نشریه علمی-تخصصی
پژوهش های نوین علوم مهندسی
ISSN: 2538-3809
سال هفتم، شماره ۲ (پیاپی: ۳۸)، تابستان ۱۴۰۱، جلد دو

تحلیل مسائل و چالش‌های امنیتی در اینترنت اشیاء

مهدی رضاتبار[1]*، یاسره یوسف تبار[2]

تاریخ دریافت: ۱۴۰۱/۰۴/۰۵
تاریخ پذیرش: ۱۴۰۱/۰۶/۰۸
کد مقاله: ۵۲۰۴۲

چکـیده

اینترنت در حال حاضر همه مردم را به هم وصل می‌کند ولی با اینترنت اشیاء تمام ابزارها و وسایل به هم متصل می‌شوند. اینترنت اشیاء نقش بسیار مهمی را پس از حضور خود بازی می‌کند، چرا که اینترنت اشیاء از تجهیزات معمولی و رایج گرفته تا کل لوازم خانگی را پوشش می‌دهد. با پتانسیل بسیار بزرگ اینترنت اشیاء، چالش‌هایی نیز به وجود آمده است. این مقاله بر روی مسائل و چالش‌های امنیتی تمرکز دارد. از آنجایی که اینترنت اشیاء بر پایه‌ی اینترنت ایجاد شده است، مسائل امنیتی اینترنت در اینترنت اشیاء نیز ظاهر خواهد شد. در این مقاله تقسیم‌بندی لایه‌ها و زیرلایه‌های اینترنت اشیاء معرفی می‌گردد. سپس مسائل امنیتی لایه‌ها به طور جدا تحلیل شده و سعی در یافتن راه‌حل‌هایی برای مسائل امنیتی و حریم خصوصی شده است. همچنین مسائل ادغام ناهمگن لایه‌ی متقابل مورد تحلیل قرار گرفته و در مورد مسائل امنیتی اینترنت اشیاء به عنوان یک سیستم کامل بحث می‌گردد.

واژگـان کلـیدی: اینترنت اشیاء، امنیت، ناهمگن، RFID، 6LowPAN.

۱- کارشناس ارشد مهندسی IT، شبکه‌های کامپیوتری، دانشگاه مازندران (نویسنده مسئول)، *mrezatabar@gmail.com*
۲- کارشناس ارشد مهندسی کامپیوتر، نرم افزار، دانشگاه مازندران

۱- مقدمه

با توسعه سریع اینترنت اشیاء[1]، انواع کاربردهای اینترنت اشیاء وجود دارند که در زندگی روزمره ما همکاری و کمک می‌کنند. این کاربردها از تجهیزات معمولی و رایج گرفته تا کل لوازم خانگی را در برمی‌گیرند، که کمک می‌کنند زندگی انسان بهتر شود (Tsai, C. et al., 2014). در همین حال، چالش‌هایی برای اینترنت اشیاء در راه هستند. از نظر مقیاس‌پذیری، کاربردهایی از اینترنت اشیاء که نیاز به تعداد زیادی از وسایل دارند، اغلب برای پیاده‌سازی دشوار هستند و علت آن نیز محدودیت زمان، حافظه، پردازش و محدودیت‌های انرژی است. برای مثال، محاسبه‌ی روزانه‌ی تغییرات درجه حرارت در سراسر کشور ممکن است نیاز به میلیون‌ها وسیله و حسگر داشته باشد و به مقدار داده‌ی غیرقابل مدیریتی منجر شود. از طرفی، سخت‌افزار مستقر شده در اینترنت اشیاء اغلب مشخصات عملیاتی مختلفی دارند و همه‌ی این عوامل در شکل‌گیری شبکه‌ی ناهمگن[2] اینترنت اشیاء همکاری دارند و داده‌های اینترنت اشیاء نیز ناهمگنی عمیقی خواهند داشت. علاوه بر این، ممکن است هکرها، نرم‌افزارهای مخرب و ویروس‌ها در طی فرآیند ارتباطی به یکپارچگی[3] و صحت[4] داده‌ها و اطلاعات آسیب وارد کنند. با توسعه‌ی فناوری اینترنت اشیاء، ناامنی اطلاعات به طور مستقیم کل سیستم اینترنت اشیاء را تهدید خواهد نمود.

امروزه، اینترنت اشیاء به طور گسترده‌ای در کاربردهای زندگی اجتماعی مانند شبکه‌ی توزیع برق هوشمند، حمل و نقل هوشمند، امنیت هوشمند، و خانه‌ی هوشمند مورد استفاده قرار می‌گیرد (Sundmaeker, H. et al., 2010). کاربردهای اینترنت اشیاء می‌توانند راحتی و آسایش را برای مردم به ارمغان بیاورند، ولی اگر اینترنت اشیاء نتواند امنیت حریم خصوصی افراد را تضمین کند، آنگاه اطلاعات خصوصی آنها ممکن است در هر زمانی در معرض خطر قرار داشته باشند. بنابراین امنیت اینترنت اشیاء نمی‌تواند نادیده گرفته شود. هنگامی که سیگنال اینترنت اشیاء دزدیده می‌شود یا قطع می‌گردد، به طور مستقیم بر روی امنیت کل اطلاعات اینترنت اشیاء تاثیر خواهد گذاشت. با انتشار گسترده‌ی اینترنت اشیاء، این حوزه اطلاعات بسیار ارزشمندی را فراهم خواهد کرد که خطر افشای چنین اطلاعاتی بالا خواهد رفت. اگر اینترنت اشیاء نتواند راه‌حل خوبی برای مسائل امنیتی داشته باشد، آنگاه توسعه‌ی آن تا حد زیادی محدود خواهد شد. بنابراین، فراتر از تمام مسائل اینترنت اشیاء، مشکل امنیتی به طور خاص مهم است.

۲- مسائل امنیتی در کاربردهای اینترنت اشیاء

در زمینه‌های خاصی از اینترنت اشیاء، مانند موقعیت‌یابی، مشکل امنیتی برای حریم خصوصی[5] وجود دارد که می‌توان به حریم خصوصی مکان و حریم خصوصی پرس و جو[6] اشاره کرد. مکان در اینجا به مکان فعلی یا گذشته‌ی یک کاربر اشاره دارد و حریم خصوصی پرس و جو به کاوش اطلاعات حساس اشاره می‌کند. اگر یک کاربر اغلب رستوران‌ها یا بیمارستان‌ها را در منطقه‌ی خاصی جستجو می‌کند، آنگاه این رکوردهای پرس و جو می‌توانند توسط برخی افراد غیرمجاز برای تحلیل مکان اقامت کاربر، درآمد، شیوه‌ی زندگی، رفتارها، وضعیت سلامت و دیگر اطلاعات حساس در نظر گرفته شوند که باعث افشای اطلاعات شخصی وی خواهند شد. حفاظت از حریم خصوصی شامل استتار محل، فضای ناشناس، رمزنگاری[7] فضا و غیره است (Suo, H. et al., 2013).

۳- تحلیل مسائل امنیتی اینترنت اشیاء

با توجه به معماری پیشنهاد شده توسط اتحادیه بین‌المللی مخابرات[8] در ITU-T Y.2002، اینترنت اشیاء به سه لایه حس‌کردن یا ادراک، لایه انتقال و لایه کاربرد تقسیم شده است (Liu, L. A., & Lai, S. L., 2006). در جدول ۱ این لایه ها نشان داده شده است.

جدول ۱: معماری امنیتی پیشنهاد شده توسط ITU

لایه کاربرد (Application)	برنامه کاربردی اینترنت اشیاء
	لایه پشتیبانی از برنامه کاربردی
لایه انتقال (Transportation)	شبکه محلی
	هسته شبکه
	دسترسی به شبکه
لایه حس‌کردن (Perception)	شبکه حس‌کردن
	گره حس‌کردن

1 Internet of Things (IoT)
2 Heterogeneous
3 Integrity
4 Validity
5 Privacy
6 Query
7 Encryption
8 International Telecommunication Union (ITU)

لایه‌ی حس‌کردن شامل امنیت RFID[1]، امنیت شبکه‌های حسگر بی‌سیم[2]، امنیت RSN[3] و هر نوع دیگر است. لایه‌ی انتقال شامل امنیت دسترسی به شبکه، امنیت هسته شبکه و امنیت شبکه محلی است. در زیرلایه دسترسی به شبکه، زیرلایه‌های امنیت شبکه ادهاک[4] و امنیت وای‌فای[5] نیز وجود دارند. امنیت در لایه پشتیبانی شامل امنیت فناوری نرم‌افزار، امنیت بستر محاسبات ابری و غیره است.

۳-۱. لایه‌ی حس‌کردن

لایه حس‌کردن یا لایه ادراک به طور عمده در مورد جمع‌آوری اطلاعات، حس‌کردن اشیاء و کنترل اشیاء است. لایه حس‌کردن می‌تواند به دو بخش تقسیم شود: گره حس‌کردن که شامل حسگرها یا کنترل‌کننده و غیره می‌باشد، و شبکه حس‌کردن که با شبکه انتقال ارتباط برقرار می‌کند. گره حس‌کردن برای به دست آوردن داده‌ها و کنترل داده‌ها استفاده می‌شود، شبکه حس‌کردن داده‌های جمع شده را به دروازه[6] می‌فرستد یا دستورات کنترلی را به کنترل‌کننده می‌فرستد. فناوری‌های لایه‌ی حس‌کردن شامل RFID، RSN، GPS[7] و غیره می‌باشد.

۳-۱-۱. مسائل امنیتی فناوری RFID و راه‌حل‌ها

RFID (شناسایی فرکانس رادیویی) یک تکنولوژی شناسایی خودکار بدون تماس مستقیم است، که می‌تواند به طور خودکار سیگنال برچسب هدف را جهت به دست آوردن داده‌های مرتبط شناسایی کند، فرآیند شناسایی نیازی به مداخله دستی توسط انسان ندارد، و می‌تواند در محیط‌های صنعتی و نامناسب نیز کار کند (Hu, F., & Wang, F., 2010). از آنجا که این فناوری به طور گسترده مورد استفاده قرار می‌گیرد، با مشکلات زیادی روبرو می‌شود که در ادامه شرح داده می‌شوند.

۳-۱-۱-۱. کدنویسی واحد و یکپارچه

در حال حاضر استاندارد رمزگذاری بین‌المللی واحدی برای برچسب RFID وجود ندارد. از مطرح‌ترین استانداردها می‌توان به استاندارد UID[8] (شناسایی جهانی) اشاره کرد که توسط ژاپن پشتیبانی می‌شود و استاندارد EPC[9] (کد الکترونیکی محصول) که توسط اروپا حمایت می‌گردد. از آنجا که هنوز استاندارد واحدی شکل نگرفته است، این امر ممکن است باعث به وجود آمدن مشکلاتی شود که کارتخوان RFID نتواند اطلاعات برچسب را به دست آورد یا در فرآیند خواندن باعث رخ دادن خطاهایی شود.

۳-۱-۱-۲. تداخل

تداخل RFID به دو دسته‌ی تداخل برچسب‌ها و تداخل کارتخوان‌های RFID تقسیم می‌شود (Finkenzeller, K., 2003). هنگامی که تعداد زیادی از برچسب‌ها در حوزه‌ی کاری کارتخوان قرار داشته باشند، به طور همزمان داده‌های اطلاعات خود را به کارتخوان RFID ارسال می‌کنند، که این امر ممکن است باعث شود تا کارتخوان RFID نتواند داده‌ها را به درستی دریافت کند، این پدیده تداخل برچسب‌ها نامیده می‌شود (Lv, B. Y. et al., 2008). با استفاده از الگوریتم‌های ضد تداخل می‌توان از ارسال هم‌زمان اطلاعات توسط چندین برچسب به کارتخوان جلوگیری نمود. اینترنت اشیاء نیاز به پوشش طیف وسیعی از حسگرهای RFID را دارد و همکاری چندین کارتخوان نیز بسیار مهم است، ولی حوزه کاری کارتخوان‌ها هم پوشانی خواهد داشت. بنابراین ممکن است اطلاعات تکراری ثبت شوند که باعث افزایش بار کاری بر روی شبکه انتقال خواهد شد. این مورد تداخل کارتخوان‌ها نامیده می‌شود.

۳-۱-۱-۳. حفاظت از حریم خصوصی RFID

برچسب‌های کم هزینه منجر به منابع محدود RFID از قبیل ظرفیت کم ذخیره‌سازی و قابلیت‌های محاسباتی ضعیف می‌شود، بنابراین نیاز به راه‌حل‌های کم حجم برای حفاظت از حریم خصوصی دارد که شامل حریم خصوصی داده‌ها و حریم خصوصی مکان است.

حریم خصوصی داده‌ها: سبک‌های مختلف سازمانی برای اینترنت اشیاء نیازمند روش‌های مختلف توافق‌های حفاظت از حریم خصوصی است. یک راه حل سازش‌کارانه برای مسائل حریم خصوصی داده‌ها این است که اطلاعات کم اهمیت‌تر در برچسب RFID ذخیره شود، و اطلاعات مهم در سرویس سطح بالا ذخیره شود.

1 Radio Frequency Identification
2 Wireless Sensor Network (WSN)
3 RFID Sensor Network
4 Ad-Hoc
5 WiFi
6 Gateway
7 Global Positioning System
8 Universal Identification
9 Electronic Product Code

حریم خصوصی مکان: اگر چه برچسب‌های RFID اطلاعات مهم را ذخیره نمی‌کنند، ولی هکرها همچنان می‌توانند اطلاعات شناسه‌ی برچسب را با هدف ردیابی موقعیت برچسب به دست آورند (Lakafosis, V. et al., 2011). به عنوان مثال، هنگامی که یک کارتخوان RFID مجهز به اطلاعات GNSS[1] (سامانه ماهواره‌ای ناوبری جهانی) خودرو، اطلاعات برچسب را می‌خواند، آنگاه این کارتخوان می‌تواند به راحتی اطلاعات مکان تقریبی برچسب را با توجه به محدوده عملیاتی موثر آن به دست آورد.

۳-۱-۲. مسائل امنیتی و راه‌حل‌های فنی در شبکه‌های حسگر بی‌سیم

شبکه‌های حسگر بی‌سیم منابع محدودی دارند از جمله فضای ذخیره‌سازی کم، قابلیت محاسباتی ضعیف و محدوده‌ی حس‌کردن کوچک که منجر به یک سری از خطرات امنیتی شبکه می‌شود. در طی فرآیند جمع‌آوری داده‌ها در لایه حس‌کردن، پیام ممکن است با استراق سمع، مسیریابی مخرب، دستکاری پیام و دیگر مسائل امنیتی روبرو شود، که امنیت کل سیستم اینترنت اشیاء را تحت تاثیر قرار خواهد داد. مسائل امنیت داده‌ها می‌توانند به محرمانگی داده‌ها[2]، صحت داده‌ها[3]، تمامیت داده‌ها[4]، و تازگی داده‌ها[5] خلاصه شوند. این چهار نوع از مسائل امنیتی می‌توانند از جنبه‌هایی از جمله الگوریتم‌های رمزنگاری و مسیریابی امن حل شوند.

۳-۱-۳. مسائل ادغام ناهمگن

RSN (شبکه حسگر RFID) به طور گسترده‌ای در اینترنت اشیاء استفاده می‌شود، که ادغامی از RFID و شبکه‌های حسگر بی‌سیم است (Ren, F. Y. et al., 2003). ما می‌توانیم از فناوری RSN برای حل مشکل داده‌های ناهمگن استفاده کنیم.

در اینترنت اشیاء، تعداد زیادی از داده‌هایی که به طور گسترده‌ای توزیع شده هستند باید جمع‌آوری شوند. با این حال، داده‌هایی که با روش‌های متفاوت یا پروتکل‌های مختلف جمع‌آوری شده‌اند، در فرمت‌های مختلف نیز هستند. ما نمی‌توانیم تحلیل این داده‌ها را بدون متحدالشکل کردن آنها به طور موثری انجام دهیم، و اگر نتوانیم فناوری ادغام درستی به دست آوریم، آنگاه داده‌ها نابود خواهند شد، گم شده یا به خطر خواهند افتاد، اگر گره‌ها مانیتور و در اختیار گرفته شوند، اطلاعات به سرقت خواهند رفت، که در نتیجه حریم خصوصی در معرض خطر قرار خواهد گرفت. RFID و شبکه‌های حسگر بی‌سیم به همکاری نزدیک در سطح نرم‌افزاری برای ادغام در سطح سیستم نیاز دارند. بنابراین ما باید کدگذاری استاندارد داده‌ها و پروتکل تبادل اطلاعات برای RFID و شبکه‌های حسگر بی‌سیم در زمینه‌ی اینترنت اشیاء را یکپارچه و واحد نماییم.

۳-۲. لایه‌ی انتقال

لایه‌ی انتقال عمدتاً محیطی با دسترسی همه جا حاضر برای لایه‌ی حس‌کردن، انتقال و ذخیره‌سازی اطلاعات حس شده، و بارگذاری اطلاعات مرتبط دیگر توسط لایه‌ی برنامه‌ی کاربردی را فراهم می‌کند (Zhang, L., & Wang, Z., 2006). لایه انتقال می‌تواند بر اساس عملکرد به سه لایه تقسیم شود: دسترسی به شبکه، هسته‌ی شبکه و شبکه محلی. این لایه در واقع ترکیبی از انواع شبکه‌های ناهمگن است.

۳-۲-۱. مسائل امنیتی لایه‌ی انتقال

لایه‌ی انتقال اینترنت اشیاء در برابر ویروس‌ها و دیگر حملات نیز آسیب‌پذیر است که این تهدیدات در نتیجه منجر به افشای اطلاعات، فلج شدن شبکه و برخی دیگر از حملات مانند حملات بازپخش[6]، حملات دسترسی[7]، و حملات فیشینگ[8] سایت‌ها می‌شوند (Anti-Phishing Working Group, 2009). اگر چه حملات مسائل مشترک زیادی دارند، اما استفاده از روش‌های تشخیص نفوذ و روش‌های احراز هویت مناسب می‌توانند با تشخیص به موقع، از حملات جلوگیری کنند (Zhang, L., & Wang, Z., 2006). از آنجا که لایه‌ی انتقال در وسط سیستم اینترنت اشیاء قرار می‌گیرد، اهمیت زیادی دارد.

۳-۲-۱-۱. دسترسی به شبکه

وقتی که لایه حس‌کردن به هسته شبکه دسترسی دارد آنگاه لایه‌ی حس‌کردن و هسته‌ی شبکه مسائل امنیتی خواهند داشت. دسترسی به شبکه شامل شبکه‌های بی‌سیم، شبکه ادهاک و غیره است. با توجه به تفاوت‌ها در ساختار شبکه، شبکه‌های بی‌سیم را می‌توان به شبکه‌ی مرکزی و شبکه‌ی غیرمرکزی تقسیم نمود. در شبکه‌ی مرکزی، ارتباط بین گره‌های سیار باید با استفاده از یک

1 Global Navigation Satellite System
2 Data Confidentiality
3 Data Authenticity
4 Data Integrity
5 Data Freshness
6 Replay Attacks
7 Access Attacks
8 Phishing Attacks

ایستگاه پایه از قبیل شبکه‌های سلولی رایج و شبکه محلی بی‌سیم تنظیم شود. در شبکه‌ی غیرمرکزی، ارتباط بین گره نیازی به تنظیم با ایستگاه پایه ندارد (Li, C., & Chen, C. L., 2011). وای‌فای یک شبکه مرکزی و ادهاک یک شبکه غیرمرکزی است.

- **تحلیل مسائل امنیتی وای‌فای**

امنیت شبکه در وای‌فای یک نگرانی است. وقتی که کاربران دسترسی به صفحه‌ی وب اینترنت دارند، این احتمال وجود دارد که با یک سایت فیشینگ روبرو شوند، رمز عبور و حساب کاربران در معرض خطر قرار خواهد گرفت (Anti-Phishing Working Group, 2009). به طور خلاصه، مسائل امنیتی وای‌فای عبارتند از حملات دسترسی، نقطه‌ی دسترسی فیشینگ مخرب، و حملات DoS[2]/DDoS[1].

به منظور حل مسائل امنیتی وای‌فای، کنترل دسترسی و رمزنگاری شبکه مورد ارزیابی قرار می‌گیرد. کنترل دسترسی به این مورد اشاره دارد که تنها کاربران مجاز می‌توانند به شبکه وای‌فای دسترسی داشته باشند. رمزنگاری شبکه به معنی این است که تنها دریافت‌کننده یعنی کسی که می‌تواند به درستی رمزگشایی کند، می‌تواند محتوای داده‌ها را نیز متوجه شود.

- **تحلیل مسائل امنیتی ادهاک**

در اینترنت اشیاء، شبکه ادهاک می‌تواند ناهمگنی را بین گره‌های لایه‌ی حس‌کردن با استفاده از پروتکل مسیریابی شبکه ادهاک کاملاً رفع کند (Avudainayagam, A. et al, 2003). اگر گره‌های شبکه تغییر کنند، آنگاه شبکه ادهاک قادر است تا حدودی خودش را با این تغییرات وفق دهد. تهدیدات امنیتی شبکه ادهاک معمولی ناشی از کانال رادیویی و شبکه‌ها هستند. کانال بی‌سیم در برابر استراق سمع و دخالت آسیب‌پذیر است. علاوه بر این، شبکه‌های غیرمرکزی و خود سازمان[3] از تهدیدات آسیب‌پذیری، تقلب و دیگر اشکال حمله نیز رنج می‌برند. امنیت مسیریابی شبکه، می‌تواند با روش‌های رمزنگاری بررسی شود.

۳-۲-۱-۲. هسته‌ی شبکه

هسته‌ی شبکه‌ی اینترنت اشیاء عمدتاً مسئول انتقال داده‌ها است و به طور عمده اینترنت می‌باشد. از آنجا که تعداد زیادی از گره‌ها نیاز به دسترسی به اینترنت دارند، آدرس‌های IP زیادی را نیز نیاز دارند، اینترنت معمولی که مبتنی بر IPv4 است، قادر به پاسخگویی به بسیاری از حسگرها نمی‌باشد، به طوری که نسل بعدی اینترنت که مبتنی بر IPv6 است، می‌تواند این مشکل را حل نماید. با توجه به اینکه استفاده از IPv6، به دلیل ۱۲۸ بیتی بودن آن، برای حافظه و قدرت پردازشی سنسورهای کوچک سنگین به حساب می‌آید، در نتیجه راه حل این مشکل، تعریف فناوری 6LowPAN[4] که نسخه سبک تر از IPv6 می‌باشد، بوده است که برای استفاده از شبکه‌های حسگر IPv6 با مصرف توان کم برای ادغام ناهمگن در نظر گرفته شده است.

فناوری 6LowPAN از لایه‌ی PHY[5] و لایه‌ی MAC[6] از IEEE802.15.4 استفاده کرده، و در لایه‌ی انتقال از پروتکل IPv6 بهره می‌برد (Montenegro, G., et al., 2007). به منظور دستیابی به اتصال یکپارچه‌ی لایه‌ی MAC و لایه‌ی انتقال، بین این دو لایه، لایه‌ی انطباق اضافه شده است که برای کامل نمودن فشرده‌سازی سرآیند بسته، قطعه‌بندی و اتصال قطعه‌ها، پشتیبانی از چندپخشی، ایجاد توپولوژی شبکه، هدایت مسیریابی و انتساب آدرس‌ها مورد استفاده قرار می‌گیرد. این پشته پروتکلی که توسط IEEE[7] و IETF[8] ایجاد شده، در مرجع (Palattella M. et al., 2013) بحث شده و در جدول ۲ نیز نمایش داده شده است.

جدول ۲: پشته پروتکلی ایجاد شده توسط IEEE و IETF

لایه کاربرد (Application)
لایه شبکه/مسیریابی (Network/Routing)
لایه انطباق (Adaptation)
لایه کنترل دسترسی رسانه (MAC)
لایه فیزیکی (PHY)

1 Distributed Denial of Service
2 Denial of Service
3 Self-Organization
4 Low power Wireless Personal Area Networks
5 Physical Layer
6 Medium Access Control Layer
7 Institute of Electrical and Electronics Engineers (IEEE)
8 Internet Engineering Task Force (IETF)

۳-۲-۱-۳. شبکه‌ی محلی

در اینترنت اشیاء، کنترل دسترسی به شبکه برای تضمین این مورد است که منابع شبکه به طور مجاز استفاده می‌شوند، که استراتژی اصلی حفاظت از امنیت شبکه است. سایر موارد، از قبیل عدم پذیرش کدهای مخرب، خاتمه دادن یا حذف نمودن سرویس‌های غیرضروری از سیستم، به‌روزرسانی بسته‌های سیستم عامل به طور مداوم، استفاده از کلمه عبور امن می‌تواند برای حافظت از امنیت شبکه محلی اینترنت اشیاء استفاده شود.

۳-۲-۲. مسائل مربوط به حمله‌ها

حمله DDoS از رایج‌ترین حمله‌های شبکه به ویژه در اینترنت اشیاء است. به علت ناهمگنی و پیچیدگی شبکه اینترنت اشیاء، لایه‌ی انتقال در برابر حمله‌ها آسیب‌پذیر است. معمولاً راه‌حل برای مقابله با این حمله به صورت ارتقاء سیستم و استفاده از روش‌های تشخیص و پیشگیری از حمله‌ی DDoS می‌باشد (Yi, K. M., 2010).

۳-۳. لایه‌ی کاربردی

لایه‌ی برنامه‌ی کاربردی شامل نرم‌افزارهای خاص تجاری، فردی یا ادغام شده است. مسائل امنیتی که این لایه با آنها روبرو است، نمی‌توانند در دیگر لایه‌های اینترنت اشیاء حل شوند، مانند مسئله‌ی حفاظت از حریم خصوصی، که در لایه‌های حس‌کردن و انتقال رخ نمی‌دهد، ولی می‌تواند به یک تقاضای واقعی در برخی از زمینه‌های خاص در لایه‌ی برنامه‌ی کاربردی تبدیل شود، یا می‌تواند به عنوان یک تقاضای امنیتی خاص در لایه‌ی کاربردی لحاظ شود (Wang, K. et al., 2010).

لایه پشتیبانی از کاربرد، یک لایه‌ی پیشرفته بر بالای لایه‌ی انتقال است، که از انواع سرویس‌های تجاری پشتیبانی می‌کند و محاسبات هوشمند و تخصیص منابع را در غربالگری، تولید و پردازش داده‌ها تحقق می‌بخشد. در حین کل فرآیند، لایه‌ی پشتیبانی از کاربرد می‌تواند داده‌های معتبر، داده‌های هرز (اسپم) و حتی داده‌ها مخرب را تشخیص داده، و آنها را به موقع فیلتر کند.

۳-۳-۱. مسائل امنیتی لایه‌ی پشتیبانی از کاربرد

در اینترنت اشیاء، میان‌افزار[1] بر روی فناوری هسته‌ای خاص، مانند سرورهای میان‌افزار سنتی به عنوان مؤلفه‌ی ارتباطی توسعه داده می‌شود، که به نرم‌افزار اجازه‌ی استقرار بر روی بسترها یا سیستم‌عامل‌های متفاوت را می‌دهد. با این حال داده‌ها در اینترنت اشیاء گسترده و پویا است، در نتیجه میان‌افزار اینترنت اشیاء باید ظرفیت بزرگی داشته و بتواند برای ذخیره‌ی داده‌های در حال افزایش به صورت خطی گسترش یابد (Sweeney, L., 2002). ضمن اینکه توابع داخل میان‌افزار اینترنت اشیاء مانند کنترل درجه حرارت محیط دارای پیچیدگی خاصی می‌باشند.

۳-۳-۱-۱. تهدیدات امنیتی

بستر محاسبات ابری، داده‌ها را رمزگذاری نموده و از داده‌های کاربران پشتیبان‌گیری خواهد نمود که تا مدت زمان معینی حذف نخواهند شد. محاسبات ابری شامل اطلاعات کلیدی خاصی از شرکت‌ها است، بنابراین شرکت‌ها و افراد به اهداف هکرها تبدیل شده‌اند. هر چند این یک مسئله‌ی رایج نیست، ولی رویداد امنیتی ممکن است رخ دهد. با توجه به مسئله‌ی امنیتی، شرکت‌هایی با داده‌های حساس از قبیل شرکت‌های پزشکی و شرکت‌های مالی توصیه نمی‌شود که از فناوری محاسبات ابری استفاده کنند.

۳-۳-۱-۲. مسئله‌ی حمله و وقفه در سرویس

قطع شدن سرویس ابری امری رایج است، که شامل پشتیبان‌گیری از داده‌ها، خاموش شدن سیستم از این جمله‌اند که البته قابل جلوگیری هستند. همچنین حمله‌ی DDoS نیز در کنار قطع شدن سرویس وجود دارد. حمله‌ی DDoS به نوعی از حمله اشاره دارد که می‌تواند از اینکه کاربران عادی به سرویس‌های ابری دسترسی داشته باشند، جلوگیری کند، این حمله باعث می‌شود که برخی از سرویس‌های بحرانی ابری، منابع سیستمی زیادی از قبیل فرآیندها، حافظه، فضای ذخیره سازی و پهنای باند شبکه مصرف کنند، که این امر باعث می‌شود تا پاسخ ابری بسیار کندتر شده یا پاسخ به طور کامل قطع شود.

۳-۳-۱-۳. بررسی مسائل حسابرسی[2]

در محاسبات ابری، سرویس‌های محاسباتی، ذخیره‌سازی، پهنای باند شبکه می‌توانند به طور سراسری در دسترس باشند، ولی اطلاعات حساب‌های ارائه شده توسط کاربران می‌تواند تقلبی باشد. بنابراین جرم‌های شبکه‌ای مبتنی بر بستر محاسبات ابری به

1 Middleware
2 Accounting

سختی قابل ردیابی هستند. اگر شرکت‌ها به صورت عجولانه و بدون اینکه درک کاملی از محیط فراهم‌کننده‌ی سرویس ابری، کاربردهای اینترنت اشیاء و مسئولیت‌های عملیاتی (مانند مسئولیت‌هایی برای حادثه، مسائل رمزنگاری، نظارت بر امنیت) داشته باشند، خود را بر محاسبات ابری انطباق دهند، آنگاه با خطرات نامعلومی مواجه خواهند شد.

۴- امنیت اینترنت اشیاء به عنوان یک سیستم کامل

مسائل امنیتی زیادی وجود دارند که نیاز است به عنوان یک سیستم کامل در نظر گرفته شوند. نیازهای امنیتی برای اینترنت اشیاء نمی‌توانند به سادگی با کنار هم قرار دادن راه‌حل‌های هر زیر لایه در کنار یکدیگر به دست آید.

همانطور که می‌دانیم، برخی از نیازهای امنیتی نمی‌توانند تنها با استفاده از یک فناوری خاص در یک لایه‌ی تنها برطرف شوند. به عنوان مثال، برای یک سیستم با لایه برنامه کاربردی ضعیف، مهم نیست که ما چقدر برای حفظ حریم خصوصی داده‌ها در لایه‌ی حس‌کردن تلاش کنیم، چون یک مهاجم به راحتی می‌تواند تمام اطلاعات خصوصی را به دست آورد. از آنجا که لایه برنامه کاربردی به برنامه کاربردی مرتبط است، به همین دلیل مسائل امنیتی نمی‌توانند در لایه‌های دیگر اینترنت اشیاء حل شوند. بنابراین، به همکاری بین لایه‌های مختلف و نیز به طراحی فناوری‌های مربوط برای استفاده در لایه‌های متقابل نیاز داریم.

۵- نتیجه‌گیری

اینترنت اشیاء نشان دهنده تکامل اینترنت در آینده می باشد و ارتباطات میان اشیا با دیدگاه «هر زمان، هرمکان و با هر وسیله» را امکان پذیر می‌سازد. با توجه به این که اینترنت اشیاء جزئی از اینترنت آینده[1] خواهد بود از این پس خود داده‌ها و اطلاعات باید نقطه‌ی تمرکز راهکارهای ارتباطی و شبکه بندی باشد. از این رو، مشخص است که در میان تمام چالش‌های موجود، چالش تأمین امنیت و حفظ حریم خصوصی افراد باید به دقت مطالعه شود و راهکارهای ویژه‌ی اینترنت اشیاء ارائه شود.

هرچند اینترنت اشیاء دروازه بزرگ و مهمی برای ورود به دنیایی با قابلیت های 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. کاربر/شهروند نهایی نیز نقش مهمی را در دسترسی به داده‌ها و اطلاعات بازی می‌کند. مردم باید قوانین بین‌المللی امنیت سایبری را برای برقراری ارتباط بهتر و بدون خطا یاد بگیرند. همچنین نکته‌ای بصورت مکرر از سوی متخصصان امنیتی به آن اشاره شده که اقدامات پیشگیرانه و استفاده از عقل سلیم در برقراری ارتباطات، مهم ترین نکته برای خنثی کردن این تهدیدات است.

اینترنت اشیاء در کنار همه مزایایش، مشکلاتی هم دارد. از طرفی دغدغه‌های امنیتی پیش روی این فناوری باید به دقت مورد بررسی قرار گیرد و سیاست‌های مناسب برای مقابله با این تهدیدات، توسط دولت‌ها و کشورها جهت تمایل به استفاده از این فناوری، اتخاذ گردد. صاحب نظران و سیاست گذاران باید از هم‌اکنون در اندیشه مقابله با چالش‌های آن باشند. در این مقاله به بررسی برخی از چالش‌ها و روشهای بهبود امنیت در اینترنت اشیا پرداخته شده است، ولی همچنان جای بحث‌های فراوانی در این حوزه باقیست.

منابع

1. Anti-Phishing Working Group. (2009). Phishing activity trends report, 4th Quarter/2009.
2. Avudainayagam, A., Lou, W., & Fang, Y. (2003). DEAR: A device and energy aware routing protocol for heterogeneous Ad hoc networks, Parallel and Distributed Computing, 63(2), pp. 228-236, doi: 10.1016/S0743-7315(02)00066-7.
3. Finkenzeller, K. (2003). RFID handbook fundamentals and applications in contactless smart cards and identification (2nd ed.), West Sussex: Wiley, ISBN: 978-0470844021.
4. Hu, F., & Wang, F. (2010). Study of recent development about privacy and security of the internet of things, In Proceedings of the international conference on web information systems and mining, pp. 91-95, doi: 10.1109/WISM.2010.179.
5. Lakafosis, V., Traille, A., & Lee, H. (2011). RFID-CoA: The RFID tags as certificates of authenticity, In Proceedings of the IEEE international conference on RFID, pp. 207-214.
6. Li, C., & Chen, C. L. (2011). A multi-stage control method application in the fight against phishing attacks, In Proceeding of the 26th computer security academic communication across the country, p. 145-153.
7. Liu, L. A., & Lai, S. L. (2006). ALOHA-based anti-collision algorithms used in RFID

1 Future Internet (FI)

system, In Proceedings of the IEEE international conference on networking and mobile computing, pp. 1-4, doi: 10.1109/WiCOM.2006.342.

8. Lv, B. Y., Pan, J. X., Ma, Q., & Xiao, Z. H. (2008). Research progress and application of RFID anti-collision algorithm, In Proceedings of the international conference on telecommunication engineering, 48(7) , pp. 124-128.
9. Montenegro, G., Kushalnagar, N., Hui, J., & Culler, D. (2007). Transmission of IPv6 packets over IEEE 802.15.4 networks, https://datatracker.ietf.org/doc/rfc4944/.
10. Palattella M., Accettura N., Vilajosana, X. et al. (2013). Standardized Protocol Stack for the Internet of (Important) Things, Communications Surveys & Tutorials, IEEE, 15(3), pp. 1389-1406, doi: 10.1109/SURV.2012.111412.00158.
11. Ren, F. Y., Huang, H. N., & Lin, C. (2003). Wireless sensor networks, Journal of Software, 7, pp. 1282-1290.
12. Sundmaeker, H., Guillemin, P., Friess, P., & Woelffle, S. (2010). Vision and challenges for realising the internet of things, Cluster of European Research Projects on the Internet of Things—CERP IoT, ISBN: 978-92-79-15088-3.
13. Suo, H., Liu, Z., Wan, J., & Zhou, K. (2013). Security and privacy in mobile cloud computing, In Proceedings of the 9th IEEE international wireless communications and mobile computing conference (IWCMC), pp. 655–659, Cagliari, Italy, doi: 10.1109/IWCMC.2013.6583635.
14. Sweeney, L. (2002). K-anonymity: A model for protecting privacy, International Journal of Uncertainty, Fuzziness, and Knowledge-Based Systems, 10(5), pp. 557-570, doi: 10.1142/S0218488502001648.
15. Tsai, C., Lai, C., & Vasilakos, V. (2014). Future internet of things: Open issues and challenges, ACM/Springer Wireless Networks, pp. 2201-2217, doi:10.1007/s11276-014-0731-0.
16. Wang, K., Bao, J., Wu, M., & Lu, W. (2010). Research on security management for internet of things, In Proceeding of the IEEE international conference on computer application and system modeling (ICCASM), vol. 15, pp. 133-137, doi: 10.1109/ICCASM.2010.5622549.
17. Yi, K. M. (2010). Preliminary study of IoT security, Internet Police Detachment of Public Security Bureau in Taian City.
18. Zhang, L., & Wang, Z. (2006). Integration of RFID into wireless sensor networks: architectures, opportunities and challenging problems, In Proceeding of the IEEE fifth international conference on grid and cooperative computing workshops (GCCW), 06(58), pp. 463-469.