شهر هوشمند

مقدمه‌ای بر شهر هوشمند و بررسی چالش‌های امنیتی آن

چکیده

امروزه، اینترنت، بستر گسترده‌ای را جهت ارتباطات بشر، حتی در فواصل طولانی، فراهم آورده‌است. انسان توانسته است به کمک این ارتباط، به روشی جالب جهت کنترل و اداره‌ی اشیا دست پیدا کند و با در اختیار داشتن یک سرور مرکزی، اشیای پیرامون خود را کنترل نماید و اطلاعات دقیق و لحظه به لحظه‌ای از نحوه‌ی عملکرد آنها داشته‌باشد. اینترنت اشیا (IoT)، از مزایای مطلوب و متعددی برخوردار است. یکی از برجسته‌ترین این مزایا، کاهش خطای انسانی است. به کمک این روش، می‌توان عملیات وسیعی انجام داد. به‌عنوان مثال، خانه‌ای را درنظر بگیرید که تمام اجزای آن، به این سیستم مجهز شده‌باشند. کاملا واضح است که کنترل و نظارت بر خانه، نه تنها به امری ساده تبدیل می‌شود، بلکه در بسیاری موارد نیز، زمان انجام کارها را به نصف کاهش می‌دهد. باید به یاد داشته‌باشیم که فاکتور زمان، نقش به‌سزایی در امور روزمره‌ی انسان ایفا می‌کند.

حال اگر بخواهیم این سیستم هوشمند را از یک خانه به یک شهر تعمیم دهیم، چه اتفاقی رخ می‌دهد؟ روشن است که این‌کار، مستلزم سازمان‌دهی بسیار پیشرفته و قوی است. همچنین، پیش‌بینی بسیاری از عوامل، جزء لاینفک این عمل به‌شمار می‌رود. به‌طور مثال، می‌توان به سیستم حمل و نقل عمومی، سیستم ترافیک شهری، سیستم روشنایی معابر، و غیره اشاره نمود. به قطع یقین، حجم بسیار وسیعی از داده‌ها وجود دارند که نیازمند جمع‌آوری، پردازش و بازگردانی دستورات به عملگرها هستند. لذا، حفاظت از این اطلاعات و مقاوم‌سازی آنها در برابر حملات، بسیار مهم و برای حفظ سیستم، حیاتی است. در این گزارش، به بررسی چگونگی عملکرد شهر هوشمند و نیز چالش‌های امنیتی آن می‌پردازیم. شایان ذکر است، چنان‌چه این سیستم مقاوم نباشد، می‌تواند تبعات جبران‌ناپذیری، نظیر مختل کردن شهر، را با خود به‌همراه داشته‌باشد.

مقدمه‌ای بر شهر هوشمند و بررسی چالش‌های امنیتی آن

1 مقدمه

با پیشرفت رو به‌رشد و روزافزون تکنولوژی، بشر، به سوی رفاه و امنیت بیشتر گام برمی‌دارد. یکی از مهم‌ترین فرایندهای حال حاضر، که رقابت بر سر آن بسیار داغ و مهیج است، به‌کارگیری فناوری‌های جدید در شهرها است و تمایل شهرهای بزرگ به هوشمند شدن، به‌طور روزافزون در حال افزایش است. این در حالی است که تمامی شهرها، خواه یا ناخواه، با تکنولوژی در ارتباط هستند. حال ممکن است که در میزان آن تفاوت‌هایی وجود داشته‌باشند و شهری نسبت به دیگری هوشمندتر باشد، اما تمامی شهرها، به‌نحوی، با فناوری آمیخته شده‌اند.

از جمله شهرهایی که گامی اساسی در هوشمندسازی برداشته‌اند، می‌توان به شهرهای نیویورک، سان‌فرانسیسکو، لس‌آنجلس، واشنگتون، سیاتل، و میامی در ایالات متحده آمریکا اشاره کرد. این در حالی است که هوشمندشدن شهرها، تنها دغدغه‌ی کشور آمریکا نیست. دامنه‌ی این هوشمندسازی حتی به برخی شهرهای اروپا، از قبیل لندن، بارسلونا، آمستردام، پاریس، و استکهلم کشیده شده‌است. سایر نقاط جهان نیز، همچون آسیا، خاورمیانه، آفریقا، و آمریکای جنوبی از این قاعده مستثنی نیستند و شهرها به‌صورت پیوسته، در راستای توسعه و هوشمندسازی، گام برمی‌دارند.

در این گزارش، به چگونگی عملکرد شهرهای هوشمند و همچنین مشکلات احتمالی و امکانات الزامی امنیتی خواهیم پرداخت و برخی از چالش‌های موجود و خطرات ناشی از حملات هکرها را بررسی خواهیم نمود.

2 شهر هوشمند

معانی مختلف و متعددی از شهر هوشمند وجود دارد، اما منظور از شهر هوشمند در این گزارش، آمیختگی شهر با جدیدترین فناوری‌ها است. برای این‌منظور، به هر میزان که شهری از نظر تکنولوژیکی به‌روز و پیشرفته باشد، آن شهر هوشمندتر است.

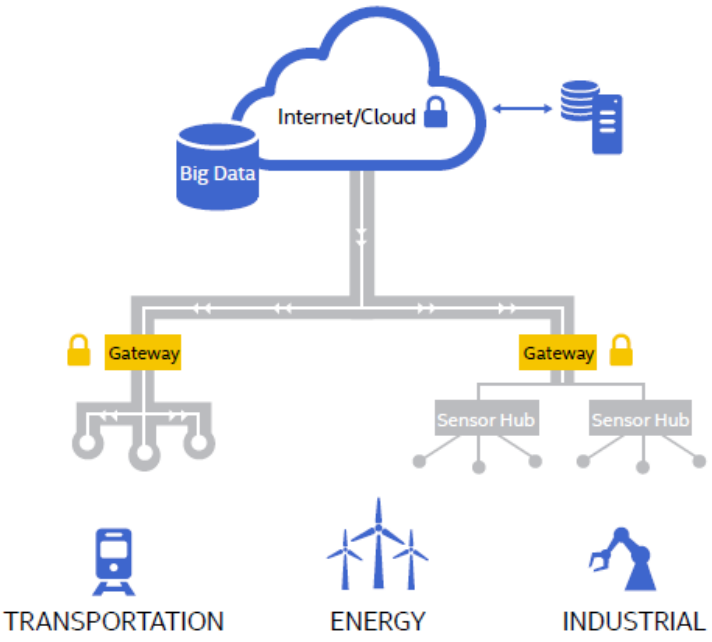
شهر هوشمندی که تمام مجموعه‌های آن به شکل پیشرفته اداره شوند، شهر هوشمند ایده‌آل تلقی می‌گردد. در حال حاضر، بشر به چنین قدرتی دست نیافته‌است که بتواند شهری با این ویژگی بسازد، اما ساختن آن، با توجه به ترقی‌های جدید علمی، دور از ذهن نیست. بنابر آمار و ارقام اعلام‌شده، شهرهای هوشمند کنونی، هزینه‌های کلانی را جهت هوشمندسازی شهر خود صرف کرده‌اند.

اکنون، به بررسی مقدماتی شهر هوشمند می‌پردازیم. بستر مبنایی شهر هوشمند را اینترنت اشیا (IoT)[1] تشکیل می‌دهد. در این شهر، تعداد زیادی سنسور مختلف به‌کار رفته‌است که هر کدام، پیام جداگانه و مختص به‌خود را دریافت می‌نماید. پس از دریافت داده‌های جمع‌آوری‌شده‌ی مختلف توسط سنسورها، این داده‌ها به سرور مرکزی شهر، که تحت تدابیر امنیتی ویژه‌ای قرار دارد، ارسال می‌گردد. اطلاعات مذکور، در فضای ابرگونه حفظ و نگهداری می‌شود و عمل پردازش بر آنها انجام می‌پذیرد. در نهایت، پس از اتخاذ

[1] Internet of Things (IoT)

تصمیم نهایی، دستورات لازم به عملگرها ارسال می‌شود و فرایند تکمیل می‌گردد [1].

تصویر (1)، شهر هوشمند مبتنی بر IoT را نشان می‌دهد. سنسورها در IoT، نقطه (مُت)[2] نامیده می‌شوند. این مُت‌ها، به‌صورت گسسته پراکنده شده‌اند و اطلاعات مختلفی، از قبیل فشار، دما، صوت، تصویر، و حتی اطلاعات خاص (مانند باز شدن در)، را فراهم می‌کنند. همچنین، می‌توانند مستقلاً، به‌عنوان تغذیه‌ی ویدیوهای خیابانی، ایستگاه‌های هواشناسی خودکار، و یا تغییرات تجهیزات قانونی، به‌کار روند. همان‌گونه که در تصویر زیر مشاهده می‌شود، فیلترسازی اولیه، توسط پردازنده‌های محلی (هاب‌های سنسوری) اِعمال می‌گردد. این هاب‌ها، در لبه‌ی شبکه‌ی سنسوری تعبیه می‌شوند. به‌عنوان مثال، می‌توان به دوربین کنترل ترافیکی اشاره نمود که به‌گونه‌ای برنامه‌ریزی شده‌است که تنها قادر است تخطی و عبور از چراغ قرمز را



شکل 1: سیستم شهر هوشمند مبتنی بر IoT [2]

ثبت نماید.

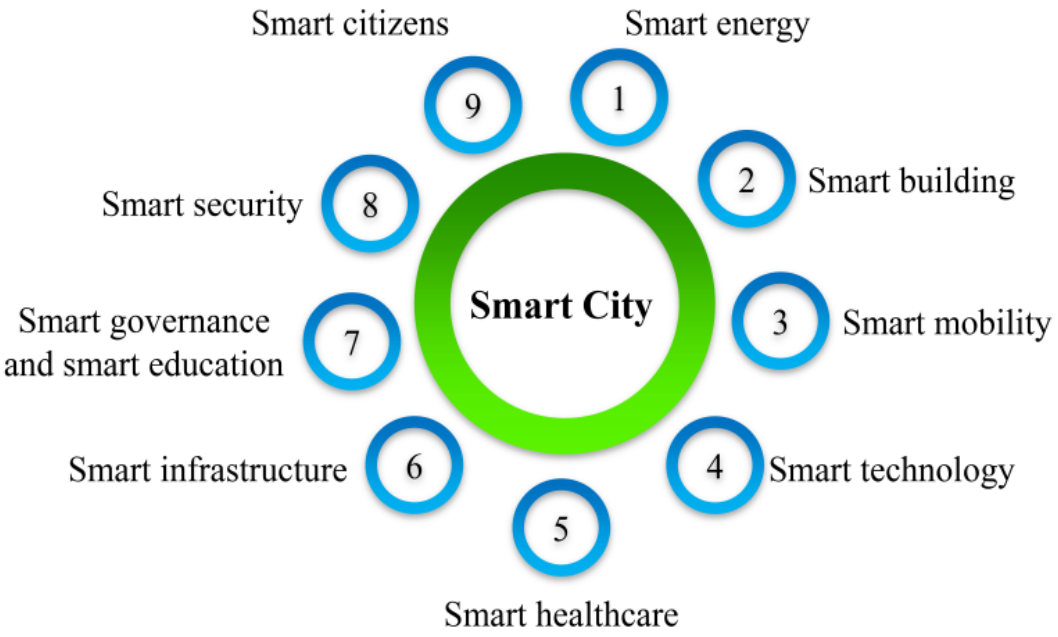
از جمله تمهیدات مهم در این نوع سیستم‌ها، حفظ یکپارچگی داده‌ها است. فرض می‌شود داده‌هایی که از سنسورها و یا هاب‌ها به‌دست می‌آیند، قابل اعتماد نیستند. دروازه‌ها[3]، این اطلاعات را دریافت و غربال

[2] Mote
[3] Gateways

می‌کنند تا اطمینان حاصل نمایند که این اطلاعات دچار خرابی و یا دستکاری نشده‌اند. سپس، اطلاعات را جهت مصرف، به سرور داده می‌فرستند.

3 بخش‌های مختلف شهر هوشمند

شهر هوشمند، از بخش‌های هوشمند مختلفی تشکیل شده‌است. از جمله‌ی این بخش‌ها می‌توان به بیمارستان‌های هوشمند، خانه‌های هوشمند، حمل و نقل هوشمند، خطوط ترافیکی هوشمند، ورزشگاه‌های هوشمند، هواشناسی هوشمند، و اتومبیل‌های هوشمند اشاره نمود. در واقع، ارتباط و پیوستگی این بخش‌ها، شهر هوشمند را پدید می‌آورد و آن را توسعه می‌دهد. در ادامه، بخش‌های مختلف شهر هوشمند را بررسی

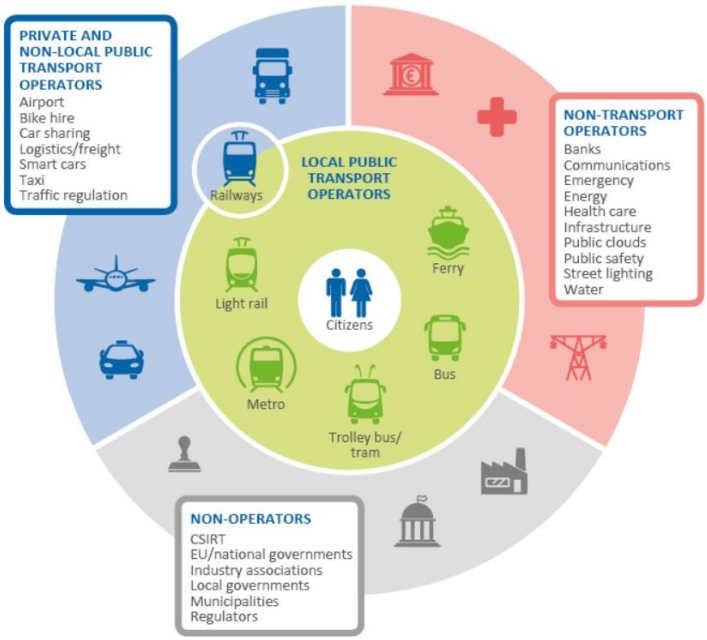


خواهیم نمود [4].

موجودیت‌های مختلفی در شهر هوشمند دخالت دارند که می‌توان آن را به چهار دسته‌ی اصلی عامل‌های حمل و نقل خصوصی و عمومی غیرمحلی، عامل‌های حمل و نقل عمومی محلی، عامل‌های غیر حمل و نقلی، و غیر عامل‌ها اشاره نمود. تصویر (2)، شِمای کلی موجودیت‌های مذکور را نشان می‌دهد [3].

عامل‌های حمل و نقل عمومی محلی (قسمت سبزرنگ شکل)، شامل وسایل حمل و نقل عمومی، مانند مترو، تاکسی، اتوبوس، و غیره است که گستره‌ی وسیعی از شهر را تحت پوشش خود قرار می‌دهد. شایان

ذکر است، خدمات حمل و نقل عمومی محلی، متفاوت از حمل و نقل خصوصی و عمومی غیرمحلی (بخش آبی‌رنگ شکل) است که بر خدمات ملی و بین‌المللی (مانند خدمات هوایی و سرویس‌های خط ریل غیرمحلی) و نیز خدمات اختصاصی برای شهروندان (مانند به‌کارگیری دوچرخه و عملگرهای اشتراک



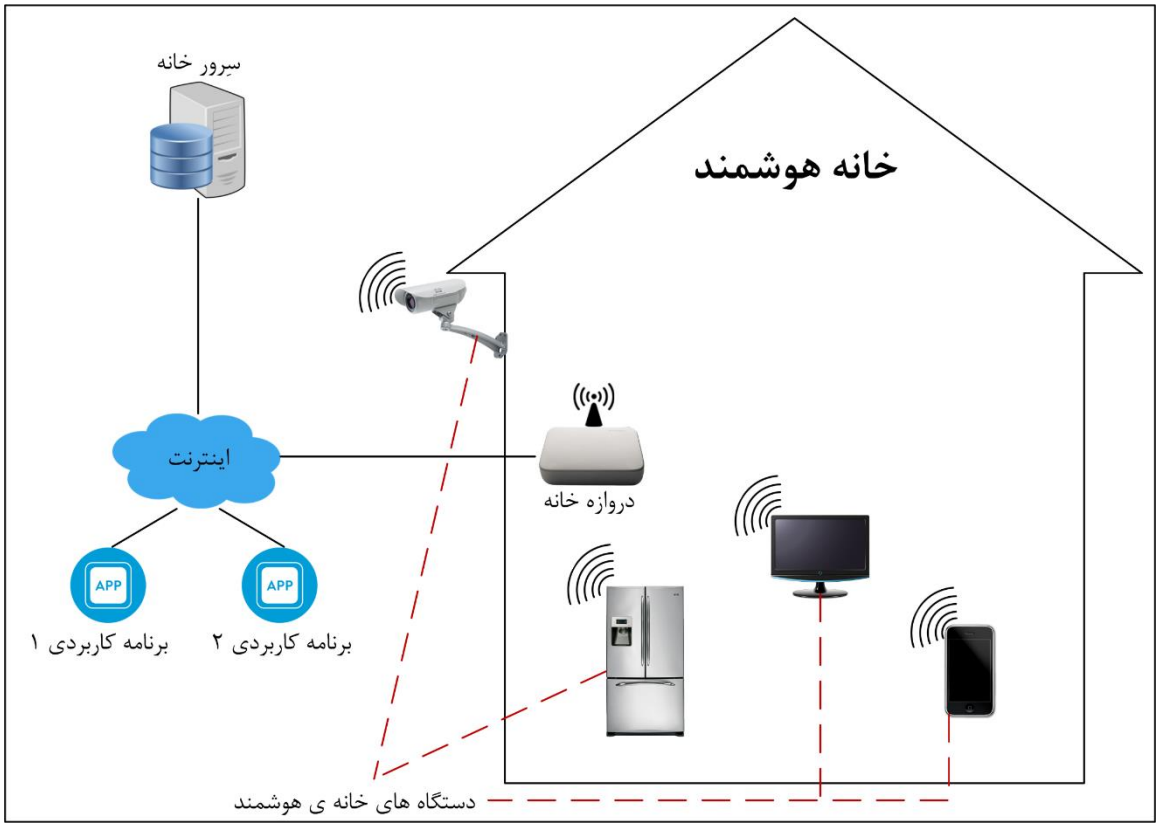
شکل 2: شِمای کلی موجودیت‌های شهر هوشمند [3]

ماشین) تمرکز دارد. همان‌گونه که در تصویر مشاهده می‌شود، بخش‌هایی از قبیل بانک‌ها، انرژی، سلامت هوشمند، ایمنی عمومی، و غیره وجود دارند که به حمل و نقل مرتبط نیستند، اما نقش مهمی را در شهر هوشمند ایفا می‌نمایند (قسمت قرمزرنگ شکل). البته، این بخش کاملا منفک از عامل‌های مرتبط با حمل و نقل نیست، زیرا برخی از مؤلفه‌های عامل‌های آن (مانند چراغ معابر)، به حمل و نقل مرتبط می‌شوند [3].

1.3 خانه‌های هوشمند

به‌طور کلی، سیستم خانه‌ی هوشمند می‌تواند همانند آن‌چه که در تصویر (3) نشان داده شده‌است، پیکربندی شود. همان‌گونه که در این تصویر مشاهده می‌شود، سیستم خانه‌ی هوشمند شامل سه مؤلفه‌ی اصلی سِرور خانه، دروازه‌ی خانه، و دستگاه‌های خانه‌ی هوشمند است. ابتدا، سِرور خانه فرآیندهای ذخیره‌سازی، تجمیع، و توزیع اطلاعات گردآوری‌شده از رسانه‌های مختلف موجود در خانه را انجام می‌دهد. سپس، دروازه‌ی خانه مبادرت به رله می‌نماید، و یا در واقع، صاحب شبکه‌ی دسترسی را به شبکه‌ی خانگی بی‌سیم/سیمی متصل

می‌کند. در نهایت، دستگاه‌های خانه‌ی هوشمند قادر خواهند بود اطلاعات را میان دستگاه‌ها مبادله کرده و به اینترنت خارجی نیز دسترسی پیدا کنند [4][13].



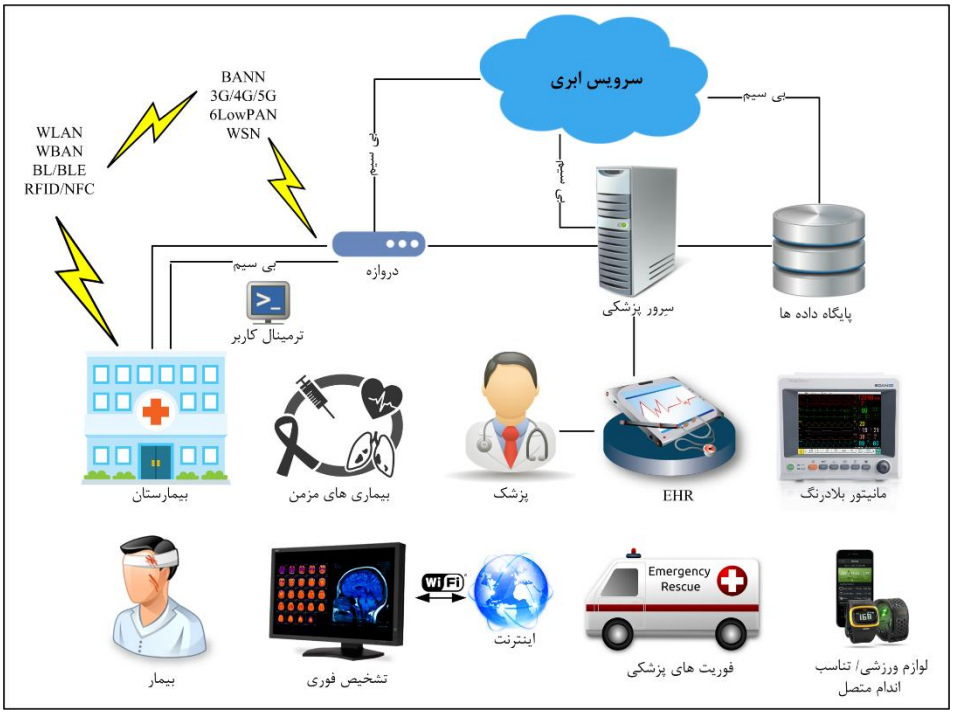
شکل 3: سیستم خانه‌ی هوشمند [13].

2.3 سلامت هوشمند

مراکز بهداشت و درمان، یکی از جذاب‌ترین حوزه‌های کاربردی IoT به‌شمار می‌روند. در واقع، اینترنت اشیا این پتانسیل را دارد تا کاربردهای درمانی متعددی، مانند کنترل سلامت از راه دور، برنامه‌های تناسب اندام، بیماری‌های مزمن، و درمان کهنسالان را گسترش دهد. بنابراین، دستگاه‌های درمانی متنوع، سنسورها، و دستگاه‌های تشخیص و عکس‌برداری می‌توانند به‌عنوان دستگاه‌های هوشمند یا اشیای تشکیل‌دهنده‌ی بخش مرکزی IoT درنظر گرفته شوند. انتظار می‌رود سرویس‌های مبتنی بر IoT، هزینه‌ها را کاهش داده، کیفیت زندگی را افزایش دهند، و تجربه‌ی کاربران را ارزشمند سازند [4][14].

شکل (4)، گرایشات سلامت هوشمند اخیر را نشان می‌دهد. یکی از گرایشات مهم، سهولت تعاملات مقرون به‌صرفه ازطریق اتصالات یکپارچه و امن بین بیماران، کلینیک‌ها، و سازمان‌های سلامت و درمان

است. انتظار می‌رود شبکه‌های سلامت هوشمند به‌روز مبتنی بر تکنولوژی‌های شبکه‌های بی‌سیم، موارد مختلفی، از قبیل بیماری‌های مزمن، تشخیص‌های زودهنگام، نظارت بلادرنگ، و فوریت‌های پزشکی را



شکل 4. گرایشات سلامت هوشمند [14].

پشتیبانی نمایند. دروازه‌ها[4]، سِرورهای پزشکی، و پایگاه داده‌های سلامت نقش مهمی را در خلق سوابق سلامت و تحویل سرویس‌های سلامت مبتنی بر تقاضا به سهام‌داران احراز هویت‌شده ایفا می‌کنند [14].

3.3 حمل و نقل هوشمند

یکی از بخش‌های بنیادین و حیاتی شهر هوشمند، که همواره مستعد مواجهه با چالش‌های امنیتی است، حمل و نقل هوشمند نام دارد. یکی از خدمات بسیار جالب شهرهای هوشمند، در دست داشتن لحظه به لحظه‌ی زمان‌بندی و برنامه‌ریزی وسایل حمل و نقل عمومی است. در این نوع حمل و نقل، زمان دقیق حضور وسایلی مانند قطار، مترو، و اتوبوس، در اختیار شهروندان قرار خواهد گرفت و در صورت وقوع هرگونه تأخیر، شهروند می‌تواند با جایگزین کردن وسیله‌ای دیگر، خود را به موقع به محل موردنظر برساند [6, 5].

4.3 کنترل هوشمند شرایط ترافیکی

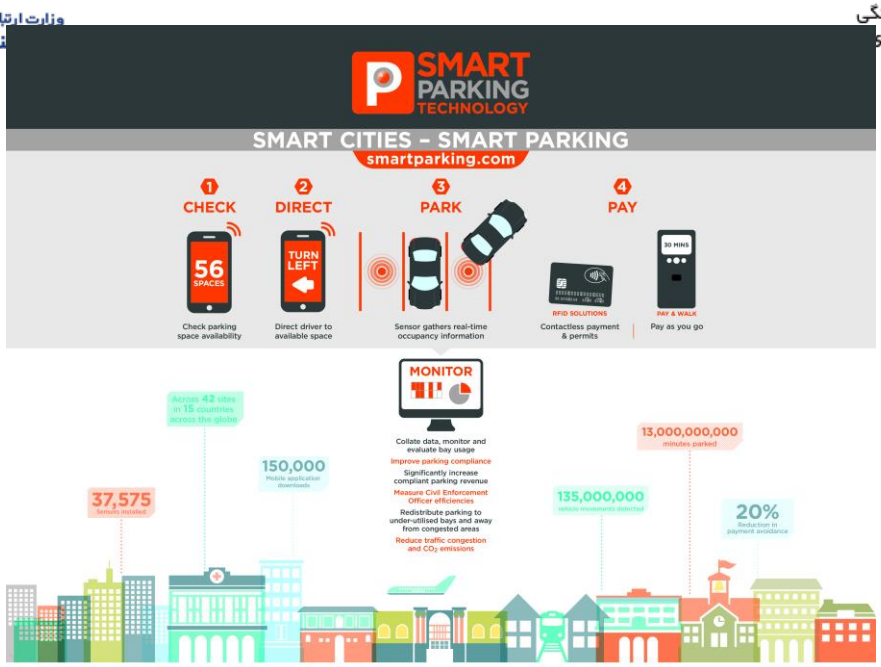
[4] Gateways

می‌توان با بهره‌گیری از سیستم اینترنت اشیا و در دست داشتن حجم وسیعی از اطلاعات، که توسط سنسورها به پایگاه‌داده فرستاده می‌شوند، در مدت زمان کوتاهی، شرایط ترافیکی را بررسی نموده و با کنترل هرچه دقیق‌تر و کاراتر چراغ‌های راهنمایی و رانندگی، شرایط ترافیکی را به‌نحوی اداره نمود که ترافیک به

شکل روان و سبک، تحت کنترل قرار گیرد [6].

5.3 پارکینگ هوشمند

شهروندان می‌توانند به کمک پارکینگ هوشمند، از فضای پارکینگ موجود مطلع گردند و از تمامی جهات، از قبیل مدت زمان نیاز به محل پارک، موقعیت مکانی محل پارک، و غیره، هزینه‌ی پارکینگ را برآورد نمایند. این در حالی است که حتی شهروند به محل پارک نرسیده‌است و می‌تواند با در اختیار داشتن اطلاعاتی گسترده و همه‌جانبه، پارکینگ خود را انتخاب کند. از اثرات مثبت این سیستم می‌توان به صرفه‌جویی قابل توجه در زمان، مصرف سوخت، و همچنین، کاهش آلاینگی اشاره نمود [6].



6.3 چراغ معبر هوشمند

این سیستم، موجب صرفه‌جویی در مصرف انرژی می‌شود و می‌تواند با در اختیار قرار دادن دید کافی برای راننده، عابرین، و غیره، خطر تصادفات ناشی از کمبود روشنایی را تا درصد بالایی کاهش دهد. همچنین، می‌توان با برنامه‌ریزی این روشنایی‌ها و بهره‌مندی از سنسورهای حساس به نور، از خطرات و حوادث جلوگیری به‌عمل آورد [5-7].

7.3 کنترل هوشمند انرژی

در این بخش، وجود یک شبکه‌ی هوشمند، بسیار موثر است. به‌عنوان مثال، اگر خانه‌ای مجهز به سیستم‌های هوشمند باشد می‌تواند در صورت عدم نیاز ساکنین به آب گرم، انرژی را قطع کند. بدین‌ترتیب، به‌مراتب، در مصرف انرژی صرفه‌جویی می‌شود. همچنین، شبکه‌ی مذکور این قابلیت را دارد که با برقراری ارتباط با منابع مسئول، برنامه‌ای را به ساکنین ارائه دهد تا در ساعات اوج مصرف، میزان مصرف خود را کاهش دهند. در نتیجه، هزینه‌های ناشی از مصرف انرژی بسیار کاهش می‌یابد [6].

8.3 سیستم‌های آب و آب و هوای هوشمند

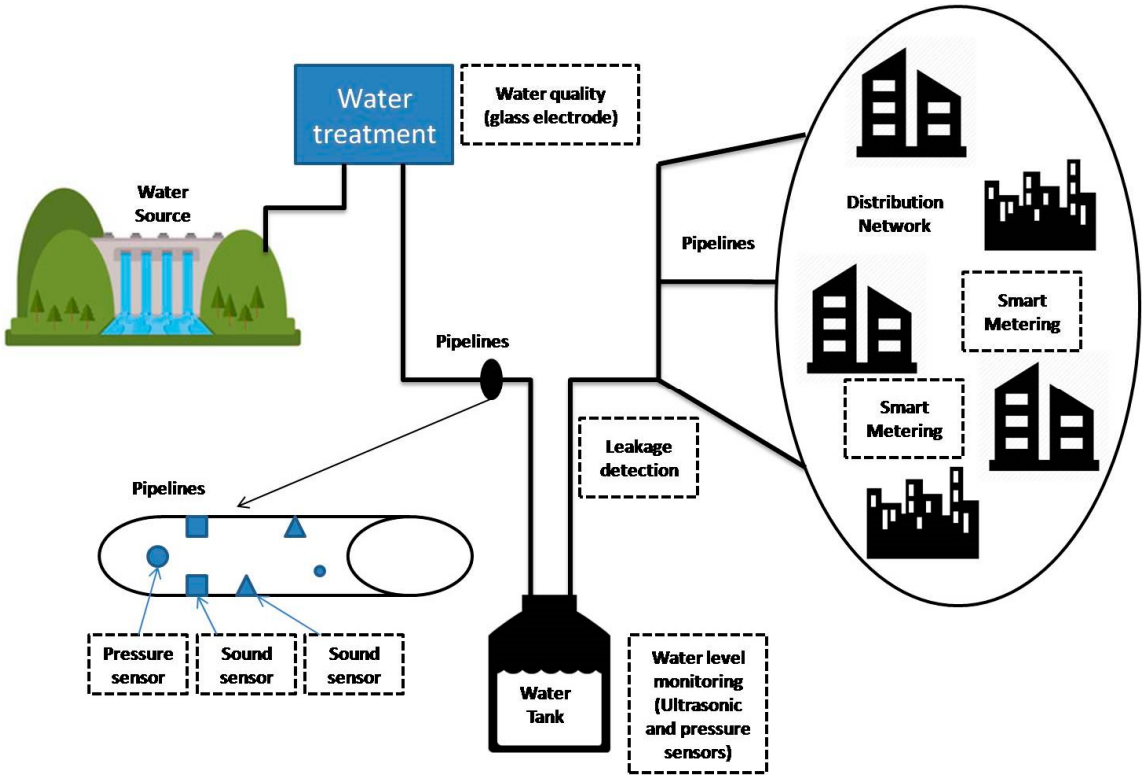
یکی از مهمترین بخش‌های شهر هوشمند، بخش کنترل هوشمند شبکه‌ی آب‌رسانی و نیز مدیریت هوشمند وضعیت آب و هوایی است. در واقع، شهر هوشمند این امکان را فراهم می‌آورد تا با بهره‌گیری از تجهیزات هوشمند، هم در مصرف آب صرفه‌جویی شود، و هم شهروندان را از وضعیت آب و هوا مطلع سازد [4].

1.8.3 مدیریت وضعیت آب و هوایی

سیستم‌های آب و هوایی، از سنسورهای مختلفی جهت تأمین داده‌های مناسب، از قبیل دما، باران، تابش نور خورشید، و سرعت باد بهره می‌جوید تا بهره‌وری شهر هوشمند را افزایش دهد. در واقع، سیستم هوشمند مدیریت وضعیت آب و هوایی قادر است با اندازه‌گیری مؤلفه‌های مذکور، شرایط آب و هوایی را پیش‌بینی نماید و کاربر را مطلع سازد [4].

2.8.3 کنترل هوشمند آب‌رسانی

شِمای کلی کنترل هوشمند آب‌رسانی، در تصویر (5) نشان داده شده‌است. این سیستم می‌تواند با در دست داشتن اطلاعات متعدد از لوله‌ها، میزان آب مصرفی را کنترل نماید و چنان‌چه مشکلی در سیستم آب‌رسانی (نظیر نشتی آب) پیش آید، عیب‌یابی به سریع‌ترین شکل ممکن، قابل اجرا است. از سایر خدمات این

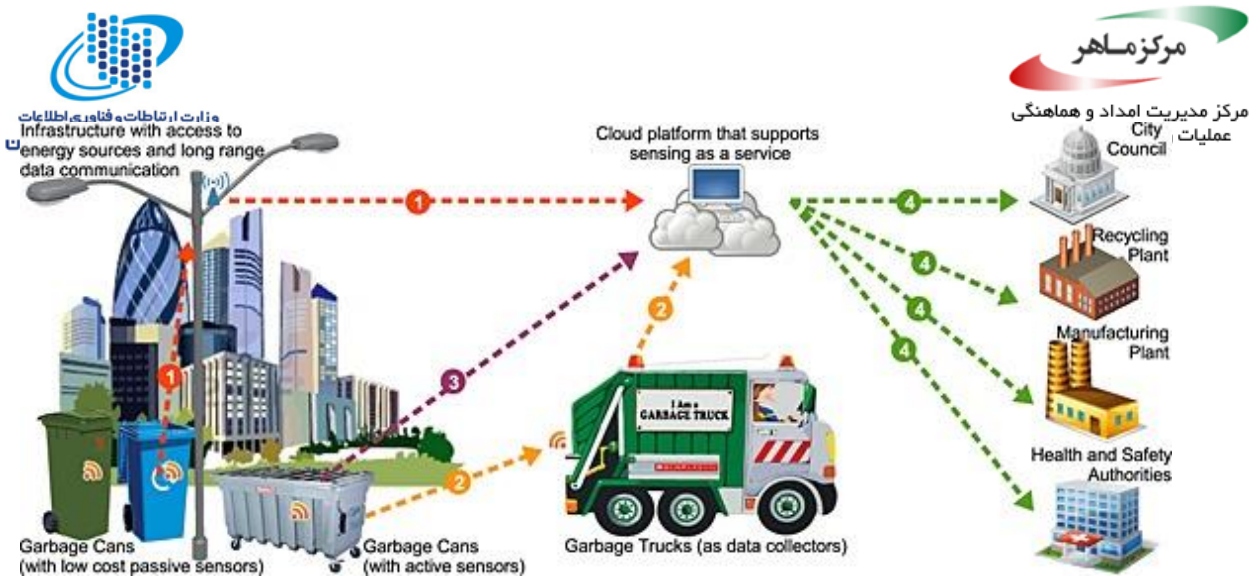


شکل 5: آب‌رسانی هوشمند [4]

سیستم می‌توان به توزیع آب مناسب اشاره نمود [6, 4].

9.3 سیستم دفع زباله‌ی هوشمند

هوشمندسازی سیستم دفع زباله، این امکان را فراهم می‌آورد تا بتوان محیط را با سرعت بیشتری پاک‌سازی نمود. برای مثال، ماشین مخصوص این‌کار، لزوماً نیازی به تخلیه‌ی سطل‌های زباله‌ی شهری خالی ندارند و با تشخیص وزن سبک سطل، از کنار آن رد می‌شود و یا حتی ابتدا آن زباله‌هایی را پاک‌سازی می‌کند که با بوی نامطبوع، فضا را مشمئزکننده نموده‌اند [6].



10.3سیستم‌های امنیتی هوشمند

در شهرهای هوشمند می‌توان به کمک دوربین‌های کنترل ترافیک، دوربین‌های امنیتی، و حسگرهای تشخیص تیراندازی، کنترل موارد متعدد و حفظ امنیت محدوده‌های مشخص را با سرعت و دسترسی بسیار مناسب، تأمین کرد. به‌عنوان مثال، می‌توان به کمک شماره‌های تلفن و امواجی از قبیل وای‌فای و بلوتوث، تعداد افراد حاضر در محلی مانند خیابان یا پارک را تحت کنترل قرار داد و هویت اشخاص مختلف را شناسایی نمود. این موضوع، خود، به تنهایی موجب کنترل و حفظ امینت در سطوح امنیتی بسیار بالایی است [6].

4 تسهیلات زندگی در شهر هوشمند

در این‌بخش، به توصیف یک روز زندگی شهروندی در یک شهر هوشمند می‌پردازیم. از جمله امکاناتی که شهر هوشمند برای افراد فراهم می‌آورد، می‌توان به موارد زیر اشاره نمود:

- فرد، جهت آماده‌سازی و رفتن به محل کار خود، از خانه‌ی خود و به کمک گوشی خود و سیستم اشتراک‌گذاری اطلاعات شهری، از شرایط مختلف جوی آگاه می‌شود. این بدان معنا است که شخص موردنظر می‌تواند پیش از ترک منزل و غافل‌گیر شدن، خود را برای هر مسئله‌ای آماده سازد. به‌عنوان مثال، اگر این احتمال وجود داشته‌باشد که باران ببارد، شخص می‌تواند با استفاده از چتر، خود را مصون نگه دارد و یا اگر میزان گزارش‌شده‌ی بارش به حد زیادی باشد، از وسیله‌ی نقلیه‌ی شخصی استفاده نماید.
- فرد می‌تواند به کمک گوشی همراه هوشمند خود، از زمان دقیق استفاده از وسایل حمل و نقل عمومی مطلع شود و بدون این‌که زمانی را از دست دهد، وسیله‌ی موردنظر را انتخاب نماید و به مقصد برسد. حال اگر برای وسیله‌ی موردنظر وی مسئله‌ای پیش آید که موجب تأخیر شود، این

تأخیر هم به کمک سیستم اطلاع‌رسانی پیوسته، به تمامی شهروندان مخابره می‌گردد و آنها قادر خواهند بود که وسیله‌ی مناسبی را جایگزین کنند. در این‌صورت، نه تنها شهروندان زمانی را از دست نمی‌دهند، بلکه سیستم حمل و نقل عمومی در سریع‌ترین زمان ممکن، به بروز مشکل در واحدهای خود پی می‌برد و به رفع مشکل می‌پردازد.

در بخش ترافیکی نیز، به دلیل این‌که شرایط بار ترافیکی در محورهای مختلف به‌صورت پیوسته به مرکز کنترل ارسال می‌شود، عوامل مرکز می‌توانند به‌صورت خودکار و با کنترل صحیح علایم رانندگی، از قبیل چراغ‌های راهنمایی و رانندگی، بار ترافیکی سنگین در محورها را با ایمنی بیشتر هدایت کنند که این امر، کمک به‌سزایی به سبک‌تر شدن هرچه سریع‌تر ترافیک شهری می‌کند.

- در بخشی دیگر، اگر میزان آلودگی هوا بالا باشد، والدین ضمن باخبر شدن به موقع از شرایط می‌توانند فرزندان خود را در برابر این آلودگی تجهیز کنند و یا حتی برای حفظ سلامت آنها، اقدامات لازم را در اسرع وقت انجام دهند.
- یکی دیگر از خدمات این سیستم، پارکینگ هوشمند است که امکانات موردنیاز موجود را با توجه به نیاز شهروند، فراهم می‌نماید. چنان‌چه شخصی به پارکینگ نیاز داشته‌باشد، کافی است تا از گوشی هوشمند خود کمک بگیرد و با استفاده از برنامه‌ی کاربردی موجود، پارکینگ خود را با توجه به زمان پارک، فاصله از مقصد، و قیمت محل پارک، رزرو کرده و حتی مبلغ آن را با گوشی خود پرداخت کند و بدون صرف زمان زیاد در شلوغی شهر، به سمت پارکینگ خود حرکت نماید. لازم به ذکر است، از آن‌رو که سلامت محیط زیست اهمیت بسیار ویژه‌ای دارد، امکانات به‌وجودآمده توسط سیستم هوشمند شهری، کمک شایانی به این امر می‌نماید. به طور عمده، به کمک سیستم پارک هوشمند، میزان چشم‌گیری از گاز CO_2، که توسط اتومبیل‌هایی که با سوخت فسیلی کار می‌کنند تولید می‌شود، کاهش می‌یابد.

5 تهدیدات و چالش‌های امنیتی

یکی از عمده‌ترین و اصلی‌ترین اهداف پیدایش شهرهای هوشمند، علاوه بر راحتی شهروندان، برقراری ارتباطات پیشرفته و وسیع در شهر و حتی برقراری ارتباط بین شهرهای مختلف است. بدین‌منظور، از تکنولوژی‌های ارتباطی پیشرفته‌ی امروزی، مانند شبکه‌های IOT، استفاده می‌شود تا بتوان به کمک اینترنت، اشیا را کنترل نمود [6].

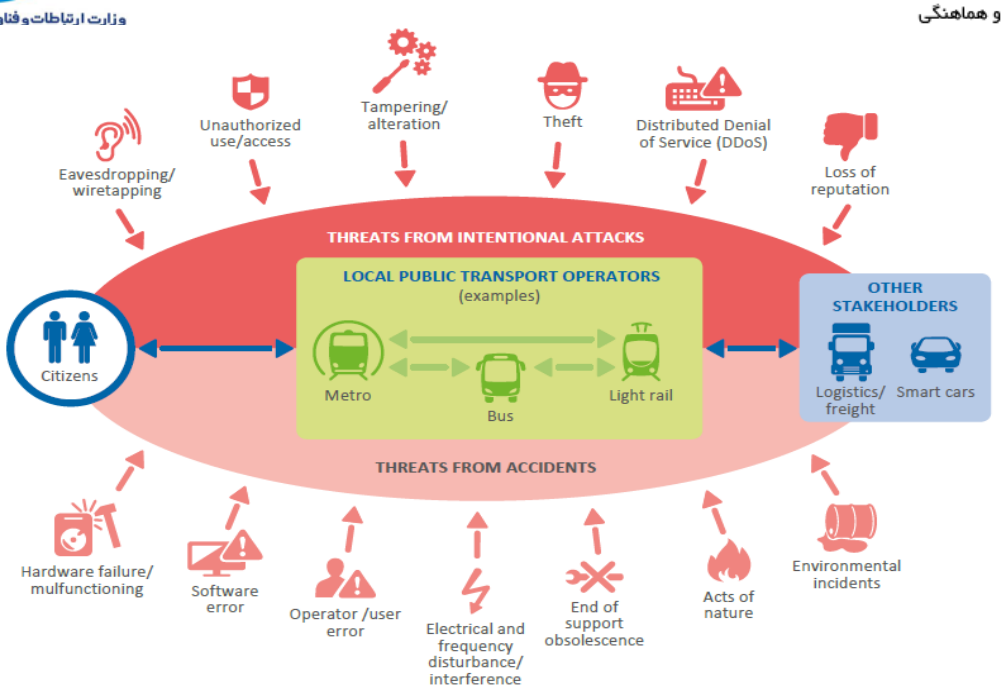
مبرهن است که هرگونه پیشرفت در تکنولوژی و افزایش ارتباطات، خطرات امنیتی را با خود به‌همراه خواهد داشت. در واقع، بستر اینترنت این امکان را برای مهاجمان و هکرها فراهم می‌آورد تا با تلاش برای نقض تمهیدات امنیتی (مانند محرمانگی، یکپارچگی، و دسترسی‌پذیری داده‌ها)، امنیت سیستم را به چالش بکشند. در ادامه، برخی از تهدیدات احتمالی، بررسی و طبقه‌بندی می‌شوند.

- **تهدیدات دسترسی‌پذیری**: یکی از تهدیدات متداول این سیستم، دسترسی به داده‌ها است که می‌توان به حمله‌ی موسوم به انکار خدمات (DoS)[5] اشاره نمود [3].
- **تهدیدات یکپارچگی**: تهدیدات یکپارچگی، شامل دسترسی غیرمجاز، تغییر و تخریب، و گاها از بین بردن اطلاعات محدودشده است. چنین تهدیداتی می‌توانند با بهره‌گیری از حملات و نرم‌افزارهای مخرب، عملی گردند [3].
- **تهدیدات اعتبارسنجی**: تشخیص هویت، یکی از بااهمیت‌ترین چالش‌ها در سیستم‌های هوشمند به‌حساب می‌آید، زیرا تمام دستگاه‌ها توانایی دریافت، ارسال، و پخش پیام‌ها را دارند. در چنین بستری، تشخیص صحت پیام و منبع آن، امری مهم و در برخی موارد، دشوار است [3].
- **تهدیدات محرمانگی**: این تهدیدات، شامل خطراتی، از قبیل دسترسی غیرقانونی به اطلاعات است که با استفاده از روش‌هایی مانند استراق سمع، تجزیه، و تحلیل پیام‌های ترافیکی، صورت می‌پذیرد [3].
- **تهدید انکارناپذیری/پاسخ‌گویی**: در این شاخه، به اهمیت اجرا شدن دستورات اشاره می‌شود، به‌صورتی‌که اطمینان از عدم انکار دستورات ارسال و یا دریافت‌شده و حتی خدمات خاص خواسته‌شده، حاصل گردد [3].

1.5 تهدیدات خاص

تهدیدات خاص به تبادل اطلاعات میان عملگرها و سایر عوامل مرتبط بازمی‌گردند و پیامدهای احتمالی آنها، بسته به بلوغ شهر مربوطه در زمینه‌ی هوشمندسازی، متفاوت است. تصویر (6)، نمایی از حملات عمدی و سهوی را معرفی می‌کند.

[5] Denial of Service (DoS)



شکل 6: تهدیدات عمدی و سهوی شهر هوشمند [3]

1.1.5 خطرات ناشی از حملات عمدی

خطر حمله در این شاخه، از تهدیدات عمدی بوده و به روش‌های مختلفی، قابل اجرا است. برای مثال، می‌توان به استراق سمع، سرقت، دستکاری، تغییر، یا استفاده‌ی غیرمجاز و دسترسی به اطلاعات اشاره نمود [3].

- **استراق سمع/تَپ‌گذاری سیمی**: متاسفانه، در هوشمندسازی شهرها به نکات امنیتی توجه کافی نشده‌است. برای چنین تکنولوژی‌هایی، استراق سمع، شایع‌ترین تهدید محسوب می‌شود، زیرا مهاجمین می‌توانند با تَپ‌گذاری[6]، اطلاعات حیاتی سیستم (از قبیل نحوه‌ی اتصال دستگاه‌ها به یکدیگر) را به‌دست آورند. نقشه‌ی شبکه‌ی یک سیستم، حیاتی‌ترین اطلاعاتی است که دست‌یابی به آن، پیامدهای ناگواری را با خود به‌همراه خواهد داشت. حملاتی از این دست، منجر به افشای عمدی اطلاعات حیاتی سیستم، مانند نقشه‌ی شبکه و ارتباطات سیستم، اطلاعات شخصی و امنیتی موجودیت‌ها، اطلاعات مالی، و غیره خواهد شد [3].
- **سرقت**: نوع دیگری از حملات عمدی است که در آن، اطلاعات حیاتی سیستم، به سرقت می‌رود. به‌عنوان مثال، می‌توان به سرقت کلیدهای رمزنگاری سیستم خرید بلیط غیرمتمرکز اشاره نمود که طی آن، مشکلات مالی جدی و انکارناپذیری پدید می‌آید. فارغ از چنین سرقت‌هایی، سرقت

[6] Tapping

تجهیزات فیزیکی (مانند گوشی هوشمند و لپ‌تاپ) شهروندان نیز، شایع است. تجهیزات مذکور، اطلاعات حساسی از نقشه‌ی شبکه، نحوه‌ی ارتباطات و تبادل داده‌ها را با خود به‌همراه دارند [3].

- **دستکاری/تغییر**: عبارت است از دستکاری یا تغییر اطلاعات سیستم، که منجر به نقض محرمانگی و یکپارچگی داده‌ها خواهد شد. در شهر هوشمند، تجهیزاتی از قبیل سیگنال‌های ترافیکی، خوانندگان برچسب عوارض، و دوربین‌ها، مستعد قرار گرفتن در معرض چنین حملاتی هستند.
- **دسترسی/استفاده‌ی احراز هویت‌نشده**: منشأ تمامی تهدیدات است. این نوع از تهدید می‌تواند پیامدهای ناخوشایندی را با خود به‌همراه داشته‌باشد: دسترسی احراز هویت‌نشده به شبکه؛ نشت داده، مرور فایل‌ها؛ و دست‌یابی به داده‌ها، تکنولوژی‌ها، و برنامه‌های کاربردی محرمانه [3].
- **انکار خدمات توزیع‌شده (DDoS)**[7]: شامل اتصال همزمان چندین مبدأ به یک مقصد، با هدف سرریز نمودن اتصالات است. این حمله، به‌خصوص در سیستم‌های هوشمند، امری رایج است، زیرا یکی از تجهیزات کارا در این نوع حملات، تجهیزات مبتنی بر IP است. چنین وسایلی، از قبیل دوربین‌های هوشمند، به وفور در سیستم شهر هوشمند مشاهده می‌شوند.
- **فقدان اعتبار**: بر کسب و کار اثر می‌گذارد. در صدد است تا یک عملگر را تحت تأثیر قرار دهد و از اعتبار آن بکاهد. در نتیجه، شهروندان، شرکا، تأمین‌کنندگان، و شهرداری‌ها، به آن سازمان هوشمند اعتماد نخواهند نمود.

2.1.5 خطرات ناشی از حملات سهوی

رخدادهای ناشی از این تهدیدات، به‌صورت سهوی صورت می‌پذیرند. مهمترین انواع این تهدیدات، مرتبط با بحث تبادل داده‌ها است و گونه‌های آن عبارتند از: خرابی/عدم کارکرد صحیح سخت‌افزاری، خطای نرم‌افزاری، خطای عملگر/کاربر، اتمام پشتیبانی/ماندگاری، اختلال/وقفه‌ی برقی و فرکانسی، کنش‌های طبیعت، و رخدادهای محیطی [3].

- **خرابی/عدم کارکرد صحیح سخت‌افزاری**: می‌تواند به‌دلایل مختلفی، از قبیل طول عمر بالای تجهیزات، عدم نگهداری، و گرمای بیش از حد رخ دهد. در اکثر مواقع، خرابی تجهیزات منجر به در دسترس نبودن خدمات می‌شود. برخی از خرابی‌های تجهیزاتی، مانند خرابی چراغ‌های ترافیکی، پیامدهای سختی را به‌همراه خواهد داشت. البته، می‌توان تمهیدات بازیابی را برای این دستگاه‌ها تعبیه نمود [3].

[7] Distributed DoS (DDoS)

- **خطای نرم‌افزاری**: هر کد فرعی یا نادرست در سیستم‌عامل یا برنامه‌ی کاربردی که منجر به خطاهای پردازشی، خطاهای خروجی داده‌ها، یا تأخیرات پردازشی شود، در زمره‌ی خطای نرم‌افزاری قرار می‌گیرد. این خطا، دسترسی‌پذیری و جامعیت داده‌ها را تحت تأثیر قرار می‌هد. به‌عنوان مثالی در دنیای شهر هوشمند، مجددا می‌توان به بلیط‌فروشی هوشمند اشاره نمود که در صورت بروز خطای نرم‌افزاری، این امکان وجود دارد که بلیط، بدون دریافت مبلغی، تحویل داده‌شود [3].
- **خطای عملگر/کاربر**: به انتخاب و یا رفتار نادرست کاربر/کارمند بازمی‌گردد که می‌تواند منجر به تأخیر در پردازش‌ها، آسیب تجهیزات، و یا فقدان و تغییر داده‌ها گردد. چنین تهدیداتی می‌توانند رفتار غیرمنتظره‌ی مؤلفه‌ها را با خود به‌همراه داشته‌باشند که آن نیز، کند شدن و یا ازکار افتادگی خدمات، و یا قطع ارتباطات را پدید خواهد آورد [3].
- **اتمام پشتیبانی/ماندگاری**: اغلب تولیدکنندگان، ارائه‌دهندگان و فروشندگان، زمانی‌که برنامه‌ها و فناوری‌ها منسوخ می‌شوند، پشتیبانی از آنها را متوقف می‌نمایند. این امر، منجر به وقوع آسیب‌پذیری‌هایی برای آن‌دسته از برنامه‌ها می‌شود که نقشی حیاتی را در تبادل داده‌ها ایفا می‌نمایند. تهدیدات اتمام پشتیبانی، دسترسی‌پذیری و جامعیت داده‌ها را به خطر می‌اندازد [3].
- **اختلال/وقفه‌ی برقی و فرکانسی**: ممکن است دسترسی‌پذیری را تحت تأثیر قرار دهد. برق، لازمه‌ی غالب کاربردها و اتصالات موجود در شهر هوشمند است. از سویی دیگر، ارتباطات بی‌سیم نیز از طریق فرکانس‌ها صورت می‌پذیرند. نبود این دو مؤلفه‌ی حیاتی، سیستم شهر هوشمند را مختل خواهد نمود [3].
- **کنش‌های طبیعت**: ناشی از شرایط جوی و بلایای طبیعی است. از انواع آن می‌توان به خشکسالی و سیل، برف، بوران، تندباد، زمین‌لرزه، آتشفشان و غیره اشاره نمود [3].
- **رخدادهای محیطی**: از انواع آن می‌توان به قطع برق و نشت مایعات (انفجار و نشت لوله‌ها، تخلیه‌ی آب آشامیدنی) اشاره نمود، که مشابه کنش‌های طبیعت هستند و می‌توانند منجر به خرابی مؤلفه‌های میدانی، وسایل نقلیه، و زیرساخت‌ها شوند. غالبا، تبادل داده را تحت تأثیر قرار می‌هند [3].

2.5 فناوری‌های آسیب‌پذیر شهر هوشمند

تمامی فناوری‌های استفاده‌شده توسط شهرها، به‌همراه تمام مشکلات مربوط به امنیت سایبری که پیش از این توصیف شده‌اند، امکان وقوع چندین حمله‌ی سایبری را فراهم می‌سازند. هر فناوری جدید شهری،

فرصت نوینی را برای مهاجمان اینترنتی ایجاد می‌نماید. در این بخش سعی بر آن است تا فناوری‌های آسیب‌پذیر شهر هوشمند را موردمطالعه قرار دهیم [6].

1.2.5 سیستم‌های کنترل ترافیک

محققان دانشگاه میشیگان دریافته‌اند که سیستم‌های کنترل ترافیک هوشمند، به‌راحتی هک می‌گردند. طبق تحقیقات، مشخص شده‌است که تعدادی دستگاه اکونولیت[8] در این سیستم‌ها به‌کار رفته‌است که فاقد هرگونه رمزنگاری اتصالات میان سیستم‌های کنترل ترافیک و سایر مؤلفه‌های ترافیکی، از قبیل چراغ‌های ترافیکی، کنترل‌کننده‌های ترافیکی، و موارد مشابه هستند. چنین نقصی، به هکرها اجازه می‌دهد تا مستقیما چراغ‌های ترافیکی را تغییر دهند. با چنین شرایطی، 100,000 تقاطع در ایالات متحده و کانادا، در معرض خطر قرار دارند [6].

2.2.5 چراغ معابر هوشمند

سیستم‌های چراغ معابر بی‌سیم، در بسیاری از شهرهای جهان، گسترش یافته‌اند. غالب سیستم‌ها، از ارتباطات بی‌سیم بهره می‌جویند و از مشکلات رمزنگاری مرسوم، رنج می‌برند. حملات چراغ‌های معابر خیابانی بسیار پیچیده نیست و می‌تواند منجر به خاموشی خیابان‌ها در نواحی گسترده شود. به‌عنوان مثال، حمله به چراغ‌های معبر جزیره‌ی ویرجین ایالت متحده می‌تواند کل خیابان‌های جزیره را در خاموشی مطلق فرو بَرَد [6].

3.2.5 سیستم‌های مدیریت شهری

هر شهر، شامل صدها سیستم جهت مدیریت خدمات و وظایف مختلف است. هک چنین سیستم‌هایی، گزینه‌های متعددی را جهت آسیب رساندن به شهر، برای مهاجم پدید می‌آورد. به‌عنوان مثال، یک هکر می‌تواند اطلاعات نقشه‌ی شهر را دستکاری نماید و کارگران را، بدون این‌که مطلع باشند، به سوی کندن حفره‌ای در لوله‌های گاز یا آب و یا کابل‌های ارتباطی سوق دهد تا به این امکانات، آسیب رساند [6].

4.2.5 سنسورها

سیستم‌های شهر هوشمند، جهت تصمیم‌گیری و انجام کُنش مناسب، به‌شدت بر داده‌های سنسورها متکی هستند. غالب سنسورها، از فناوری بی‌سیم بهره می‌جویند و مترصد خطرات ناشی از این تکنولوژی هستند.

[8] Ecomolite

حملاتی از قبیل دستکاری سنسور و ارسال داده‌های جعلی، از حملات شایع است که بر روند سیستم تأثیر می‌گذارد. مهاجمین می‌توانند از این‌طریق، رخدادهای جعلی، مانند زمین‌لرزه، ریزش تونل، شکستن پل، سیل، شلیک اسلحه، و موارد این‌چنینی را ایجاد نمایند، آلارم‌ها را به صدا درآورند و منجر به وحشت عمومی شوند. در مثالی دیگر، مهاجم می‌تواند با ارسال داده‌ی جعلی از سنسورهای بویایی و سطح زباله‌ی موجود در زباله‌دان‌های خالی، زمان و منابع دستگاه‌های جمع‌آوری هوشمند زباله را هدر دهد [6].

5.2.5 داده‌های عمومی

گاهی، داده‌های عمومی، به‌صورت بلادرنگ، در اختیار مهاجمین قرار می‌گیرد. این داده‌ها می‌توانند در تعیین بهترین زمان حمله، زمان‌بندی حملات، ایجاد اهداف حمله، حملات هماهنگ، و غیره، به مهاجمین کمک کنند. نیازی نیست که مهاجمان، کورکورانه عمل کنند، بلکه قادرند با تکیه بر داده‌های واقعی، با دقت هرچه تمام‌تر اقدام نمایند. به‌عنوان مثال، مهاجمین می‌توانند از زمان دقیق رسیدن اتوبوس یا قطار مطلع شوند؛ ببینند که چه زمانی ترافیک در سنگین‌ترین وضعیت قرار دارد؛ در چه زمانی افراد بیشتری در یک مکان گرد هم می‌آیند؛ و غیره [6].

6.2.5 برنامه‌ها کاربردی موبایل

برنامه‌های کاربردی موبایل، گستره‌ی تهدیدات وسیعی را، از حمله‌ی مرد میانی ساده تا حملات پیچیده، شامل می‌شود. مهاجمین می‌توانند به شرکت‌های توسعه‌ی برنامه‌ها حمله کنند، و یا انحصارا، داده‌های برنامه‌های کاربردی را مورد هدف قرار دهند. هک برنامه‌های کاربردی، مستقیما بر رفتار شهروندان تأثیر می‌گذارد. به‌عنوان مثال، اگر برنامه‌ی حمل و نقل عمومی، تأخیری در یک اتوبوس را نشان دهد، شهروند تصمیم می‌گیرد که برای رفتن به اداره، از ماشین استفاده نماید. حال اگر صدها نفر در ناحیه‌ای با تراکم جمعیت بالا، مبادرت به اتخاذ چنین تصمیمی نمایند، ترافیک سنگینی ایجاد می‌شود و یک حمله‌ی DoS شهری به‌وقوع می‌پیوندد [6].

7.2.5 راه‌حل‌های ابری و SaaS

سرورهای شهری و زیرساخت ابری، در معرض حملات رایج DDoS قرار می‌گیرند. این تجهیزات، اهداف ارزان‌تری برای مجرمان و یا تروریست‌های امنیتی به‌شمار می‌روند. همچنین، مؤلفه‌ی نرم‌افزار به‌عنوان

سرویس (SaaS)[9]، این امکان را برای مهاجم فراهم می‌سازد تا یک تأمین‌کننده‌ی سرویس را هک نماید و سپس، حملات متعددی را همزمان، علیه چندین شهر اجرا کند [6].

8.2.5 گرید هوشمند

انرژی، شاهرگ حیاتی هر شهر است. بدون انرژی، شهر هوشمندی نیز وجود نخواهد داشت. در شهر هوشمند، حسگرهای اندازه‌گیری مختص انرژی، که اندازه‌گیر هوشمند (SM)[10] نام دارند، به‌کار می‌روند. تحقیقات نشان داده‌است که مهاجمین قادرند با دستکاری SMها، شهرهای وسیع را خاموش نمایند و از این‌طریق، مشکلات رمزنگاری برای فناوری ارتباطات خطوط برق (PLC)[11] پدید آورند [6].

9.2.5 حمل و نقل عمومی

شهروندان، از سیستم‌های اطلاعات حمل و نقل عمومی استفاده می‌نمایند تا از زمان رسیدن (به) و یا ترک ایستگاهِ وسایل نقلیه‌ی عمومی، مطلع گردند تا بتوانند تأخیرات احتمالی را برآورد کنند. کوچکترین تغییر و یا دستکاری داده‌های این سیستم، اثرات سوئی بر رفتار شهروندان خواهد گذاشت و منجر به تأخیر، ازدحام، و مسائل این‌چنینی خواهد شد. به‌عنوان مثال، مهاجمان می‌توانند با تغییر اطلاعات مربوط به یک مترو، شهروندان را به خط دیگری منتقل کنند و در آنجا، ازدحام به‌وجود آورند. در نمونه‌ای دیگر، مهاجمین می‌توانند سیستم‌های پرداخت را مورد حمله قرار دهند که در این‌صورت، مشکلات متعددی پیش می‌آید: شهروندان می‌توانند به‌صورت رایگان از وسایل نقلیه استفاده نمایند؛ و یا هزاران نفر قادر خواهند بود شمارنده‌های سرویس مشتری را دچار تراکم و یا مسدود کنند و از خطوط تلفن، شکایت نمایند [6].

10.2.5 دوربین‌ها

دوربین‌ها، به‌طور گسترده در سراسر جهان استفاده می‌شوند. دوربین‌های ترافیکی و نظارتی، حکم چشمان بینای شهر را دارند و با حمله به آنها، شهر، بینایی خود را از دست خواهد داد. حملات DDoS، رایج‌ترین نوع حملات به این دوربین‌ها است که به آسانی صورت می‌پذیرد، زیرا معمولا، از دوربین‌های یک برند در سطح شهر استفاده می‌شود. در نتیجه، نقض امنیت یک دستگاه، منجر به حمله به تمامی دوربین‌های شهر خواهد شد [6].

[9] Software as a Service (SaaS)
[10] Smart Meter (SM)
[11] Power-Line Communication (PLC)

11.2.5 رسانه‌ی اجتماعی

رسانه‌ی اجتماعی را می‌توان به‌عنوان پلتفرم تقویت حملات درنظر گرفت. آثار آن، در هک‌های اخیر شرکت‌ها مشاهده شده‌است. به‌عنوان مثال، مهاجمان می‌توانند تأثیر ناشی از حمله را با ایجاد وحشت در جمعیت، افزایش دهند. اگر تنها یک حمله‌ی ساده تحقق یابد، زمینه برای رشد و توسعه‌ی سایر حملات بزرگ‌تر، فراهم می‌گردد. در چنین شرایطی، حتی اگر هم حملات بزرگ مذکور هرگز اتفاق نیفتند، اما همچنان، رعب و وحشت ناشی از وقوع آنها در دل شهروندان وجود دارد [6].

12.2.5 سرویس‌های مبتنی بر مکان

مبتنی بر مکان بودن بسیاری از سرویس‌ها، امکان جاسوسی GPS و سایر حملات محتمل را افزایش می‌دهد. شهروندان، اطلاعات مکان را به‌صورت بلادرنگ دریافت می‌کنند. در صورتی‌که اطلاعات اشتباه باشد، تصمیمات نامناسبی را بر اساس این اطلاعات اشتباه اخذ خواهد نمود [6].

6 حملات صورت‌گرفته به شهر هوشمند

همان‌گونه که در بخش‌های پیشین سند موردمطالعه مطرح گردید، IoT، اساس ارتباطی شهر هوشمند را تشکیل می‌دهد. همواره، سیستم‌های مبتنی بر IoT، با چالش‌های امنیتی دست و پنجه نرم می‌کنند. بنابر تحقیقات صورت‌گرفته، راه‌های مختلفی برای حمله به شهر هوشمند وجود دارد، که در بخش پیشین، بررسی شدند. در این بخش، سعی بر آن است تا حملات صورت‌گرفته به شهر هوشمند، در دنیای واقعی، مورد مطالعه قرار گیرند.

1.6 حمله به خودروهای الکتریکی تسلا

گروه خودروسازی تسلا، برندی معتبر در ساخت خودروهای الکتریکی است. در دهه‌ی اخیر، برند تسلا، اتومبیل‌های پیشرفته‌ی الکتریکی را که با فناوری و کامپیوتر آمیخته شده‌اند، تولید نموده و سعی بر آن داشته‌است تا در محصولات خود، از به‌روزترین ابزار تکنولوژیکی بهره برد. این در حالی است که صاحبان شرکت، تمهیدات امنیتی را نادیده گرفتند. در پی این کم‌توجهی، مهاجمین توانستند از طریق استراق سمع، به نقشه‌ی ارتباطی اتومبیل دسترسی پیدا کنند. این امر، تبعات ناگواری را برای صاحبان شرکت به‌همراه داشت. آنها متوجه شدند که هک کردن سیستم‌های اتومبیل شرکت برای هکرهای ماهر، امری امکان‌پذیر است.

بنابراین، شرکت تسلا توانست با کوشش بسیار، از شرکت اپل کمک گیرد و با استخدام هکری حرفه‌ای، محصولات خود را در برابر حملات احتمالی، ایمن سازد [8].

2.6 انفجار خط لوله‌ی گاز در تگزاس

در ژوئن 2010، حفر چاله‌هایی برای خطوط برق توسط کارگران، منجر به انفجار و آتش‌گرفتن یک لوله‌ی گاز 36 اینچی در جانسون کانتی تگزاس گردید. یک کارگر کشته شد و هشت نفر زخمی گردیدند. علت اصلی این فاجعه، مشخص نبودن خط لوله، به‌دلیل سردرگمی در مکان و وضعیت ساخت و ساز اعلام گردید

[6].

3.6 اختلال در چراغ‌های ترافیکی واشنگتن

در سال 2015 میلادی، حمله‌ای سایبری در واشنگتن صورت گرفت که در راس آن، تنها یک هکر قرار داشت. وی با هدف قرار دادن چراغ‌های کنترل ترافیک توانست در مدت یک روز، یکی از سنگین‌ترین ترافیک‌های اخیر را به‌وجود آورد و راه‌های اصلی شهر را به مدت یک روز، مسدود نماید. او با ارسال سیگنال‌های مشابه، کنترل چراغ‌های راهنمایی و رانندگی را در دست گرفت و از آنها به‌گونه‌ای استفاده کرد که راه موردنظر خود را پاک‌سازی و سایر راه‌ها را مسدود نمود [8].

4.6 قطعی برق اونتاریو کانادا و هشت ایالت آمریکا

در آگوست سال 2013 میلادی، یک خاموشی عظیم اتفاق افتاد که 10 میلیون نفر را در اونتاریو کانادا و 45 میلیون تَن را در هشت ایالت آمریکا، دچار دردسر کرد. علت اولیه‌ی خاموشی، یک اشکال نرم‌افزاری در سیستم آلارم اتاق کنترل شرکت FirstEnergy بود که از راه دور، در اوهایو استقرار داشت. در واقع، خطوط انتقال سرباریافته، توسط شاخ و برگ‌های هرس‌نشده‌ی گیاهان، دچار آسیب شده‌بودند و نبود آلارم، عملگرها را از توزیع مجدد توان، مطلع نمی‌ساخت [8].

5.6 دستکاری سیستم کنترل ترافیک لس‌آنجلس

در سال 2006 میلادی، دو تن از مهندسین ترافیک لس‌آنجلس، متهم به دستکاری سیستم کنترل ترافیک این شهر شدند. در واقع، آنها توانسته بودند توالی چراغ ترافیکی چهار تقاطع شهر را به‌هم بریزند و منجر به

بروز مشکلاتی شدند که طی چند روز متمادی، ادامه داشت [8].

6.6 ترافیک بزرگ‌راه اینتراِستیت 80

علت اصلی وقفه‌ی بزرگ‌راه اینتراِستیت 80[12]، قطعی کامپیوتر بود. دادگاه شهرستان پِلِیسِر کانتی[13]، به‌طور تصادفی، 1200 نفر را به عنوان هیئت‌منصفه، در همان صبح احضار کرد. ساکنین، تلاش کردند تا بنابر وظیفه، رأس ساعت 8 صبح، در محل کار خود حضور یابند. این امر موجب شد که آنها با اعضای هیئت‌منصفه، در یک خط ترافیکی قرار گیرند و در نتیجه، ترافیک سنگینی را ایجاد نمایند [8].

7.6 خاموشی حمل و نقل سریع منطقه‌ی خلیج سان‌فرانسیسکو

در نوامبر 2013 میلادی، حمل و نقل سریع منطقه‌ی خلیج سان‌فرانسیسکو (BART)[14] از کار افتاد. به‌علت یک قطعی نرم‌افزاری عمده، که در اوایل صبح رخ داده‌بود، سرویس از کار افتاد. در واقع، عامل اصلی این اتفاق، وجود یک مشکل فنی در تغییر مسیر بود که از نیمه‌های شب آغاز گردید و 19 قطار را با حدود 500 الی 1000 نفر مسافر، دچار دردسر نمود. مسافرین، از اواخر عصر الی اوایل صبح، در قطار گیر افتادند.

[12] Interstate 80
[13] Placer County
[14] San Francisco Bay Area Rapid Transit (BART)

8.6 هک سیستم مونی سان‌فرانسیسکو

در سال 2016 میلادی، یک باج‌افزار توانست به کامپیوترهای سیستم حمل و نقل شهری سان‌فرانسیسکو راه یابد و به سیستم راه‌آهن این شهر، موسوم به مونی[15]، آسیب رساند. هکرها، مبلغ 100 بیت‌کوین (معادل 70,000 دلار) را به‌عنوان باج، درخواست نمودند تا کنترل سیستم مونی را بازگردانند [9].

[15] Muni

9.6 هک علائم ترافیکی الکترونیکی در دالاس

شخصی موفق شده‌است علائم ترافیکی الکترونیکی شهر دالاس را حذف نماید و پیام "گوریل سزاوار آن است" را به جای علامت، در تابلو قرار دهد [10]. پیش از این نیز، فردی در اعتراض به ریاست جمهوری دونالد ترامپ، پیام‌هایی را در تابلوهای ترافیکی الکترونیکی قرار داده‌بود [11].

10.6حمله به سیستم آلارم دالاس

نیمه‌شب جمعه، مورخ 7 آوریل 2017 میلادی، تمامی تمامی 156 آژیر هشدار شهر، به‌صورت همزمان، به صدا درآمدند. این سیستم هشدار، که برای آگاه نمودن شهروندان از وقوع بلایای طبیعی (مانند طوفان، تندباد، و غیره) طراحی شد، سیلی از 911 تماس تلفنی از جانب شهروندان نگران را با خود به‌همراه داشت.

در واقع، حمله‌ی سایبری به این سیستم، منجر به پیدایش چنین معضلی گردید [12].

7 نتیجه‌گیری

هوشمندسازی شهرها با تکیه بر IoT، تسهیلات فراوانی را برای شهروندان فراهم آورده‌است. امروزه، شاهد آن هستیم که بزرگترین شهرهای دنیا، درصددند تا با به‌کارگیری بستر اینترنت اشیا، خدمات آنی و حاضر در همه‌جا را برای ساکنین خود فراهم سازند. مبرهن است که مکانیزم‌ها و سیستم‌های مبتنی بر اینترنت، از آسیب‌ها و تهدیدات امنیتی رنج می‌برند. در این سند، تلاش گردید تا مفهوم دقیقی از شهر هوشمند و زیرساخت‌های آن ارائه شود؛ تهدیدات و چالش‌های امنیتی آن مورد بررسی قرار گیرند؛ و در نهایت، چندین حمله‌ی صورت‌گرفته به این شهرها ذکر شود تا بتوان در تحقیقات آینده، تمهیدات امنیتی مناسبی را برای شهرهای هوشمند، تعبیه نمود.

مراجع

[1] C. Gokulnath, J. Marietta, R. Deepa, R. S. Prabhu, M. P. K. Reddy, B. R. Kavitha, "Survey on IOT based Smart City," International Journal of Computer Trends and Technology (IJCTT), Vol. 46, No. 1, pp. 23-28, April 2017.

[2] R. R. Harmon, E. G. Castro-Leon, S. Bhide, "Smart Cities and the Internet of Things," 2015 Proceedings of PICMET '15: Management of the Technology Age, pp. 485-494, 2015.

[3] ENISA, "Cyber Security for Smart Cities: An Architecture Model for Public Transport," Dec 2015.

[4] S. Talari, M. Shafie-khah, P. Siano, V. Loia, A. Tommasetti, J. P. S. Catalão, "A Review of Smart Cities Based on the Internet of Things Concept," Energies, Vol. 10, No. 421, Mar 2017.

[5] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, P. Siano, "IoT-based Smart Cities: a Survey," Environment and Electrical Engineering (EEEIC), 2016 IEEE 16th International Conference on, June 2016.

[6] C. Cerrudo, "An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks," IOActive, 2015.

[7] A. Kadam, V. Ovhal, A. Paradhi, K. Dhage, "A Survey on Smart City using IoT (Internet of Things)," International Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, Issue. 2, Feb 2016.

[8] L. Franceschi-Bicchierai, "All the Ways to Hack a Smart City," Apr 2015, https://motherboard.vice.com/en_us/article/5394e5/all-the-ways-to-hack-a-smart-city.

[9] T. Fox-Brewster, "Ransomware Crooks Demand $70,000 After Hacking San Francisco Transport System – UPDATED," Nov 2016, https://www.forbes.com/sites/thomasbrewster/2016/11/28/san-francisco-muni-hacked-ransomware/#131183084706.

[10] L. Farmer, "The Latest Electronic Traffic Sign to Be Hacked In Dallas Says, 'Gorilla Deserved It'," Jun 2016, https://www.dallasnews.com/news/news/2016/06/05/the-latest-electronic-traffic-sign-to-be-hacked-in-dallas-says-gorilla-deserved-it.

[11] K. Mettler, "Somebody keeps hacking these Dallas road signs with messages about Donald Trump, Bernie Sanders and Harambe the gorilla," Jun 2016, https://www.washingtonpost.com/news/morning-mix/wp/2016/06/06/somebody-keeps-hacking-these-dallas-road-signs-with-messages-about-donald-trump-bernie-sanders-and-harambe-the-gorilla/?utm_term=.15988cb43f38.

[12] "The Cyberattack that Put an Entire City on High Alert," Apr 2017, http://www.pandasecurity.com/mediacenter/news/dallas-cyberattack-smart-cities/.

[13]مرکز ماهر، "مقدمه‌ای بر خانه‌های هوشمند و بررسی چالش‌های امنیتی این خانه‌ها،" مستند امنیتی مرجع، فروردین 1396.

[14]مرکز ماهر، " بررسی چالش‌های امنیتی سلامت هوشمند،" مستند امنیتی مرجع، اردیبهشت 1396.