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

زهرا دهقانیان* دکتر رضا صفابخش
دانشجوی نرم افزار دانشگاه امیرکبیر استاد دانشگاه امیرکبیر

چکیده

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، وسایل اسباب‌بازی و هر وسیله‌ای که قابلیت متصل شدن به اینترنت را داشته باشد. این اشیاء طبق زیرساخت مشخص و پروتکل‌های استاندارد خاصی به اینترنت متصل شده و اینترنت اشیاء شکل می‌گیرد. اشیاء در اینترنت هوشمند می‌توانند حقیقی یا مجازی و ثابت یا متحرک باشند. 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. از حوزه‌های اینترنت اشیاء می‌توان به حوزه نقل و انتقال هوشمند، درمان هوشمند، کشاورزی هوشمند، خانه هوشمند، وسایل نقلیه هوشمند، مدرسه هوشمند، بازار هوشمند، و صنعت هوشمند نام برد. در این تحقیق ما به تهدیدات امنیتی حانه هوشمند پرداخته و برای امن‌سازی این تهدیدات راهکارهای مناسب ارایه می‌دهیم.

واژه‌های کلیدی: اینترنت اشیاء، خانه هوشمند، تهدیدات امنیتی، امن‌سازی

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 می شود. اینترنت اشیا به طور مفهومی می تواند به عنوان یک زیر ساخت شبکه سراسری پویا با قابلیت های خود پیکربندی و مبتنی بر استانداردها و پروتکل های ارتباطی جمعی و مشارکتی تعریف شود که در آن "اشیا" فیزیکی و مجازی دارای شناسه‌ها، صفات فیزیکی و مشخصه های مجازی، از واسطه های هوشمند استفاده کرده و به طور یکنواخت و مستمر در یک شبکه اطلاعات مجتمع شده اند. مساله امینت در IOT را می توان مهم‌ترین چالش توسعه این فناوری در نظر گرفت. در این رابطه استانداردهای مختلفی در حال توسعه است؛ ولی همچنان نیازمندی های امنیتی اینترنت اشیا و حتی مخاطرات آن به خوبی شناسایی و تحلیل نشده است. 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، وسایل اسباب‌بازی و هر وسیله‌ای که قابلیت متصل شدن به اینترنت را داشته باشد. این اشیاء طبق زیرساخت مشخص و پروتکل‌های استاندارد خاصی به اینترنت متصل شده و اینترنت اشیاء شکل می‌گیرد. اشیاء در اینترنت هوشمند می‌توانند حقیقی یا مجازی و ثابت یا متحرک باشند. 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. از حوزه‌های اینترنت اشیاء می‌توان به حوزه نقل و انتقال هوشمند، درمان هوشمند، کشاورزی هوشمند، خانه هوشمند، وسایل نقلیه هوشمند، مدرسه هوشمند، بازار هوشمند، و صنعت هوشمند نام برد. سیستم خانه هوشمند می‌تواند همانند آنچه در تصویر زیر نشان داده شده، پیکربندی شود؛ سیستم خانه هوشمند شامل سه مؤلفه اصلی سرور خانه، دروازه خانه و دستگاه‌های خانه هوشمند است

*ارایه دهنده

[۱] Internet Of Things

۲ مرور سوابق و پیشینه

اینترنت اشیا توسط فن‌آوری ناهمگن ایجاد می‌شود که موفق به تأمین خدمات نوآورانه در حوزه های مختلف نرم‌افزار است. در این سناریو، رضایت از امنیت و حریم خصوصی نقش اساسی مورد نیاز بازی می‌کند. محرمانه بودن اطلاعات و احرازهویت، کنترل دسترسی در شبکه اینترنت اشیا، حفظ حریم خصوصی و اعتماد در میان کاربران از اهمیت زیادی برخوردار است، بنابر این در حوزه فعالیت‌های تحقیقاتی زیادی انجام گرفته و مقالات فراوانی نوشته شده است، که به برخی از آنها اشاره می‌شود. آقای رسلین و همکاران[۱] در مقاله خود تهدیدات امنیتی خانه هوشمند را بررسی کرده است. بنگالی و همکاران[۲] با استفاده فناوریGSM امنیت خانه هوشمند را بررسی و راهکارهای امنیتی مرتبط را ارایه کرده است. توسعه دستگاه‌ها و سرویس‌های خانه هوشمند توسط فروشندگان دستگاه و تأمین‌کنندگان خدمات: در طول این فاز، فروشندگان و تأمین‌کنندگان خدمات، نیازمندیهای محصول، طراحی، توسعه و تست محصول را تعریف می‌کنند. بهره‌مندی از دستگاه‌ها و سرویسها تا پایان حیات آنها: کاربر نهایی فارغ از تعاملات مستقیم و محلی با دستگاه خود، از فروشنده درخواست حمایت کرده و از سرویسهای برخط مرتبط با دستگاه از طریق کانالهای ارتباطی مختلف استفاده می‌کند بنابراین شاید این فاز بر تعاملات با فروشنده دستگاه، تأمین‌کننده سرویس یا تأمین‌کننده خدمات الکترونیکی برای استفاده و انهدام دلالت دارد.

۳ طرح پیشنهادی

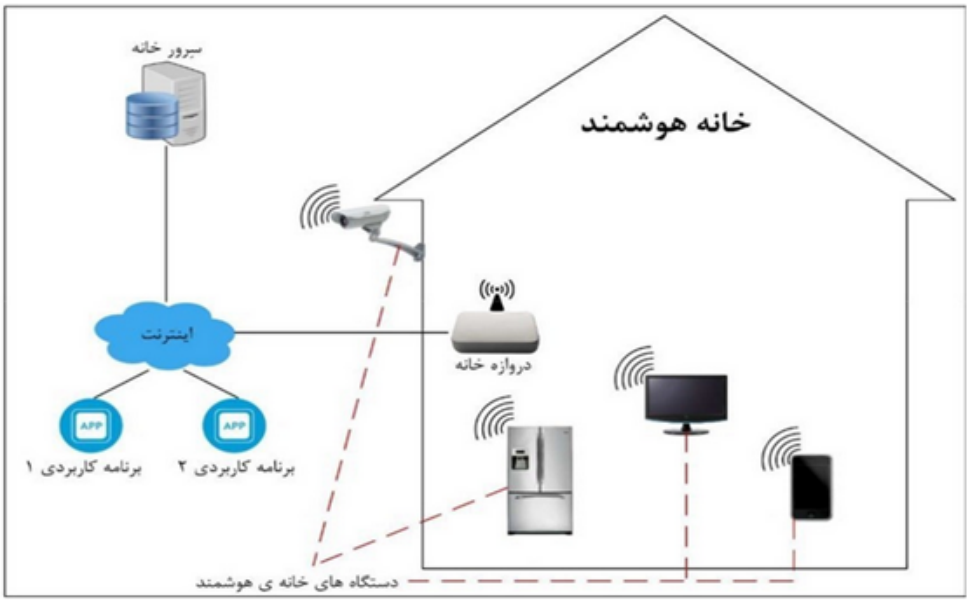
سیستم خانه هوشمند مطابق شکل۱ می‌تواند پیکربندی شود، سیستم خانه هوشمند شامل سه مؤلفه اصلی سرور خانه، دروازه خانه و دستگاه‌های خانه هوشمند است. ابتدا سرورخانه فرآیندهای ذخیره‌سازی، تجمیع و توزیع اطلاعات گردآوری شده از رسانه‌های مختلف موجود در خانه را انجام می‌دهد، سپس دروازه‌خانه، صاحب شبکه دسترسی را به 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. استفاده از مکانیزمهای امنیتی اختصاصی بسته به راه‌حل استفاده شده تغییر می‌یابد؛ چندین روش از لایه انتقال به لایه کاربرد به کار گرفته می‌شوند.

- پروتکلهای احراز هویت ـ اعتبارسنجی کاربر، مانند $Oauth/OpenIDXACML/SAML$، ثبت‌نام و غیره
- پروتکل حفاظت از ارتباط مانند SSL/TLS در سرتاسر TCP/IP، یا $DTLS$ در طول UDP
- استفاده از الگوریتمهای رمزنگاری برای امن کردن لایه انتقال، که در میان شمار تعدادی از پروتکلهای ارتباطی یافت می‌شود.

۱.۳ 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 شده‌اند 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.



شکل ۱: سیستم خانه هوشمند

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 جبران ناپذیری 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. **استراق سمع، ممانعت و سرقت:** سوءاستفاده ناهنجار به تهدیدات سایبری و نیز حریم شخصی 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 از دست دادن 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.

۴ محصولات طرح

- شناخت دقیق نواقص پیشرو و علل ایجاد آن‌ها
- بررسی راه حل های مختلف امنیتی
- معرفی راه حل های جامع و کامل

اغلب تهدیدات امنیتی ناشی از پارامترهای زیر می‌باشد، که در این طرح بایستی به آن‌ها پاسخ داده شود.

۱.۴ احراز هویت

دستگاه ها باید در برابر سیستمهای دیگر تصدیق شوند و برای این منظور به یک شناسه منحصر بفرد و کلمه عبور نیاز دارند . هم چنین برای پیاده سازی رمز نگاری (SSH) به کلیدهای احراز هویت برای تایید هویت دستگاه های متصل را دارد . دستگاه های هم چون تلویزیون مدار بسته $(CCCTV)$ و یا دستگاه های DVRویدئویی و تجهیزات آنتن ماهواره می توانند 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 .

۱.۱.۴ حریم خصوصی

دستگاه اینترنت اشیا مجریان اعتماد مبتی بر سخت افزار $(Hardware-based)$ می باشند ولی همزمان از اعتماد بوسیله فرآیندهای خاصی استفاده می کنند تا بدین شکل بتوانند مطالب خود را به صورت خصوصی نگهدارند و در برابر حملات نرم افزارهای غیرقابل اطمینان از آنان محافظت نمایند . اطلاعات موجود بر روی تراشه های داده های متصل به اینترنت اشیا می تواند مورد سرقت قرار گیرد برای همین با استفاده از رمز گذاری و رمز گشایی از اطلاعات محافظت می شود . دسستگاه های اینترنت اشیا بوسیله رمزگذاری و استفاده از پروتکل های مانند TLS به انجام تراکنش های حساس مانند تراکنش های مالی می پردازند . TLS می تواند مانع حمله مرد میانی شود و برای موارد محرمانه بسیار پرکاربرد خواهد بود . استفاده از $Firewall$ برای کنترل دسترسی نیز ایده مناسبی می‌باشد

۲.۱.۴ $Botnets$

اینترنت اشیا می تواند در معرض بات نت ها و $thingbot$ها قرار گیرد (بات نت ها شبکه هایی هستند که با در اختیار گرفتن مجموعه ای از کامپیوترهایی که bot نامیده می شوند ، تشکیل می شوند این شبکه ها توسط یک و یا چند مهاجم که $botmasters$ نامیده می شوند ، با هدف انجام فعالیت های مخرب کنترل می گردند . به عبارت بهتر ربات ها کدهای مخربی هستند که بر روی کامپیوتر میزبان اجرا می شوند تا امکان کنترل میزبان را از راه دور فراهم آورنند). در واقع یک بات نت یک گروه خصوصی مهار سیستم از طریق نرم افزارهای مخرب کنترل می باشد . بات نت ها اغلب برای حملات $DDOS$ مورد استفاده قرار می گیرند و سیستم را با هدف انتقام ، اخاذی و اختلال فلج می نمایند . برای مقابله با این بدافزارها استفاده از یک اسکنر توصیه می شود که آلودگی و آسیب پذیری دستگاه ها و تجهیزات را به نرم افزرهای مخربی از جمله $Mirai$ نشان می دهد . نسخه بتا این اسکنرها در حال حاضر در دسترس عموم قرار دارد . هم چنین به استفاده کنندگان تجهیزات اینترنت اشیا توصیه می شود که همواره از رمزعبورهای قوی که به راحتی حدس زده نشوند استفاده شود هم چنین به روزرسانی بی دلیل این تجهیزات هم یک تهدید امنیتی محسوب می شود . دستگاه های که بر پایه لینوکس هستند در این زمینه آسیب پذیر هستند چرا که برخی از فروشندگان می توانند بدون اجازه به بروزرسانی دستگاه اقدام کننده می‌کنند.

۵ مراحل انجام

- تکمیل مطالعات و تدوین دقیق نیازمندي‌ها و فرضیات اولیه
  ۱. آشنا با تاریخچه اینترنت اشیاء
  ۲. بررسی تهدیات امنیتی اینترنت اشیاء
- تنظیم ساختار(طراحي معماري سیستم پیشنهادي به‌طور دقیق و با جزئیات)
  ۱. تهیه بخش‌های مختلف شامل مقدمه، محتوی اصلی، نتیجه‌گیری، چکیده و منابع
  ۲. مشخص کردن ترتیب مباحث
  ۳. تهیه‌ی فهرست مباحث اصلی و فرعی
  ۴. مطالعه و یادداشت برداری
  ۵. مطالعه مقالات اینترنتی و کتاب‌های مرتبط
  ۶. مطالعه، بررسی و یادداشت‌برداری از پایان‌نامه‌های مرتبط
- اجرای بخش عملی
  ۱. شبیه‌سازی محیط اینترنت اشیاء
  ۲. شبیه‌سازی سنسورهای اینترنت اشیاء
  ۳. شبیه‌سازی ارتباط بین سنسورها و سرور مرکزی
  ۴. شبیه‌سازی قوانین حاکم بر ارتباط سنسورها
  ۵. پیاده‌سازی رابط کاربری
  ۶. تعریف سناریو امنیتی
  ۷. اجرای سناریو
- ارزیابي بخش عملی
  ۱. ثبت نتایج حاصل از شبیه‌سازی
  ۲. مقایسه نتایج حاصل با نتایج کارهای مشابه
  ۳. تهیه و ارایه گزارش نهایی
  ۴. مستندسازی و نوشتن گزارش نهایی
  ۵. کسب آمادگی برای ارایه گزارش شفاهی
- تهیه مقاله
- آماده کردن مقاله و ارسال آن یک مجله معتبر

۶ زمانبندی طرح

ردیف	فعالیت	۱	۲	۳	٤	٥	٦	۷	۸	۹	۱۰
۱	تکمیل مطالعات و تدوین دقیق نیازمندی‌ها و فرضیات اولیه										
۲	تنظیم ساختار(طراحی معماری سیستم پیشنهادی به‌طور دقیق و با جزئیات)										
۳	مطالعه و یادداشت برداری										
٤	اجرای بخش عملی										
٥	ارزیابی بخش عملی										
٦	تهیه و ارایه گزارش نهایی										
۷	تهیه مقاله										

شکل ۲: زمان‌بندی طرح

۷ امکانات لازم

۱. سنسورهای خانه هوشمند(یا توابع شبیه‌سازی سنسورها)

۲. محیطی جهت برنامه نویسی

۳. شبکه اینترنت جهت تست

مراجع

[1] Rosslin John Robles , and Tai-hoon Kim , A Review on Security in Smart Home Development , 2nd ed , International Journal of Advanced Science and Technology Vol. 15, February, 2010

[2] Jayashri Bangali1 and Arvind Shaligram2, Design and Implementation of Security Systems for Smart Home based on GSM technology , 2nd ed , International Journal of Advanced Science and Technology Vol. 15, February, 2013

پست الکترونیکی: zahra.dehghanian97@gmail.com