تجزیه و تحلیل امنیت مبتنی بر تهدید برای اینترنت اشیا

چکیده

اینترنت اشیاء (IoT) یک پارادایم در حال ظهور است که بر اتصال درونی اشیاء یا وسایل با یکدیگر یا و کاربران تمرکز دارد. پیش بینی می شود که این فناوری نقطه عطفی در توسعه خانه ها و شهرهای هوشمند گردد. موفقیت و دستیابی به استفاده فراگیر برای هر فناوری مستلزم جلب اعتماد کاربران از طریق فراهم آوردن امنیت کافی و تضمین حریم خصوصی است. با وجود علاقه رو به رشد جامعه پژوهش به IoT و ظهور مطالعات و مقالات متعددی در خصوص معماری و عناصر آن؛ همچنان جای خالی تحلیلی جامع از ویژگی‌های امنتیی و حریم خصوصی مورد نیاز یک سیستم که دستگاه‌های تشکیل دهنده آن از قابلیت‌های متفاوتی برخوردارند احساس می‌شود. در این مقاله یک مدل تهدید مبتنی بر یوزکیس های (use-case) اینترنت اشیاء را ارائه می دهیم. که می‌تواند در تعیین چگونگی صرف (سرمایه‌گذاری) تلاش‌ها به منظور ایجاد امنیت در این سیستم‌ها مورد استفاده قرار گیرد. پایان کار را با ارائه پیشنهاد شاخص‌هایی که می‌توانند در استفاده از اینترنت اشیاء امنیت و تضمین حریم خصوصی را فراهم آورند جمع بندی خواهیم نمود.

کلمات کلیدی: امنیت؛ اینترنت اشیاء؛ تهدید

1. مقدمه

در سال های اخیر جهان با پیشرفت تکنولوژی سریعی روبرو گشته است که هر یک تاثیر قابل توجهی در زندگی روزمره دارد. ظهور فن آوری هایی همچون گوشی های هوشمند؛ تبلت ها؛ لپ تاپ ها و رایانه های شخصی در طول زمان و در بعد فاصله ای موجب افزایش ارتباط متقابل شده است. فن آوری معاصر فراتر از تقویت ارتباط بین انسان ها است و در حال حاضر برای دستیابی به یک هدف مشترک ارتباط بین انسان ها و اشیاء و در واقع ارتباط اشیاء با یکدیگر را تسهیل می کند؛ این تعریف اینترنت اشیاء (IoT) نامیده می شود. اعتقاد بر این است که اینترنت اشیاء نقطه عطفی در تحول تکنولوژی جهان است که در کمتر از 6 سال گذشته دارای نرخ توسعه 270 درصدی بیشتر از دستگاه های موبایل بوده است. طبق این پیش بینی بسیاری از دولت ها و شرکت های بزرگ بودجه قابل توجهی برای تحقیقات روی موضوع اینترنت اشیاء اختصاص داده اند.

اینترنت اشیاء نقشی اساسی در شکل دهی به آینده شهرهای هوشمند ایفا می کند. از دیدگاه کاربر شخصی؛ اینترنت اشیاء خود را در کاربرد ابزارهای داخلی در محل کار آشکار می کند به عنوان مثال سیستم هایی همچون ترموستات هوشمند؛ ماشین های هوشمند و جامعه هوشمند. علاوه بر این؛ با توجه به محیط های شرکتی اینترنت اشیاء قادر به خودکار سازی کارها؛ ارائه محیط های هوشمند تر برای کارمندان و مدیریت مصرف انرژی با هدف کاهش هزینه ها خواهد بود. اینترنت اشیاء با استفاده از تکنولوژی های دیگر مانند سنسورها؛ شناسه های فرکانسی رادیو (RFIDs)؛ محرک ها و مترهای هوشمند می تواند به اهداف فوق الذکر دست یابد. این دستگاه ها برای ایجاد یک رفتار جدید که هر شی برای دستیابی به قابلیت مورد نظر کمک می کنند به یکدیگر لینک می شوند. یک مثال قابل توجه از چنین کاربردی یک سیستم ترموستات است که دما را حس می کند و خود را با یادگیری الگوهای رفتاری کاربران خود تنظیم می کند.

واجب است که همه جنبه های امنیت و حریم خصوصی به طور کامل در نظر گرفته شود. در واقع رسیدگی به چنین حقایقی ضمن یک چالش از همه ضروری تر است. از آنجایی که اینترنت اشیاء ملقمه ای از فن اوری های بزرگ فردی است بسیاری از آنها ممکن است با توجه به حریم خصوصی و امنیت نقص هایی داشته باشند؛ در صورت عدم

استطاعت توجه کافی به موضوع این مقاله ممکن است اینترنت اشیاء به شیوه ای تهدید آمیز و نادرست ابزار سازی شود.

ماهیت پیچیده امنیت در اینترنت اشیاء حول محور این حقیقت است که ؛ با این حال که ارتباط چندین فن اوری به یکدیگر یک چالش بزرگ است اما سیستم تلاش می کند که دستگاه های محدود به محاسبات؛ انرژی و ذخیره سازی را به صورت ایمن با یکدیگر مرتبط کند. برخی از دستگاه های استفاده شده توسط اینترنت اشیاء تنها می توانند مکانیزم های بسیار اساسی امنیتی را تطبیق دهند و نظیر هریک ناتوان از حفظ یکپارچگی و محرمانگی اطلاعات کابران است. علاوه بر این دستگاه هایی همچون سنسورها و RFID ها فاقد یک رابط کاربری ساده مانند یک کلید خاموش/روشن یا نشانگر وضعیت است بنابراین هنگامی که مردم به این دستگاه ها اعتماد می کنند یک محدودیت روانی بصری برای آن ها به وجود می آید. امروزه نگرانی های حریم خصوصی تبدیل به یک مانع شده است و پیشرفت بسیاری از فن آوری ها را کاهش می دهد.

به تازگی بسیاری از فن اوری ها برای حفظ امنیت کافی و مکانیزم های حریم خصوصی با شکست مواجه شده اند و در نتیجه موجب آزردگی بسیاری از افرادگشته اند. در اینترنت اشیاء برای جلب اعتماد عموم باید تضمین کرد که برای امنیت و حریم شخصی این سیستم ها چنین مشکلاتی به وجود نخواهد آمد.

در این مقاله اینترنت اشیاء را از دیدگاه موارد استفاده -use cases مورد بحث قرار می دهیم. بخش های بعدی یک دید کلی از کارهای انجام شده در این زمینه را ارائه می دهد؛ بخش 3 چندین سناریو جالب که مربوط به دنیای امروز است را به طور مفصل بیان می کند؛ بخش 4 یک مدل تهدید را مورد بحث قرار می دهد؛ بخش5 تجزیه و تحلیل امنیتی را بر اساس این یوزکیس ها به دستگاه های اینترنت اشیاء ارائه می دهد؛ بخش 6 ویژگی های مطلوب امنیتی و شخصی را در سیستم های اینترنت اشیاء فهرست می کند و درنهایت در بخش 7 به کارهایی که در آینده در این زمینه برنامه ریزی کرده ایم نگاهی اجمالی خواهیم داشت. به طور ویژه برنامه اصلی ما به این صورت است:

- تعریف چندین یوزکیس برای اینترنت اشیاء.
- ایجاد مدل سازی تهدید ب عنوان روشی برای تجزیه و تحلیل موارد استفاده تعریف شده.

- فرموله کردن مجموعه ای از ویژگی های امنیتی و خصوصی مطلوب برای اینترنت اشیاء

2. کارهای مرتبط

با توجه به علاقه روزافزون به اینترنت اشیاء نشریات متعددی در امنیت و حریم خصوصی در این زمینه وجود دارد. در حال حاضر هزاران تعریف از چشم انداز اینترنت اشیاء؛ برنامه های کاربردی و فن آوری ها وجود دارد که به طور خلاصه برخی از جنبه های امنیتی و شخصی را مورد خطاب قرار می دهد.آتزوری و همکاران اهمیت امنیت در زمینه اینترنت اشیاء را مورد بحث قرار داده اند و بر جنبه های امنیت عناصر تمرکز دارند. در این مطالعه اشاره شد که به علت محدودیت دستگاه های ساخته شده اینترنت اشیاء و ویژگی های پروتوکل های ارتباطی جاری؛ اعمال مکانیزم های امنیتی پیچیده بسیار چالش برانگیز است. برخی از دستگاه ها ممکن است قادر به کنترل دسترسی برای کاربران مختلف؛ طرح تصدیق پشتیبانی کافی یا حتی استفاده از کانال های ارتباطی امن بین دستگاه ها نباشند. با این حال به خاطر داشته باشید که اقدامات امنیتی مورد نیاز وابسته به کاربرد است. برای مثال در Near Field Communication (NFC) مجاورت فیزیکی برای ایجاد ارتباط بسیار حیاتی است که این فن آوری را برای کاربردهای مختلف مفید می سازد. بنابراین به علت این ویژگی برخی از برنامه ها که از NFC استفاده می کنند ممکن است نیازمند طرح امنیتی پیچیده ای مانند کانال رمزگذاری شده نباشند. برای مثال در برخی موارد ممکن است کاربران به دیگر کاربرانی که ردوبدل اطلاعات در حضور انها مشاهده می شود توجه نکنند. برای مثال در یک کاربرد داخلی برای اینترنت اشیاء برای جلوگیری کودکان از تماشای تلویزیون بدون نظارت بزرگسالان؛ ممکن است کاربر نیازمند پروتکل های ارتباطی پیچیده نباشد و تنها استفاده از مکانیزم های کنترل دسترسی برای دسترسی به دستگاه یا رمزنگاری متقارن به جای رمزنگاری نامتقارن برای برقراری ارتباط کافی باشد.

اینترنت اشیاء با توجه به ماهیت ناهمگن خود با چالش های امنیتی و حریم خصوصی متعددی مواجه می شود. گروه های تحقیقاتی مختلف قانون های مختلفی را برای پرداختن به این مسائل در نظر گرفته اند. رومان و همکاران فن آوری های متعددی را در زمینه اینترنت اشیاء ارائه کرده اند؛ فن آوری های جاری و امکان پذیری آنها برخی از

دستگاه های اینترنت اشیاء را مورد بحث قرار داده اند و مجموعه ای از نیازمندی های امنیتی را برای دستگاه های اینترنت اشیاء ارائه کرده اند. همان گروه در مطالعه بعدی معماری متمرکز و توزیع شده اینترنت اشیاء و و پیامد آنها بر جنبه های امنیتی را مقایسه کرده اند. علاوه بر این کازلاو و همکاران تهدید های امنیتی و حریم شخصی را در معماری اینترنت اشیاء برای تحلیل تهدیدها در سطوح مختلف معماری با استفاده از یک رویکرد سیستماتیک مورد بحث قرار داده اند.

مدل های تهدید برای اینترنت اشیاء توسط بابر و همکاران ارائه شده است. بابر مدل تهدید عمومی را بیان کرد که مختص اینترنت اشیاء نیست اما می تواند روی آن منعکس شود. با این حال این عرصه همچنان فاقد یک مرجع روشن برای تهدیدهای حقیقی موجود در اینترنت اشیاء است و در برخی از کاربردها امنیت بسیار مهم تر است. ابی و همکاران بر یک امنیت تطبیقی مبتنی بر ریسک در یک برنامه بهداشت و درمان تمرکز کرده اند و این برنامه رویکرد مدیریت ریسک که موضوع نظریه بازی را برای توسعه یک مدل تصمیم گیری امنیتی تطبیقی اتخاذ می کند را در نظر میگیرد. به طور مشابه گان و همکاران بر تحلیل های امنیتی نقاط شبکه تمرکز کردند و برای برخی مسائل راه حل هایی پشنهاد دادند.

بر طبق ویتمور و همکاران کار زیادی روی امنیت و حریم خصوصی در زمینه اینترنت اشیاء انجام نشده است و بیشتر تحقیقات بر دستگاه ها به عنوان موجودیت های فردی به جای بخشی از یک سیستم اینترنت اشیاء متمرکز می شود. علی رغم تلاش های مختلف برای پرداختن به مضوعات امنیت و حریم خصوصی در اینترنت اشیاء همچنان با عدم یک تحلیل جامع و ارزیابی ریسک مواجه ایم. با توجه به فقدان نیازمندی های امنیت و حریم خصوصی؛ اینترنت اشیاء نیازمند غلبه بر موانعی است که ممکن است از تطبیق گسترده آن جلوگیری کنند.

برای درک خطر های امنیت و حریم خصوصی مربوط به اینترنت اشیاء باید آنها را به یک برنامه ویژه ارتباط دهیم؛ به طوری که هر سناریو معضلات خود را اشکار کند بنابراین این کار با یک تعریف واضح از تهدیدهای مرتبط با هر یوزکیس ارائه می شود. در این مقاله چشم انداز اینترنت اشیاء را با ارائه چندین یوزکیس شرح می دهیم و از روش

تحلیل امنیت مبتنی بر تهدید استفاده می کنیم که این کار به فرموله سازی نظریه های امنیت و حریم شخصی کمک می کند تا به برخی از چالش های اصلی در اینترنت اشیاء غلبه کند.

3. یوزکیس های اینترنت اشیاء

در این بخش سه نماینده از یوزکیس های اینترنت اشیاء را ارائه می دهیم که درحال حاضر با احتمال بالایی در کارهای روزمره و در آینده نزدیک به صورت یکپارچه می باشند. چگونگی پشتیبانی عناصر اینترنت اشیاء مانند سنسورها؛ محرک ها ؛ RFID ها؛ اینترنت و Near Field Communication از برنامه های مختلف را شرح می دهیم و به افزایش اتخاذ اینترنت اشیاء کمک می کنیم. تجزیه و تحلیل عملکرد عناصر اینترنت اشیاء در سناریوهای مختلف روشی است که اجازه می دهد تحلیل های امنیتی مبتنی بر کیس را انجام دهیم و ویژگی های امنیت و حریم خصوصی که با استفاده از اینترنت اشیاء توسط بسیاری از کاربران پشتیبانی می شوند را فرموله سازی کنیم.

A. مدیریت انرژی

یکی از برجسته ترین کاربردهای یک اینترنت اشیاء مبتنی بر سیستم هوشمند مدیریت مصرف انرژی در هر دو بخش خصوصی و صنعتی است. در جهانی ک منابع انرژی در حال کمیاب شدن است وجود چنین سیستم های هوشمندی برای کمک به حفظ منابع ضروری است. قدرت سیستم مدیریت انرژی قادر به مدیریت اجرای دستگاه مختلف است در حالی که مصرف انرژی را درمرزهای مجاز حفظ می کند. این کار با استفاده از یک متر هوشمند قابل انجام است که این متر هوشمند سیستم را با داده های زمان واقعی برای برنامه ریزی عملیات دستگاه ها تامین می کند. به عنوان مثال زمانی که یک دستگاه مکث می کند دیگر دستگاه ها کار خود را ادامه می دهند و کاربر می تواند بین دو دستگاه همگام شود.

سیستمی که از یک سنسور و یک محرک استفاده می کند می تواند انرژی را ذخیره کند و مصرف انرژی را توسط داده های زیست محیطی مدیریت کند و این هدف با استفاده از سنسور به دست می اید و با توجه ب طرح صرفه

جویی انرژی از پیش تعیین شده از طریق عملیات محرک پاسخ می دهد. برای مثال در یک خانه هوشمند یک سیستم ترموستات داخلی یک جزء ضروری برای کنترل دما است. این ترموستات از یک سنسور دما استفاده می کند که می تواند به دمای اتاق نظارت داشته باشد و زمانی که هر گونه انحرافی از این مقادیر را تشخیص دهد بازخوردی را به یک محرک ارسال میکند تا تغییرات را آغاز کند. این امر شامل تنظیم دما در محدوده مشخصی می باشد که توسط کاربر تعریف شده است. ترموستات سپس برای حفظ دمای اتاق بین محدوده تعیین شده فعالیت خود را تنظیم می کند. این ترموستات همچنین می تواند دستگاه را زمانی که به سقف رسیده باشد خاموش کند یا می تواند تنها زمانی که شرایط زیست محیطی موجود باشند روشن شود به عنوان مثال درجه حرارت داخلی.

استعامل یک شبکه بیشتر کنترل کاربران را تقویت می کند و مدیریت ترموستات از راه دور را امکان پذیر می سازد و بنابراین دمای اتاق را برای ورود آماده می کند؛ زمانی که کاربرد وارد خانه می شود اتاق دارای یک درجه حرارت مناسب است. سیستم می تواند از مزایای موقعیت دستگاه که به گوشی هوشمند متصل می شود استفاده کند این دستگاه می تواند بر اساس فاصله از موقعیت دستگاه سیگنال هایی را به سیستم روشن/خاموش ارسال کند. دستگاه دیگری حتی با کنترل بهتر؛ یک سنسور حرکت است که حرکت را تشخیص می دهد و بر این اساس برای بهبود مصرف انرژی زمانی که کاربر در یک مدت طولانی در اتاق مشخصی نیست سیستم را خاموش می کند. پس از گذشت چند روز سیستم عادات کاربر را یاد میگیرد و به طور خودکار واکنش نشان می دهد برای مثال؛ زمان بیدار شدن در صبح سیستم را روشن می کند و زمان خوابیدن آن را خاموش می کند.

B. ماشین هوشمند

در دنیای خودکار دیگر نیاز نیست که پشت فرمان نشست و از رانندگی طولانی رنج برد دانشمندان بر این باورند که تا سال 2020 مردم از فن آوری جدید راننده اتوماتیک لذت خواهند برد. در جهان مدرن گوشی های هوشمند به عنوان یک کنترل دسترسی برای بازکردن قفل ماشین به جای کلید معمولی استفاده خواهند شد. بنابراین مشکل

مقیاس پذیری داشتن یک کلید برای هر کاربر حل خواهد شد. Field Communication Near به علت محدوده ارتباطی کوتاه که حضور فیزیکی کاربر را تضمین می کند یک کاندید مناسب برای این آینده است.

هنگامی که یک کاربر مجاز است ماشین را بازکند می تواند به اینترنت متصل شود و نقشه جاده ها را دانلود کند به زیرساخت های شهر متصل شود و به روز رسانی های ترافیک؛ سیگنال های چراغ های راهنمایی را به دست آورد و حتی برای کمک به یک سیستم بزرگتر مثل Vehicular Network وضعیت را گزارش دهد. خودرو برای برنامه ریزی مسیر خود برای رسیدن به مقصد در سریع ترین و اقتصادی ترین راه از این اطلاعات استفاده خواهد کرد. با اطلاع از زمان تغییر در چراغ راهنمایی می تواند سرعت خود را تنظیم کند بنابراین سوخت کمتری مصرف خواهد شد و تخمین زمان دقیق تری برای رسیدن به مقصد حاصل می شود. خودرو همچنین برای هماهنگی رانندگی در خیابان با خودروهای اطراف ارتباط برقرار می کند. برای مثال زمانی که یک خودرو قصد دارد از خودروی دیگری عبور کند با سیستم خود ارتباط برقرار خواهد کرد و عبور را به صورت امن سازماندهی خواهد کرد.

علاوه بر این گزارشات مبنی بر حوادثی که کودکان در اتومبیل رها می شوند رو به افزایش است، بر اساس Safe Kids Worldwide: در هر ده روز یک کودک بر اثر گرمازدگی در اتومبیل جان می سپارد بنابراین اتخاذ مکانیزم های هشدار بسیار موثر است مانند سنسور حرکت که قادر به شناسایی کودک یا حیوان رها شده در یک اتومبیل قفل شده است و بخش مربوطه را از این موضوع آگاه می کند. درنهایت به منظور ایجاد سفری راحت تر کاربران می توانند به کانال های تلویزیونی در خانه متصل شوند و برنامه مورد علاقه خود را هنگام سفر تماشا کنند.

یک اتومبیل هوشمند می تواند برای خلق جهانی امن تر بسیار موثر باشد، می تواند مانع رانندگی/استفاده کاربران غیرمجاز از اتومبیل شود و می تواند در برابر سرقت از اتومبیل محافظت کند. تنها کاربران مجاز که متعلق به لیست سفید می باشند می توانند از اتومبیل استفاده کنند. به طور مشابه از رانندگی نوجوانان بی دقت بدون گواهینامه رانندگی یا افراد مسن که موجب خسارت و مرگ می شوند جلوگیری می کند.

اتخاذ اتومبیل های هوشمند قبل از ظهور در خیابان ها باید چندین مرحله را پشت سر بگذارد. یک نمونه اولیه از این سیستم در یک فرودگاه استفاده شده است، در این مکان وسایل نقلیه بین ساختمان های خلوت حرکت می کنند و تا حد زیادی برای خودکارسازی عملکرد فرودگاه سودمند است.

C. سیستم بهداشت و درمان هوشمند

با افزایش طول عمر و بیماری های مزمن جدید، جمعیت در حال رشدی که در آن بیماران خاص نیازمند نظارت می باشند مستلزم توجه بیشتری به مراقبت های پزشکی است. با این حال امکانات فعلی در بیمارستان ها و کلینیک ها بسیار محدود است و پاسخگوی جمعیت نیست. بنابراین افزایش قابلیت پیگیری شرایط بیماران در خانه یا در بیمارستان ضروری است. این مهم می تواند با استفاده از نظارت شرایط بیماران حاصل شود و گزارشات را از طریق اینترنت به سیستمی ارسال کند که داده های به دست آمده را تحلیل می کند و به اعضا هشدار می دهد، بنابراین به سیستم مراقبت و درمان اجازه می دهد که مشکلات مربوطه را زودتر شناسایی کند و سریع تر به شرایط اضطراری پاسخ دهد. در سال های اخیر درمان از راه دور در قالب دستگاه هایی مانند پمپ های انسولین و واحدهای ضربان قلب ابداع شده اند که به بیمار وصل می شوند و در مواقع ضروری واکنشی سریع و خودکار ارایه می دهند. در یک بیمارستان هوشمند RFID ها می توانند برای تشخیص بیماران، آیتم ها و پزشکان به راحتی و به سرعت استفاده شوند برای مثال در مواردی که یک فرد ناشناس تصادفی وارد می شود و بدون هیچ گونه تاخیری نیازمند مراقبت های پزشکی است. همچنین اجازه می دهد که به منظور زمان واکنش بهتر در شرایط اضطراری کارکنان موقعیت پزشکان را در اختیار داشته باشند. اتصال تگ های RFID محدود به افراد نمی شود یک از مسایل اصلی در بسیاری از بیمارستان ها فقدان دارو و استفاده غیرمجاز از ابزار پزشکی گران قیمت است. بنابراین ردیابی اشیاء با RFID ها این فقدان ها را می تواند کاهش دهد و به ردیابی آنها کمک کند.

4. مدل تهدید

A. منابع تهدید

پس از بحث در مورد ویژگی های اینترنت اشیاء و چگونگی کاربرد آنها در سناریوهای مختلف در یک جهان هوشمند، اکنون تهدیدات بالقوه که در معرض یوزکیس های ارایه شده در بخش قبل قرار میگرد قابل شناسایی است. سه موجودیت اصلی موجود است که موجب خطرهایی در رابطه با امنیت و حریم خصوصی در اینترنت اشیاء می شود:

1) کاربر مخرب: صاحب دستگاه اینترنت اشیاء است که به منظور یادگیری اسرار تولید کننده و دسترسی به عملکرد محدود دارای پتانسیل انجام حملات است. کاربرمخرب با کشف نواقص در سیستم قادر به حصول اطلاعات، فروش اسرار به اشخاص ثالث یا حتی حمله به سیستم های مشابه است.

2) تولید کننده بد: تولید کننده دستگاه با توانایی بهره برداری از فن آوری برای حصول اطلاعات در مورد کاربران یا دیگر دستگاه های اینترنت اشیاء است. چنین تولیده کننده ای به منظور دسترسی به اطلاعات کاربر و افشای آن به اشخاص ثالث می تواند چاله های امنیتی را به عمد در طراحی ابداع کند. تولید ضعیف محصولات ایمن به همان اندازه موجب به خطر انداختن حریم خصوصی کاربران می شود. علاوه بر این در اینترنت اشیاء که اشیاء مختلف به یکدیگر متصل می شوند یک تولید کننده می تواند به دستگاه های دیگر رقبا حمله کند و موجب خدشه دار شدن شهرت آنها گردد.

3) دشمن خارجی: یک موجودیت بیرونی است که بخشی از سیستم نیست و حق دسترسی به سیستم را ندارد. یک دشمن سعی دارد اطلاعات کاربران سیستم را برای اهداف مخربی همچون آسیب مالی و تضعیف اعتبار کاربران به دست آورد. همچنین با دستکاری داده های حسی مانند انتقال موجب خرابی سیستم می شود.

B. کلاس های بردارهای حملات

دسته بندی حملات روی یک سیستم برای درک خطرات بسیار ضروری است. چندین دسته را برای شناسایی تهدیدات انتخاب می کنیم. این تهدیدات در تحلیل های امنیتی یوزکیس های ارایه شده در بخش III به طور مفصل تری مورد بررسی قرار خواهند گرفت.

1) دستکاری دستگاه : دستگاه اینترنت اشیاء دستگاه کوچکی است که در سیستم های دیگر همچون اتومبیل، اجاق گازها و غیره قرار می گیرد. برخی از دستگاه های اینترنت اشیاء بیشتر اوقات بدون نظارت است بنابراین می توانند به راحتی به سرقت روند. یک بار که دستگاه به اشتباه در اختیار فردی قرار گیرد، مجموعه مختلفی از حملات مانند سرقت اسرار، دستکاری نرم افزار و سخت افزار می تواند صورت گیرد. ذکر این موضوع مهم است که یک دشمن می تواند سیستم را دستکاری کند و برای فریب به دستگاه آن را استفاده کند، و دستگاه را به طرز نادرست و خارج از عملکرد اصلی خود استفاده کند.

2) افشای اطلاعات: عمل فاش اطلاعات به موجودیتی است که اجازه دسترسی به آن را ندارد که عبارتند از افشای تصادفی، حمله هدف دار و استنتاج یا همبستگی . یک حمله کننده با استراق سمع در کانال های شبکه، دسترسی فیزیکی به دستگاه یا از طریق دسترسی به دستگاه شبکه می تواند اطلاعات را به دست آورد.

3) نقض حریم خصوصی: با وجود افشای اطلاعات یک دشمن لزوما نیازمند دسترسی به اطلاعات محرمانه کاربر نیست. دشمن می تواند اطلاعات خصوصی را از دیگر منابع همچون داده های متا و تجزیه و تحلیل ترافیک استنباط کند.

4) محرومیت از خدمات: به ویژگی های غیرقابل هنگامی که توسط یک کاربر مجاز درخواست شده است اشاره دارد. سیستم باید توانایی ادامه عملیات را داشته باشد حتی زمانی که یک اقدام نامطوب توسط کاربران مخرب در حال انجام است. این کلاس از حملات با سرقت دستگاه، دستکاری نرم افزار آن یا اختلال در کانال ارتباطی می تواند انجام شود.

5) فریب کاری: به کاربرد اختیارات متعلق به دیگران برای دسترسی به سرویس های غیرقابل دسترس اشاره دارد. اختیارات می تواند به طور مستقیم از یک دستگاه، استراق سمع در کانال ارتباطی یا فیشینگ حاصل شود.

6) ارتقاء امتیاز: زمانی است که یک کاربر غیرممتاز به دسترسی های یک دستگاه /سرویس ممتاز دسترسی داشته باشد. این موضوع می تواند با نصب یک فریب دهنده در سسیستمی حاصل شود که وانمود می کند یک دستگاه دیگر است و دارای دسترسی ممتاز در سیستم است.

7) تزریق سیگنال: زمانی است که یک حمله کننده برای تغییر داده های حسی مانند انتقال سیگنال های الکترومغاطیسی به یک سنسور داده های جعلی را به سیستم وارد می کند.

8) کانال جانبی: بر طبق اطلاعاتی مانند تحلیل زمانی اجرا، مصرف انرژی، تحلیل ترافیک، تحلیل نقص و تحلیل الکترومغناطیسی دستگاه، اطلاعات خصوصی و محرمانه داده ها می توانند استنباط شوند.

5. اثر حمله

به منظور ارایه پیشنهاداتی بر چگونگی ایمن سازی اینترنت اشیاء و درک شدت تهدیدات، فهرست کردن خطرات بالقوه بدون در نظر گرفتن جامعی از تاثیرات واقعی خود و احتمال، وابسته به مفاد خواهد شد. بیشتر آثار گذشته تنها بر جنبه های فنی دستگاه های اینترنت اشیاء تمرکز دارد و به به سختی به امنیت برنامه ها توجه می کند، شکافی در این ادبیات تشخیص دادیم و سعی داریم که این شکاف را از طریق نگرشی متفاوت به تحلیل امنیت و ملزومات حریم خصوصی در اینترنت اشیاء پر کنیم. در این بخش یک تحلیل حمله ارایه می دهیم و به معضلات امنیت و حریم خصوصی برای هر دستگاه با استفاده از یوزکیس های مربوط به بخش 3 می پردازیم، سپس یک مرورکلی بر اقدامات امنیتی دقیق تر قابل اجرا داریم.

A. محرک ها

عملکرد محرک در زمینه اینترنت اشیاء معادل با عملیات نوشتن در رایانه های شخصی است. در جهان اشیاء، یک محرک می تواند با دریافت شیگنال ها از دیگر دستگاه ها یا فعال شدن فیزیکی توسط کاربران روی شبکه عمل کند. امنیت: یک حمله روی این دستگاه در محدوده مختلف می تواند باعث آسیب به کاربر شود. در سناریو مدیریت انرژی، به علت مصرف انرژی بیش از حد فعالیت غیرمجاز محرک می تواند موجب فقدان مالی شود. این آسیب حتی می تواند در سناریو اتومبیل هوشمند شدید تر شود و یک سوء عملکرد در محرک می تواند منجر به مرگ شود. در سیستم بهداشت و درمان هوشمند، یک محرک می تواند فعال کننده برای تزریق دارو به یک بیمار نظارت شده در

خانه باشد و هر گونه اشتباهی یا سوءعملکردی در این زمینه می تواند موجب یک دوز اشتباه دارو شود که آثار کشنده ای در پی دارد.

B. سنسورها

سنسورها داده هایی که برای تحلیل به دیگر اجزاء منتقل می شوند را در سیستم جمع آوری می کنند و موجب یک واکنش یا فعالیت مشخص می شود.

امنیت: داده های جمع آوری شده می توانند منبع یک حمله باشند مانند زمانی که به علت حمله فیزیکی داده جعل می شود و موجب یک رفتار غیرمنتظره از دیگر موجودیت های سیستم می شود. در یوزکیس مدیریت انرژی، داده های جعلی از سنسورها موجب رفتار متفاوتی توسط محرک می شود، بنابراین فعال کردن ترموستات در زمان نادرستی موجب خسارات مالی برای کاربران می شود. با این حال یادگیری اسرار اساسی در مورد کاربر از داده های حسی در این سیستم نامحتمل است. در سیستم بهداشت و درمان داده های جعلی می تواند موجب تشخیص نادرست بیماری، مدیریت داروی نادرست شود که منجر به واکنش آلرژیک یا حتی زندگی در معرض خطر می شود. همچنین می تواند هشدارهای جعلی را ارسال کنند و موجب فقدان مالی شود برای مثال با ارسال یک تیم پزشکی برای یک بیمار اشتباهی.

حریم خصوصی: اگر داده های جمع آوری شده از این دستگاه ها اسرار کاربران را فاش نکند می تواند اطلاعاتی را درمورد عادات کاربران فاش کند. برای مثال در یوزکیس مدیریت انرژی زمانی که کاربر خانه را ترک می کند، به خواب می رود یا از خواب بیدار می شود حمله کننده ها می توانند از تحلیل اساسی داده های سنسور حرکت یاد بگیرند. در سیستم بهداشت و درمان سیگنال های سنسورها برای گزارش شرایط بیمار استفاده می شوند و می توانند عملکرد پزشکی دستگاه را نشان دهند در نتیجه اطلاعات شخصی دارندگان را فاش می کنند.

C. تگ های RFID

RFID ها شامل استفاده از دستگاه خواننده برای شناسایی یک تگ می شود. این دستگاه به علت هزینه پایین شهرت می یابد در حالی که توانایی مسیریابی و شناسایی اشیاء را همچنان حفظ می کند. با این حال این فن آوری معضلات امنیت و حریم خصوصی را افزایش می دهد.

امنیت: محدودیت در سخت افزار و انرژی این عناصر از اتخاذ مکانیزم های امنیتی کافی جلوگیری می کند. برای مثال، دارندگان تک های RFID نباید توسط یک حمله کننده با یک خوانند تگ شناسایی شوند بنابراین مکانیزم های کنترل دسترسی اندک ممکن است منجر به افشای اطلاعات شوند. در مثال اتومبیل هوشمند، یک حمله کننده در محدوده نزدیک به کاربر ممکن است زمان دسترسی به وسیله نقلیه قادر به رهگیری سیگنال ها باشد که در آن برخی از این سیگنال ها می توانند در اختیار کاربر باشند. یک حمله کننده می تواند از این اختیارات برای سرقت ماشین استفاده کند.

حریم خصوصی: یک ویژگی اصلی RFID ها توانایی ردیابی است. بنابراین زمانی که مورد سوء استفاده قرار میگیرد معضل حریم خصوصی بزرگ را در پی خواهد داشت. در سناریوی بهداشت و درمان، زمانی که کارمندان از این سیستم استفاده میکنند حریم خصوصی معضل اصلی برای آنها است زیرا آنها می توانند به طور مداوم ردیابی شوند. یک حمله کننده با قطع سیگنال های RFID می تواند از شرایط سلامتی بیمار آگاه شود.

D. شبکه، NFC و اینترنت

دستگاه های اینترنت اشیاء از طریق اتصال شبکه با یکدیگر ارتباط برقرار می کنند. پروتکل های ارتباطی بر طبق عملکرد خود تغییر می کنند بنابراین در سطوح امنیتی و خصوصی خود با یکدیگر تفاوت دارند. در اینجا امنیت و حریم خصوصی ارتباط را به اختصار ذکر می کنیم و تجزیه و تحلیل دقیق تر پروتکل های ارتباطی را به آینده موکول می کنیم.

امنیت: به علت محیط ناهمگن اینترنت اشیاء پروتکل های ارتباطی متفاوت با سطوح امنیتی مختلفی اتخاذ می شوند. دستگاه های اینترنت اشیاء ممکن است از طریق کانال های بی سیم با یکدیگر ارتباط برقرار کنند و این کار آسیب پذیری سیستم برای استراق سمع و حملات ماسک را افزایش می دهد. یک حمله کننده می تواند از کانال های ارتباطی برای جمع آوری اطلاعاتی همچون موقعیت، اعتبار، و عملیات کاربران استفاده کند. یک حمله نوعی در یوزکیس اتومبیل هوشمند زمانی انجام می شود که اتومبیل سعی دارد در رابطه با عبور از اتومبیل دیگری مذاکره کند با این حال اطلاعات نادرستی دریافت می کند که می تواند منجر به هرج ومرج، تصادف و مرگ شود. همچنین یک دشمن می تواند سیگنال های ارسال شده از دستگاه هایی را اصلاح کند که موجب واکنش غیرمنتظره یا مخالف از دیگر دستگاه های سیستم می شود مانند روشن کردن یک دستگاه به جای خاموش کردن آن.

حریم خصوصی: شبکه وسیله اصلی برقراری ارتباط بین دستگاه های اینترنت اشیاء است بنابراین نقاط بحرانی را برای افشای اطلاعات وضع می کند. برای مثال، زمانی که یک اتومبیل هوشمند برای دانلود نقشه ها یا به روز رسانی اطلاعات ترافیک به یک گره محلی دسترسی پیدا می کند یک حمله کننده می تواند از مقصد راننده آگاه شود. علاوه بر این، از آنجایی که اتومبیل ها می توانند به راحتی به یک شبکه گسترده دسترسی داشته باشند و عناصر متعددی همچون استریو، میکروفون و اتصال به اینترنت داشته باشند. تولیدکنندگان بی اعتبار می توانند از فن آوری کاربران برای آگاهی از اطلاعات آن ها استفاده کنند.

6. ویژگی های امنیت مطلوب و حریم خصوصی

در این بخش به منظور فرموله کردن ویژگی های امنیت و حریم خصوصی برای اینترنت اشیاء سیستم، خطرات و تحلیل های امنیتی را از بخش های قبل کامل می کنیم. مانند ویژگی های زیر، زمانی که توسعه چارچوب اینترنت اشیاء به منظور ارایه یک سیستم امن، جذاب و قابل اعتماد به بسیاری از کاربران ضروری است.

A. ویژگی های امنیت

هدف نهایی حفظ محرمانگی و یکپارچگی سیستم است. اقدامات مختلفی برای هر نقطه ضعف باید اعمال شود، بین ویژگی های امنیت برای مسیرهای حمله در بخش IV-B متصل می شویم.

محرک ها، سنسورها و RFID ها

SP1: دستگاه باید در برابر برنامه نویسی مجدد غیرمجاز و سرقت مخفی منفعل غیرقابل نفوذ باشد. دستگاه باید ویژگی های امنیتی خود را حفظ کند مانند حفظ یکپارچگی و محرمانگی اطلاعات کاربران و دستگاه. زمانی که یک حمله فیزیکی رخ می دهد و از انکار خدمات جلوگیری می کند. با این حال، به روز رسانی سخت افزار روی دستگاه باید برای کاربران امکان پذیر باشد.

SP2: دستگاه اینترنت اشیاء باید یک حافظه محافظت شده با حفظ اطلاعات رمز شده برای حفظ محرمانگی اطلاعات کاربران روی دستگاه داشته باشد. برای مثال، استفاده از ویژگی های امنیتی سخت افزار مانند ARM TrustZone.

SP3: به منظور جلوگیری از دسترسی غیرمجاز از به خطر انداختن کل سیستم کنترل دسترسی مکانیزم ها در هر دستگاه الزامی است. در برخی از دستگاه های اینترنت اشیاء مثل سنسورها و محرک ها اتخاذ مکانیزم های کنترل دسترسی پیچیده به علت حافظه محدود دشوارتر است. با این حال، در برخی از برنامه ها کنترل دسترسی که یک دستگاه را به خطر می اندازد می تواند کل سیستم را به خطر اندازد و منجر به افشای اطلاعات، سرقت اعتبار و محرومیت از خدمت شود.

اینترنت، شبکه و NFC

SP4: برای حفظ یکپارچگی و محرمانگی کاربر داده های مبادله شده بین کاربر و اینترنت اشیاء باید ایمن باشد. اگر یکپارچگی سیستم به خطر بیافتد، عملیات عادی سیستم مختل می شود و می تواند منجر به آسیب های مالی و فردی به کاربران شود.

SP5: مکانیزم های شناسایی و اختیار باید اعمال شوند. تنها کاربرهای مجاز با مجوز های مختلف خواندن و نوشتن می توانند به دستگاه اینترنت اشیاء دسترسی داشته باشند. دستگاه اینترنت اشیاء نیازمند شناسایی دستگاه ها در سیستم است و قادر است هر فریب دهنده ای را شناسایی کند.

محرک ها، سنسورها، RFID ها، شبکه

SP6: سیستم باید در پارامترهای معمولی در دسترس باشد و هنگامی که برخی از اقدامات نامطلوب مانند آسیب فیزیکی توسط کاربر مخرب به یک دستگاه انجام می شود اتخاذ شود. همچنین آسیب منعکس شده از دشمن باید حداقل تاثیر را روی سیستم داشته باشد.

B. ویژگی های حریم خصوصی

ویژگی های حریم خصوصی در برابر نواقص حریم خصوصی در بخش IV-B مقابله می کند درحالی که یک موجودیت مخرب می تواند از اطلاعات شخصی کاربران اطلاع یابد.

PP1: داده های مبادله شده بین یک کاربر و دستگاه های اینترنت ا شیاء باید حفاظت شود به طوری که یک حمله کننده که روی ارتباطات استراق سمع می کند نتواند اطلاعات کاربر را استنباط کند. زمانی که یک کاربر حاضر یا غایب است یک حمله کننده نباید قادر به استنابط زمان، هویت کاربر یا هر اطلاعات حساس دیگری باشد.

PP2: پیام های مبادله شده بین دستگاه های اینترنت اشیاء نباید هویت اطلاعات شخصی (PII) کاربران را فاش کند.

PP3: سیگنال های یک دستگاه باید به روش حفظ حریم خصوصی ارسال گردد به طوری که عملکرد دستگاه ها را فاش نکند زیرا می تواند اطلاعات کاربران را فاش کند.

PP4: دستگاه های اینترنت اشیاء تنها زمانی که کاملا ضروری است باید یک رکورد از اطلاعات شخصی کاربر را حفظ کنند و چنین موردی تنها باید برای زمانی محدودی باشد.

PP5: تنها داده هایی که اطلاعات شخصی کاربران را فاش نمی کنند می توانند جمع آوری شوند برای مثال، حفظ یک رکورد از تعداد افراد در یک ساختمان اما توجه کنید که اطلاعات مربوط به هویت مانند نام، ID وتصویر بصری باشد.

PP6: کاربر باید آگاه شود که چه اطلاعاتی و چه زمانی ضبط می شوند.

PP7: کاربر باید قادر به حذف همه اطلاعات از دستگاه باشد برای مثال اگر دستگاه مجددا فروخته شود.

7. کار آینده

امنیت برای هم سیستم قابل طراحی مجدد نیست، قصد داریم گروه های یوزکیس و چارچوب های مورد نیاز که موجب معماری، میان افزار و کتابخانه می شود را شناسایی کنیم. ساخت تحلیل های امنیتی که در اینجا انجام داده ایم و ویژگی های مختلف دستگاه ها در یک سیستم اینترنت اشیاء به منظور توسعه یک بسته امنیت ی که می تواند برای هر یوزکیس توسط طراحان استفاده شود در دستور کارمان در آینده قرار می گیرد. هدف از توسعه این بسته، عرضه یک بسته کامل به کاربران است که شامل انواع مکانیزم های مناسب برای دستگاه ها و سطوح امنیتی مختلف است. سپس طراحان قادر به ساخت ترکیبات شخصی این اقدامات بر طبق برنامه مطلوب می باشند و حتی می توانند به سطح ریسک در طراحی خود دسترسی داشته باشند.

همانطور که پیشتر گفته شد سیستم اینترنت اشیاء شامل دستگاه هایی با ویژگی های متمایز و محدود است. دستگاه های کوچک مانند RFID ها، سنسورها و دستگاه های تعبیه شده محدودیت های حافظه، انرژی و منطق محاسبات را متحمل می شوند. از سوی دیگر، دستگاه های قدرتمند مانند لپ تاپ ها، کامپیوترهای شخصی و سرورها در اقدامات امنیتی پیچیده دارای محدودیت کمتری می باشند. بسته شامل حداقل مجموعه ای از عملکردها برای تضمین مکانیزم امنیتی پایه با دستگاه های محدود است. علاوه بر این، زمانی که سطح امنیت بالا از دستگاه های محدود تر موردنیاز است مکانیزم های معمولی می توانند در برامد افزایش هزینه ها یا نیازمندی انرژی استفاده شوند.

این یک پرسش معمولی نیست که آیا چنین بسته ای امکان پذیر است و هدف ما کشف چنین بسته ای در آینده نزدیک است.

A. ارزیابی ریسک مقدماتی

ارزیابی ریسک سطح امنیت را برای سیستم های متعددی تعیین خواهد کرد. بر اساس تحلیل حمله ارایه شده در بخش های قبل یک ارزیابی ریسک مقدماتی برای هر یوزکیس از بخش 3 ارایه می دهیم. ارزیابی ریسک علاوه بر شدت حمله ها احتمال وقوع را نیز محاسبه می کند. آن را به سه دسته از بالا به پایین تقسیم کرده ایم. می دانیم که عواملی دیگر همچون "چه کسی " حمله کننده است وجود دارد که بر این تعداد تاثیر می گذارد. جدول 1 سطوح مخلف ریسک را در زمینه یوزکیس ها برای هر تهدید خلاصه می کند. اینها به صورت مستقیم از تحلیل ویژگی های امنیتی دستگاه ها استنباط می شوند. در اینجا یک کاربر بی خطر را فرض می کنیم و این بررسی مقدماتی را تنها بر اساس دشمن خارجی محدود می کنیم. بر اساس ارزیابی ریسک، مکانیزم های امنیتی متفاوت باید با استفاده از یک سناریو مبتنی بر رویکرد اتخاذ شوند. ارزیابی ریسک یک نقش اساسی در طراحی سیستم های اینترنت اشیاء ایفا خواهد کرد با این حال مطالعات گسترده بیشتری مورد نیاز است و در کارهای بعدی پوشش داده خواهد شد.

مسیر حملات	مدیریت انرژی	اتومبیل هوشمند	مراقبت های بهداشتی
تهدید فیزیکی	1	2	3
افشای اطلاعات	2	3	2
محرومیت از خدمت	1	3	2
فریب کاری	1	2	2
ارتقای امتیاز	1	2	3

جدول1. ارزیابی ریسک

1- ریسک کم 2- ریسک متوسط 3- ریسک زیاد

8. نتیجه گیری

اینترنت اشیاء در نهایت از دوران ابتدایی گامی فراتر نهاده است و مورد توجه بیشتر محققان و جامعه صنعتی قرار گرفته است. در این مقاله چشم اندازی از اینترنت اشیاء را بررسی کردیم و در زمینه امنیت و حریم خصوصی آن را به کارهای گذشته ارتباط دادیم. به طور ویژه رویکردهای مختلفی که توسط بسیاری از محققان بررسی شده اند را ارایه کردیم. درحالی که بسیار از محققان بر امنیت و حریم خصوصی دستگاه های تشکیل دهنده اینترنت اشیاء تمرکز دارند، مقاله های کمی به مدل های تهدید، امنیت و تحلیل حریم خصوصی سیستم ها می پردازند. در این مقاله، برای ارایه یک مدل تهدید به عنوان روشی برای تحلیل اثر تهدیدات در برنامه های مختلف یک تحلیل تهدید مبتنی بر رویکرد را اتخاذ کردیم. ویژگی های امنیت و حریم خصوصی را از مدل تهدید استنباط کردیم. این ارزیابی کارهای آینده را هدایت خواهد کرد به طوری که تلاش های قابل توجه بیشتری در توسعه مکانیزم های امنیتی برای اینترنت اشیاء باید انجام شوند.

REFERENCES

[1] Y. Montcheuil, "How to make the most of the Internet of Things," *http://www.itproportal.com/2014/04/25/how-to-make-the-most-of-the-internet-of-things/*.

[2] C. Buckl, S. Sommer, A. Scholz, A. Knoll, A. Kemper, J. Heuer, and A. Schmitt, "Services to the Field: An Approach for Resource Constrained Sensor/Actor Networks," in *2009 International Conference on Advanced Information Networking and Applications Workshops*. IEEE, May 2009, pp. 476–481.

[3] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the Internet of things," *IEEE Internet Computing*, vol. 14, no. 1, pp. 44–51, Jan. 2010.

[4] A. Serbanati, C. M. Medaglia, and U. B. Ceipidor, "Building blocks of the internet of things: State of the art and beyond," *Deploying RFID-Challenges, Solutions, and Open Issues, C. Turcu, Ed., InTech*, 2011.

[5] Nest labs, "Nest, Smart thermostat system," 2014.

[6] H. Xu, T. Dinev, J. Smith, and P. Hart, "Information privacy concerns: linking individual perceptions with institutional privacy assurances," in *Journal of the Association for Information Systems*. Citeseer, 2011.

[7] University of Oxford, "How internet affects young people at risk of self-harm, suicide – ScienceDaily."

[8] A. Hawks, "Leaked cell phone photos Archives - starcasm.net."

[15] R. H. Weber, "Internet of Things New security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, Jan. 2010.

[16] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, no. 9, pp. 51–58, Sep. 2011.

[17] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[18] D. Kozlov, J. Veijalainen, and Y. Ali, "Security and privacy threats in iot architectures," in *Proceedings of the 7th International Conference on Body Area Networks*, ser. BodyNets '12. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, pp. 256–262.

[19] N. Meghanathan, S. Boumerdassi, N. Chaki, and D. Nagamalai, Eds., *Recent Trends in Network Security and Applications*, ser. Communications in Computer and Information Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, vol. 89.

[20] H. Abie and I. Balasingham, "Risk-based adaptive security for smart iot in ehealth," in *Proceedings of the 7th International Conference on Body Area Networks*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, pp. 269–275.

[21] G. Gan, Z. Lu, and J. Jiang, "Internet of Things Security Analysis," in *2011 International Conference on Internet Technology and Applications*. IEEE, Aug. 2011, pp. 1–4.

[22] A. Whitmore, A. Agarwal, and L. Xu, "The Internet of ThingsA survey of topics and trends," *Information Systems Frontiers*, Mar. 2014.

[23] M. Venables, "Smart meters make smart consumers," *Engineering & Technology*, vol. 2, no. 4, pp. 23–23, Apr. 2007.

[9] J. Best, "Man HACKS into 10-month-old's baby monitor and shouts at sleeping infant - Mirror Online."

[10] S. Hinduja and J. Patchin, "Bullying, cyberbullying, and suicide," *Archives of Suicide Research*, 2010.

[11] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, 2010.

[12] Cisco, "CISCO: The Internet of Things: How the next Evolution of the Internet is changing everything from http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf," Tech. Rep.

[13] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.

[14] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[24] S. Rosenblatt, "Google's self-driving car turns out to be a very smart ride," 2014.

[25] S. Clark, "Orange and Valeo demonstrate NFC car key concept," 2010.

[26] Telekom, "Intelligent car key in a cell phone."

[27] H. Moustafa and Y. Zhang, *Vehicular Networks: Techniques, Standards, and Applications*, 1st ed. Boston, MA, USA: Auerbach Publications, 2009.

[28] J. Null, "Fact Sheet - Heatstroke Deaths of Children in Vehicles."

[29] Arup Laboratories, "Using RFID to track Equipment and Patients," 2011.

[30] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat modeling as a basis for security requirements," in *Symposium on requirements engineering for information security (SREIS)*, vol. 2005, 2005, pp. 1–8.

[31] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for internet of things (iot)," in *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*. IEEE, 2011, pp. 1–5.

[32] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 447–462.

[33] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM conference on Computer and communications security - CCS '02*. New York, New York, USA: ACM Press, Nov. 2002, p. 41.

[34] A. Parmar, "Hacker shows off vulnerabilities of wireless insulin pumps."

[35] W. Alexander, "Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode — VICE Canada."

[36] D. Molnar and D. Wagner, "Privacy and security in library RFID: issues, practices, and architectures," *... on Computer and communications security*, 2004.

[38] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Security in pervasive computing*. Springer, 2004, pp. 201–212.

[37] M. O. Lehtonen, F. Michahelles, and E. Fleisch, "Trust and Security in RFID-Based Product Authentication Systems," *IEEE Systems Journal*, vol. 1, no. 2, pp. 129–144, Dec. 2007.

[39] P. Rotter, "A Framework for Assessing RFID System Security and Privacy Risks," *IEEE Pervasive Computing*, vol. 7, no. 2, pp. 70–77, Apr. 2008.

[40] I. Gudymenko, K. Borcea-Pfitzmann, and K. Tietze, "Privacy implications of the internet of things," in *Constructing Ambient Intelligence*. Springer, 2012, pp. 280–286.

[41] W. Hu, H. Tan, P. Corke, W. C. Shih, and S. Jha, "Toward trusted wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 7, no. 1, pp. 1–25, Aug. 2010.

[42] I. Cha, Y. Shah, A. Schmidt, A. Leicher, and M. Meyerstein, "Trust in M2M communication," *IEEE Vehicular Technology Magazine*, vol. 4, no. 3, pp. 69–75, Sep. 2009.

[43] C. Namiluko, A. J. Paverd, and T. De Souza, "Towards Enhancing Web Application Security Using Trusted Execution," in *Workshop on Web Applications and Secure Hardware - WASH'13*, 2013.