نشریه علمی-تخصصی
پژوهش های نوین علوم مهندسی
ISSN: 2538-3809
سال هشتم، شماره ۵ (پیاپی: ۴۶)، زمستان ۱۴۰۲

بررسی مکانیزم‌های امنیتی و حفظ حریم خصوصی برای اتصال وسایل هوشمند در اینترنت اشیاء

یاسره یوسف تبار[1]*، مهدی رضاتبار[2]

تاریخ دریافت: ۱۴۰۲/۱۰/۰۹
تاریخ پذیرش: ۱۴۰۲/۱۱/۱۱
کد مقاله: ۶۳۱۹۱

چکـیده

وقتی میلیاردها وسیله‌ی هوشمند تحت پدیده‌ی اینترنت اشیاء در حال اتصال به اینترنت هستند، آنگاه نیاز به روش‌های امنیتی قوی وجود دارد تا اطلاعات صحیح را به اشیاء صحیح و در مکان و زمان صحیح و از طریق کانال صحیح تحویل دهند. در عین حال، در ایجاد ارتباط میان تمام افراد، اشیاء، و ماشین‌ها نیز مسلماً امنیت مورد نیاز است. علاوه بر این، هکرها هم اغلب تلاش می‌کنند تا اطلاعات استراتژیک برای تجارت خود را بدون در نظر گرفتن قوانین سایبری یا اخلاقی سرقت نمایند. در این مقاله، مفهوم وسایل هوشمند و اتصال آن‌ها بررسی و در مورد روش‌های امنیتی در وسایل هوشمند و با تاکید بر روش‌های رسیدگی فیزیکی و منطقی در داخل سناریوهای اینترنت اشیاء مورد بررسی قرار می‌گیرد.

واژگـان کلـیدی: امنیت، حریم خصوصی، اینترنت اشیاء، وسایل هوشمند.

۱- کارشناس ارشد، مهندسی کامپیوتر/ نرم افزار، دانشگاه مازندران (نویسنده مسئول)
y.youseftabar@gmail.com
۲- کارشناس ارشد، مهندسی فناوری اطلاعات/ شبکه های کامپیوتری، دانشگاه مازندران.

۱- مقدمه

در حال حاضر بسیاری از خودروها، خانه‌ها، یخچال‌ها و لوازم و وسایل دیگر به اینترنت متصل شده‌اند و در آینده‌ای نزدیک، اشیاء فیزیکی بیشتری نیز به اینترنت آینده[1] متصل خواهند شد. یک چشم‌انداز کامل برای اینترنت اشیاء در واقع جهانی از حسگرهای کم هزینه است که برای زندگی روزمره‌ی ما طراحی، توسعه و تعبیه خواهند شد که به عبارت دیگر بتوانند از طریق اتصال وسایل هوشمند سرویس‌های بهتری را به انسان ارائه دهند. اصطلاح وسیله‌ی هوشمند[2] در واقع هر شئ فیزیکی مرتبط با منابع محاسباتی و قادر به برقراری ارتباط را تعریف می‌کند که می‌تواند با دیگر اشیاء مشابه از طریق رسانه انتقال فیزیکی و پروتکل‌های منطقی یا با انسان از طریق یک واسط کاربری استاندارد ارتباط برقرار کند (Carabelea C, Boissier O, 2003).

وسایل هوشمند می‌توانند برنامه‌ریزی شوند و یا به صورت سخت‌افزاری هم وصل شوند تا مثلاً چراغ‌های اتاق خواب کسی طوری رفتار کند که روشنایی آن به تدریج از زمانی افزایش یابد که شخص در حال بیرون آمدن از خواب عمیق است. حسگرها می‌توانند شبانه‌روز کار کنند تا همه چیز را از رژیم غذایی شخص گرفته یا حتی رفتار خواب شخص را اندازه‌گیری و نظارت کنند. نمونه‌ای از یک مشاهده در بیمارستان به این صورت است که فشار خون بیمار، نوار قلب[3]، سطح قند خون، اکسیژن، مقدار آب و دیگر پارامترهای پزشکی مرتبط، به وسیله‌ی حسگرها، کامپیوترها، و وسایل هوشمند پزشکی مربوط به نظارت، اتوماسیون، و کنترل به طور کامل اندازه‌گیری شده و در نهایت برای رسیدگی بیشتر اطلاعاتی در اختیار پرستاران و پزشکان قرار می‌گیرد. این یک نمونه‌ی ایده‌آل برای نشان دادن این مطلب است که چگونه وسایل هوشمند می‌توانند برای رسیدگی و درمان بهتر پزشکی مورد استفاده قرار گیرند. این نوع از اتصال وسایل، اینترنت اشیاء نامیده می‌شود.

۲- اینترنت اشیاء

اینترنت اشیاء، الگوی جدیدی است که در آن اشیاء شناسه‌های دیجیتالی، و قابلیت‌های نظارتی با هوش مصنوعی[4] داشته و می‌توانند به طور خودکار، مستقر و ردیابی شوند و همچنین مورد نظارت قرار گرفته و کنترل شوند. یک وسیله هوشمند در واقع یک وسیله الکترونیکی قادر به ارتباط با دیگر وسایل است که به طور کلی به دیگر وسایل الکترونیکی از طریق شبکه‌های با پهنای باند بالا و با کمک فناوری‌های بی‌سیم از قبیل بلوتوث، ارتباطات میدان-نزدیک[5]، وای فای، و 4G/5G متصل می‌شود. این وسایل هوشمند می‌توانند گوشی‌های هوشمند، اندرویدها، تبلت‌ها، iPadها، کامپیوترها، لپ‌تاپ‌ها، تلویزیون‌ها، کنسول‌ها، و دوربین‌های IP باشند (Noda C, Walter T, 2005).

ظهور اینترنت اشیاء محیطی را فراهم نموده که در آن اشیاء روزمره به اینترنت وصل شده و بر روی یک سیستم با یکدیگر همکاری و مشارکت کنند، که این امر همگرایی لوازم هوشمند و قابلیت اتصال آنها را به دیگر لوازم می‌دهد. اساس اینکه هر وسیله‌ی هوشمند به صورت کارآمد عمل کند در واقع با کمک فناوری‌های جاسازی شده‌ی اینترنت اشیاء است. اینترنت اشیاء، که سیستم‌های فیزیکی-سایبری[6] نیز نامیده می‌شود، در حال ایجاد تسلط بر روی تمام اشیاء زنده و همچنین غیر زنده بر روی زمین است. این مفهوم از طریق فناوری‌های مختلف متصل همه جا حضور دارد و پتانسیل این را دارد که به طور خودکار به نظارت و کنترل اشیاء حتی در شرایطی از بلایای طبیعی بپردازد. در اینترنت اشیاء، همه چیز واقعی به صورت مجازی در می‌آید، این مفهوم بدین معنی است که هر شخص و هر شئ دارای یک همتایی با قابلیت تعیین مکان، آدرس‌دهی، و قابل خواندن بر روی اینترنت است (Yong W et al., 2006). با اجازه دادن به اینکه همه‌ی اشیاء قابلیت اتصال داشته باشند، آنگاه اشیاء قابلیت شناسایی، تعیین مکان، حس شدن، کنترل‌پذیری، و مدیریت را خواهند داشت. در واقع، مفهوم اساسی، حضور گسترده اشیاء، از قبیل برچسب‌های شناسایی فرکانس رادیویی، محرک‌ها، تلفن‌های موبایل و حسگرها است (Atzori L et al., 2010).

۳- امنیت در اینترنت اشیاء

امنیت یک مفهوم جدیدی نیست. از زمان تولد تا مرگ، هر شخصی باید مراقب جنبه‌های متعدد امنیتی از نظر غذا، سرپناه، کودکان، مقالات علمی و تحقیقاتی، امور مالی و بسیاری از جنبه‌های دیگر باشد. به طور مشابه، وقتی میلیاردها وسیله‌ی هوشمند تحت چتر پدیده‌ی اینترنت اشیاء در حال اتصال به اینترنت هستند، آنگاه نیاز به روش‌های امنیتی قوی وجود دارد تا اطلاعات صحیح را به اشیاء صحیح و در مکان و زمان صحیح و از طریق کانال صحیح تحویل دهند. در عین حال، در ایجاد ارتباط میان تمام افراد، اشیاء، و ماشین‌ها نیز مسلماً امنیت مورد نیاز است. علاوه بر این، ممکن است هکرهایی وجود داشته باشند که اغلب تلاش می‌کنند تا اطلاعات استراتژیک برای تجارت خود را بدون در نظر گرفتن قوانین سایبری یا اخلاقی هک کنند. سازمان‌ها نیاز به محافظت از اطلاعات خود در برابر مهاجمان یا رقبا دارند چرا که این امر می‌تواند به از دست دادن داده‌های حرفه‌ای و تخصصی

1- Future Internet (FI)
2- Smart Device (SD)
3- Electro Cardio Graphy (ECG)
4- Artificial Intelligence (AI)
5- Near-Field Communication (NFC)
6- Cyber-Physical Systems

منجر شود. امنیت اطلاعات به اقدامات اتخاذ شده برای جلوگیری از استفاده‌ی غیر مجاز، سوء استفاده، دستکاری، یا انکار دانش، حقایق، داده‌ها یا قابلیت‌ها اشاره دارد (Maiwald E, 2004).

مسائل اساسی امنیتی در اینترنت اشیاء با مسائل امنیتی در کل حوزه فناوری اطلاعات یکی است. با این حال، در مورد اینترنت اشیاء، حساسیت و محرمانگی خیلی بیشتر مورد نیاز است. حساسیت فناوری‌های اینترنت اشیاء مبتنی بر نیازهای مختلف امنیتی از قبیل محرمانگی، تمامیت، اعتبار، حریم خصوصی، دسترس‌پذیری و مقررات است و امنیت برترین اصل برای عملکرد امن و قابل اطمینان وسایل متصل در اینترنت اشیاء است. به طور کلی مسائل امنیت وسایل هوشمند شامل مسائل فیزیکی و منطقی است. مسائل منطقی اکثراً در قالب نرم‌افزارهای مخرب از جمله ویروس‌ها، کرم‌ها، اسب‌های تروجان، و جاسوس‌افزارها هستند. وسایل هوشمند از نظر توان محاسباتی و حافظه قابلیت‌های محدودی دارند و ممکن است با منبع تغذیه‌ای از نوع باتری باشند، در نتیجه نیاز به اتخاذ فناوری‌های ویژه‌ی انرژی کارآمد کاملاً محسوس است. این وسایل در هر ثانیه مقدار زیادی داده حتی در حد پتا-بایت[1] در ثانیه تولید می‌کنند. استقرار اینترنت اشیاء نیز مسائل امنیتی زیادی را ایجاد کرده است که عبارتند از (۱) ماهیت اشیاء هوشمند، به عنوان مثال اتخاذ الگوریتم‌های رمزنگاری سبک و کم حجم، از نظر نیازهای پردازشی و حافظه؛ و (۲) استفاده از پروتکل‌های استاندارد، به عنوان مثال، نیاز به حداقل رساندن مقدار داده‌های تبادل شده بین گره‌ها (Cirani S et al., 2013).

روش اینترنت اشیاء یک روش کاربردی جدید است و افراد اغلب تمرکز بیشتری بر روی کاربردهای جدید دارند بدون اینکه به مسائل امنیتی آن توجهی داشته باشند، حال آنکه اهمیت امنیت در مورد شبکه‌های حسگر بی‌سیم در اینترنت اشیاء بسیار مهم است (Heer T et al., 2011). برای حرکت به سمت امنیت خاص اینترنت اشیاء، مسائل متعددی از قبیل الگوریتم‌های رمزنگاری، پروتکل‌های احراز هویت، کنترل دسترسی، اعتماد یا حریم خصوصی، و چارچوب‌های مدیریتی وجود دارند (Srivastava L, 2006). از این رو، بررسی وضعیت فناوری‌های کلیدی از جمله روش رمزنگاری، امنیت ارتباطات، حفاظت از داده‌های حسگر، و الگوریتم‌های رمزنگاری باید در نظر گرفته شوند (Suo H et al., 2012).

۴- امنیت در وسایل هوشمند

امنیت به عنوان توانایی مقابله با یک تهدید خاص به وسیله‌ی خنثی نمودن آن تعریف شده است. یک تعریف گسترده‌تر نیز به آزادی‌های نسبی از تسلط‌های متعدد خطرات و ریسک‌ها اشاره دارد و شامل جنبه‌های ذاتی شناختی و روان‌شناختی در یک سیستم امنیتی می‌شود. در نتیجه، امنیت نگرشی است که به شدت به ماهیت محیطی بستگی دارد که باید حس و درک شود (Gariup M, 2013). بازار وسایل مانند گوشی‌های موبایل، ساعت‌های چند منظوره، و دستیارهای شخصی به سرعت در حال رشد است و کاربران این وسایل سیار برای کاربردهای تجارت الکترونیک آینده‌ی خود نیاز به امنیت دارند. در حین اینکه فناوری جدید بسیاری از تجارت‌ها و تراکنش‌های شخصی را ساده کرده، ولی درب را نیز برای جرم‌های با فناوری‌های بالا باز نموده است (Pfitzmann A et al., 1997).

بسیاری از افراد حقوقی برای فعالیت‌های تجاری خود، و مردم عادی نیز برای کارهای روزانه‌ی خود به صورت شبانه‌روز و در سراسر جهان از وسایل هوشمند استفاده می‌کنند. در حال حاضر، از تبلت‌ها، Apple iPadها و تلفن‌های مبتنی بر اندروید توسط میلیونها نفر در سراسر جهان برای ارسال و دریافت اطلاعات مالی و عملیات تجاری خود مورد استفاده قرار می‌گیرد. برنامه‌های کاربردی متعددی در این وسایل هوشمند جاسازی و تعبیه شده‌اند مانند برنامه‌های کاربردی آفیس، تماس تلفنی، ایمیل و شبکه‌های اجتماعی که داده‌های مختلفی را از جمله متنی، صوتی و ویدئویی ارسال می‌کنند. این وسایل نیاز دارند که هم از نقطه نظر فیزیکی و هم منطقی در برابر تهدیدات امن شوند. بنابراین، هم امنیت فیزیکی و هم امنیت منطقی وسایل بصورت جدی مورد نیاز است. سرویس‌های امنیتی، مانند احراز هویت و کنترل دسترسی، باید به صورت غیر دخالت‌کننده، هوشمند، و قادر به انطباق سریع با تغییرات زمینه در فضاها باشند (Al-Muhtadi J et al., 2003). در ادامه، امنیت وسایل هوشمند در بخش‌های امنیت فیزیکی، امنیت منطقی و امنیت نرم‌افزاری به تفکیک شرح داده می‌شود.

۴-۱- امنیت فیزیکی

امنیت فیزیکی یکی از بخش‌های ضروری در وسایل هوشمند و اینترنت اشیاء است. امنیت فیزیکی نه تنها شامل سخت‌افزار سیستم است بلکه همچنین مکان‌های سیم‌کشی استفاده شده برای اتصال سیستم‌ها، پشتیبانی از سرویس‌ها، اقدامات پشتیبان‌گیری، و هر بخش دیگری از سیستم‌ها که به عنوان وسایل هوشمند در نظر گرفته می‌شوند، را نیز در بر می‌گیرد. اشیاء فیزیکی در یک خانه شامل لامپ‌ها، یخچال‌ها، پنکه‌ها، هیترها، پرده‌ها، پنجره‌ها، تخت‌ها، روتختی‌ها و ملحفه‌ها، صندلی‌ها، و دیگر لوازم خانگی مانند ظروف آشپزخانه است. در هنگام نصب یک شبکه یا اتصال خانه‌ای به شبکه‌ی خانگی[2] و شبکه‌ی گسترده[3] یا اینترنت، ما در واقع در حال ایجاد یک زیرساخت هستیم و اقدامات امنیتی برای اطمینان از این است که شبکه و وسایل برای

1- Peta-byte (10^{15} Bytes)
2- Home Area Network (HAN)
3- Wide Area Network (WAN)

صاحبان خانه و اعضای خانواده‌ی آنها قابل اطمینان باشند. قطعی برق برای بسیاری از تاسیسات، به دلیل دستکاری انسان، چه تصادفی و چه غیر تصادفی اغلب رخ می‌دهد. شبکه‌ها شامل اجزای فیزیکی از قبیل سیم‌ها، مودم‌ها، دیواره آتش[1] (فایروال)، باکس‌ها، و وسایل WiFi هستند، که می‌توانند به سادگی خراب شوند.

در بسیاری از تاسیسات، مردم هدف از وسیله‌ی الکترونیکی نصب شده را درک نخواهند کرد، و کنجکاوی ممکن است آنها را به آزمایش وا دارد. آنها ممکن است اهمیت یک کابل متصل به یک پورت ورودی/خروجی را درک نکنند. ممکن است کسی یک کابل اترنت را جدا کند یا جهت دوربین را تغییر دهد به طوری که این افراد می‌توانند لپ‌تاپ یا وسیله‌ی موبایل هوشمند خود را به مدت ۵ الی ۱۰ دقیقه به کابل اترنت جدا شده وصل کنند یا با تغییر جهت دوربین به اجرای عمل سرقت یا حرکت دادن یک سوئیچ بپردازند چرا که این موارد در مسیر آنها قرار گرفته است. یک دو شاخه ممکن است از منبع برق جدا شود به دلیل اینکه کسی به پریز آن نیاز دارد. اطمینان از امنیت فیزیکی تاسیسات بسیار جدی است، علائم و برچسب‌ها نیز تنها برای افرادی مفید خواهد بود که می‌توانند زبان ما را بخوانند. قرار دادن اشیاء در مکانی دور از مسیر و محدود کردن دسترسی، بهترین ابزار برای اطمینان از عدم وقوع حوادث و بی‌دقتی‌ها است. گاهی اوقات، افراد بسیار علاقمند به وسایل هوشمند، آخرین گجت‌ها، و وسایل الکترونیکی بوده و با در نظر گرفتن فرصت نیز به انجام سرقت می‌پردازند. ماشین‌های لباسشویی هوشمند، خشک‌کن‌های چرخشی، تهویه مطبوع، یخچال‌ها و فریزرها، آب گرم‌کن‌های برقی، و بخاری‌های برقی نیز ممکن است جزو این بخش باشند. از این رو، امنیت فیزیکی یکی از جنبه‌های حیاتی در امنیت ارتباطات وسایل هوشمند است.

۴-۲- امنیت منطقی

امنیت منطقی از فناوری‌ای استفاده می‌کند که به افراد این اجازه را می‌دهد تا به داده‌ها، اطلاعات، اشیاء، وسایل و سیستم‌ها بر اساس این که چه کسی هستند و نقش آنها در داخل یک سازمان یا مکان مسکونی یا شبکه چه می‌تواند باشد دسترسی داشته باشند. دسترسی به منابع اطلاعاتی باید به آن دسته از افرادی محدود شود که نیاز به دسترسی دارند. تعیین مالکیت[2] داده‌ها و اطلاعات و حقوق دسترسی به فرآیندی برای نظارت که افراد دسترسی مناسب و مجاز را داشته باشند، همگی بخش‌هایی از یک استراتژی موثر امنیتی هستند. عناصر امنیتی شامل احراز هویت، حریم خصوصی، سیاست‌های استانداردسازی و نظارت هستند. سرویس‌های امنیتی، مانند احراز هویت و کنترل دسترسی، نباید ناخوانده و پُرزحمت باشند، همچنین باید هوشمند و قادر به انطباق سریع با تغییرات رخ داده در فضاها باشند. امنیت منطقی در روش‌های مختلف در بخش‌های بعدی توضیح داده شده‌اند.

۴-۲-۱- احراز هویت

پیش از اینکه اجازه‌ی دسترسی به منابع و وسایل شبکه در اینترنت اشیاء داده شود، کاربران باید در ابتدا احراز هویت شوند. در یک دنیای ایده‌آل، هر کاربر سیمی و بی‌سیم یک شناسه خواهد داشت که منحصربفرد، غیرقابل تغییر، و قابل آدرس دادن است، و نمی‌تواند توسط کاربران دیگر جعل هویت شود. در غیر این صورت، این مورد تبدیل به یک مسئله‌ی بسیار دشوار خواهد شد که باید در دنیای واقعی حل شود. یک برنامه‌ی کاربردی پزشکی را در نظر بگیرید که در آن اطلاعات بیمار در سیستم اطلاعات پزشکی[3] و سیستم اطلاعات سلامتی[4] ذخیره می‌شود. دسترسی به داده‌ها با احراز هویت توسط چندین کاربر شامل بیمارستان، پزشکان، کارکنان، پرستاران، محققان پزشکی، و شرکت‌های بیمه باید معتبر و قابل اعتماد باشد.

وسایل باید با کمک دوربین مدار بسته/ دوربین‌های IP و نیروهای امنیتی فیزیکی امن شوند. این احراز هویت افراد هوشمند و وسایل هوشمند با استفاده از ابزار مختلفی از جمله آدرس MAC، RFID و کدهای QR است.

۴-۲-۲- کنترل دسترسی به رسانه (MAC)

یکی از اصلی‌ترین ویژگی‌ها در احراز هویت، داشتن یک شناسه‌ی منحصربفرد مانند آدرس کنترل دسترسی رسانه[5] است. این آدرس در واقع یک عدد ۴۸ بیتی است که توسط کارخانه‌ی سازنده به هر دستگاه اترنت و بی‌سیم تخصیص داده می‌شود. با استفاده از فیلتر کردن MAC در نقاط دسترسی[6]، ما می‌توانیم کاربران را بر اساس آدرس MAC آنها احراز هویت کنیم. با این ویژگی، نقطه‌ی دسترسی یک جدول داخلی از آدرس‌های تایید شده را نگهداری می‌کند. وقتی یک کاربر بی‌سیم سعی می‌کند که به نقطه‌ی دسترسی مورد نظر وصل شود، آنگاه آدرس MAC کاربر باید در لیست مورد تایید قرار داشته باشد؛ در غیر این صورت، وابستگی تکذیب خواهد شد. همچنین، نقطه‌ی دسترسی ممکن است جدولی از آدرس‌های MAC شناخته شده و بد را نیز نگهداری کند و به دیگر وسایلی که در لیست نیستند، اجازه‌ی دسترسی را ندهد. برخی از قابلیت‌ها در لایه‌ی MAC در IEEE

1- Firewall
2- Ownership
3- Medical Information System (MIS)
4- Health Information System (HIS)
5- Medium Access Control (MAC)
6- Access Point (AP)

ISSN: 2538-3809

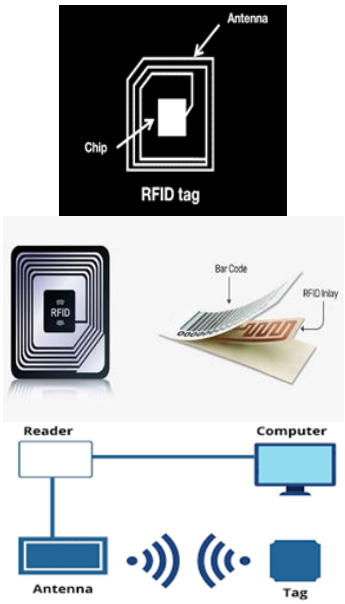
802.15.4 پیشنهاد می‌شود که می‌توانند توسط لایه‌های بالاتر برای دستیابی به سطح امنیتی بهتر مورد استفاد قرار گیرند. برخی از شرکت‌ها از شبکه‌های بی‌سیم برای اجازه دادن به افراد جهت مجهز کردن یا عدم مجهز کردن سیستم خود از راه دور، تماشای ویدئوهای زنده، تشخیص آب در زیرزمین، فعال کردن اعلان‌های ایمیل به صورت بی‌درنگ، و سیستم‌های کنترل بحرانی مانند چراغ‌ها، ترموستات‌ها، و لوازم خانگی کوچک به صورت از راه دور استفاده می‌کنند.

۴-۲-۳- شناسایی فرکانس رادیویی (RFID)

فناوری شناسایی فرکانس رادیویی[1] مفهوم پیشرفته‌ای را نسبت به دیگر فناوری‌های متعدد دارد. RFID یک فناوری قدرتمند است که نه تنها برای خودکارسازی بازرسی یا شناسایی محصولات استفاده می‌شود بلکه همچنین برای تقویت سیستم‌های موقعیت‌یابی مرسوم نیز مورد استفاده قرار می‌گیرد (Roman R er al., 2011).

کاربردهای شناسایی فرکانس رادیویی عبارت از کاربردهای نظامی، هواپیمایی، کتابخانه‌ای، امنیتی، مراقبت از سلامتی، ورزش‌ها، مزارع حیوانات و دیگر موارد می‌باشد. RFID بی‌سیم است، از الکترومغناطیس فرکانس رادیویی بدون تماس در زمینه‌ی انتقال داده‌ها استفاده می‌کند، به منظور شناسایی و ردیابی برچسب‌های متصل شده به اشیاء به طور خودکار استفاده می‌شود. بدون کنترل‌های امنیتی مناسب، برچسب‌های جاسازی شده در محصولات مصرفی می‌توانند به طور بالقوه اطلاعات مهمی را فاش کنند. حتی اگر محتویات برچسب امن شده باشد، آنگاه پاسخ‌های قابل پیش‌بینی برچسب می‌تواند ردیابی شده و حریم خصوصی مکان فرد را نقض نماید (Weis SA, 2003).

در یک رویکرد پایین به بالا، رمزنگاری سنگ بنای حفاظت از زیرساخت شبکه است. اگر چه پیاده‌سازی استانداردهای موجود مانند استاندارد رمزنگاری پیشرفته[2] ممکن است، ولی گاهاً پیاده سازی در برخی از انواع برچسب‌های RFID ممکن است با محدودیت مواجه گردد. روش‌های رمزنگاری حتی الامکان باید کوچکتر و سریعتر شوند در عین اینکه سطح امنیت نباید کم شود یا خیلی کم کاهش یابد. فناوری برچسب‌های شناسایی فرکانس رادیویی در شکل ۱ نشان داده شده است.



شکل ۱- فناوری RFID

۴-۲-۴- کد پاسخ سریع (QR)

کدهای QR[3] یکی از آخرین روش‌های احراز هویت است که در آن اهداف، اشیاء، یا رویدادها می‌توانند شناسایی شده یا تشخیص داده شوند. این کد که توسط گوشی موبایل نیز قابل اسکن می‌باشد، می‌تواند حاوی لینکی باشد که فرد را بلافاصله به صفحه‌ی وب سایت یک محصول خاص هدایت نماید که در آن جزئیات دقیق در مورد آن محصول خاص توضیح داده شده است. کدهای QR به صورت بارکُدهای ۲ بُعدی هستند که به صورت بصری بیت‌های اطلاعات را رمز می‌کنند که به صورت نقاط مربعی سیاهی بر روی یک صفحه مربعی سفید مشخص می‌شوند.

شکل ۲ – نمونه‌ای از کدهای QR

پروتکل‌های امنیتی کد QR، به خالق کد اجازه‌ی حفاظت از داده‌های ذخیره شده در کدهای QR را به وسیله‌ی رمزنگاری می‌دهد. این امر به کاربران نهایی اجاز می‌دهد تا پیام خود را با نسخه‌ی قبلی بررسی کنند تا دستکاری نشده باشد. شکل ۲ نمونه‌ای از کدهای QR را نشان می‌دهد.

۴-۳- نرم‌افزار و ابزار امنیتی

نرم‌افزار در واقع مجموعه‌ای از دستورالعمل‌های اجرایی برای حل مسئله‌ای است و نرم‌افزار امنیتی در واقع یک برنامه‌ی کامپیوتری است که برای ارتقای امنیت اطلاعات طراحی شده است. انفجار ترافیک اینترنت تقاضاهای بی‌شماری را برای متخصصان امنیتی سیستم اطلاعاتی ایجاد کرده است. در این حالت، تمام فایل‌هایی که سیستم عامل[4] باز یا استفاده می‌کند، پیش از اینکه به طور کامل باز شوند در ابتدا اسکن می‌شوند. امنیت باید در سرتاسر چرخه‌ی حیات نرم‌افزار وسیله هوشمند دقیقاً از

1- Radio Frequency Identification (RFID)
2- Advanced Encryption Standard (AES)
3- Quick Response
4- Operating System (OS)

طراحی اولیه، برنامه‌نویسی، و توسعه گرفته تا محیط عملیاتی و نگهداری رسیدگی شود. برای مقابله با حملات توزیع شده‌ی انکار سرویس[1]، کارکنان امنیت اطلاعات باید مطمئن شوند که اتصالات بحرانی شبکه، پهنای باند و افزونگی کافی برای پیشگیری از حملات آسان را دارند زیرا اتصالات با سرعت کمتر می‌توانند به سادگی توسط مهاجم در هم شکسته شوند (Li B, Li W, 2008). حملات توزیع شده‌ی انکار سرویس نمی‌توانند تنها به وسیله‌ی پهنای باند کافی برطرف شوند، بلکه روش‌های اضافی برای رسیدگی به این حملات نیز باید به کار گرفته شود. این روش‌ها عبارتند از نصب سیستم‌های تشخیص نفوذ برای پیش‌بینی یک حمله‌ی احتمالی، سیستم‌های تشخیص نفوذ به عنوان هشدار دهنده‌ی سارق شبکه، و گوش دادن به ترافیک شبکه و تطبیق آن با امضاهای رایج حمله‌ها که در پایگاه داده ذخیره شده‌اند (Sukhai NB ,2004).

کدهای امنیتی، آشکارسازهای حرکتی، و دوربین‌ها، اطلاعاتی را برای سیستم امنیت خانه‌ی هوشمند فراهم می‌کنند، و این اطلاعات به سیستم اجازه می‌دهند تا بتواند تشخیص دهد که آیا یک فرد حس شده یکی از ساکنان منزل، یا یک بازدیدکننده‌ی پاک، یا یک مزاحم است. آشکارسازهای حرکتی، هشداری را فعال می‌کنند و به برنامه‌ی هوش مصنوعی این اجازه را می‌دهند تا بداند که کسی یا چیزی برای ارزیابی وجود دارد. نرم‌افزار تشخیص چهره و کدهای امنیتی به سیستم امنیت این اجازه را می‌دهند تا به ساکنان منزل اجازه‌ی ورود به منزل را بدهد، در حالی که بر اساس اطلاعات برنامه‌ریزی شده دسترسی برای سایر افراد محدود می‌باشد (Robles RJ et al., 2010).

جدای از این، راه‌اندازی و بوت شدن امن یعنی وقتی که منبع برق در ابتدا به یک وسیله‌ی هوشمند وصل می‌شود، صحت و یکپارچگی نرم‌افزار سیستم باید بر روی وسیله هوشمند با استفاده از امضاهای دیجیتالی تولید شده به صورت رمز نگارانه مورد تایید و اعتبارسنجی قرار بگیرند. همانگونه که شخصی یک گواهینامه‌ی حقوقی را امضاء می‌کند، نرم‌افزار نیز باید از طریق یک امضای دیجیتال وصل شده به کپی نرم‌افزار توسط وسیله هوشمند اعتبارسنجی شود تا اطمینان حاصل شود که تنها نرم‌افزار مجاز بر روی وسیله هوشمند در هنگام بوت شدن و راه‌اندازی اجرا شود. در عین حالی که پایه و اساس اعتماد ایجاد شده است، ولی وسیله همچنان به محافظت از تهدیدات مختلف زمان اجرا و مقاصد مخرب نیاز دارد.

۴-۳-۱- امنیت سطح سیستم

امنیت سطح سیستم برای وسایل هوشمند، کامپیوترها، تبلت‌ها، و سرورها ضروری است. دیواره آتش در وسایل هوشمند باید همیشه در سطح سیستم عامل فعال باشد. پروتکل‌های دستگاه در اشیاء یا وسیله‌ی الکترونیکی در شبکه خانگی[2]، شبکه محلی[3]، یا شبکه جهانی[4] باید به طور خاص تعریف شوند. تمام وسایل خانگی متصل با نام کاربری و کلمه‌ی عبور در هنگام ورود محافظت می‌شوند. اگر این امر مورد نیاز باشد، آنگاه یک روش این است که از روش‌های امنیتی ورود دو سطحی با کلمه‌ی عبور مانند سیستم‌های امنیتی بانکی استفاده شود. این امر تضمین می‌کند که شخص ثالث یا وسایل جعلی نتوانند از اطلاعات خانگی شخصی دزدی کنند. واضح است که باید در مورد به اشتراک‌گذاری کلمات عبور امنیتی خانه هوشمند توسط کودکان با دوستان خود احتیاط لازم در نظر گرفته شود. این احتیاط همچنین در مورد کلمات عبور لپ‌تاپ و کامپیوتر، کلید هوشمند درب، اتصال هوشمند گاز، توزیع هوشمند کنتور، و هر گونه یخچال هوشمند قفل شونده نیز باید اعمال شود. به همراه این موارد، همیشه باید نرم‌افزار را به آخرین نسخه‌ی آن به روزرسانی کرد. بسته‌های نرم‌افزاری به سطح عملیات بهتر امنیتی وسیله‌ی هوشمند کمک خواهند کرد و به ارتباطات امن و بهتر منجر خواهند شد.

۴-۳-۲- آنتی ویروس‌ها

هر وسیله‌ی هوشمند می‌تواند تحت تاثیر نرم‌افزارهای مخرب قرار بگیرد. نرم‌افزار مخرب یک اصطلاح جامع و فراگیر برای برنامه‌های مخرب مانند ویروس‌ها، اسب‌های تروجان، کرم‌ها، و نرم‌افزارهای جاسوسی است، که برای آلوده کردن و تحت کنترل در آوردن وسیله‌ی هوشمند طراحی شده‌اند. وسیله‌ی هوشمند شخصی که آلوده شده است، آنگاه مجرمین می‌توانند تمام ضربه‌ها به صفحه کلید وی را ضبط و ثبت نمایند، اطلاعات حیاتی وی را به سرقت برده، و از وسایل استفاده کنند. از این رو، نرم‌افزار آنتی ویروس موردنیاز است. آنتی ویروس شامل برنامه‌های کامپیوتری است که برای شناسایی، پیشگیری، و از بین بردن ویروس‌های کامپیوتری و دیگر نرم‌افزارهای مخرب تلاش می‌کنند. آنتی ویروس معمولاً از دو روش متفاوت برای به انجام رساندن مأموریتش استفاده می‌کند؛ روش اول: بررسی فایل‌ها برای جستجوی ویروس‌های شناخته شده‌ای که با تعاریف موجود در یک فرهنگ لغات[5] ویروس‌ها مطابقت دارد و روش دوم: شناسایی رفتار مشکوک از هر برنامه‌ی کامپیوتری که ممکن است آلوده شده باشد. چنین تحلیلی ممکن است شامل ضبط داده‌ها، نظارت بر پورت، و دیگر روش‌ها باشد.

1- Denial-Oof-Service (DoS)
2- Home Area Network (HAN)
3- Local Area Network (LAN)
4- World Area Network (WAN)
5- Virus Dictionary

این برنامه‌ها دو حالت اساسی دارند؛ حالت اول: اسکن ایستای[1] فایل، که این حالت زمانی مفید است که شما مجبورید فایل‌ها را بررسی کنید تا ببینید که در حال حاضر با نرم‌افزار مخربی آلوده شده‌اند یا خیر؛ و حالت دوم: اسکن پویای بی‌درنگ[2]، که این مورد واقعاً چیزی است که برای پیشگیری کامپیوتر از آلوده شدن در همان ابتدا مورد نیاز است. برای امنیت بهتر، باید از نرم‌افزاری دارای مجوز کامل به همراه آخرین بسته‌های به روزرسانی شده استفاده شود.

۴-۳-۳- دیواره آتش

دیواره آتش، مجموعه‌ای یکپارچه از اقدامات امنیتی می‌باشد که برای پیشگیری از دسترسی الکترونیکی غیرمجاز به یک سیستم کامپیوتری شبکه شده و همچنین وسایل اینترنت اشیاء طراحی شده است. همین اصل برای تمام وسایل هوشمند نیز کار خواهد کرد. یک دیواره آتش شبکه مشابه دیواره‌های آتش موجود در ساختمان‌ها است، زیرا در هر دو مورد سعی شده است که یک شبکه یا بخشی از دیگر قسمت‌ها جدا شود. استفاده‌ی موفقیت‌آمیز از یک دیواره آتش به انتخاب یک محصول مناسب وابسته است. فیلتر کردن بسته در دیواره‌های آتش بر اساس قوانین متعددی اقدام به قبول یا رد بسته‌ها می‌کنند که به پورت‌های مبدأ و مقصد بسته‌ها و دیگر معیارهای نفوذ بستگی دارد. سطح امنیتی برای وسایل هوشمند در اینترنت اشیاء به تنظیمات و سفارشی‌سازی نرم‌افزار دیواره آتش بستگی دارد.

۴-۳-۴- نظارت بر اشیاء و وقایع

نظارت بر مردم یا اشیاء یا رویدادها با استفاده از وسایل هوشمند یکی از وظایف حیاتی در خانه، ساختمان یا شرکت است. این مورد می‌تواند به وسیله‌ی CCTV[3] (تلویزیون مدار بسته) یا دوربین IP[4] (پروتکل اینترنت) یا امنیت فیزیکی انسانی انجام شود. نظارت بر اشیاء و رویه‌ها به طور پیوسته در تمام اماکن بدون دوربین‌های CCTV/IP بسیار دشوار است. به عنوان مثال، نظارت بر تعدادی از شرکت‌کنندگان و امنیت آن‌ها در یک جلسه عمومی به مدت ۶ ساعت بدون هیچ خطری با استفاده از دوربین‌های IP می‌تواند ممکن باشد. مثال دیگر نظارت بر الگوهای رشد گل رز، یاسمن و یا نیلوفر آبی با استفاده از حسگر Koubachi برای حیات این گیاهان است. این حسگر گزارش‌هایی را در مورد نیازهای اساسی اندازه‌گیری‌های نور، رطوبت، هیدروژن، اکسیژن، و دی اکسید کربن به گوشی هوشمند کاربر خود ارسال خواهد کرد.

الف- دوربین CCTV/IP: یک دوربین IP در واقع یک دوربین ویدئویی است که می‌تواند به طور مستقیم بدون نیاز به یک کامپیوتر جدا به اینترنت وصل شود. تجهیزات دوربین در اماکن عمومی و همچنین خانه‌ها مورد استفاده قرار می‌گیرند چرا که ظرفیت جمع‌آوری مقدار زیادی از مواد تصویری را دارند (Yung et al., 2000). در حال حاضر، راه‌های موثری جهت تحلیل داده‌های ویدئویی به طور خودکار و تشخیص موقعیت‌های خطرناک بالقوه به صورت پیشرفته توسط نرم‌افزارهای تحلیلی وجود دارد. در کارخانه‌های صنعتی، در مواقعی که محیط برای انسان‌ها مناسب نیست، تجهیزات CCTV می‌تواند برای مشاهده‌ی بخش‌هایی از روند تولید محصول از یک اتاق کنترل مرکزی مورد استفاده قرار گیرد. سیستم‌های CCTV ممکن است به طور مداوم و یا تنها وقتی که نظارت بر یک رویداد خاص مورد نیاز باشد عمل نمایند. CCTV در واقع بخشی از راه حل است و راه حل کاملی برای ایمنی و امنیت عمومی نمی‌باشد. CCTVها درک عمومی از ایمنی و بازداشتن و دور کردن رفتار ضد اجتماعی و جُرم را بهبود می‌دهند (Ganeriwal S, Srivastava MB, 2004).

برای برنامه‌های کاربردی مبحث امنیت شبکه یک نگرانی مهم است؛ استقرار دوربین‌های IP در محیط‌های ترجمه‌ی آدرس شبکه[5] به همراه مکان‌های پویا معمولاً مطلوب و مورد نظر است. با این حال، بدون اطلاعات آدرس IP ایستا، دسترسی به سرور وب مرتبط با دوربین‌های IP دشوار خواهد بود (Hintermaier W, Steinbach E, 2010). در کاربردهای استخراج از معادن، دوربین‌های IP و وسایل RFID به منظور ارائه‌ی امنیت برای کارگرها و تشخیص رانش زمین یا انفجار غیرمنتظره از نفوذ آب به صورت ۲۴ ساعت در شبانه‌روز در طول کل سال مورد استفاده قرار می‌گیرند.

ب- شبکه حسگر بی‌سیم (WSN): شبکه حسگر بی‌سیم[6] یکی از محبوب‌ترین انواع اتصال وسایل هوشمند مستقر شده در سیستم‌های امنیتی خانه‌ی هوشمند یا دفتر هوشمند است که اغلب، وسایل بی‌سیم متعددی را با خانه‌ی هوشمندمان ادغام می‌کنند تا امکان تشخیص مزاحم را از راه دور فراهم نموده و جریان تصویری را به گوشی تلفن همراه ما از طریق یک بستر امنیتی ترکیب شده ممکن سازند، که همه‌ی این موارد می‌توانند به صورت از راه دور با وسیله‌ی موبایل ما کنترل شوند. امنیت نقش مهمی را در شبکه حسگر بی‌سیم بازی می‌کند چرا که گره‌ها در محیط‌های خشن در معرض خطر حمله‌ها قرار دارند. انگیزه‌ی اصلی در تحقیقات انجام شده برای شبکه‌های حسگر بی‌سیم در واقع کاربردهای نظامی بود. نمونه‌هایی از شبکه‌های حسگر نظامی شامل سیستم‌های نظارت صوتی بر اقیانوس در مقیاس بزرگ برای تشخیص زیردریایی‌ها، نظارت بر شبکه‌های حسگر بی‌سیم مستقر

1- Static File Scanning
2- Real-time Dynamic Scanning
3- Closed-Circuit Television (CCTV)
4- Internet Protocol (IP)
5- Network Address Translation (NAT)
6- Wireless Sensor Network (WSN)

شده به صورت تصادفی و خود–سازمانده در میدان جنگ، و اتصال میکروحسگرها به سلاح‌ها برای نظارت دسته‌جمعی می‌باشد (Dagada R, Eloff MM, 2013). فضای کاربردی برای شبکه‌های حسگر بی‌سیم بسیار بزرگ و به شدت در حال گسترش است. وقتی که گره‌ها در محیط بدون نظارت پراکنده شده‌اند آنگاه طول عمر شبکه می‌تواند با فراهم کردن امنیت و حریم خصوصی در برابر حملات لایه‌ی شبکه ارتقاء یابد. به منظور حفاظت از یک شبکه، با استفاده از تعدادی از پروتکل‌های مسیریابی از قبیل پروتکل‌های حسگر برای حفاظت از اطلاعات از طریق الگوریتم امنیتی مبتنی بر افزونگی مسیر برای شبکه‌های حسگر بی‌سیم همگن و روش‌های امنیتی و احراز هویت در برابر حملات مختلف قابل تشخیص است (Perrig A et al., 2001). برخی از پروتکل‌های مسیریابی امن در شبکه‌های حسگر ناهمگن نیز می‌توانند گره‌های مخرب و تحویل موفقیت‌آمیز بسته‌ها را به چاهک[1] تشخیص دهند. شبکه‌های حسگر بی‌سیم در برابر بسیاری از انواع حملات آسیب‌پذیر هستند (Sami et al., 2007).

از آنجایی که شبکه‌های حسگر بی‌سیم بر اساس استانداردهای ارتباطی و داده‌های ارسال شده بر روی یک کانال همه‌پخشی[2] هستند، احتمال ایجاد حمله‌هایی برای استراق سمع[3] و دستکاری[4] بسته وجود دارد. در سال‌های اخیر، طرح‌های پیشنهادی بسیاری با استفاده از رمزنگاری برای تضمین امنیت ارتباطات وجود داشته است. با این وجود، تنها رمزنگاری برای مقاومت گره در برابر حملات و رفتارهای مخرب جدید در شبکه‌های حسگر کافی نیست (Xiaojiang Du et al., 2006).

۵- حریم خصوصی وسایل هوشمند

حفظ حریم خصوصی از کلمه‌ی لاتین "Privatus" و "Privo" مشتق شده است که به معنی محروم کردن می‌باشد (Curtin L, 1981). در لغت‌نامه‌ی زبان انگلیسی، حریم خصوصی به صورت کنار کشیدن از دید عموم یا شرکت و زندگی خصوصی یک فرد تعریف شده است (Rawnsley M, 1980). حریم خصوصی محافظت شده که به مدت طولانی به عنوان حق قانونی افراد، گروه‌ها، یا موسسات پذیرفته شده است، آنها خودشان تصمیم می‌گیرند که چه زمانی، چگونه، و چه نوع از اطلاعاتی در مورد خودشان را در ارتباط با دیگران به اشتراک بگذارند (Webster's, 1986). با پیشرفت عصر دیجیتال و فناوری اینترنت اشیاء، آسیب‌پذیری‌های اطلاعات شخصی افزایش یافته است. اطلاعات حریم خصوصی ممکن است با استفاده از روش‌های زیادی محافظت شود؛ از جمله رمزنگاری، احراز هویت، و پوشش داده‌ها و هر تلاشی برای اطمینان حاصل کردن از اینکه داده‌ها تنها در دسترس افراد مجاز قرار گیرد. حریم خصوصی اطلاعات یکی از مهمترین جنبه‌های به اشتراک‌گذاری اطلاعات در حین برقراری ارتباط با وسایل هوشمند در نظر گرفته می‌شود. نیاز به حفظ حریم خصوصی اطلاعات در جمع‌آوری اطلاعات شخصی از قبیل سوابق پزشکی، داده‌های مالی، سوابق جنایی، و اطلاعات سیاسی کاملاً محسوس می‌باشد و درک حریم خصوصی شامل ابعاد قابلیت اطمینان[5] و اعتبار[6] است که به اشتراک‌گذاری اطلاعات میان کاربران IT مربوط می‌شود (Westin A, 1967).

در هنگام برقراری ارتباط با وب سایت، کاربران زیادی بر اساس روال‌های خاص از حجم بسیار زیادی از اطلاعات استفاده می‌کنند. بنابراین اعتبار و قابلیت اطمینان، از مسائل مهم در این تراکنش‌ها هستند (Yousafazi SJ et al., 2003).

گره‌های سیار (موبایل) در اینترنت اشیاء از یک خوشه به خوشه‌ی دیگر حرکت می‌کنند، که در این مورد پروتکل‌های مبتنی بر رمزنگاری نیاز به فراهم کردن احراز هویت سریع و محافظت از حریم خصوصی دارند. در یک ارتباط پیشرفته‌ی فناوری اینترنت اشیاء، که در آن هر شئ برای ارتباط به یک شئ یا انسان یا ماشین وصل می‌شود، حفظ اعتبار و قابلیت اطمینان بسیار ضروری است. تمام داده‌های خصوصی تولید شده توسط اشیاء باید به شدت استانداردهای امنیتی را دنبال کنند (Choate T, 2000).

پروتکل تک مرحله‌ای برای پیوستن گره‌ی موبایل به یک خوشه‌ی جدید ارائه شده است. نوجوانان به عنوان کاربران فعال رسانه‌های اجتماعی می باشند که به نظر می‌رسد مراقب حریم خصوصی خود هستند، ولی در واقعیت مقدار قابل توجهی از اطلاعات شخصی خود را فاش می‌کنند (JingjunMiao, Liangmin Wang, 2012).

حریم خصوصی اجتماعی به عنوان کنترل بر تعامل واقعی با دیگران و محتوای تعامل می‌باشد. حریم خصوصی روانی فرد از نفوذ بر افکار، احساسات، و ارزش‌ها و آزادی فرد محافظت می‌کند تا فرد بتواند تصمیم بگیرد که نزد چه کسی افکار و احساسات خود را آشکار نماید. حریم خصوصی اطلاعات در واقع توانایی کنترل این مورد است که چه کسی و در چه شرایطی اطلاعاتی را در مورد خود جمع‌آوری و منتشر می‌کند. از این رو، کار بر روی توسعه‌ی وسایلی با حریم خصوصی ضروری می‌باشد.

۶- بحث و نتیجه‌گیری

وقتی که تمام اشیاء به اینترنت متصل می‌شوند و آماده‌ی دسترسی از طریق گوشی‌های هوشمند و دیگر PDAها از هر مکانی برای هر سرویسی هستند، مسائل امنیتی نباید نادیده گرفته شوند. امنیت وسایل هوشمند، به طور اساسی به صورت ارزیابی

1- Sink
2- Broadcast
3- Sniffing
4- Spoofing
5- Reliability
6- Credibility

خطرهای تهدیدآمیزی است که از دست رفتن داده‌های با ارزش و آسیب‌پذیری‌های بیشتر را از طریق وسیله‌ی هوشمند باعث می‌شوند. برای امنیت بهتر، محافظت‌ها می‌توانند در زمینه‌ی تشخیص، پیشگیری، و اصلاح باشند. توسعه‌های امروز در وسایل و برچسب‌های هوشمند باعث تغییر ناگهانی فناوری شده است که این روند شکل جدیدی از تعاملات اجتماعی را ایجاد می‌کند که انتظار فرد از حریم خصوصی یا محرمانگی را تغییر می‌دهد.

وسایل ممکن است به صورت نا امن رها شوند چرا که صاحبان آنها انتظار دارند که این وسایل در کنترل فیزیکی آنها خواهد ماند؛ با این حال، اگر این وسایل کنترل فیزیکی صاحب خود را از دست بدهند، آنگاه برای استفاده توسط دیگر افراد باز و بی‌حفاظ هستند. از این رو، امنیت فیزیکی از طریق سیستم‌های نظارتی ضروری است. طراحی اخلاقی، و توسعه‌ی سخت‌افزار و نرم‌افزار هوشمند، باید از سوی کدنویسان نرم‌افزار یا توسعه‌دهندگان آن به همراه استقرار مناسب در برنامه‌های کاربردی مناسب انجام شود. مراجع استاندارد سازی بین‌المللی باید بر توسعه‌ی وسایل، نرم‌افزار، و شبکه‌ها نظارت داشته باشند. در نهایت، باید قابلیت همکاری مبتنی بر اعتمادی میان وسایل اینترنت اشیائی باشد که بهم متصل می‌شوند. کاربر یا 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. به منظور پیشگیری از سوءاستفاده از داده‌ها باید تنبیه‌هایی برای مجرمان سایبری در نظر گرفته شود. اتحادیه‌ی بین‌المللی مخابرات[1]، موسسه مهندسان برق و الکترونیک[2]، معماری‌های اینترنت اشیاء[3] و موسسه ملی استانداردها و فناوری[4]، برخی از موسسات استانداردسازی جهانی در امر استاندارد کردن وسایل و ارتباطات بدون هیچگونه نقض امنیتی هستند. امنیت وسایل هوشمند امروزه در حال تبدیل به یک نیاز اساسی در این جهان فنی است. از این رو، امنیت وسایل هوشمندی که تحت مفهوم اینترنت اشیاء هستند نیز یک نیاز اساسی به شمار می‌رود.

منابع

1. Al-Muhtadi J, Ranganathan A, Campbell R, Mickunas MD, (2003). "Cerberus: a context-aware security scheme for smart spaces", Pervasive computing and communications (PerCom 2003), Proceedings of the first IEEE international conference, pp. 489–496.
2. Atzori L, Iera A, Morabito G, (2010). "The internet of things: a survey", Computer Networks, vol 54, pp. 2787–2805, doi: 10.1016/j.comnet.2010.05.010.
3. Carabelea C, Boissier O, (2003). "Multi-agent platforms on smart devices: dream or reality", Proceedings of the Smart Objects Conference (SOC03), Grenoble, France, pp. 126–129.
4. Choate T, (2000). "5 keys to customer conversion", Catalog Age, I Merchant, August, pp. 14–15.
5. Cirani S, Ferrari G, Veltri L, (2013). "Enforcing security mechanisms in the IP-based internet of things: an algorithmic overview", Algorithms, vol 6(2), April, pp. 197–226, ISSN: 1999-4893, doi: 10.3390/a6020197.
6. Curtin L, (1981). "Privacy: Belonging to oneself", Perspect Psychiatry Care, vol 19(3–4), pp. 112–115, doi: 10.1111/j.1744-6163.1981.tb00124.x
7. Dagada R, Eloff MM, (2013). "Integration of policy aspects into information security issues", South African organizations, vol 7(31), pp. 3069–3077, August, doi: 10.5897/AJBM12.979.
8. Ganeriwal S, Srivastava MB, (2004). "Reputation-based framework for high integrity sensor networks", Proceedings of ACM SASN, doi: 10.1145/1362542.1362546.
9. Gariup M, (2013). "European security culture: language, theory, policy", Ashgate Publications, ISBN 9780754675556.
10. Heer T, Garcia-Morchon O, Hummen R, Keoh SL, Kumar SS, Wehrle K, (2011). "Security challenges in the IP-based internet of things", Wirel Pers Commun, vol 61, pp. 527–5421.
11. Hintermaier W, Steinbach E, (2010). "A system architecture for IP camera based driver assistance applications", IEEE Intelligent Vehicles Symposium (IV), San Diego, June, pp. 540–547.
12. JingjunMiao, Liangmin Wang, (2012). "Rapid identification authentication protocol for mobile nodes in internet of things with privacy protection", J Netw, vol 7(7), pp. 1099–1105.

1- International Telecommunication Union (ITU)
2- Institute of Electrical and Electronics Engineers (IEEE)
3- Internet of Things - Architectures (IoT-A)
4- National Institute of Standards and Technology (NIST)

13. Li B, Li W, (2008). “Logistics information fusion application research based on RFID and GPS”, Proceedings of 27th Chinese control conference, China, pp. 389–393.
14. Maiwald E, (2004). “Fundamentals of network security”, McGraw-Hill Technology Education, New York, ISBN: 9780072230932.
15. Noda C, Walter T, (2005). “Smart devices for next generation mobile services”, Construction and analysis of safe, secure, and interoperable smart devices, Springer, Berlin Heidelberg, pp. 192–209.
16. Perrig A, Szewczyk R, Wen V, Culler D. Tygar JD, (2001). “SPINS: security protocols for sensor networks”, Proceedings of ACM annual international conference on mobile computing and networking, pp. 189–199, ISBN:1-58113-422-3, Rome, Italy.
17. Pfitzmann A, Pfitzmann B, Schunter M, Waidner M, (1997). “Trusting mobile user devices and security modules”, Computer, vol 2, pp. 61–68.
18. Rawnsley M, (1980). “The concept of privacy”, Adv Nurs Sci 2(2), pp. 25–31.
19. Robles RJ, Kim TH, Cook D, Das S, (2010). “A review on security in smart home Development”, Int J Adv Sci Technol vol 15, pp. 13–22.
20. Roman R, Najera P, Lopez J, (2011). “Securing the internet of things”, Computer, vol 44(9), pp. 51–58, doi:10.1109/MC.2011.291.
21. Sami, Al-Wakeel S, Al-Swailem A, (2007). “PRSA: a path redundancy based security algorithm for wireless sensor networks”, Proceedings of IEEE wireless communication and networking conference, pp. 4156–4160, ISBN: 1-4244-0658-7, Kowloon, China.
22. Srivastava L, (2006). “Pervasive, ambient, ubiquitous: the magic of radio”, European Commission conference, From RFID to internet of things, Bruxelles, Belgium.
23. Sukhai NB, (2004). “Hacking and cybercrime”, Proceedings of 1st annual conference on information security curriculum development, pp. 128–132.
24. Suo H, Wan J, Zou C, Liu J, (2012). “Security in the internet of things: a review”, Computer Science and Electronics Engineering (ICCSEE), international conference, vol 3, pp. 648–651, IEEE.
25. Webster’s New World Dictionary, (1986). Prentice-Hall, New York.
26. Weis SA, (2003). “Security and privacy in radio-frequency identification devices”, Doctoral dissertation, Massachusetts Institute of Technology.
27. Westin A, (1967). “Privacy and freedom”, Atheneum, New York.
28. Xiaojiang Du, Sghaier Giyani, Yang Xiao, Hsiao-Hwa Chen, (2006). “A secure routing Protocol for heterogeneous sensor networks”, Proceedings of IEEE Global Telecommunication Conference (GLOBECOM’06), pp. 1–5, ISBN: 1-4244-0356-1, San Francisco, California, December.
29. Yong W et al, (2006). “A Survey of security issues in wireless sensor networks”, Commun Surv Tutorials, IEEE, vol 8, pp. 2–23.
30. Yousafazi SJ, Pllister JG, Foxall GR, (2003). “A proposal model of e-trust for electronic banking”, Technovation 23, pp. 847–860.
31. Yung, Nelson HC, Pang Grantham KH, Fung George SK, (2000). “A novel camera calibration technique for visual traffic surveillance.”