal Holloway,April 2010.

D. G. Padmavathi and M. Shanmugapriya. (2009).A survey of attacks, security mechanisms and challenges in wireless sensor networks, International Journal of Computer Science and Information Security vol. 4, pp. 68-60.

G. Shen and B. Liu. (2011).The visions, technologies, applications and security issues of Internet of Things, in 2011 International Conference on E-Business and E-Government (ICEE), pp.4-1.

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.

Gartner's Hype Cycle Special Report for 2011, Gartner Inc, 2012. Available online: http://www.gartner.com/technology/research/hype-cycles/ (accessed on 10 August 2011).

Hung-Min Sun and Wei-Chih Ting, A Gen2-Based RFID Authentication Protocol for Security and Privacy, IEEE TRANSACTIONS ON MOBILE COMPUTING, Vol. 8, No. 8, PP [1052-1062], August 2009. Published by the IEEE CS, CASS,

Comp Soc, IES, & SPS.

I. F. Akyildiz, et al. (2002).A survey on sensor networks, Communications magazine, IEEE, vol. 40, pp. 114 - 102.

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

ITU. The Internet of Things; ITU Report: Genf, Switzerland, 2005.

J. Malhotra. (2015).Review on Security Issues and Attacks in Wireless Sensor Networks, International Journal of Future Generation Communication and Networking, vol. 8, pp. 88-81

K. Sharma, et al. (2010).A comparative study of various security approaches used in wireless sensor networks, International journal of advanced science and technology, vol. 17, pp. 44-31.

KU, W. C, Chang S. T. Impersonation attack on dynamic ID based remote user authentication using smartcards,IEICE,pp.2165-2167,2005

Lyne,James. (2014),security threat train 2015,Sophos security Research Center,2014.

M. R. Sohizadeh Abyaneh, «Passive Cryptanalysis of the UnConditionally Se-cure Authentication Proto col for RFID Systems, Cryptology ePrint Archive,2010.

M. Saxena. (2007).Security in wireless sensor networks-a layer based classification, Department of Computer Science, Purdue University, pp. 125-115

Nasour Bagheri, Masoumeh Safkhani et.al, «Cryptanalysis of RAPP, an RFID Authentication Protocol»Cryptology ePrint Archive: Report 2012/702

P M.Madhura et al.«A Survey Internet Of Things: Security And Privacy Issues»(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVETECHNOLOGY AND RESEARCHVolume No.3, Issue No.3,Page 2069 – 2074, April - May (2015)

S. Ghildiyal, et al. (2015).Analysis of Denial of Service (DoS) Attacks in Wireless Sensor Networks, IJRET: International Journal of Research in Engineering and Technology, pp.1163-2319.

S. Konomi and G. Roussos, «Ubiquitous computing in the real world: lessons learnt from large scale RFID deployments, Pers. Ubiq.

Computing, 2007.

Sundmaeker, H; Guillemin, P; Friess, P; Woelfflé, S. Vision and Challenges for Realising the Internet of Things; European Commission—Information Society and Media: Brussels, Belgium, 2010.

Suo, H, Wan, J, Zou, C, & Liu, J. (2012). Security in the internet of things: a review. In Computer Science

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

Thomas S. Heydt-Benjamin, Dan V. Bailey, Kevin Fu, Ari Juels, and Tom O'Hare, Vulnerabilities in first-generation RFID-enabled credit cards.«In Proceedings of the Eleventh International Conference on Financial Cryptography and Data Security, Lowlands, Scarborough, Trinidad/Tobago, February 2007.

Y. Liu. (2012).Wireless sensor network applications in smart grid: recent trends and challenges, International Journal of Distributed Sensor Networks, vol 93, pp. 41-33.

http://www.rfidjournal.com
http://www.gartner.com/technology/research/hype-cycles
www.IDTechEx.com/research, 2014

محمد حسین حبیبی، دسته‌بندی حملات بر روی پروتکل‌های RFID، تحلیل امنیتی و حمله به برخی از پروتکل‌ها و بهبود یکی از آنها، پایان‌نامه مقطع کارشناسی ارشد مخابرات، دانشکده برق، دانشگاه امام حسین، ۱۳۹۰