عنوان

تهدیدات امنیتی خانه هوشمند در لایه اشیا و راه های مقابله با آن

نگارش

زهرا دهقانیان

استاد راهنما

دکتر رضا صفابخش

پاییز ۹۶

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

عنوان

تهدیدات امنیتی خانه هوشمند در لایه اشیا و راه های مقابله با آن

نگارش

زهرا دهقانیان - ۹۴۳۱۰۳۹

استاد راهنما

دکتر رضا صفابخش

درس

روش تحقیق و گزارش نویسی

پاییز ۹۶

از پدر عزیزم که در تهیه این گزارش با لطف بی حدشان مرا یاری کردند ، کمال تشکر را دارم و از خداوند منان خواهان طول عمری با برکت برای ایشان هستم.

چکیده

اینترنت اشیاء بستری است که در آن شبکه اینترنت موجود از سیستم های رایانه‌ای به اشیاء یا موجودیت‌های دنیای واقعی متصل هستند؛ اشیاء شامل تمام عناصر موجود در یک خانه هوشمند همانند: وسایل برقی خانگی، ابزار، وسایل اسباب بازی و هر وسیله ای که قابلیت متصل شدن به اینترنت را داشته باشد، می‌شود.

در این گزارش سعی شده است تا پس از بررسی مفاهیم پایه این حوزه همانند: اشیاء، زیرساخت‌های موجود و پروتکل‌های استاندارد اتصال به اینترنت برای اشیاء هوشمند، به بررسی دقیق فن‌آوری‌های بکار رفته در خانه-های هوشمند، چالش‌های اصلی این حوزه و تهدیدات امنیتی موجود پرداخته شود و در نهایت برای حفظ حریم خصوصی و رفع دغدغه‌های مطرح شده امنیتی، راهکارهای مناسب ارایه داده شود.

واژه های کلیدی: اینترنت اشیاء، خانه هوشمند، تهدیدات امنیتی، امن‌سازی و حریم‌خصوصی

فهرست

فهرست اشکال

۱ مقدمه

اینترنت اشیا یا IOT[۱] بخشی از اینترنت آینده است که شامل اینترنت موجود و در حال رشد و همچنین توسعه‌های آینده شبکه می‌شود. اینترنت اشیا به طور مفهومی می‌تواند به عنوان یک زیر ساخت شبکه سراسری پویا با قابلیت‌های خود پیکربندی و مبتنی بر استانداردها و پروتکل‌های ارتباطی جمعی و مشارکتی تعریف شود که در آن" اشیا "فیزیکی و مجازی دارای شناسه‌ها، صفات فیزیکی و مشخصه‌های مجازی، از واسطه‌های هوشمند استفاده کرده و به‌طور یکنواخت و مستمر در یک شبکه اطلاعات مجتمع شده‌اند.

همچنین با پیشرفت در محاسبات و ارتباطات بی‌سیم، یک رویکرد جدید در اینترنت اشیاء تحت عنوان خانه هوشمند شناخته شده است و به سرعت تحقیقات جالب و انقلاب صنعتی مهمی را به راه انداخته است. بنابراین اینترنت اشیاء را می توان به عنوان یک شبکه فراگیر و جهانی تعریف نمود که سیستمی را برای نظارت و کنترل جهان فیزیکی از طریق جمع‌آوری، پردازش و تجزیه و تحلیل اطلاعات تولید شده توسط دستگاه‌های حسگر اینترنت اشیا فراهم می‌آورد. این دستگاه در رابطه با سنجش و ارتباطات مانند حسگرها، دستگاه‌های شناسایی فرکانس رادیویی، دستگاه‌های موقعیت‌یاب جهانی، حسگرهای مادون قرمز، لیزر، اسکنرها، دیسک، شبکه‌های محلی بیسیم ساخته شده‌اند. در واقع " همه چیز "را می توان به اینترنت متصل کرد و از این رو مدیریت از راه دور کنترل و مدیریت نمود.

اینترنت اشیا میتواند به عنوان تلفیقی از شبکه‌های ناهمگن در نظر گرفت که نه تنها چالش‌های امنیتی یکسانی را در شبکه‌های حسگر، ارتباطات تلفن‌های همراه و اینترنت به ارمغان می‌آورد بلکه برخی مسائل عجیب و برجسته، مانند، مشکلات مربوط به حفظ حریم خصوصی در شبکه، چالش های احراز هویت و چالش‌های کنترل و مسیریابی امن در این میان دستگاه‌های ناهمگن به همراه دارد [۱] .

بنابراین مساله امینت در IOT را میتوان مهم‌ترین چالش توسعه این فناوری در نظر گرفت. در این رابطه استانداردهای مختلفی در حال توسعه است؛ ولی همچنان نیازمندیهای امنیتی اینترنت اشیا و حتی مخاطرات آن به خوبی شناسایی و تحلیل نشده است.

---

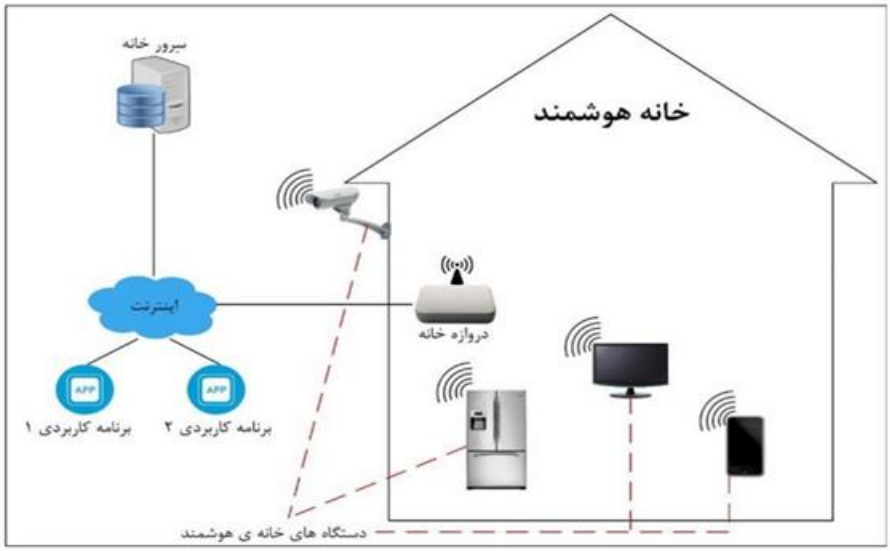
[۱] Internet Of Things

در این تحقیق، در فصل دوم ابتدا فناوری موجود در یک خانه هوشمند را بررسی کرده و در ادامه به بررسی تهدیدات امنیتی موجود در شبکه پرداخته می‌شود. در فصل سوم ضمن اشاره به چالش‌های امنیتی موجود در این بستر، راهکارهای مناسب معرفی می‌گردد. در نهایت در فصل آخر جمع‌بندی و نتیجه پایانی ارایه می‌شود.

۲ خانه هوشمند

اینترنت اشیاء بستری است که در آن شبکه اینترنت موجود از سیستم‌های رایانه‌ای به اشیاء یا موجودیت‌های دنیای واقعی متصل هستند؛ اشیاء ممکن است شامل موجودیت‌ها، وسایل برقی خانگی، دستگاه‌ها، ابزار و... باشد؛ وقتی این اشیاء طبق زیرساخت مشخص و پروتکل‌های استاندارد خاصی به اینترنت متصل می‌شوند، «اینترنت اشیاء» نامیده می‌شود. اشیاء در اینترنت هوشمند می‌توانند حقیقی یا مجازی و ثابت یا متحرک باشند در حالیکه اشیاء، شرکت‌کنندگان فعال در کل سیستم هستند، اشیاء، می‌توانند با یکدیگر و با انسان تعامل داشته باشند که این ارتباطات به ترتیب، ارتباط شی به شی و ارتباط شی با انسان نامیده می‌شوند [۲] .

سیستم خانه هوشمند می‌تواند همانند آنچه در شکل۲-۱ نشان داده شده، پیکربندی شود؛ سیستم خانه هوشمند شامل سه مؤلفه اصلی سرور خانه، دروازه خانه و دستگاه‌های خانه هوشمند است:



شکل ۲-۱ سیستم خانه هوشمند

ابتدا سرورخانه فرآیندهای ذخیره‌سازی، تجمیع و توزیع اطلاعات گردآوری شده از رسانه‌های مختلف موجود در خانه را انجام می‌دهد، سپس دروازه‌خانه، صاحب شبکه دسترسی را به شبکه خانگی متصل می‌کند؛ در نهایت دستگاه‌های خانه هوشمند قادر خواهند بود اطلاعات را میان دستگاه‌ها مبادله کرده و به اینترنت خارجی نیز دسترسی پیدا کند. مؤلفه‌های تشکیل‌دهنده سیستم خانه هوشمند در مواجهه با تهدیدات داخلی یا خارجی قرار دارند زیرا اغلب این مؤلفه‌ها به اینترنت متصل هستند؛ برای غلبه بر چنین تهدیدات امنیتی، مانند تزریقات بدافزاری، دسترسی احراز هویت شده کاربر، افشای اطلاعات اساسی، لازم است تمهیدات امنیتی مطابق بر مشخصه‌های مؤلفه‌ای سیستم خانه هوشمند به کار گرفته شود.

۲-۱ فناوری های موجود

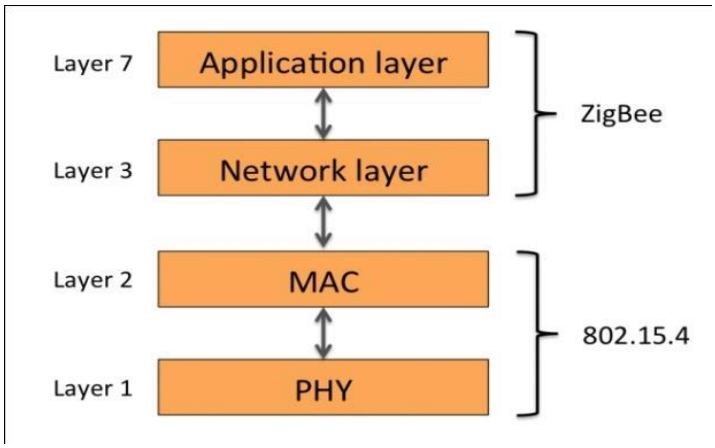
در اینترنت اشیا برای ارتباط و تعامل اشیا با یکدیگر و با شبکه اینترنت فناوری های متفاوتی وجود دارد که در اینجا جدیدترین فناوری های مورد نیازبرای پیاده سازی آن را معرفی می کنیم.

Zigbee ۲-۱-۱

فناوری zigbee جزء فناوری‌های نو ظهوری می‌باشد که در سال های اخیر رشد چشمگیری داشته است. نام zigbee از الگوی غیر ترتیبی زیگزاگی که زنبورها حین گرده افشانی دنبال می کنند، گرفته شده است [۳]. zigbeeیک پروتکل مبتنی بر استاندارد IEEE802.15.4 برای کنترل و نظارت بر اهداف و سیستم‌هایی است که به نرخ بالای ارسال داده نیاز نداشته ولی هزینه پایین و جریان مصرفی کم از ملزومات آنها به شمار می‌آید. در این فناوری نودها می‌توانند تا زمانی که بی استفاده هستند در حالت خواب قرار بگیرند. zigbee به منظور تعریف یک تکنولوژی ساده‌تر، ارزانتر و موثرتر از بلوتوث در مصرف انرژی و طول عمر، برای شبکه‌های شخصی بیسیم بوجود آمده است. به کمک Zigbee می‌توان بیش از ۶۴۰۰۰ وسیله را بطور بیسیم از طریق شبکه به هم متصل نمود.

پشته پروتکل Zigbee شامل چهار لایه است: لایه فیزیکی، لایه کنترل دسترسی رسانه لایه شبکه و لایه کاربرد. از نقطه نظر عملکرد، لایه فیزیکی فراهم کننده ارتباطات رادیویی و لایه کنترل دسترسی میانی، فراهم

آورنده انتقال تک‌گام مطمئن می‌باشد. لایه شبکه توپولوژی‌های پیچیده‌تر و مسیریابی را معین می‌کند و لایه کاربرد مشخص کننده توابع مدیریتی شبکه و دستگاه‌ها و همچنین قالب پیام را مشخص می‌کند.



شکل ۲-۲ پشته پروتکلی zigbee

بسیاری از دستگاه‌هایی که تحت فناوری zigbee عمل می‌نمایند، نیازمند نرخ داده ارتباطی پایینی می‌باشند. نمونه بارز این موضوع، بحث روشنایی می‌باشد که با در نظر گرفتن یک بیت صفر یا یک برای روشن یا خاموش نمودن آن بکار می‌رود. در نتیجه با توجه به کم مصرف بودن این فناوری باتری می‌تواند بالغ بر ۱۰ سال کار کند. کاربردهای زیر از مواردی است که zigbee برای آن توسعه داده شده است:

- هزینه پایین
- توان کم
- نرخ انتقال پایین
- امنیت
- انعطاف پذیری
- قابلیت توسعه آسان و ارزان
- قابلیت اطمینان

۲-۱-۲ برچسب هوشمند

فناوری برچسب هوشمند یا RFID[۲] بیانگر سیستم‌هایی است که از امواج رادیویی برای انتقال اطلاعات مربوط به هویت یک شیء استفاده می‌کنند. این تگ‌ها نوع پیشرفته‌تری از بارکدها هستند چراکه هم قابلیت خواندن و هم قابلیت نوشتن دارند، داده‌هایی که روی تگ‌های RFID ذخیره می‌شوند را می‌توان تغییر داد، به روز رسانی کرد و یا حتی قفل کرد. این فناوری موفق شده است تا قابلیت و کارایی خود را به عنوان یک ابزار مقرون به صرفه در بهبود عملکرد و کاهش زمان و هزینه‌های نیروی انسانی و منابع در بسیاری از موارد ثابت نماید.
افراد با قرار دادن تگ‌های RFID مرتبط در محیط‌های هوشمند، به اتوماتیکی کردن آن محیط کمک می‌کنند. در یک سناریوی کلی وقتی که قسمت های تولیدی به پردازش می‌رسند، به وسیله دستگاه برچسب خوان یک رویداد مانند خواندن شماره RFID و ذخیره آن رخ می دهد، که اطلاعات مهمی را در اختیار ما قرار می دهد .
اجزاء بکار رفته در RFID عبارتند از:

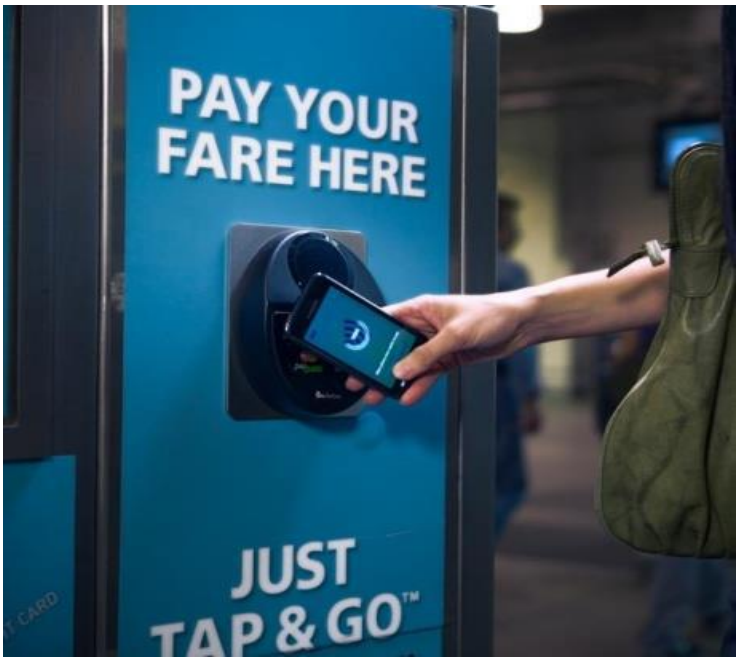
- برچسب
- برچسب خوان
- آنتن
- نرم افزار مدیریت اطلاعات

اگر بخواهیم برچسب‌ها را بر اساس منبع انرژی که استفاده می‌کنند، تقسیم‌بندی کنیم سه نوع اصلی از آنها را خواهیم داشت. برچسب‌های فعال، غیرفعال و نیمه غیر فعال. برچسب‌های فعال انرژی مورد نیاز خود را از باتری همراهشان دریافت می‌کنند درحالیکه برچسب‌های غیرفعال به خودی خود دارای منبع انرژی نبوده و برای به کار افتادن باید از انرژی امواج الکترومغناطیسی منتشرشده از برچسب‌خوان استفاده نمایند و البته محدوده و دامنه خواندن کمتری نسبت به برچسب‌های فعال دارند. نوع دیگری از برچسب نیز برچسب نیمه غیرفعال می-باشدکه علاوه بر استفاده از باتری داخلی‌اش، می تواند از انرژی امواج منتشر شده از برچسب‌خوان نیز استفاده نماید.

[۲] Radio Frequency Identification

۲-۱-۳ ارتباطات میدان نزدیک

ارتباطات میدان نزدیک عبارتست از قابلیت ارتباطی جدید که میتوان برای اتصال امن بین دو دستگاهی که در فاصله کمی از یکدیگر قرار دارند استفاده کرد .علاوه بر مجاورت دو ابزار لازم است تا هر دوی آنها از سخت افزار مخصوصی بهره ببرند. در حقیقت NFC[۳] نسخه جدیدتری از RFID است که برد ارتباطی آن به چهار اینچ محدود شده است. این موضوع NFC را برای کاربردهای حساس مانند موارد استفاده از کارت اعتباری(مثل پرداخت‌های الکترونیک با استفاده از گوگل والت)و یا ورود به محل های امنیتی بسیار کارامد می‌کند. دستگاه-هایی که از فن‌اوری NFC پشتیبانی می کنند به آسانی این امکان را به کاربر می‌دهند که اطلاعات مورد نظر را با یک لمس یا نزدیک کردن دستگاه خود به دستگاه دیگر ارسال یا مبادله کنند.



شکل ۲-۳ NFC

[۳] Near Field Communication

۲-۱-۴ شبکه‌های موبایلی

نسل پنجم شبکه‌های مخابراتی موبایل با شتاب بالایی در حال انجام است. علی‌رغم اینکه هنوز برخی از کشورها شبکه‌ی ارتباطی خود را به نسل چهارم ارتقا نداده‌اند، اما نسل پنجم در حال توسعه است و دانشمندان با هیجان بالایی در مورد آن صحبت می‌کنند. استفاده از پهنای باند بالا، نرخ انتقال دادهی زیاد و تسهیل در ارتباطات مبتنی بر اینترنت همچون مکالمات ویدئویی، تنها گوشه‌ای از قابلیت‌هایی است که با پیاده‌سازی شبکه‌های نسل پنجم در اختیار کاربران قرار خواهد گرفت. یکی از مواردی که نیاز به پهنای باند بالا را افزایش می‌دهد، مفهوم اینترنت اشیا است.

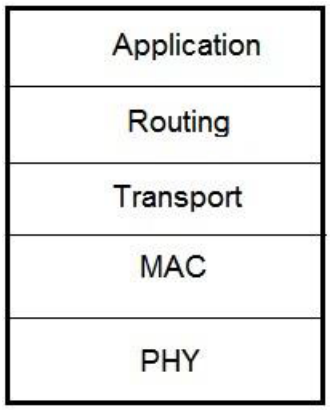
۲-۱-۵ بلوتوث

بلوتوث یک فناوری بی سیم برای ارتباط کوتاه برد است که مبتنی بر استاندارد IEEE 802.15.1 می‌باشد. بلوتوث کم انرژی (BLE[۴]) تبدیل به یک بلوک ساختمانی کلیدی برای اینترنت اشیاء شده است. سازندگان تراشه در تلاشند تا با استفاده از فن‌آوری، منجر به کاهش مصرف برق دستگاه شوند و به توسعه دهندگان برای اجراسازی آن کمک کنند. نسخه ۴,۲ این فناوری در سال ۲۰۱۴ معرفی شد و درآن برخی ویژگی‌های اساسی برای اینترنت اشیاء اضافه شده است. سرعت و امنیت بلوتوث ۴,۲ نسبت به نسخه‌های قبلی بهینه شده و در عین حال توان مصرفی کمتر است. این ویژگی‌ها بلوتوث کم انرژی را به رقیبی جدی در برابر فناوری zigbee تبدیل کرده است. یکی از ویژگی‌های اساسی استاندارد بلوتوث این است که نسخه جدید، با نسخه های قبلی سازگاری دارند. بلوتوث بر خلاف فرستنده مادون قرمز و گیرنده آن که می‌بایست در مقابل هم قرار بگیرند تا ارسال اطلاعات صورت گیرد، می‌تواند در صورت وجود داشتن مانعی در بین راه، انتقال اطلاعات را به درستی انجام دهد [۴].

[۴] Bluetooth Low Energy

Z-Wave ۶-۱-۲

Z-Wave یک پروتکل ارتباطی بی سیم است که توسط زنسیس طراحی شده است و توسط ائتلاف Z-Wave برای اتوماسیون در محیط‌های مسکونی و تجاری کم تراکم ترویج شده است. هدف اصلی Z-Wave ارایه یک انتقال مطمئن از پیام های کوتاه از یک واحد کنترل به یک یا چند گره دیگر در شبکه است. Z-Wave دارای معماری پنج لایه‌ای است که عبارتند از: لایه فیزیکی، لایه مک ، لایه انتقال، لایه مسیریابی و لایه کاربرد. لایه مک مربوط به این فناوری، مکانیسمی را تعریف می ند که امکان ارسال فریم را در زمان در دسترس بودن کانال فراهم می‌کند. در صورتی که کانال در دسترس نباشد، انتقال به زمانی دیگر موکول می‌شود و این زمان به صورت تصادفی است. لایه انتقال ارتباط بین دو گره متوالی را مدیریت می‌کند و این لایه یک مکانیسم انتخابی برای انتقال مجدد را براساس تصدیق فراهم می‌کند. Z-Wave دو نوع از تجهیزات را تعریف می‌کند: کنترل کننده‌ها و پیروها. کنترل‌کننده‌ها دستورات را صادر و به پیروها ارسال می‌کنند و تجهیزات پیرو دستورات را اجرا می‌کنند [۵].



شکل ۲-۴ پشته پروتکلی Z-Wave

۲-۲ تهدیدات خانه هوشمند

خانه‌های هوشمند از مؤلفه‌های متعددی تشکیل شده‌اند؛ این مؤلفه‌ها همواره در معرض تهدیدات مختلفی قرار دارند. حملات خانه‌های هوشمند به هفت گروه تقسیم شده اند [۶]که عبارتند از:

۱- **حملات فیزیکی:** به دستکاری فیزیکی دستگاه‌ها اطلاق می‌شود؛ این حملات می‌تواند به انواع مختلفی از خطرات مانند فعالیت، سوءاستفاده نابهنجار یا استراق سمع، ممانعت یا سرقت منجر شود؛ معمولا یک حمله فیزیکی تمامی اموال را تحت تأثیر قرار می‌دهد.

۲- **خسارات ناخواسته (تصادفی):** ممکن است از اطمینان نادرست و نابجا به افراد و آشنایان یا اشتباهات شخصی (مدیریتی، طراحی، عملکرد وغیره) ناشی شود؛ می‌تواند مراتب جبران‌ناپذیری همچون نشر اطلاعات، تغییرات غیرمعتبر یا حتی فقدان اطلاعات را با خود به همراه داشته باشد.

۳- **فجایع و قطع برق:** انکار خدمات برای کاربر را با خود به همراه دارد.

۴- **آسیب و فقدان:** نه تنها منجر به تخریب سرویس می‌شود، بلکه نشر اطلاعات را با خود به همراه دارد؛ در واقع باعث حذف اطلاعات حیاتی می‌شود.

۵- **خرابی‌ها و بد عملکردها:** مهمترین نقطه شروع حمله توسط مهاجم است؛ مهاجم با بهره‌جویی از این فرصت، مبادرت به فعالیت، سوءاستفاده نابهنجار و استراق سمع، ممانعت و سرقت می‌کند.

۶- **استراق‌سمع، ممانعت و سرقت:** سوءاستفاده ناهنجار به تهدیدات سایبری و نیز حریم‌شخصی مربوط می‌شود؛ این دو مقوله به عنوان تهدیدات امنیتی در نظر گرفته می‌شود؛ مهاجم با تغییر طراحی یا به کارگیری نواقص، یک یا چند دارایی و موجودیت را به خطر خواهد انداخت که در نتیجه منجر به نقض محرمانگی داده‌های خصوصی یا ازدست‌دادن کنترل یک دستگاه خواهد شد.

۷- **قانونی:** این نوع تهدید مراتبی همچون تهدیدات گذشته خواهد داشت اما نسبت به سایر تهدیدات از وقوع کمتری برخوردار است.

۳ چالش‌ها و راهکارها

زمانی که تمامی اشیاء اطراف انسان قابلیت کاربرد اینترنت را پیدا نموده و در نهایت مفهوم اینترنت اشیاء محقق گردد، انواع جدیدی ازکاربردها موجود خواهند بود. دو مبحث امنیت و حریم‌خصوصی به‌عنوان دو مولفه اساسی و مهم در حوزه اینترنت اشیاء نقش پررنگی در این کاربردها خواهند داشت [۷] که در ادامه به این دو مهم می-پردازیم.

۳-۱ چالش امنیت اطلاعات

امنیت اصلی‌ترین نگرانی شبکه‌هایی است که در مقیاس بزرگ پیاده‌سازی می‌شوند. دنیای دیجیتال، با داده-های شخصی و اشتراکی و ثبت‌شده توسط افراد اشباع شده است و نگرانی‌هایی را در زمینه امنیت و حفاظت از اطلاعات افراد و دولت‌ها فراهم کرده است. همچنین مشکلات ناشی شده از انتقال و پردازش داده‌های ناخواسته، موجب نگرانی‌های کاربران و مسائل قانونی شده است. در صورت نقض امنیت، رخداد حمله و اختلال در عملکرد، مزایای هوشمندسازی کمرنگ می‌شود . چنانچه هکرها کنترل شبکه را به عهده بگیرند رویدادهای ناگواری به وقوع خواهد پیوست. برای مثال با در دست گرفتن کنترل درب خانه توسط نفوذگران به شبکه می‌تواند زمینه سرقت از خانه را فراهم کند. به‌طور کلی، سرویس‌های امنیتی که در این حوزه قرار است ارائه شوند باید ویژگی-های محرمانگی، تمامیت و دسترسی‌پذیری را فراهم نمایند. در ادامه به بررسی این عناصر می‌پردازیم.

۳-۱-۱ محرمانگی

اولین قدم برای برقراری امنیت، برآورد محرمانگی است. محرمانگی بدین معنی است که مهاجم نباید هیچ دانشی از محتوای پیام های تبادلی مابین موجودیت های حاضر در اینترنت اشیاء همانند یک گرهی حسگر و هر موجودیت اینترنتی دیگری به دست آورد.

۳-۱-۲ تمامیت

در حالت کلی در مبحث امنیت ، موجودیتی "تمام" است که سه ویژگی زیر را داشته باشد:

یکپارچگی: در تمامی مراحل ارتباط، داده رد و بدل شده باید بدون تغییر باقی بماند .به عبارت دیگر، هرگونه تغییر (احتمالی) در پیام‌ها باید توسط گیرنده پیام قابل تشخیص باشد.

تازگی: این ویژگی تضمین می‌کند که پیام‌های قدیمی‌تر تکرار نمی‌شوند. این امر به جهت تضمین کانال ارتباطی در مقابل حملات تکرار مهم است.

صحت: این ویژگی نیز تضمین کننده‌ی درستی اطلاعات در تمامی مراحل ارتباط می‌باشد.

۳-۱-۳ دسترسی پذیری

اطلاعات باید زمانی که مورد نیاز توسط افراد مجاز هستند در دسترس باشند. این بدان معنی است که باید از درست کارکردن و جلوگیری از اختلال در سیستم‌های ذخیره و پردازش اطلاعات و کانال‌های ارتباطی مورد استفاده برای دسترسی به اطلاعات اطمینان حاصل کرد. سیستم‌های با دسترسی بالا در همه حال حتی به علت قطع برق، خرابی سخت‌افزار، و ارتقاء سیستم در دسترس باقی می‌ماند. یکی از راه‌های از دسترس خارج کردن اطلاعات و سیستم اطلاعاتی درخواست‌های زیاد از طریق خدمات از سیستم اطلاعاتی است که در این حالت چون سیستم توانایی و ظرفیت چنین حجم انبوه خدمات‌دهی را ندارد از سرویس دادن بطور کامل یا جزیی عاجز می‌ماند.

۳-۲ چالش حریم خصوصی

مفهوم حریم‌خصوصی همواره همراه با امنیت به کار برده شده است، اما در این تحقیق مناسب است که توجه جداگانه‌ای به آن شود؛ چرا که در اینترنت اشیاء اطلاعات خصوصی بیشتری نسبت به وضعیت کنونی بر روی شبکه قرار می‌گیرد. حریم خصوصی شامل قابلیت پنهان نگهداشتن اطلاعات شخصی و همچنین توانایی کنترل آنچه با این اطلاعات اتفاق می‌افتد است. طبیعت اشیاء متصل و کاربردهای گسترده، متنوع و همه جا حاضر اینترنت اشیاء و از همه مهم‌تر، تأثیر این اشیاء در بالابردن کیفیت زندگی باعث نفوذ روزافزون آنها در زندگی روزمره‌ی انسان‌ها می‌گردد؛ از طرفی دیگر، چنین سیستم‌هایی که فعالیت‌های روزانه‌ی افراد را جمع‌آوری و ثبت می‌نمایند می‌توانند به آسانی به عنوان سیستم‌های جاسوسی و استراق‌سمع توزیع شده مورد استفاده قرار گیرند. به دلیل آنکه اطلاعات مربوط به فعالیت‌های روزانه‌ی کاربران (برای نمونه مسیرهای مسافرتی، عادت‌های خریدکردن و غیره) توسط بسیاری از انسان‌ها در زمره اطلاعات شخصی و محرمانه در نظر گرفته می‌شوند که نباید فاش شوند، حفظ حریم خصوصی یکی از ملزومات کاربردهای همه‌جاحاضر محسوب می‌گردد . هرچند بسیاری از مردم در ارتباط با موج جدید فن‌آوری که در حال آمدن است یک جنبه احتیاطی در پیش گرفته‌اند؛ اما واقعیت این است که این دستگاه‌ها به گونه‌ای طراحی شده‌اند تا اطلاعات شخصی زندگی انسان را با بیشترین جزییات ممکن، جمع‌آوری کنند. برای مثال یکی از این اطلاعات خصوصی، سبک زندگی افراد است؛ این که چه ساعاتی را در خانه به سر می‌بریم، به کجا مسافرت می‌کنیم، با چه کسانی معاشرت می‌کنیم، چه فیلم‌هایی تماشا می‌کنیم و حتی این که چه غذایی می‌خوریم. کمی خطرناک به نظر می‌رسد، که ما به سرعت اقدام به طراحی و بازیابی راه‌حل‌هایی با هدف بهبود زندگی روزمره شهروندان داشته باشیم؛ به طوریکه برخی از جنبه-های حریم‌خصوصی یا امنیت اطلاعات را در این زمینه نادیده بگیریم. ضمن اینکه فن‌آوری‌های کلیدی اینترنت اشیا هنوز به بلوغ خود نرسیده‌اند و همچنین تحقیقات و کاربردهای اینترنت اشیا در مراحل اولیه خود هستند. پس برای حضور و فراگیر شدن اینترنت اشیا در زندگی روزمره، امنیت و حریم‌خصوصی باید به طور جدی‌تری در نظر گرفته شود.

۳-۳ راهکارها

برای ارایه پاسخ مناسب به دغده‌های اصلی در خانه هوشمند، راه‌حل‌های زیر ارایه می‌شود [۸].

۳-۳-۱ احراز هویت

دستگاه‌ها باید در برابر سیستم‌های دیگر تصدیق شوند و برای این منظور به یک شناسه منحصر بفرد و کلمه عبور نیاز دارند. دستگاه‌های هم چون تلویزیون هوشمند یا دوربین مدار بسته و یا دستگاه‌های ویدئویی و تجهیزات آنتن ماهواره می‌توانند در این زمینه مورد استفاده قرار گیرند. در هنگام به روز رسانی یک دستگاه باید حتما احراز هویت صورت پذیرد و سرورهای داخلی و دستگاه های مجاز بازیابی شوند. برای جلوگیری کنترل غیرمجاز با استفاده از پروتکل‌های امنیتی (مانند پروتکل‌هایTLS, SSL) کاربران تصدیق هویت می‌شوند و با این روش امکان کنترل غیرمجاز از بین می‌رود.

۳-۳-۲ رمزنگاری

دستگاه اینترنت اشیا مجریان اعتماد مبتی بر سخت‌افزار[۵] می‌باشند ولی همزمان از اعتماد بوسیله فرآیندهای خاصی استفاده می‌کنند تا بدین شکل بتوانند مطالب خود را به صورت خصوصی نگهدارند و در برابر حملات نرم افزارهای غیرقابل اطمینان از آنان محافظت نمایند. برای حفظ محرمانگی اطلاعات شخصی و رعایت حریم-خصوصی، تمامی اطلاعات به‌صورت رمزشده ذخیره و یا تبادل می‌شود. با این روش اطلاعات حساس و مهم شخصی در مقابل دسترسی غیرمجاز محافظت می‌شوند. به‌عنوان مثال اطلاعات موجود بر روی تراشه های داده-های متصل به اینترنت اشیا می‌تواند مورد سرقت قرار گیرد برای همین با استفاده از رمز گذاری و رمز گشایی از اطلاعات محافظت می‌شود. دستگاه‌های اینترنت اشیا بوسیله رمزگذاری و استفاده از پروتکل های مانند TSL به انجام تراکنش های حساس مانند تراکنش های مالی می پردازند. TLS می‌تواند مانع حمله مرد میانی شود و برای موارد محرمانه بسیار پرکاربرد خواهد بود.

[۵] Hardware-based

۳-۳-۳ دیواره آتش[۶]

یکی از چالش اصلی حملات منع‌سرویس (DOS[۷]) می‌باشد، که مهاجم با مراجعات مداوم عملا سیستم را مختل می‌کند. با این روش از دستیابی غیرمجاز به یک سیستم رایانه جلوگیری می‌کنند. در برخی از این نرم‌افزارها، برنامه‌ها بدون اخذ مجوز قادر نخواهند بود از یک رایانه برای سایر رایانه‌ها، داده ارسال کنند.

[6] Firewall

[7] Denial Of Service

۴ نتیجه‌گیری

در این تحقیق ابتدا مزایای خانه هوشمند را بررسی کردیم. در گام بعد با فناوری‌هایی که در خانه‌های هوشمند مورد استفاده قرار می‌گیرد، آشنا شدیم و در ادامه به مخاطرات استفاده از خانه‌های هوشمند و چالش-های اصلی این حوزه اشاره کردیم. در پایان تحقیق برای مقابله با تهدیدات و مخاطرات امنیتی، راه‌حل‌های موجود را برشمردیم و در نهایت با توجه به ارزش‌گذاری به دو اصل امنیت و حریم‌خصوصی، راهکارهای احراز هویت، رمزنگاری و دیواره آتش را از میان دیگر راهکارهای موجود برگزیدیم.

البته باید توجه داشت که امنیت در خانه هوشمند یک موضوع نسبی است و بسته به اهمیت و حساس بودن اطلاعات، می‌توان توابع ارزش‌دهی متفاوت و درنهایت راهکارهای دیگری را انتخاب کرد.

۵ منابع

[۱] *IoT Security*: Ongoing Challenges and Research Opportunities. Zhang, Zhi Kai and Yi Cho, Michael Cheng. s.l. : IEEE, 2014.

[۲] *Internet of Things (IoT): A vision, architectural elements, and future directions.* Gubbi, Jayavardhana, et al., et al. s.l. : elsevier, 2013, Future Generation Computer Systems.

[۳] *Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards.* Baronti, Paolo, Pillai, Prashant and Chook, Vince W.C. 7, s.l. : elsevier, Computer Communications, Vol. 30.

[۴] *Bluetooth SIG, Inc.* [Online] https://www.bluetooth.com/.

[۵] *z-wavealliance.* [Online] http://z-wavealliance.org.

[۶] *Security in the Internet of Things: A Review.* Suo, H, Wan, J and Zou, C. s.l. : IEEE, 2012.

[۷] *Survey on secure communication protocols for the Internet of Things.* K.-T. Nguyen, M. Laurent, N. Oualha,. s.l. : Ad-hoc Networks, 2015, pp. 1-15.

[۸] Song, Yuanjun. Security in Internet of Things. Stockholm, Sweden : KTH Information and Communication Technology, 2013.