دانشگاه صنعتی امیر کبیر
(پلی تکنیک تهران)
دانشکده مهندسی کامپیوتر

پروژه کارشناسی
گرایش هوش مصنوعی

بررسی روش های تامین امنیت سایبری در شهر هوشمند مبتنی بر اینترنت اشیا

نگارش
عرفان افشار

استاد راهنما
دکتر رضا صفا بخش

استاد مشاور
دکتر مهدی راستی

تیر ۹۹


بسم الله الرحمن الرحيم

دانشکده مهندسی کامپیوتر

باسمه تعالی

فرم اعلام آمادگی دفاع از پروژه کارشناسی

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

نام استاد پروژه :

اینجانب عرفان افشار به شماره دانشجویی (۹۶۳۱۰۰۷) آمادگی دفاع از پایان نامه خود تحت عنوان بررسی روش های تامین امنیت سایبری در شهر هوشمند مبتنی بر اینترنت اشیا را دارم. خواهشمند است نسبت به تعیین داور پروژه اقدام نمایید.

امضاء دانشجو

تاریخ ۹۹/۱/۱۶

مدیرمحترم گروه آموزشی

برگزاری دفاع از پایان نامه کارشناسی آقای عرفان افشار درتاریخ ۹۹/۳/۱۷ درمحل سالن اجتماعات دانشکده از نظر اینجانب بلامانع است.

داوران پیشنهادی عبارتند از:

۱- دکتر علی محمدی

۲- دکتر رضا علیزاده

امضاء استاد پروژه

تاریخ ۹۹/۱/۲۰

درخواستدفاع از پروژه کارشناسی آقای عرفان افشار در جلسه گروه دانشکده مورخ ۹۹/۱/۱۸ مطرح و برگزاری جلسه دفاع با حضور داورزیر به تائید رسید.

۱- دکتر علی محمدی

امضاء مدیر گروه

تاریخ. ۹۹/۱/۱۹

دانشگاه صنعتی امیرکبیر
(پلی‌تکنیک تهران)

به نام خدا

تعهدنامه اصالت اثر

تاریخ: تیر ۹۹

اینجانب عرفان افشار متعهد می‌شوم که مطالب مندرج در این پایان‌نامه حاصل کار پژوهشی اینجانب تحت نظارت و راهنمایی اساتید دانشگاه صنعتی امیرکبیر بوده و به دستاوردهای دیگران که در این پژوهش از آنها استفاده شده است مطابق مقررات و روال متعارف ارجاع و در فهرست منابع و مآخذ ذکر گردیده است. این پایان‌نامه قبلاً برای احراز هیچ مدرک هم‌سطح یا بالاتر ارائه نگردیده است.

در صورت اثبات تخلف در هر زمان، مدرک تحصیلی صادر شده توسط دانشگاه از درجه اعتبار ساقط بوده و دانشگاه حق پیگیری قانونی خواهد داشت.

کلیه نتایج و حقوق حاصل از این پایان‌نامه متعلق به دانشگاه صنعتی امیرکبیر می‌باشد. هرگونه استفاده از نتایج علمی و عملی، واگذاری اطلاعات به دیگران یا چاپ و تکثیر، نسخه‌برداری، ترجمه و اقتباس از این پایان نامه بدون موافقت کتبی دانشگاه صنعتی امیرکبیر ممنوع است. نقل مطالب با ذکر مآخذ بلامانع است.

عرفان افشار

امضا

این پروژه را به پدر و مادرم تقدیم می نمایم

سپاس گزاری

با تشکر فراوان از دکتر صفابخش و راستی بابت تمام کمک هایشان به بنده در انجام این پروژه و اتمام آن

عرفان افشار

تیر۹۹

چکیده

توسعه ی سریع شهر های هوشمند با استفاده از تکنولوژی اینترنت اشیا باعث شده است توجهات زیادی به این زمینه در دنیای فناوری جلب شود. این فناوری نو ظهور می تواند انقلابی در شهر ها ایجاد کند. به طوری که به هیچ وجه شهر های آینده با شهر های فعلی قابل مقایسه نخواهند بود. با وجود توجه فراوان به توسعه شهر ها و هوشمند سازی آنها به بحث های امنیتی مورد نیاز در این شهر ها توجه کمتری شده است. اگر شهر های مان را بدون توجه به نکات امنیتی مورد نیاز در این شهر های هوشمند کنیم در آینده مشکلات بسیار زیادی در زمینه های مختلف مانند حریم خصوصی و زندگی روزمره افراد خواهیم داشت. و در صورتی که حملات سایبری گسترده در این گونه شهر ها رخ دهد می تواند شهر هوشمند تماما کارایی خود را از دست بدهد. در حقیقت می توان گفت توسعه این شهر ها بدون توجه به نیازمندی های امنیتی کار بیهوده ای می باشد. در این نوشته ابتدا اینترنت اشیا و شهر هوشمند تا حدی تشریح شده اند سپس به بیان مشکلات و خطرات امنیتی موجود در شهر ها و خانه های هوشمند پرداخته شده است. و در انتها نیز برخی از راه ها برای تامین امنیت شهر های هوشمند مبتنی بر اینترنت اشیا بیان شده است.

واژه های کلیدی:

اینترنت اشیا ، امنیت ، شهر هوشمند ، خانه هوشمند ، حمله سایبری

فهرست مطالب

فهرست شکل ها

فصل اول

مقدمه

گسترش بی سابقه خدمات اینترنت اشیا باعث ایجاد رقابت فزاینده ای در معرفی محصولات جدید و نوآورانه برای برنامه های کاربردی شهر هوشمند شده است. توسعه دهندگان سیستم به طور معمول برای جلوگیری از از دست دادن مزیت رقابتی خود مجبور به رعایت مهلت های سختگیرانه هستند. این روند توسعه شتاب زده اغلب با الزامات امنیتی و حفظ حریم خصوصی سر و کار ندارد که بعدا می تواند به عنوان ویژگی به سیستم اضافه شود. در نتیجه این فرایند منجر به محصولاتی نا بالغ می شود که نیازهای امنیتی و حریم خصوصی برنامه های هدف خود را برآورده نمی کنند. که هر دو از اهمیت بالایی در اینترنت اشیا و به تبع آن شهرهای هوشمند برخوردار هستند[۱].

تصمیم برای تحقق بخشیدن به جنبه های امنیتی و حریم خصوصی ، دلالت بر مفهوم شهر هوشمند دارد. تحقیقات بیشتر به کاوش در برنامه های کاربردی ممکن و نتایج آن در شهرهای هوشمند متمرکز شده است. امنیت و حفظ حریم خصوصی در سیستم های شهر هوشمند تا زمان حملات غیرمنتظره اخیر و در مقیاس بزرگ مانند DDoS و تهدیدات باج افزار (مانند wannacry) به عنوان یک جنبه مهم تلقی نمی شد. پیامدهای این حملات باعث ایجاد بی اعتمادی نسبت به اینترنت اشیا شد[۱].

اینترنت اشیا و جوامع شهری هوشمند با ایجاد موج جدیدی از تحقیقات به منظور تحقیق در مورد امنیت سایبری و حریم خصوصی داده ها در چارچوب شهر هوشمند نسبت به این تحولات واکنش نشان داده اند. شرکت ها تبلیغات امن محصولات هوشمند شهر را آغاز کرده اند. با این وجود ملاحظات یاد شده در فضای مجازی شهر هوشمند بسیاری از این محصولات امن را در معرض حملات سایبری غیر متعارف قرار داده است. طراحی خدمات مستحکم و ایمن به درک جنبه های مختلف در زمینه امنیت سایبری در شهرهای هوشمند وابسته است[۱].

تحقیقات در زمینه امنیت سایبری و حفظ حریم خصوصی اینترنت اشیا در دو شاخه موازی و در عین حال مکمل پیش می رود. در شعبه اول محققان و سیاست گذاران درگیر مانند ادارات و سازمان های فدرال انواع تهدیدات را که عمدتاً از منظر اجتماعی و مالی است ، شناسایی و دسته بندی می کنند. سهم اصلی این تلاش شامل بررسی عمق و وسعت پیامدهای حملات سایبری است. و خروجی اغلب اساس سیاست ها و مقررات جدید را تعیین می کند. شعبه دوم متشکل از دانشمندان و محققان رایانه است که ابزارهای فنی را برای برآورده کردن شرایط امنیتی و حفظ حریم خصوصی مقررات شهر هوشمند بازرسی می کنند[۱].

جامعه پژوهش به این واقعیت رسیده است که اجرای فنی امنیت شهر هوشمند نیز یک مسئله چند وجهی است که در آن امنیت کلی سیستم با ضعیف ترین پیوند تعیین می شود. این مشاهده اثبات می کند که منشاء بسیاری از آسیب پذیری ها در سیستم های موجود شهر هوشمند است جایی که توسعه دهندگان به اشتباه تصور می کنند که می توانند با امنیت بخشی به سیستم و بی توجهی به دیگران امنیت محصولات خود را بهبود بخشند[۱].

یکی دیگر از مشکلات اساسی ناشی از ناهمگونی سیستم است. پروتکل ها و معماری های مورد استفاده در یک شهر هوشمند متنوع و ناسازگار است. قابلیت همکاری در بین این پیاده سازی های مختلف تضمین نشده است. این اتفاق بر جنبه های مختلف سیستم از جمله ملاحظات امنیتی و حریم خصوصی تأثیر می گذارد. این ناهمگونی همچنین حاکی از آن است که یک ابتکار عمل برای امنیت و حفظ حریم خصوصی نمی تواند به اندازه کافی جامع باشد تا نیازهای همه برنامه ها را برآورده سازد[۱].

در این گزارش تعدادی از روش های موجود برای تامین و افزایش امنیت در اینترنت اشیا و شهر های هوشمند بیان شده است. همچنین اینترنت اشیا و شهر هوشمند نیز در این نوشته تا حدودی تشریح شده اند. علاوه بر آن برخی نیازمندی های موجود در اینترنت اشیا و همچنین بعضی از خطرات موجود در شهر هوشمند پرداخته شده است.

در فصل دوم این نوشته در بخش اول آن ابتدا با اینترنت اشیا و مفهوم آن سپس دلایلی برای چرایی استفاده از آن و همچنین دلایلی برای اینکه چرا هنوز نمی توانیم از آن به خوبی استفاده کنیم می پردازیم. سپس در بخش دوم این فصل ابتدا شهر هوشمند را تعریف خواهیم کرد و سپس به بیان برخی کاربرد های فعلی اینترنت اشیا در شهر هوشمند و همچنین برخی از کاربرد های آینده اینترنت اشیا در این شهر ها خواهیم پرداخت.

در فصل سوم ابتدا در بخش اول به بیان نیازمندی های مختلف موجود در شهر هوشمند مانند احراز هویت افراد و در دسترس بودن خدمات و سایر نیازمندی ها می پردازیم. سپس در بخش دوم مسائل و موضوعات امنیتی را در سه بخش سطح پایین ، متوسط و بالا بررسی می کنیم. و در بخش آخر این فصل یعنی بخش سوم نیز به بیان برخی از خطرات موجود در شهر هوشمند مانند خطرات موجود در سیستم حمل و نقل و ساختمان های هوشمند می پردازیم.

در فصل چهارم که بحث اصلی این گزارش می باشد به بیان تعدادی از روش های مناسب برای تامین و افزایش امنیت در شهر های هوشمند مبتنی بر اینترنت اشیا می پردازیم. از جمله این روش ها می توان به استفاده از رمزنگاری ، بلاک چین و یادگیری ماشینی اشاره کرد.

در فصل انتهایی یعنی فصل پنجم نیز به تشریح خلاصه مطالب بیان شده و همچنین نتیجه گیری کلی از این مطالب و برخی پیشنهادات برای تامین امنیت در شهر هوشمند خواهیم پرداخت.

فصل دوم

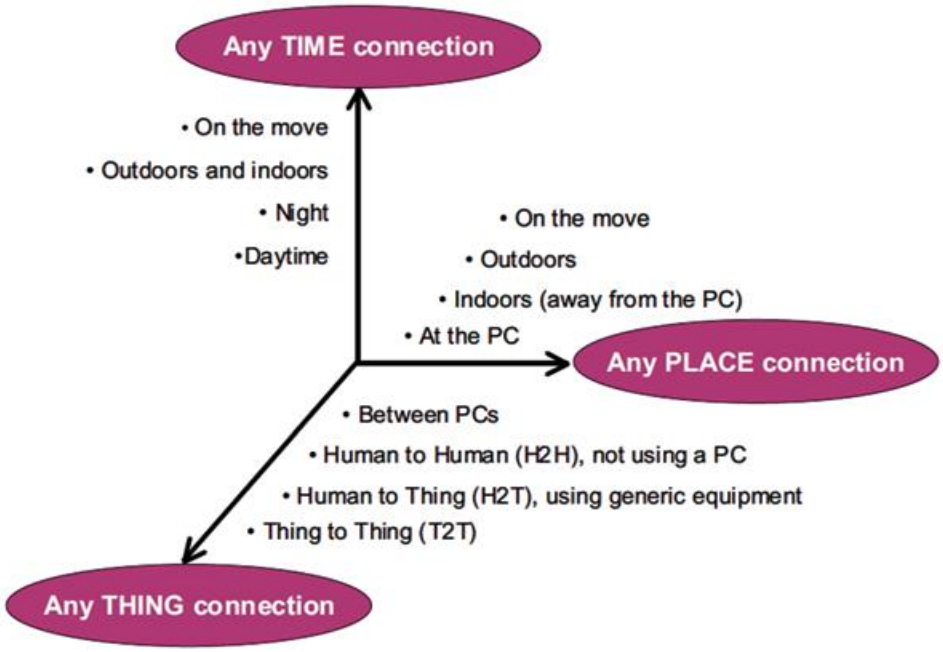
اینترنت اشیا و شهر هوشمند

در این فصل مطالبی مقدماتی در مورد اینترنت اشیا و شهر هوشمند بیان شده است. در بخش اول اینترنت اشیا را تعریف کرده و همچنین محدوده آن را مشخص می کنیم و به دلایلی که باید از این تکنولوژی استفاده کنیم می پردازیم. همچنین در ادامه به دلایلی خواهیم پرداخت که چرا در حال حاظر از اینترنت اشیا به طور کامل و همه جانبه استفاده نمی شود. و در مورد زمانی که بتوانیم به طور کامل از این تکنولوژی استفاده کنیم مطالبی خواهیم آورد. در ادامه به تعریف شهر هوشمند و چگونگی استفاده از تکنولوژی اینترنت اشیا در این شهر ها می پردازیم. و در انتها نیز به بیان تعدادی از کاربرد های فعلی و آینده اینترنت اشیا در شهر های هوشمند خواهیم پرداخت.

۲-۱ اینترنت اشیا

۲-۱-۱ اینترنت اشیا چیست ؟

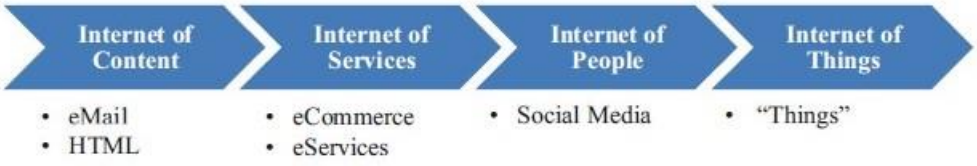
برای اینترنت اشیا تعریف مشخص و معینی وجود ندارد . در حقیقت می توان گفت که اینترنت اشیا نسل بعدی ارتباطات است که بستر آن نیز اینترنت می باشد . اینترنت اشیا به صورت کلی به این معناست که در هر زمانی ، هر چیزی با هر چیز دیگری بتوانند به تبادل اطلاعات بپردازد و فاصله فیزیکی نیز محدودیتی در این تبادل اطلاعات ایجاد نکند. همان طور که در شکل ۱ نشان داده شده است. منظور از هر چیز در تعریف گفته شده هر شی موجود در جهان مانند تلویزیون ، چراغ ها ، کولر ها و انواع دیگر اشیا موجود در جهان است که بتوانیم بر روی آن کنترل داشته باشیم[۲].



شکل ۱. گستردگی اینترنت اشیا : میزان جامع بودن تعریف اینترنت اشیا

اینترنت اشیا مانند یک جامعه انسانی است با این تفاوت که انسان ها در آن دخالت اندکی دارند و صرفا مدیریت آن را انجام می دهند و کار اصلی در این جامعه بر عهده اشیا موجود در جهان می باشد که به تبادل اطلاعات بین یکدیگر می پردازند[۲].

در فرایند تکامل اینترنت اشیا در ابتدا سیستم هایی برای انتقال محتوا بر پایه اینترنت موجود بوده است سپس به سیستم هایی برای انتقال سرویس ها بر پایه اینترنت رسیده ایم . پس از آن شبکه های اجتماعی را داریم که در آنها ارتباط بین انسان ها از طریق بستر اینترنت انجام می شود و در انتها اینترنت اشیا را خواهیم داشت که در آن بین اشیا مختلف بر بستر اینترنت ارتباط برقرار می شود.[۲]. نشان داده شده در شکل ۲.



شکل ۲. فرآیند دست یابی به اینترنت اشیا : تکامل اینترنت تا رسیدن به تکنولوژی اینترنت اشیا.

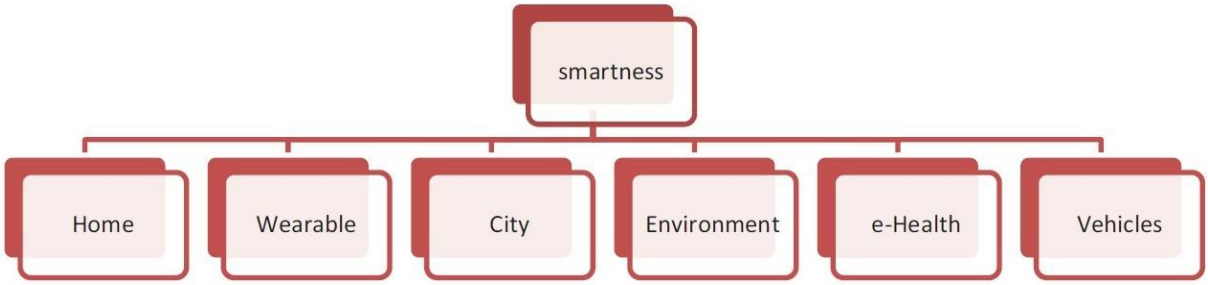
در اینترنت اشیا برای بهبود عملکرد اشیا از هوش محاسباتی استفاده می شود و سپس برای آنکه بتوانند به انتقال اطلاعات بپردازند یک بستر ارتباط شبکه ای به آنها داده می شود .نشان داده شده در شکل ۳. این بستر ارتباطات بر پایه شبکه های ابری می باشد بنابراین اشیا بر پایه یک شبکه ابری به انتقال اطلاعات می پردازند[۲].

شکل ۳. روش هوشمند سازی اشیا : ابتدا به شی هوشمندی اضافه می شود و سپس وارد شبکه می شود

۲-۱-۲ چرا از اینترنت اشیا استفاده کنیم ؟

با استفاده از اینترنت اشیا می توان زندگی روزانه راحت تر و هوشمند تری داشت . دلایل زیادی وجود دارد که اینترنت اشیا را چیزی ممکن و در دسترس می کند از جمله این دلایل وجود شبکه اینترنت به صورت گسترده در همه مکان های توسعه یافته جهان می باشد و همان طور که قبلا بیان شده است ، شبکه اینترنت زیر ساخت اینترنت اشیا می باشد . همچین پروتکل آی پی(ip) نسخه شش به ما این امکان را می دهد که به تمام اشیا موجود در جهان آدرس آی پی اختصاصی بدهیم و با این کار می توانیم تمام اشیا را از یکدیگر متمایز کنیم[۲].

کاربرد های اینترنت اشیا بسیار گسترده هستند که از جمله این کاربرد ها می توان به استفاده از آن در خانه های هوشمند ، ادارات هوشمند ، خرید هوشمند و لباس های هوشمند اشاره کرد. به عنوان مثال در حال حاضر دست بند های هوشمند را داریم که می توانند با بررسی پیوسته ، انسان را از مشکلات سلامتی اش آگاه کنند[۲].نشان داده شده در شکل ۴.

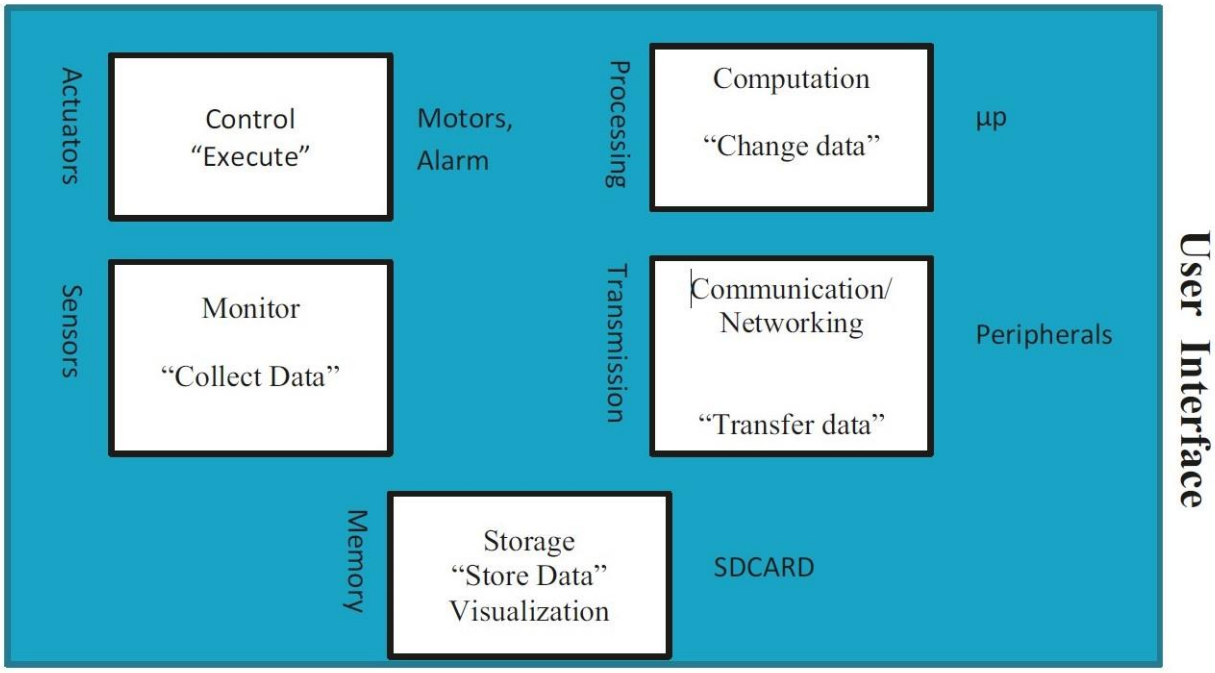


شکل ۴. کاربرد های اینترنت اشیا : استفاده از اینترنت اشیا در هوشمند سازی خانه ها و وسایل نقلیه و موارد دیگر

۲-۱-۳ چگونه از اینترنت اشیا استفاده کنیم ؟

در اینترنت اشیا هدف این است که هر چیزی که می تواند خودکار باشد ، خودکار عمل کند و این عملکرد خودکار هوشمند نیز باشد نه اینکه صرفا کنترلی بر روی اشیا وجود داشته باشد. پس برای استفاده از اینترنت اشیا نیاز داریم تا تمامی دستگاه های موجود در این شبکه ، دستگاه هایی هوشمند باشند تا بتواند کار خود را به درستی انجام دهد[۲].

اینترنت اشیا بر پایه چهار تکنولوژی سنجش ، ارتباط ، کنترل و فعال کننده ها می باشد. همان طور که در شکل ۵ نشان داده شده است. سنجش برای بررسی وضعیت محیط شی نیاز است. ارتباط به وضوح برای ایجاد ارتباط بین اشیا مختلف مورد نیاز است. کنترل برای کنترل دستگاه های مختلف موجود در شبکه اینترنت اشیا و اعمال دستورات به آنها مورد نیاز است. و فعال کننده ها نیز وسایلی مانند موتور می باشند که نقش آنها کمک به سیستم های موجود در اینترنت اشیا برای انجام عمل شان می باشد[۲].



شکل ۵. تکنولوژی های پایه اینترنت اشیا : معماری کلی اشیا موجود در شبکه اینترنت اشیا که ارتباط بین نرم افزار و سنسور ها و عمل کننده ها را نشان می دهد

برای ارتباطات بین اشیا پروتکل های زیادی وجود دارند که از جمله این پروتکل ها می توان به پروتکل بلوتوث برای فواصل نزدیک (بین سه تا شش متر)، پروتکل وای فای (Wi-Fi) برای فواصل متوسط(بین ده تا پنجاه متر) و تکنولوژی سلولار (cellular) برای فواصل دور (تا چند هزار متر) اشاره کرد[۲].

گره های شبکه اینترنت اشیا (در یک محل) با استفاده از شبکه لن (Lan) به یکدیگر متصل هستند . این شبکه ممکن است از طریق یک دروازه (gateway) به شبکه خارجی ون (Wan) متصل باشد یا اینکه صرفا محلی باشد. در صورتی که این شبکه به دنیای خارج متصل باشد می توانیم از راه دور بر روی وسایل موجود کنترل داشته باشیم. اما اگر شبکه از نوع محلی باشد صرفا می توانیم از درون شبکه با اعضای آن ارتباط داشته باشیم[۲].

اگر دو گره به دلایل و محدودیت های مختلف نتوانند بطور مستقیم با یکدیگر به تبادل اطلاعات بپردازند ، این کار را از طریق دروازه انجام می دهند ، دروازه ها همچنین توانایی ترجمه اطلاعات مختلف برای گره ها را دارند. در حقیقت عمل انتقال اطلاعات مختلف بین شبکه های مختلف برای انجام کار های مرتبط با هر شی بدون وجود دروازه ها ممکن نیست[۲].

۲-۱-۴ چه زمانی می توانیم از اینترنت اشیا استفاده کنیم ؟

به صورت کلی می توان گفت زمانی که بتوانیم بر تمام مشکلات و محدودیت های موجود در زمینه اینترنت اشیا غلبه کنیم ، می توانیم از آن به طور کامل استفاده کنیم. مشکلات موجود در این زمینه بسیار گسترده هستند و همچنین این مشکلات دسته ها و انواع متفاوتی نیز دارند و این دلایل باعث می شود که در حال حاضر نتوانیم به خوبی از اینترنت اشیا استفاده کنیم[۲].

هر سیستم اینترنت اشیا باید چهار ویژگی ساده بودن ، امن بودن ، هوشمند بودن ، مقیاس پذیر بودن را بر آورده کند. ساده بودن باعث کارایی بیشتر و گرایش بیشتر به استفاده از این شبکه می شود. امن بودن به وضوح نیازی ضروری در این شبکه است و اگر وجود نداشته باشد این شبکه به صورت کلی غیر قابل استفاده خواهد بود. هوشمند بودن وسایل برای عملکرد مناسب اجزا موجود مورد نیاز است. و در صورتی که مقیاس پذیری وجود نداشته باشد نیز نمی توانیم شبکه های بزرگ داشته باشیم که با توجه به گستردگی شبکه های فعلی امری نشدنی است[۲].

امنیت و حریم شخصی از مهم ترین چالش های موجود در اینترنت اشیا هستند . زیاد بودن تعداد اشیا ، این شبکه را مستعد حملات سایبری می کند. بنابراین نیاز به یک سطح امنیتی بالا داریم. نیاز به امنیت در زمینه های حفاظت از ابر ها ، حفاظت از ارتباطات ، حفاظت از حریم شخصی وجود دارد. اگر در هر یک از این زمینه ها امنیت کافی وجود نداشته باشد ، شبکه اینترنت اشیا با مشکلات جدی روبرو خواهد شد و همچین داده ها و حریم شخصی کاربران نیز به خطر می افتد[۲].

قابل اطمینان بودن سنسور ها یکی از محدودیت های مهم در زمینه اینترنت اشیا می باشد. در صورتی که سنسور ها قابل اطمینان نباشد می تواند کل شبکه اینترنت اشیا مختل شود. به عنوان مثال ممکن است یک سنسور تشخیص آتش سوزی ، وقوع حریق را به اشتباه تشخیص دهد و در نتیجه این تشخیص اشتباه دنباله ای از کار های بیهوده انجام می شوند و سربار اضافی برای شبکه اینترنت اشیا به وجود می آید[۲].

زمانی که تعداد اشیا زیاد باشد یکی از مشکلات اصلی توانایی شبکه برای مدیریت این اشیا می باشد و مشکل دیگر نیز مشکل مصرف انرژی در وسایل و باتری دار بودن آنها می باشد. در صورتی که مدیریت درست بر روی اشیا وجود نداشته باشد کاربر نمی تواند به خوبی از وسایل استفاده کند و از تمایلش به استفاده از شبکه کاهش می یابد. همچنین نیاز به تعویض باتری مداوم اشیا موجود در شبکه می تواند اثر مشابهی بر روی کاربر داشته باشد[۲].

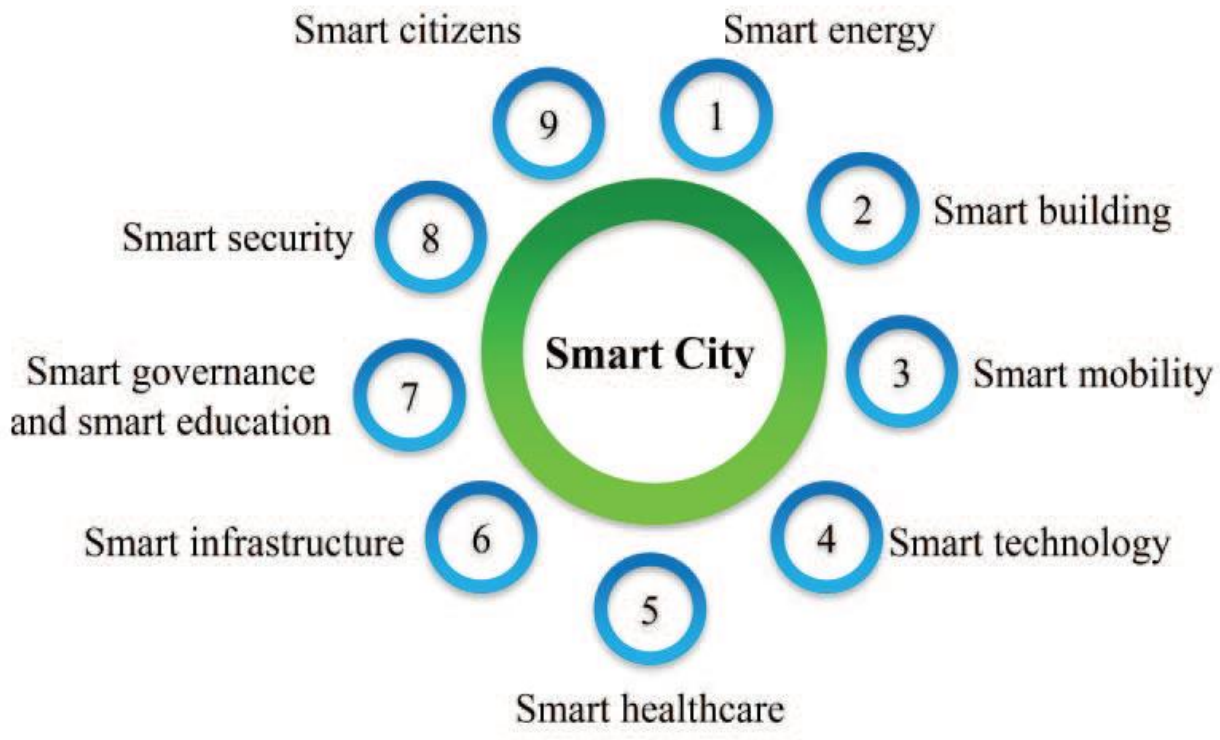
۲-۲ شهر هوشمند مبتنی بر اینترنت اشیا

۲-۲-۱ تعریف شهر هوشمند

با توجه به رشد سریع شهر ها ، نیاز به بر آورده کردن سرویس های مورد نیاز شهروندان این شهر ها ضروری است. بر این اساس درخواست برای دستگاه های دیجیتال مانند سنسور ها ، موبایل های هوشمند نیز افزایش زیادی داشته است. با استفاده از این دستگاه ها و اینترنت اشیا می توان انقلابی در شهر های جهان ایجاد کرد[۳].

اینترنت اشیا در حقیقت یک شبکه توزیع شده است که اجزای آن حافظه کم و قدرت پردازش کمی دارند. هدف آن نیز بهتر کردن قابلیت اطمینان ، کارایی و امنیت شهر های هوشمند می باشد. پس می توان گفت برای ایجاد شهر هوشمند نیاز به اینترنت اشیا داریم[۳].

شهر های فعلی نسبت به گذشته هوشمند تر شده اند دلیل آن نیز پیشرفت تکنولوژی دیجیتال می باشد. با مقایسه وضعیت فعلی جهان از لحاظ تکنولوژی با گذشته های نه چندان دور متوجه پیشرفت عظیم در این زمینه می شویم. در نتیجه در زمان کنونی امکانات موجود برای هوشمند سازی شهر ها بسیار گسترده تر از گذشته موجود است[۳]. نشان داده شده در شکل ۶.



شکل ۶. جنبه های مختلف شهر هوشمند : هوشمند سازی شهر های فعلی در زمینه های مختلف ساختمانی ، تکنولوژی ، امنیتی و دیگر زمینه ها

یک شهر هوشمند از تعدادی وسایل الکترونیکی ساخته شده است که کاربران شهر می توانند توسط برنامه های مختلف از این وسایل استفاده کنند. مانند استفاده از برنامه ای برای کنترل سیستم برق خانه . و یا این وسایل به طور خودکار عمل کرده و نقش کنترل کننده دارند و همه کاربران نمی توانند بر روی آنها کنترل داشته باشند و در آنها تغییرات ایجاد کنند مانند چراغ راهنمایی[۳].

انقلاب اینترنت زیر ساختی را فراهم می کند که در آن تعداد زیادی از مردم می توانند با یکدیگر ارتباط داشته باشند. انقلاب بعدی اینترنت امکان ارتباط مناسب بین اشیا را فراهم خواهد کرد. اینترنت اشیا تاثیر زیادی بر جنبه های مختلف زندگی مردم مانند سلامتی ، امنیت ، حمل و نقل در شهر های هوشمند خواهد داشت[۳].

۲-۲-۲ تکنولورژی اینترنت اشیا برای شهر های هوشمند

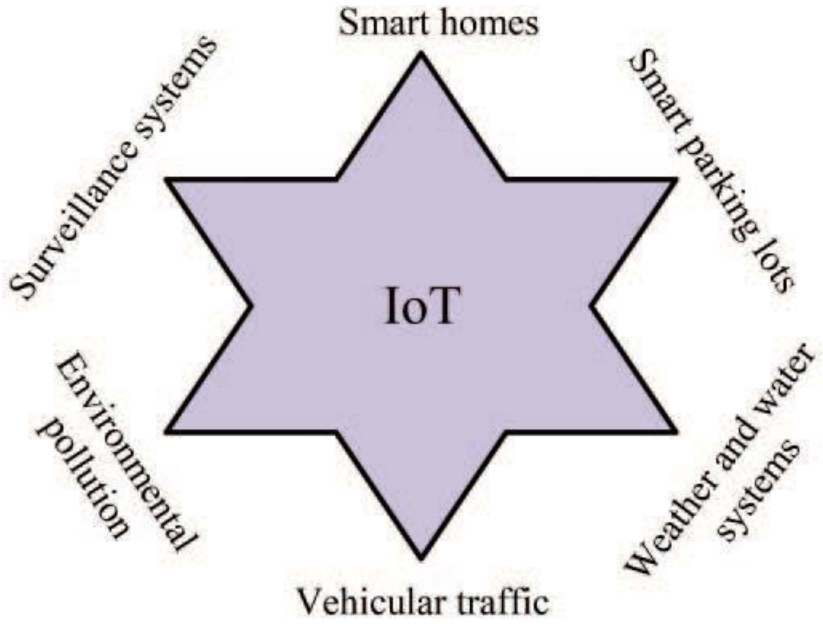
اینترنت اشیا یک شبکه است که از پروتکل های ارتباطی استاندارد استفاده می کند و نقطه همگرایی آن اینترنت است. پس در صورت نبود اینترنت با کیفیت مناسب اینترنت اشیا کاربردی نخواهد داشت[۳].

مفهوم اصلی اینترنت اشیا حضور شی هایی در سراسر جهان است که می توانند اندازه گیری کنند ، استنباط کنند و بفهمند و همچنین می توانند محیط شان را تغییر دهند. اندازه گیری به معنای هر گونه بررسی شی از وضعیت محیط اطراف خودش می باشد. استنباط کردن شی به معنای نتیجه گیری شی بر اساس اندازه گیری هایی که انجام داده است می باشد. تغییر در محیط نیز وضوح در محیط تغییری را ایجاد می کند و این تغییر بر اساس استنباط های انجام شده در مرحله قبلی خواهد بود[۳].

اینترنت اشیا از مجموعه ای از شی هایی است که یا هوشمند هستند و یا با همکاری یکدیگر یک کار مشترک را انجام می دهند. اگر این اشیا از نوع هوشمند باشند نقش شان مدیریت سایر وسایل که هوشمندی کمتری دارند و بیشتر برای انجام کار های مختلف مورد نیاز در شبکه هستند می باشد[۳].

۲-۲-۳ کاربرد های اینترنت اشیا در شهر هوشمند

اینترنت اشیا با استفاده از اینترنت بین اشیا نا همگون ارتباط برقرار می کند برای انجام این کار باید تمامی وسایل به اینترنت متصل باشند تا بتوانند اطلاعات مورد نیاز خود را گرفته و همچنین اطلاعات خود را با بقیه اشیا به اشتراک بگذارند. انواعی از کاربرد های اینترنت اشیا در شهر هوشمند به صورت زیر می باشد : نشان داده در شکل ۷..



شکل ۷. کاربرد های اصلی اینترنت اشیا : استفاده از اینترنت اشیا در زمینه های کنترل ترافیک و پیش بینی آب و هوا و غیره در شهر هوشمند

الف) خانه هوشمند

خانه های هوشمند می توانند با استفاده از داده هایی که توسط سنسور های مختلف موجود در خانه تولید می شود نظارت شوند . مثلا می توانند با استفاده از سنسور تشخیص میزان آلودگی ، صاحب خانه را از آلودگی زیاد موجود در خانه آگاه کنند[۳].

ب) پارکینگ هوشمند

با استفاده از پارکینگ های هوشمند می توان تعداد ماشین های ورودی و خروجی و همچنین زمان ورود و خروج وسایل مختلف در پارکینگ های مختلف در سطح شهر را مورد بررسی قرار داد. بنابراین این پارکینگ ها طوری طراحی می شوند که ظرفیت شان متناسب با تعداد ماشین های موجود در هر منطقه باشند . همچین پارکینگ جدید زمانی ایجاد می شود که تعداد زیادی وسیله نقلیه برای استفاده از آن موجود باشند . در نتیجه پارکینگ هوشمند برای دارندگان وسایل نقلیه و مدیران شهر هوشمند مناسب تر است[۳].

پ) سیستم آب و هوا

سیستم های بررسی وضعیت آب و هوا می توانند با استفاده از سنسور هایشان اطلاعاتی مانند دما ، باران ، سرعت باد و فشار را فراهم کنند. سپس این اطلاعات در مراکز با قدرت پردازش مناسب بررسی شده و نتیجه گیری هایی در مورد وضعیت آینده آب و هوا بدست می آید. پس با همکاری سیستم های آب و هوا کارآمدی شهر هوشمند افزایش می یابد[۳].

ت) ترافیک وسایل نقلیه

داده های مربوط به ترافیک وسایل نقلیه یکی از مهم ترین داده ها در شهر هوشمند می باشند. با بررسی و تحلیل درست این داده ها می توان به بهبود وضعیت رفت و آمد وسایل نقلیه کمکی زیادی کرد و این برای شهروندان و دولت سود بسیار زیادی خواهد داشت. شهروندان همچنین می توانند از این داده ها استفاده کرده و زمان رسیدن به مقصد شان را تعیین کنند[۳].

ث) آلودگی محیطی

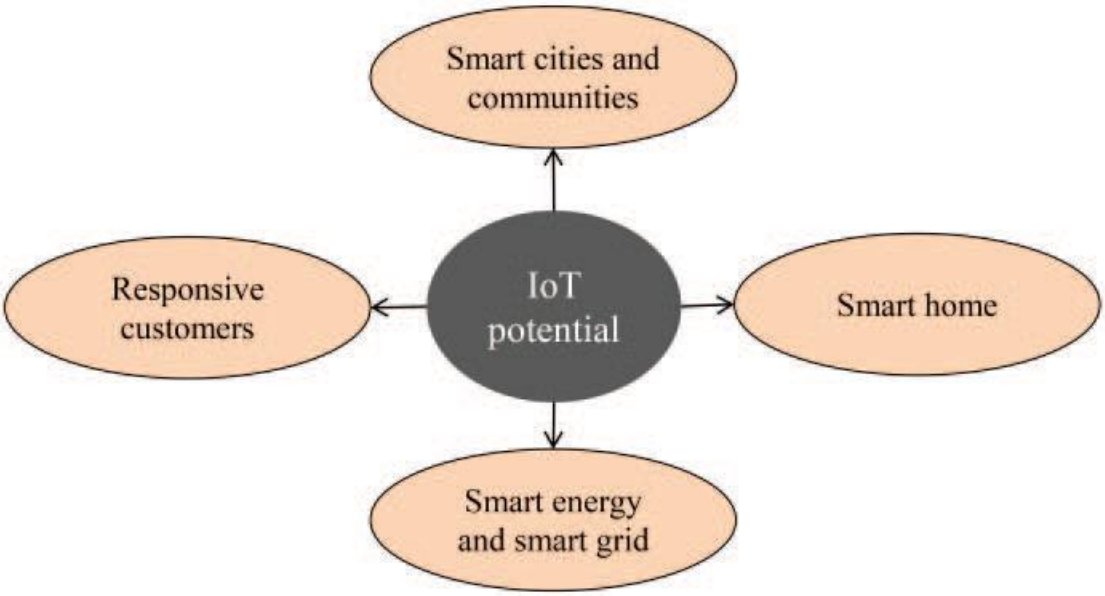
شهری که مردم آن در هوای نا سالم و آلوده باشند شهر هوشمند نیست. برای رسیدن به این مقصود شهر هوشمند باید اطلاعات مربوط به آلودگی محیط را نظارت کرده و اطلاعات مرتبط را به شهروندان برساند. مخصوصا شهروندانی که شرایط خاصی از نظر سلامتی دارند. و در صورت نیاز نیز پیشنهاد هایی را برای بهبود وضعیت هوا مانند تعطیلی بعضی از قسمت های شهر بدهد[۳].

ج) سیستم های نظارت

در شهر هوشمند امنیت مهم ترین فاکتور از دید شهروندان است. برای رسیدن به این مقصود کل شهر هوشمند باید پیوسته مورد نظارت باشد. تا اگر مورد مشکوکی یافت شد اقدامات مناسب صورت پذیرد. با این وجود تحلیل داده ها و تشخیص جرم می تواند کاملا چالش بر انگیز باشد. و کاری بسیار سخت و پیچیده است[۳].

۲-۲-۴ کاربرد های بالقوه اینترنت اشیا در شهر هوشمند

شکل ۸ برخی از برنامه های کاربردی آینده اینترنت اشیا برای شهرهای هوشمند را نشان می دهد که در این بخش مورد بحث قرار می گیرند.



شکل ۸. پتانسیل های اینترنت اشیا : کاربرد های آینده اینترنت اشیا در زمینه های خانه هوشمند و شبکه های هوشمند و دیگر زمینه ها

الف) شهر های هوشمند و اجتماعات

پیاده سازی اینترنت اشیا می تواند سرویس هایی را تولید کند که با محیط تعامل دارند . جمع آوری هوشمند داده ها فرآیند تصمیم گیری را بهبود می بخشد و به شهروندان قدرت بیشتری برای انجام کار های مختلف می دهد. علاوه بر این یک میان افزار مشترک باید برای سرویس های آینده شهر هوشمند موجود باشد[۳].

ب) خانه های هوشمند

با استفاده از اینترنت اشیا در خانه ها ، اشیا نا همگون قادر خواهند بود فعالیت هایشان را به صورت اتوماتیک انجام دهند. در حقیقت اگر اشیا را وسایل دارای اطلاعاتی در نظر بگیریم که با استفاده از اینترنتی به یکدیگر متصل هستند . ممکن است سرویس هایی را از طریق اینترنت انجام دهند . با استفاده از برنامه های کاربردی می توان از طریق اینترنت دستگاه های دیگر را از راه دور مشاهده و یا کنترل کرد[۳].

استفاده از اینترنت اشیا در زمینه کنترل روشنایی خانه و چراغ ها بسیار مورد توجه می باشد. نوزده درصد از مصرف برق جهان برای ایجاد روشنایی است. و در نتیجه شش درصد از انتشار گاز های گلخانه ای مربوط به ایجاد روشنایی می باشد. با توجه به بررسی های انجام شده انرژی مورد نیاز برای ایجاد روشنایی در صورتی که از یک سیستم هوشمند و کنترل شده برای این کار استفاده شود می تواند تا ۴۵ درصد کاهش یابد[۳].

ج) مشتریان پاسخگو

کنترل کننده های تعاملی و خیلی از وسایل هوشمند دیگر می توانند برای مدیریت خانه های هوشمند استفاده شوند . در خانه هوشمند می توان با استفاده از دروازه به کنترل کننده خانه اجازه داد که اطلاعاتش را با جمع کننده که اطلاعات را از خانه های زیادی جمع می کند به اشتراک بگذارد . با توجه به سیگنال هایی که از کنترل کننده تعاملی به جمع کننده می رسد ، جمع کننده می تواند قیمت برق مصرفی هر خانه را مشخص کند[۳].

توانایی نظارت و کنترل بر وسایل برقی خانه می تواند شرکت کردن مشتری ها در عملکرد سیستم را بهبود ببخشد . با استفاده کردن از سیستم هوشمند کاربران می توانند متوجه الگوی برق مصرفی خود بشوند و از افزایش شدید آن جلوگیری کنند[۳].

د) انرژی هوشمند و شبکه های هوشمند

استفاده از اینترنت اشیا می تواند توزیع و مصرف انرژی را در موقعیت های نا همگون به صورت هوشمند مدیریت کند . گره های اینترنت اشیا قابلیت هایی مانند ارسال اطلاعات و ارتباط با شبکه را دارند که می توانند با مدیریت هوشمند ، توزیع بار بر روی شبکه را به صورت هوشمند را کنترل کنند. این مدیریت هوشمند همچنین می تواند در زمان های بحرانی نیز مورد استفاده واقع شود[۳].

با استفاده از سیستم هوشمند می توان نقطه ای از شبکه که از کار افتاده را شناسایی کرد ، سپس آن نقطه را از مسیر سایر گره های شبکه که سالم هستند خارج کرد. در نتیجه سایر شبکه به درستی کار خواهد کرد. سپس به تعمیر قسمت از کار افتاده پرداخته می شود و پس از تعمیر آن بخش شبکه به حالت قبلی خود باز می گردد[۳].

فصل سوم

مشکلات و خطرات امنیتی در شهر هوشمند

در این فصل به بیان مطالبی در مورد خطرات امنیتی موجود در شهر های هوشمند خواهیم پرداخت. ابتدا نیازمندی های شهر هوشمند را بیان خواهیم کرد که این نیازمندی ها شامل مواردی مانند حفظ حریم خصوصی افراد و تعیین هویت افراد برای انجام کار های مختلف می باشد. سپس موضوعات امنیتی را در سه دسته مسائل امنیتی سطح پایین ، سطح متوسط و سطح بالا بررسی خواهیم کرد. همچنین در انتهای فصل به بیان برخی خطرات موجود در شهر هوشمند مانند خطرات موجود در زیر ساخت های بحرانی ، ساختمان های هوشمند ، دولت الکترونیک و غیره خواهیم پرداخت.

۳-۱ نیازمندی های امنیتی در اینترنت اشیا

برای گسترش امن اینترنت اشیا مکانیزم ها و پارامتر های مختلفی باید در نظر گرفته شده و محاسبه شوند در زیر به برخی از این مکانیزم ها اشاره شده است.

۳-۱-۱ حریم خصوصی داده ها ، محرمانه بودن و یکپارچگی

از آنجا که داده های اینترنت اشیا از طریق چندین هاپ در یک شبکه سفر می کنند ، یک مکانیزم رمزگذاری مناسب برای اطمینان از محرمانه بودن اطلاعات لازم است[۴].

وجود خدمات متنوع و داده های ذخیره شده مختلف در هر یک از دستگاه های موجود در شبکه اینترنت اشیا ، هر یک از دستگاه ها را در معرض نقض حریم خصوصی با به خطر انداختن سایر گره های موجود در یک شبکه اینترنت اشیا قرار می دهد. یک مهاجم می تواند با تغییر داده های ذخیره شده در دستگاه های آسیب پذیر برای اهداف مخرب بر یکپارچگی داده ها تأثیر بگذارد و در نتیجه داده های سیستم را نا معتبر کند[۴].

رسانه ارتباطی برای برنامه های مراقبت های بهداشتی مبتنی بر دستگاه های اینترنت اشیا پخش می شود. این در نهایت می تواند منجر به تهدیدات و مسائل مختلف حریم خصوصی شود. شخصی که از دستگاه بی سیم استفاده می کند ممکن است مشکلات جدی مانند ردیابی مکان را تجربه کند. یک دشمن می تواند ارتباطات را گوش کند. بنابراین می تواند باعث شنود اطلاعات بحرانی بیمار و ایجاد خسارت شدید برای آن شود[۵].

۳-۱-۲ تأیید اعتبار ، مجوز و حسابداری

احراز هویت بین دو طرف برای برقراری ارتباط در اینترنت اشیا لازم است. دستگاه ها برای دسترسی به سرویس ها باید احراز هویت شوند محیط هایی که از دستگاه های اینترنت اشیا پشتیبانی می کنند مشکلاتی به دلیل معماری های متنوع دستگاه های اینترنت اشیا و تنوع مکانیسم های تأیید هویت برای آنها دارند. این مشکل برای تعیین پروتکل استاندارد جهانی برای احراز هویت در اینترنت اشیا چالش بزرگی را ایجاد می کند[۴].

مکانیسم های تایید مجوز دسترسی اطمینان حاصل می کنند که دسترسی به سیستم ها یا اطلاعات صرفا به موسسه های مجاز ارائه شود. بررسی صحیح مجوز دسترسی موسسه ها و احراز هویت آنها در یک محیط باعث می شود که محیطی امن برای ارتباطات تضمین شود. مکانیسمی قابل اطمینان برای تأمین امنیت شبکه با حسابداری برای استفاده از منابع ، حسابرسی و گزارشگری فراهم می شود[۴].

۳-۱-۳ در دسترس بودن خدمات

حمله به دستگاه های اینترنت اشیا ممکن است مانع ارائه خدمات از سوی اشیا موجود در این شبکه بشود. استراتژی های مختلفی از جمله حملات سینک سوراخ ، دشمنان حریف یا حملات پخش مجدد از اجزای اینترنت اشیا در لایه های مختلف سوء استفاده می کنند . بنابراین کیفیت خدمات در اختیار کاربران اینترنت اشیا کاهش می یابد[۴].

۳-۱-۴ بهره وری انرژی

دستگاه های اینترنت اشیا معمولاً محدود به منابع هستند و دارای قدرت کمی هستند و ذخیره انرژی کمی نیز دارند. حمله به معماری اینترنت اشیا ممکن است منجر به افزایش مصرف انرژی از طریق طغیان شبکه و اتلاف منابع اینترنت اشیا از طریق درخواست خدمات اضافی یا جعلی شود[۴].

۳-۱-۵ استفاده از کلید

تنظیم کلید رمزنگاری هنگام ایجاد شبکه سنسور یک نیاز اساسی است. علاوه بر ایجاد کلید ها با همسایگان یک گره ممکن است نیاز به ایجاد کلیدهایی با گره های دیگر که به انتقال داده بین هم می پردازند نیز داشته باشد. مقیاس پذیری روش های ایجاد کلید از آنجا که زیرساخت اینترنت اشیا از صدها یا هزار دستگاه حسگر تشکیل شده است بسیار مهم است. علاوه بر این ویژگی های ذاتی شبکه های حسگر بسیاری از پروتکل های مورد استفاده در شبکه های سنتی را رد می کند. به عنوان مثال رمزنگاری کلید عمومی به دلیل قابلیت محاسباتی محدود گره های سنسور از نظر سربار سیستم گران قیمت محسوب می شود[۵].

یک روش ساده ایجاد کلید به اشتراک گذاری کلید در شبکه است. در این حالت اگر یک گره واحد در شبکه به خطر بیفتد ممکن است کلید مخفی فاش شود. بنابراین امکان رمزگشایی همه ترافیک در شبکه فراهم می شود. راه حل دیگر امکان استفاده از یک کلید مشترک مشترک برای تولید مجموعه ای از کلیدها بین هر جفت دستگاه ارتباطی و سپس پاک کردن کلید مشترک و استفاده از کلید های جدید است. در این حالت پس از استقرار اولیه هیچ گره اضافی مجاز به پیوستن به شبکه نیست[۵].

۳-۱-۶ تمامیت

حتی هنگامی که حریم خصوصی تضمین شده باشد داده ها لزوما از دستکاری خارجی محافظت نمی شوند. به عنوان مثال تغییر داده ها با اضافه کردن یا دستکاری برخی قطعات می تواند رخ دهد. در کاربرد های مهم زندگی چنین حملاتی بسیار خطرناک تلقی می شوند. و می توانند عواقب بسیار بدی داشته باشند. از طرف دیگر شبکه ارتباطی ضعیف می تواند منجر به از بین رفتن اطلاعات شود. در نتیجه شبکه ناکار آمد خواهد شد[۵].

۳-۲ طبقه بندی موضوعات امنیتی

از آنجا که اینترنت اشیا شامل طیف گسترده ای از دستگاه ها و تجهیزات اعم از تراشه های پردازش جاسازی شده کوچک گرفته تا سرورهای بزرگ رده بالا است ، باید مشکلات امنیتی را در سطوح مختلف برطرف کند. تهدیدات امنیتی را با توجه به معماری استقرار اینترنت اشیا به شکل زیر طبقه بندی می کنیم[۴].

۳-۲-۱ مسائل امنیتی سطح پایین

سطح اول امنیت مربوط به مسائل امنیتی در لایه های ارتباطی و داده های ارتباطی و همچنین سخت افزار است که در زیر شرح داده شده است.

الف) مخالفان آشفتگی

حمله به دستگاه های بی سیم در اینترنت اشیا با انتشار سیگنال های فرکانس رادیویی بدون پیروی از پروتکل خاص باعث خراب شدن شبکه می شود. تداخل رادیویی به شدت بر عملکرد شبکه تأثیر می گذارد و می تواند بر ارسال و دریافت داده ها توسط گره های معتبر تأثیر بگذارد و منجر به عملکرد نادرست یا غیرقابل پیش بینی سیستم شود[۴].

ب) اولیه سازی غیر امن

یک مکانیسم ایمن برای تنظیم اولیه و پیکر بندی اینترنت اشیا در لایه فیزیکی عملکرد مناسب کل سیستم را بدون نقض حریم خصوصی و اختلال در سرویس های شبکه تضمین می کند. همچنین لازم است ارتباط لایه فیزیکی ایمن باشد تا دسترسی آن به گیرنده های غیر مجاز غیرقابل دسترس باشد[۴].

پ) حملات سطح پایین سیبیل و کلاهبرداری

حملات سیبیل (Sybil) در یک شبکه بی سیم ناشی از گره های مخرب سیبیل است که از هویت های جعلی برای تخریب عملکرد شبکه اینترنت اشیا استفاده می کنند. یک گره سیبیل ممکن است در لایه فیزیکی از مقادیر مک (Mac) جعلی تصادفی برای محافظت در برابر دستگاههای مختلف و در عین حال با هدف از بین بردن منابع شبکه استفاده کند. در نتیجه ، گره های عادی ممکن است از دسترسی به منابع منع شوند[۴].

ت) رابط فیزیکی ناامن

چندین عامل فیزیکی تهدیدهای جدی را برای عملکرد مناسب دستگاهها در اینترنت اشیا ایجاد می کنند. ضعف امنیت فیزیکی ، دسترسی نرم افزار از طریق رابط های فیزیکی و ابزارهایی برای آزمایش / اشکال زدایی ممکن است برای سازش گره های شبکه مورد سوء استفاده قرار بگیرد[۴].

۳-۲-۲ مسائل امنیتی سطح متوسط

مسائل امنیتی سطح متوسط عمدتا مربوط به ارتباطات ، مسیر یابی و مدیریت جلسه است که در لایه های شبکه و حمل و نقل اینترنت اشیا انجام می شود ، که در زیر شرح داده شده است.

الف) حملات مجدد یا تکثیر به دلیل تکه تکه شدن

تکه تکه شدن بسته های آی پی نسخه شش برای دستگاه های سازگار با استاندارد IEEE 802.15.4 که با اندازه های فریم کوچک مشخص می شود لازم است. بازسازی زمینه های قطعات بسته در لایه 6LoWPAN ممکن است منجر به کاهش منابع ، سرریز بافر و راه اندازی مجدد دستگاه ها شود. قطعات تکراری ارسال شده توسط گره های مخرب روی مونتاژ مجدد بسته تأثیر می گذارد و از این طریق مانع پردازش سایر بسته های قانونی می شود[۴].

ب) کشف همسایه ناامن

معماری اینترنت اشیا نیاز دارد تا همه دستگاه ها به صورت منحصر به فرد در شبکه شناسایی شوند.در ارتباط پیامی که برای شناسایی بین گره ها اتفاق می افتد باید اطمینان حاصل شود که داده های منتقل شده به مقصد مشخص شده می رسند. مرحله

کشف همسایه قبل از انتقال داده ها مراحل مختلفی از جمله کشف روتر و وضوح آدرس را انجام می دهد. استفاده از بسته های کشف همسایه بدون تأیید صحیح ممکن است پیامدهای شدیدی همراه با از کار افتادن سرویس داشته باشد[۴].

پ) حمله به بافر رزرو

از آنجا که یک گره در حال دریافت داده نیاز به نگهداری فضای بافر برای مونتاژ مجدد بسته های ورودی دارد یک مهاجم می تواند با ارسال بسته های ناقص از آن سو استفاده کند. این حمله منجر به از کار افتادن سرویس می شود. زیرا سایر بسته های قطعه به دلیل فضای اشغال شده توسط بسته های ناقص ارسال شده توسط مهاجم ، دور ریخته می شوند[۴].

ت) حملات سینک سوراخ و کرم دریچه

با حملات سینک سوراخ ، گره مهاجم به درخواست های مسیریابی پاسخ می دهد ، در نتیجه مسیر یابی بسته ها از طریق گره مهاجم انجام می شود. از این طریق می توان برای انجام فعالیت های مخرب در شبکه استفاده کرد. حمله به شبکه ممکن است عملکرد آن را به دلیل حملات کرم چاله که در آن تونلی بین دو گره ایجاد می شود خراب تر کند تا بسته هایی که به یک گره می رسند به سرعت به گره دیگری برسند. این حملات پیامدهای شدیدی دارند از جمله استراق سمع ، نقض حریم خصوصی و از کار افتادن سرویس[۴].

ث) حمله سیبیل به لایه های میانی

مشابه حملات سیبیل به لایه های سطح پایین ، گره های سیبیل می توانند برای تخریب عملکرد شبکه و حتی نقض حریم خصوصی داده ها مورد استفاده واقع شوند. ایجاد ارتباط توسط گره های سیبیل با استفاده از هویت های جعلی در یک شبکه ممکن است منجر به اسپم کردن ، انتشار بدافزار یا انجام حملات فیشینگ شود[۴].

ج) احراز هویت و ارتباط امن

دستگاه ها و کاربران موجود در شبکه اینترنت اشیا باید از طریق سیستم های مدیریت احراز هویت شوند. هرگونه حفره امنیتی در لایه شبکه یا سربار زیادی برای برقراری ارتباط ممکن است شبکه را در معرض تعداد زیادی آسیب پذیری قرار دهد. به عنوان مثال به دلیل محدودیت منابع ، سربار سطح جابجایی دیتاگرام باید به حداقل برسد ، و مکانیسم های رمزنگاری شده که از برقراری ارتباط امن داده ها در شبکه اینترنت اشیا اطمینان حاصل می کنند ، باید کارایی اشیا و همچنین کمبود منابع دیگر را در نظر بگیرند[۴].

چ) سطح امنیت حمل و نقل انتها به انتها

هدف ارائه مکانیسم ایمن به گونه ای است که داده های مربوط به گره فرستنده از طریق گره مقصد مورد نظر به روشی معتبر دریافت شود. این امر به مکانیزم های تایید جامع احتیاج دارد که ارتباط پیامی ایمن را به صورت رمزگذاری شده و بدون نقض حریم خصوصی در حین کار با حداقل سربار تضمین می کند[۴].

۳-۲-۳ مسائل امنیتی سطح بالا

مسائل امنیتی سطح بالا عمدتا مربوط به برنامه های کاربردی در شبکه اینترنت اشیا است که در زیر شرح داده شده است.

الف) امنیت CoAP با اینترنت

لایه سطح بالا که شامل لایه کاربرد است نیز در برابر حملات آسیب پذیر است. پروتکل برنامه محدود که یک پروتکل انتقال وب برای دستگاه ها است از اتصال DTLS با حالتهای مختلف امنیتی برای تأمین امنیت انتها به انتها استفاده می کند. پیام های CoAP از یک فرم خاص تعریف شده در RFC-7252 پیروی می کنند ، که برای برقراری ارتباط امن باید رمزگذاری شوند. به طور مشابه پشتیبانی چند مرحله ای در CoAP نیاز به مکانیزم های ضروری مدیریت و تأیید اعتبار دارد[۴].

ب) رابط های ناامن

برای دسترسی به خدمات شبکه اینترنت اشیا رابط های مورد استفاده از طریق وب ، موبایل و ابر در برابر حملات مختلف آسیب پذیر هستند که ممکن است به شدت بر حریم خصوصی داده ها تأثیر بگذارد[۴].

پ) نرم افزار/ سیستم عامل نا امن

آسیب پذیری های مختلف در شبکه اینترنت اشیا شامل مواردی است که توسط نرم افزار / سیستم عامل ناامن ایجاد شده است. کد با زبانهایی مانند JSON، XML، SQLi و XSS باید با دقت آزمایش شود. به طور مشابه به روزرسانی های نرم افزار / سیستم عامل باید به روشی مطمئن انجام شود[۴].

ت) امنیت میان افزار

واسط اینترنت اشیا که به منظور برقراری ارتباط بین موجودات نا همگون الگوی اینترنت اشیا طراحی شده است باید به اندازه کافی برای ارائه خدمات ایمن باشد. برای ایجاد ارتباطات ایمن ، رابط ها و محیط های مختلفی باید امن بودن خود را تضمین کنند[۴].

۳-۳ خطرات امنیتی شهر هوشمند

برای بسیاری از مؤلفه های طراحی یک شهر هوشمند ، باید راه حل های مورد نیاز امنیت سایبری را نیز در نظر بگیریم.

۳-۳-۱ زیر ساخت های بحرانی

در طی چند سال گذشته ، سیستم های کنترل صنعتی به طور فزاینده ای به اینترنت وصل می شوند. سیستم های کنترل صنعتی را می توان در زیرساخت های مختلف از جمله نیروگاه های هسته ای ، نیروگاه های شیمیایی ، پالایشگاه های نفت ، سیستم های سیگنالینگ راه آهن ، توربین های بادی و غیره یافت. بسیاری از سیستم های نظارتی مانند SCADA و پروتکل های ارتباطی برای سیستم های کنترل صنعتی طراحی شده اند. سیستم SCADA از چندین ماژول سخت افزاری و دستگاه هایی مانند سرور ها ، خطوط تلفن ، واحدهای ترمینال از راه دور و کنترلر منطقی قابل برنامه ریزی تشکیل شده است[۶].

این دستگاه ها از طریق پروتکل های خاص سیستم SCADA مانند Modbus / TCP، EtherNet / IP و پروتکل شبکه توزیع شده کنترل می شوند. با این حال ، این پروتکل ها در اصل و بدون هیچ گونه اقدامات امنیتی طراحی شده اند. سوءاستفاده از آسیب پذیری ها در یک سیستم SCADA می تواند اختلال قابل توجهی در ارائه خدمات آن ایجاد کند. در سیستم های SCADA ، پروتکل های DNP3 و Modbus به سیستم نظارتی اجازه می دهند تا کنترل دستگاه های از راه دور را داشته باشد که برای کنترل ماشین ها و فرآیندها از جمله جریان آب خنک کننده در راکتور هسته ای ، موتور ها و سنسور ها استفاده می شود[۶].

در واقع ، مهندسین از مکانهای متنوع به دسترسی به این دستگاههای PLC نیاز دارند. DNP3 یک پروتکل ارتباطی است که توسط IEEE برای سیستمهای انرژی الکتریکی استاندارد شده است. Modbus پروتکل ارتباطات کنترل صنعتی است که در سال ۱۹۷۹ توسط مودیکون طراحی شده است. متأسفانه اقدامات امنیتی در طراحی اولیه DNP3 و Modbus مورد توجه قرار نگرفت[۶].

در نتیجه ، این پروتکل ها اغلب در برابر حملات سایبری مانند اجرای فرمان غیر مجاز ، حملات MITM، DoS و حمله مجدد آسیب پذیر هستند. به عنوان مثال به طور پیش فرض DNP3 هیچ مکانیسم تأیید اعتبار را بین فرستنده و دستگاههای از راه دور ارائه نمی دهد ، که می تواند منجر به عواقب خطرناکی در زیرساخت های مهم مانند سیستم توزیع آب ، سیستم توزیع گاز یا راکتور هسته ای شود. ،شرایط بحرانی نیاز به پیشبرد دارد و فایروال به طور خودکار پیکربندی سیستم SCADA را نمی آموزد[۶].

۳-۳-۲ ساختمان های هوشمند

حملات سایبری بانک ها ، شرکت ها و شبکه های دولتی را تهدید می کند. زیرساخت فناوری اطلاعات ، طراحی سیستم های کنترل ساختمان ها ، از جمله سنسور های نور و حرکت ، آبگرمکن و کولر ، پله برقی ، آشکارساز های گاز و دود ، ردیاب های نشت آب ، سیستم های امنیتی و دسترسی در دسترس شهروندان شهر هوشمند می باشد. ادغام و اتصال این سیستم های کنترل با سایر سیستم ها باعث افزایش نگرانی های امنیتی در مورد عملیات ساختمانی ، سرنشینان و مالکان خواهد شد[۶].

در ساختمان هوشمند تهدید می تواند اختلال در نظارت تصویری ، توزیع برق ، روشنایی ، برق اضطراری ، کنترل دسترسی ، آسانسور ، سیستم آتش نشانی ، کنترل آب و هوا ، نظارت و غیره باشد. هر دستگاه متصل با استفاده از برخی نرم افزارها آسیب پذیر است و هک می تواند از راه دور از طریق اینترنت انجام شود[۶].

یک مهاجم می تواند با استفاده از حمله MITM به راحتی تلویزیون هوشمند را هک کند زیرا در واقع هیچ راه حل ضد ویروس یا ضد بدافزار برای تلویزیون های هوشمند در دسترس نیست و برای برخی از مارک های تلویزیون روش احراز هویت فقط به یک آدرس آی پی نیاز دارد ، یک کنترل دسترسی به رسانه مک آدرس ، و یک نام میزبان برای تأیید اعتبار ، که به راحتی می توان آن را جعل کرد. حملات سایبری می تواند از منابع بسیاری حاصل شود منشاء آن در داخل یا خارج از یک شرکت ، توسط تروریست ها و غیره است[۶].

از پروتکل های ارتباطی مختلف در ساختمان های هوشمند استفاده می شود:

الف) BACnet پروتکل ارتباطی است که از سال ۲۰۰۳ توسط مؤسسه ملی استاندارد آمریکا و سازمان استاندارد بین المللی برای شبکه های اتوماسیون و کنترل ساختمان تهیه شده است. تعدادی از لایه های پیوند داده / لایه های فیزیکی را تعریف می کند[۶].

ب) KNX تحت استاندارد EN 50090 و ISO / IEC 14543 استاندارد شده است. این یک پروتکل ارتباطات شبکه مبتنی بر سیستم OSI برای ساختمانهای هوشمند است[۶].

پ) پروتکل ابزار دقیق کارخانه یک استاندارد اروپایی است که برای اتصال دستگاه ها در سیستم های خودکار مورد استفاده قرار می گیرد. و چندین لایه کاربردی / لینک داده / لایه های فیزیکی را تعریف می کند[۶].

با این حال ، تمام این پروتکل ها هیچگونه تدابیری در زمینه امنیت سایبری برای محافظت از ساختمان ها در برابر حملات سایبری یا مزاحمت ندارند. از این رو اقدامات امنیتی شدید باید در ساختمانهای هوشمند اعمال شود. این اقدامات باید به عنوان بخشی از یک معماری امنیتی کامل اعمال شود[۶].

۳-۳-۳ سیستم حمل و نقل هوشمند

استاندارد IEEE 1609.2 روشهای مختلفی برای ایمن سازی پیام های ویو (WAVE) در برابر استراق سمع و فریب دادن ارائه می دهد. این روشها شامل رمزنگاری کلید عمومی ، رمزنگاری منحنی بیضوی و رمزگذاری ترکیبی است. با این حال ، IEEE 1609.2 مسئله احراز هویت کاربر و حفظ حریم خصوصی کاربر را برطرف نمی کند. ارتباط نزدیکی بین نقاط شروع و انتهای سفرهای وسیله نقلیه و آدرس خانه صاحب وسیله نقلیه وجود دارد که می تواند منجر به ردیابی وسیله نقلیه شود[۶].

تلاشهای استانداردسازی فعلی بر رویکردهای مبتنی بر رمزنگاری نا متقارن متمرکز است. پیام ها با الگوریتم امضای دیجیتال Elliptic Curve (ECDSA) و گواهی کلید عمومی صادر شده توسط یک مجوز گواهی بلند مدت تأیید می شوند. هر وسیله نقلیه همچنین دارای یک گواهینامه شبه تصادفی است که به طور موقت توسط یک مجوز گواهی شبه تصادفی صادر می شود. تغییر اسم اصلی به اسم مستعار غالباً راه حل مناسبی برای حفظ حریم خصوصی مکان ارائه می دهد. اما اگر اسم های مستعار در زمان یا موقعیت نامناسب تغییر کنند ، چنین راه حل ممکن است ناکارآمد شود[۶].

۳-۳-۴ دولت الکترونیکی

مدیریت الکترونیکی یک سیستم مدرن است که توسط دولتها با استفاده از فناوری اطلاعات و ارتباطات برای پیوند نهادهای دولتی به یکدیگر و مؤسسات خصوصی اتخاذ شده است. چندین کشور دولت الکترونیک را برای ارائه خدمات الکترونیکی با کیفیت بالا به شهروندان خود تلاش کرده اند. با این حال ، براساس بررسی دولت الکترونیکی سازمان ملل متحد در سال ۲۰۱۴ ، اکثر شهروندان هنگام استفاده از خدمات دولت الکترونیکی نگران امنیت و امنیت هستند. اصلی ترین چالش های دولت الکترونیک که باید برطرف شود ، حفظ حریم خصوصی ، اعتماد و در دسترس بودن از نظر امنیت است. امنیت دولت الکترونیکی شامل خدمات امنیتی سنتی (احراز هویت ، محرمانه بودن ، صداقت و در دسترس بودن) با تأکید بیشتر بر حفظ حریم شخصی داده ها و مدیریت پیوستگی تجارت است[۶].

۳-۳-۵ سلامت الکترونیکی

خدمات پزشکی الکترونیکی سلامت توسط فرایند های الکترونیکی و ارتباطات پشتیبانی می شوند. همچنین ، متخصصان مراقبت های بهداشتی داده های بیماران را از طریق نظارت بر بیماران از طریق تلفن های هوشمند به اشتراک می گذارند ، و بیماران می توانند نسخه الکترونیکی داشته باشند. سلامت الکترونیکی به مرجع عمومی انتشار دهنده اطلاعات پزشکی یک کشور اجازه می دهد تا بحران های سلامت را با استفاده از سیستم های اطلاعاتی برای اندازه گیری ، نظارت و تصمیم گیری مدیریت کند[۶].

بسیاری از تحقیقات ، تحقیقاتی برای استفاده از شبکه های پزشکی بی سیم برای فعال کردن و بهبود کیفیت مراقبت و نظارت از راه دور پزشکی می باشند. این شبکه ها که شبکه های بی سیم بدن نیز نامیده می شوند ، با تحرک گره های شان ، استقرار شان

در شبکه و خود ساماندهی شان به افراد سالخورده ، افراد در معرض خطر و بیماران مبتلا به بیماری مزمن نظارت می کنند. با این وجود ، این شبکه ها چالش های جدید فن آوری را از نظر امنیت و حفظ حریم خصوصی باز می کنند. به عنوان مثال ، انتقال سیگنال الکتروکاردیوگرام بدون رمزگذاری تأثیر بزرگی بر حریم شخصی خواهد گذاشت[۶].

روش های متداول شامل الگوریتم های تبدیل گسسته ، تبدیل موجک و تجزیه فوری سازگار است. با این حال ، برای کاربردهای سلامت الکترونیکی ، عملکرد این روشها به کارآیی فشرده سازی (یعنی ، نسبت بین سیگنال اصلی با سیگنال بازیابی شده) ، کیفیت بازسازی (تفاوت بین سیگنال اصلی با سیگنال بازیابی شده) بستگی دارد. یافتن راه حل کارآمد یک چالش جدی است. از طرف دیگر ، انتقال به محیط ابر و ذخیره داده های سلامت بیمار در سرورهای شخص ثالث یک تهدید جدی برای حفظ حریم خصوصی داده ها است[۶].

دستگاههای بهداشت الکترونیکی که از برنامه های مراقبت های بهداشتی پشتیبانی می کنند ، به دلیل پردازنده های کم سرعت در سنسور ها و تلفن های هوشمند ، محدودیت حافظه ، محدودیت انرژی و نگرانی در مورد تحرک ، با محدودیت های مختلفی از جمله محدودیت های محاسباتی روبرو هستند. بنابراین ، تحقیقات بیشتر در مورد الگوریتم های امنیتی قوی که مصرف منابع را به حداقل می رسانند و عملکرد امنیتی را به حداکثر می رسانند (همراه با مصرف انرژی کارآمد) مورد نیاز است[۶].

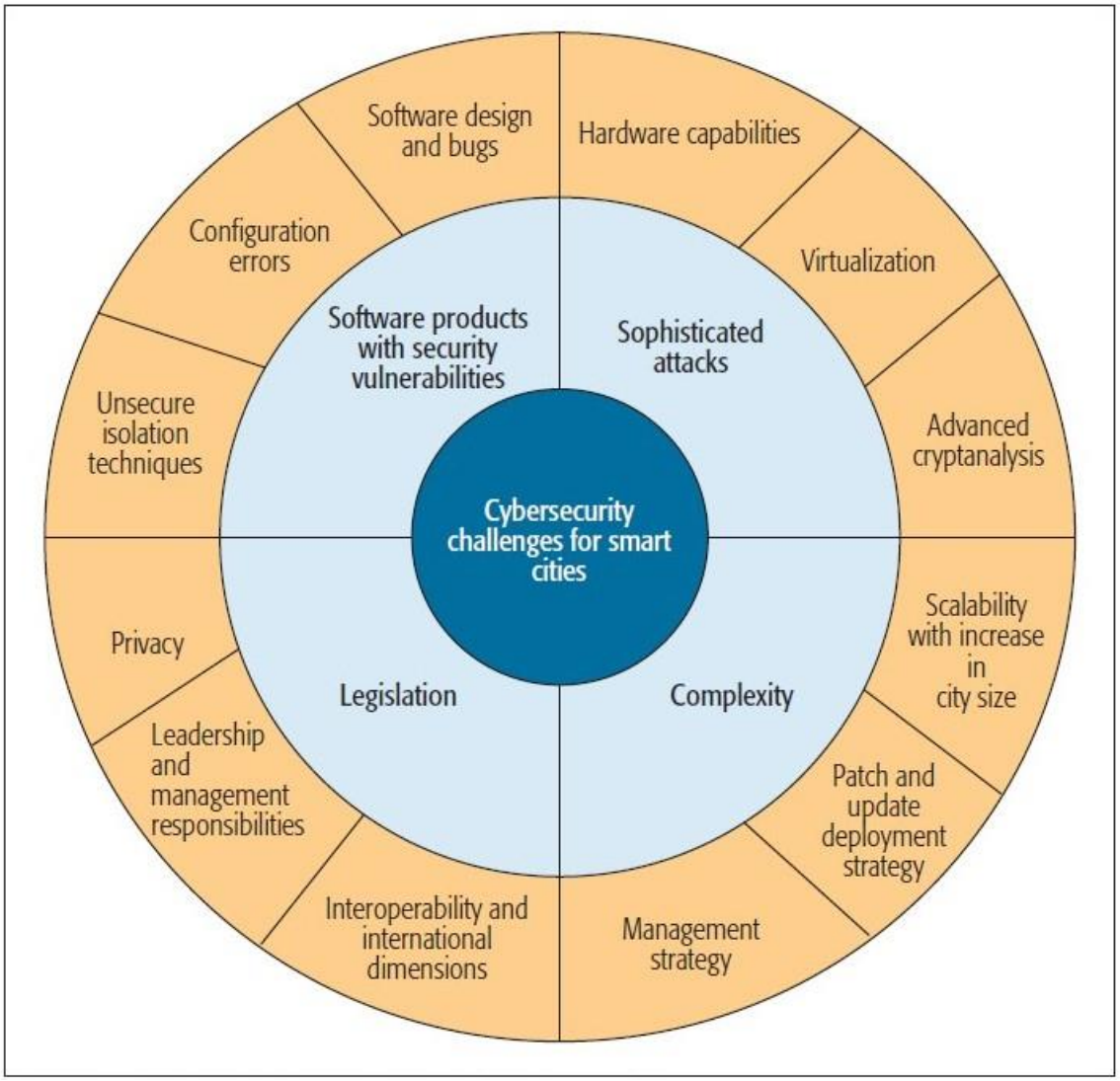
۳-۳-۶ اینترنت اشیا

چالش های کلیدی مهم اینترنت اشیا مانند نا همگونی ، قابلیت همکاری ، مقیاس پذیری ، امنیت و حفظ حریم خصوصی ، قابلیت اطمینان ، عدم درک مدلهای تجاری جدید و استانداردهای بیشمار فن آوری رقیب وجود دارد که باید در آینده مورد توجه قرار گیرند[۶].

در پیش نویس IETF ، نویسندگان معماری امنیتی و خدمات امنیتی (تأیید اعتبار ، تبادل کلید و یکپارچگی داده) اینترنت اشیا و مدل استقرار آن را تعریف می کنند. آنها پیشنهاد می کنند آنچه که در واقع مناسب ترین پروتکل برای اینترنت اشیا است ، پروتکل محدودیت کاربرد بر روی امنیت لایه های انتقال دیتاگرام است[۶].

CoAP یک پروتکل لایه سبک وزن است که به دلیل نیاز به پهنای باند کم ، مخصوصاً برای شبکه های آی پی محدود مناسب است. این امر به افزایش قابلیت اطمینان (با کاهش قطعه قطعه شدن در لایه ۲) و کاهش تأخیر در شبکه های بی سیم کم مصرف مانند IEEE 802.15.4 کمک می کند. در کنار دیدگاه های استاندارد سازی اینترنت اشیا ، نیاز به یکپارچه سازی فن آوری های نوظهور مانند محاسبات ابری ، داده های بزرگ ، شبکه تعریف شده توسط نرم افزار و مجازی سازی توابع شبکه وجود دارد. با این حال ، این ادغام خطرات و آسیب پذیری هایی را از دیدگاه امنیتی به همراه می آورد. به طور کلی ، معرفی فناوری اطلاعات و ارتباطات در شهرهای هوشمند منجر به نگرانی های مختلف امنیتی و حریم خصوصی می شود[۶].

همانطور که در شکل ۹ نشان داده شده است ، ما چهار چالش اصلی برای یک معماری امنیت سایبری برای شهرهای هوشمند را شناسایی کردیم: حملات پیشرفته ، اشکالات و آسیب پذیری های محصولات نرم افزاری ، مسائل مربوط به قانونگذاری و پیچیدگی[۶].



شکل ۹. چالش های امنیتی در شهر هوشمند : چهار گروه عمده خطرات امنیتی موجود در شهر هوشمند که شامل حملات پیشرفته ، اشکالات و آسیب پذیری های محصولات نرم افزاری ، مسائل مربوط به قانونگذاری و پیچیدگی می باشد.

حملات پیشرفته به دلیل قابلیت های سخت افزاری ، مجازی سازی و تکنیک های پیشرفته رمزنگاری است که به طور فزاینده ای در حملات شبکه استفاده می شوند[۶].

محصولات نرم افزاری با آسیب پذیری های امنیتی به دلیل ضعف / نقص طراحی نرم افزار ، خطاهای پیکربندی و یا تکنیک های جداسازی نا ایمن وجود دارند[۶].

درمورد مسائل مربوط به قانونگذاری ، در صورت عدم بررسی قوانین موجود با توجه به مطالبات جدید (به عنوان مثال ، حفظ حریم خصوصی کاربر ، رهبری شهرهای هوشمند) قوانین برای شهرهای هوشمند نمی توانند توسعه یافته و به درستی اعمال شوند[۶].

سرانجام الزامات امنیتی ، حملات جدید و مسائل مربوط به قانون در کنار هم پیچیدگی مدیریت یک شهر هوشمند را بیشتر می کند[۶].

فصل چهارم

روش های تامین امنیت

در این فصل به طور خاص به بیان روش ها و شیوه هایی برای تامین و افزایش امنیت در شهر های هوشمند خواهیم پرداخت. به عنوان مثال با رمزنگاری کردن پیام های مختلف می توان امنیت موجود در شهر هوشمند را افزایش داد و یا با استفاده از فناوری نو ظهور بلاک چین می توان با احتمال بسیار بالایی جلوی کار های تقلبی و خلاف کارانه در شبکه اینترنت اشیا را گرفت. و همچنین با روش های دیگر مانند استفاده از یادگیری ماشینی و نظریه بازی آشنا خواهیم شد.

۴-۱ رمزنگاری

الگوریتم های رمزنگاری ستون اصلی امنیت و محافظت از حریم خصوصی خدمات برنامه های هوشمند هستند. چون از دسترسی طرفین غیر قابل اعتماد به داده های ذخیره شده ، پردازش و به اشتراک گذاری آنها جلوگیری می کنند. در این زیر بخش ، ما سعی داریم تا خلاصه ای از ابزارهای رمزنگاری کنونی که برای سیستم های هوشمند به کار رفته را تشریح کنیم[۷].

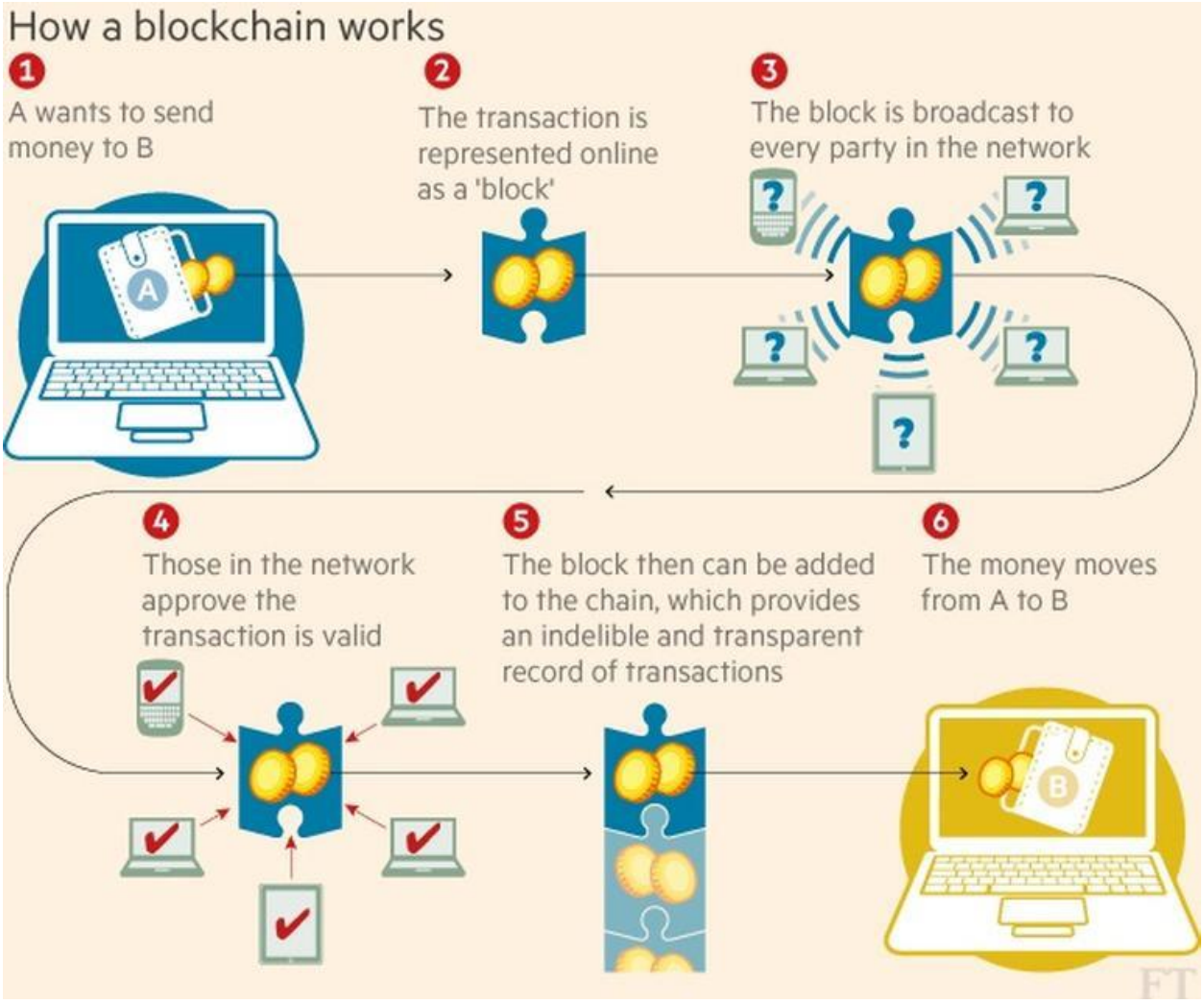
به دلیل پیچیدگی محاسباتی و مصرف انرژی ، الگوریتم و استانداردهای رمزگذاری سنتی برای دستگاههای محدود کننده منابع کاملاً مناسب نیستند. بنابراین رمزنگاری سبک وزن در عمل به یک نیاز اساسی برای کاربرد فناوری های رمزنگاری تبدیل شده است. اخیرا یک مکانیسم احراز هویت سبک برای سناریوی اینترنت اشیا ایجاد شده است که می تواند ارتباطات کاربران نهایی را از حملات DDoS محافظت کند[۷].

قابل توجه است که رمزنگاری هومورفیک که محاسبات مربوط به داده های رمزگذاری شده را قادر می سازد خدمات مختلفی را بدون در خطر قرار دادن داده های حساس انجام دهند ، توجه بیشتری را به خود جلب کرده است. به عنوان مثال HE می تواند برای محافظت از تجمع مصرف برق در یک سیستم شبکه هوشمند ، محافظت از حریم خصوصی و حل مسائل امنیتی رایانش ابری استفاده شود. اما هزینه محاسباتی بالا محدودیت این روش محسوب می شود[۷].

اثبات دانش صفر ، روشی دیگر است که در حوزه رمزنگاری استفاده می شود تا یک طرف بتواند بدون انتقال اطلاعات دیگر چیزی را به طرفهای دیگر اثبات کند. اثبات دانش صفر می تواند برای رسیدگی به مسائل تأیید اعتبار استفاده شود. به عنوان مثال ، از مدارک صفر دانش برای تهیه پروتکل تأیید هویت کارآمد برای کارتهای هوشمند استفاده شده است[۷].

۴-۲ بلاک چین

گرچه تکنیک بلاک چین یک فناوری خاص است و نه یک رشته ، اما به دلیل افزایش چشمگیر علاقه به آن در سالهای اخیر از این زیر مجموعه برای معرفی آن استفاده می شود. شیوه کار نشان در شکل ۱۰ نشان داده شده. بررسی جامع در این زمینه در سال ۲۰۱۶ انجام شد. که قابلیت تحقق استفاده از بلاک چین در حوزه اینترنت اشیا را تأیید کرد. و ارزش کاربرد قابل توجه آن را در اکوسیستم اینترنت اشیا در حال توسعه نشان داد. دلیل اصلی محبوبیت بسیاری از برنامه های اینترنت اشیا مبتنی بر بلاک چین ویژگی غیر متمرکز بودن بلاک چین است که برنامه ها را قادر می سازد تا به صورت توزیع شده کار کنند[۷].



شکل ۱۰. شیوه کار بلاک چین : برای انتقال پول از فرستنده به گیرنده این انتقال ابتدا در یک بلاک ثبت می شود سپس این اعتبار این بلاک توسط تعدادی ناظر بررسی شده و در صورت صحت به زنجیره ای از بلاک های ماندگار اضافه می شود.

در سال های اخیر یک چارچوب امنیتی مبتنی بر بلاک چین ایجاد شده است که هم می تواند امنیت ارتباطی دستگاه ها در یک شهر هوشمند را تضمین کند و هم قابلیت اطمینان و کارایی سیستم را بهبود بخشد. همچنین فن آوری یکپارچه بلاک چین و خانه هوشمند می تواند به هدف محرمانه بودن ، صداقت و در دسترس بودن دست یابد. در مطالعه دیگری مسائل امنیتی در سیستم های ارتباطی وسایل نقلیه از طریق ساختار بلاک چین مورد بررسی قرار گرفته است[۷].

برخی محققان از مزایای استفاده از بلاک چین و فن آوری شبکه تعریف شده نرم افزاری استفاده کردند تا یک معماری توزیع شده جدید را رعایت کنند که از اصول طراحی مورد نیاز مانند مقاومت ، کارایی ، سازگاری ، مقیاس پذیری و امنیت استفاده کند. واضح

است اگرچه فناوری بلاک چین در سالهای اخیر به موضوعی داغ تبدیل شده است و به کاربردهای قابل اطمینان تر و راحت تری منجر شده است اما هنوز در زمینه اینترنت اشیا در مراحل اولیه قرار دارد. ما برای برطرف کردن نگرانی های جدی درباره حفظ حریم خصوصی و امنیت باید تلاش کنیم بهترین استفاده را از این فناوری ببریم[۷].

۴-۳ بیومتریک ها

بیومتریک به طور گسترده ای در سیستم های مبتنی بر اینترنت اشیا برای تأیید اعتبار مورد استفاده است. به طور خاص ، از این فناوری می توان برای شناسایی خودکار یک شخص از طریق خصوصیات رفتاری و بیولوژیکی منحصر به فرد استفاده کرد. داده های زیستی از اثر انگشت ، صورت ، صدا ، امضا های دستی و غیره استخراج می شوند[۷].

برای محافظت از اطلاعات محرمانه کاربران در دستگاههای ذخیره سازی ، یک پروتکل مهم مذاکره و احراز هویت متقابل پیشنهاد شده است. این پروتکل جدید نه تنها حملات امنیتی را شکست می دهد بلکه در مقایسه با سایر سیستم های مرتبط هزینه ارتباطی قابل قبولی را نیز دارد. یکی دیگر از ویژگی های قابل توجه این است که اگر این روش های مبتنی بر زیست شناختی به طور مناسب استفاده نشوند خطر نقض حریم خصوصی افزایش می یابد. همچنین آینده امید بخش برای استفاده از بیومتریک در برنامه های دیگر مانند تجارت الکترونیکی وجود دارد[۷].

۴-۴ یادگیری ماشینی و استخراج اطلاعات

در موقعیت های عملی فعلی از فن آوری های یادگیری ماشینی برای بهبود کارآیی سیستم های تشخیص نفوذ استفاده شده است که یکی از متداول ترین زیر ساخت های امنیتی برای محافظت از شبکه ها در برابر حملات است. شبکه حسگر بی سیم که جزء اصلی جهان هوشمند است توجه بیشتری را به خود جلب کرده است. همچنین یک مطالعه جدید با استفاده از یک مدل استخراج و انتخاب برای شناسایی حملات در شبکه های وای فای ایجاد شده است که دارای سرعت بالایی است. علاوه بر روشهای امنیتی شبکه محور در سالهای اخیر چند فناوری یادگیری ماشینی کاربر محور برای تجزیه و تحلیل ، پیش بینی و تصمیم گیری های شخصی استفاده شده است[۷].

شبکه های حسگر و تلفن های هوشمند که به سرعت در حال گسترش هستند ، شهروندان را در معرض بسیاری از نگرانی های مربوط به حریم خصوصی و امنیتی قرار داده است. SVM برای طراحی سیستم احراز هویت مبتنی بر چند حسگر برای کاربران تلفن های هوشمند پذیرفته شده است. که ایده اصلی آن یادگیری الگوهای رفتاری کاربران و ویژگی های محیطی مربوطه است. اخیرا محققان یک مکانیزم جدید اجازه برای سیستم عامل های تلفن همراه بر اساس فناوری یادگیری ماشینی ایجاد کرده اند[۷].

با این حال تلاشهای مشابه یک مشکل مشترک دارند. داده های مورد استفاده برای تجزیه و تحلیل نمی توانند از ذهنیت شرکت کنندگان جلوگیری کنند و ممکن است به اندازه کافی وضعیت را در یک محیط واقعی منعکس نکنند[۷].

به صورت کلی بسیاری از استراتژیهای دفاعی توسط فن آوری های یادگیری ماشینی تقویت می شوند. محققان یک مدل نظریه بازی را از طریق یادگیری ماشینی معرفی کرده اند تا با استفاده از فن آوری های یادگیری ماشینی تقویت شود[۷].

در زمینه داده کاوی یک بررسی جامع نشان داده است که مقادیر زیادی از داده های جمع آوری شده توسط بسیاری از سنسور ها و دستگاه های اطراف مصرف کنندگان برای استخراج مقررات و اطلاعات جدید برای ارائه خدمات بهتر استفاده می شود. با این حال ، برخی از نگرانی های امنیتی و حریم خصوصی ناشی از فناوری های داده کاوی است زیرا ممکن است اطلاعات حساس مانند مکان کاربران و بیماری های رفتاری فاش شود. برای کاهش این گونه مشکلات برخی از فناوریهای حفظ حریم خصوصی داده کاوی در سالهای اخیر توسعه یافته اند[۷].

۴-۵ نظریه بازی

نظریه بازی یک ابزار قدرتمند ریاضی در زمینه های امنیت سایبری و محافظت از حریم خصوصی در سناریو های مختلف می باشد.

یک بررسی جامع ویژگی های رویکرد نظریه بازی و مزایای آن را در مقایسه با مکانیسم های دفاعی سنتی که در زیر شرح داده شده است گزارش داده است.

۱) ریاضیات اثبات شده

۲) دفاع قابل اعتماد

۳) اقدام به موقع

۴) راه حل های توزیع شده

پیش بینی می شود ، علاقه به استفاده از تئوری بازی برای پرداختن به مسائل امنیتی و حریم خصوصی در برنامه های مبتنی بر اینترنت اشیا در سال های آینده افزایش یابد. در یک کار تحقیقاتی دستگاه های کم مصرف هدف قرار داده شده اند و یک روش تشخیص نا هنجاری سبک پیشنهاد شده است که هم صحت را تضمین می کند و هم مصرف انرژی را کاهش می دهد. این مدل قابلیت سازگاری با برنامه های اینترنت اشیا جدید در حال ظهور مانند مراقبت های بهداشتی هوشمند ساختمان های هوشمند و شبکه های حسگر را دارد[۷].

یک مقاله اخیر یک بازی Honeypot را برای رفع مشکلات حمله در شبکه های پیشرفته زیرساخت اندازه گیری معرفی کرد. کار دیگری که انجام شده است یک بازی با مبلغ صفر را برای شناسایی حملات جعل هویت در شبکه های بی سیم به کار گرفته است[۷].

با توجه به مباحث حفظ حریم خصوصی ، بسیاری از مطالعات با ترکیب تئوری بازی با سایر فناوری های محافظت از حریم خصوصی ساز و کار هایی را ایجاد می کنند. علاوه بر این نظریه بازی ابزاری مؤثر برای ایجاد تعادل بین شدت حفاظت از اطلاعات و به اشتراک گذاری آنها می باشد[۷].

اگرچه مطالعات کمتری نظریه بازی را برای یک برنامه شهر هوشمند به کار گرفته اند و بسیاری از فناوری ها در محدوده امنیت اینترنت اشیا توسعه داده شده اند. اما در آینده با تکامل سریع شهرهای هوشمند همه چیز متصل رویکرد های نظریه بازی نقش مهمی را ایفا خواهند کرد. که نقش آنها حل برخی از مسائل جدید امنیتی و حریم خصوصی در این دوره هوشمند می باشد[۷].

۴-۶ راه های غیر فنی

استفاده از راه حل های فنی به تنهایی برای محافظت کافی نیست. محدودیت های فناوری موجود با تقویت سیاست های مربوطه ، مقررات ، حاکمیت ، آموزش و غیره قابل کاهش است. حکمرانی سالم از منظر حاکمیت و سیاست برای ایجاد یک سیستم هوشمند قابل اعتماد بسیار مهم است[۷].

با توجه به اینکه داده ها را می توان رمزگشایی کرد دولتها وظیفه دارند بررسی کنند که چه کسی حق دسترسی به این داده ها را دارد. مقررات اجرا شده توسط دولت باید از داده ها و توسعه مدل در چارچوب شهر هوشمند محافظت کند[۷].

آموزش به منظور بهبود مهارت های مرتبط با تولید کنندگان ، ارائه دهندگان خدمات و کاربران نیز مهم است. به عنوان مثال طراحان برنامه توانایی توسعه کد گذاری پایدار و انعطاف پذیر را باید از طریق آموزش کسب کنند. فروشندگان وظیفه به روزرسانی دیوارهای آتش برای رفع آسیب پذیری ها دارند. علاوه بر این تولید کنندگان دستگاه باید تا حد امکان سطح کلی ایمنی و استانداردهای کیفیت را ارتقاء دهند[۷].

هدف از برنامه های آموزش غنی سازی دانش شهروندان در مورد نحوه عملکرد برنامه های هوشمند و چگونگی محافظت از خود است. با این حال اثربخشی این آموزش ها همچنان یک چالش است. اگر چه برخی از کاربران مضرات احتمالی نشت حریم خصوصی را می شناسند اما نگرانی ها را برای راحتی استفاده نادیده می گیرند[۷].

فصل پنجم

نتیجه گیری و پیشنهاد ها

مفهوم شهر هوشمند مدرن فراتر از آنچه در این نوشته بحث شده است به نظر می رسد. شهر هوشمند اکنون نقش اساسی در اقتصاد ، دولت ، گردشگری ، آموزش و غیره دارد. بخشی از این سرویس های نوظهور را می توان تحت برنامه های سنتی قرار داد. به عنوان مثال ، خانه های هوشمند از نزدیک با ساختمان هوشمند و محیط های هوشمند درگیر هستند.

شبکه هوشمند وسایل نقلیه الکتریکی را با حمل و نقل هوشمند و با خانه هوشمند و مراقبت های بهداشتی هوشمند (از طریق سیستم های مدیریت انرژی و کنترل ترافیک در مواقع اضطراری) پیوند می دهند. این یکپارچه سازی خدمات باعث ایجاد اختلافات امنیتی مختلف می شود. ماهیت پویا و نا همگن شهر هوشمند پزشکی قانونی دیجیتال را ناکارآمد می کند. تعیین صلاحیت اشخاص مختلف براساس داده ها هنگام سفر در ایالت ها ، کشورها و سازمان های مختلف دشوار می شود.

پیشرفت های اخیر فن آوری در شعاع شهر هوشمند تهدیدات امنیتی پیش بینی نشده ای را به همراه دارد. سبد خرید ها ، هوش مصنوعی ، وسایل نقلیه هوشمند و واقعیت مجازی چالش های امنیتی اضافی را به وجود می آورند. هوش مصنوعی به دشمنان این امکان را می دهد تا دانش حساس را از داده های غیر حساس استخراج کنند.

علاوه بر این اتکای الگوریتم یادگیری ماشین به داده های ورودی (اغلب اوقات با روشی غیرقابل پیش بینی) آنها را در مقابل حملات دستکاری داده ها آسیب پذیر می کند تا جایی که مخالفان می توانند ورودی به ظاهر اصیل تولید کنند که الگوریتم را فریب دهد.

وابستگی وسایل نقلیه هوشمند به فناوری اطلاعات و ارتباطات و وسایل الکترونیکی این فرصت را به مهاجمان می دهد تا بتوانند کنترل وسیله نقلیه را به دست گیرند و امنیت و ایمنی سرنشینان و سایر رانندگان را به خطر اندازند. برنامه های واقعیت مجازی اغلب تمایل به از بین بردن حریم خصوصی دارند. همه آسیب پذیری ها با کمبود نرم افزار / سخت افزار همراه نیستند. در حقیقت یک چارچوب امنیتی همه جانبه باید بر خطاهای انسانی (چه عمدی و چه غیر از آن) مدیریت کند.

تعیین نقش های امنیتی افراد به طور واضح بسیار حائز اهمیت است. و شهرها باید برای رهبری امنیتی ارزش قائل باشند و تیم های امنیتی ویژه ای را برای انجام اقدامات امنیتی روزمره از جمله آموزش ، به روزرسانی سیستم عامل ، تدوین برنامه های واکنش اضطراری ، حفظ ارتباط با فروشندگان و ارائه دهندگان خدمات مختلف و غیره تشکیل دهند.

با وجود آنکه در سال های اخیر توجه بیشتری نسبت به گذشته به بحث های امنیتی در زمینه های اینترنت اشیا و شهر هوشمند شده است. اما باید به این نکته توجه داشته باشیم که پیشرفت شهر های هوشمند نا امن در حقیقت فایده زیادی ندارد. علت آن نیز مشخصا نبود امنیت و آسایش در شهر و در نتیجه نبود آرامش برای مردم برای زندگی در این شهر ها می باشد.

هدف از این پژوهش به صورت کلی آگاه سازی خوانندگان از خطرات موجود در هوشمند سازی شهر ها با سرعت زیاد و بدون توجه به نکات امنیتی موجود در این شهر ها می باشد. همان طور که در گزارش نیز اشاره شده است نبود امنیت در شهر های هوشمند می تواند این شهر ها را با مشکلات جدی ای رو به رو کند تا حدی که حتی این شهر ها را بلا استفاده کند. و در انتها نیز تعدادی از راه های موجود برای افزایش امنیت در شهر های هوشمند بیان شده است. تا خوانندگان با این روش ها آشنا شوند. در نتیجه در هنگام توسعه شهر های هوشمند با استفاده از تکنولوژی اینترنت اشیا باید توجه ویژه ای به مباحث امنیتی نیز داشته باشیم و صرفا

به استفاده های مختلف از این فناوری توجه نکنیم. روشی که برای افزایش امنیت در شهر های هوشمند پیشنهاد می شود استفاده از روش های فوق به صورت همزمان است. به طوری که مثلا همزمان از بلاک چین و یادگیری ماشینی در بهبود امنیت استفاده شود. نه اینکه صرفا بخواهیم با استفاده از یک روش به بهبود وضع امنیتی موجود بپردازیم و دیگر روش ها را نادیده بگیریم.

منابع و مراجع

[1] Habibzadeh, H., et al., *A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities.* Sustainable Cities and Society, 2019. **50**: p. 101660.

[2] Mohamed, K.S., *The Era of Internet of Things*. 2019: Springer International Publishing.

[3] Arasteh, H., et al. *Iot-based smart cities: a survey*. in *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*. 2016. IEEE.

[4] Khan, M.A. and K. Salah, *IoT security: Review, blockchain solutions, and open challenges.* Future Generation Computer Systems, 2018. **82**: p. 395-411.

[5] Alromaihi, S., W. Elmedany, and C. Balakrishna. *Cyber security challenges of deploying IoT in smart cities for healthcare applications*. in *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. 2018. IEEE.

[6] Khatoun, R. and S. Zeadally, *Cybersecurity and privacy solutions in smart cities.* IEEE Communications Magazine, 2017. **55**(3): p. 51-59.

[7] Cui, L., et al., *Security and privacy in smart cities: Challenges and opportunities.* IEEE access, 2018. **6**: p. 46134-46145.

واژه نامه فارسی به انگلیسی

آی پی ---------- IP

دروازه ---------- gateway

سلولار ---------- cellular

لن ---------- Lan

مک ---------- Mac

وای فای ---------- Wi-Fi

ون ---------- Wan

واژه نامه انگلیسی به فارسی

Ip ---------- آی پی

Cellular ---------- سلولار

gateway ---------- دروازه

Wi-Fi ---------- وای فای

Lan ---------- لن

Wan ---------- ون

Mac ---------- مک