مجله‌ی علمی پژوهش در علوم رایانه، شماره ۳۱، پاییز ۱۴۰۲، ص ۱۵- ۸

ISSN: 2745-3673
http://www.Rcsj.ir

مجله علمی پژوهش در علوم رایانه (سال هشتم)
شماره ۳۱ / پاییز ۱۴۰۲ / ص ۱۵- ۸

بررسی حملات امنیتی سایبری در شهرهای هوشمند و فن آوری های موبایلی مرتبط

شهرام محمدی
مربی گروه مهندسی کامپیوتر، دانشگاه فنی و حرفه ای دختران اصفهان، اصفهان، ایران.

نام نویسنده مسئول:
شهرام محمدی

تاریخ دریافت: ۱۴۰۲/۰۵/۱۰
تاریخ پذیرش: ۱۴۰۲/۰۷/۰۶

چکیده

شهر هوشمند به شهری اشاره دارد که فن آوریهای مدرن را برای خدمات رسانی خودکار و مؤثر با هم ادغام می‌کند تا شیوه زندگی شهروندان را بهبود ببخشد. مطالعات اخیر نشان می‌دهد که تا سال ۲۰۳۰، ۶۰ درصد از کل جمعیت جهان در محیط‌های شهری زندگی خواهند کرد. این جمعیت که بطور گسترده‌ای در محیط‌های شهری در حال افزایش است، نیاز به رویکردهای پیشرفته مدیریتی را ایجاب می‌کند که از آخرین پلتفرم‌ها و تکنیک‌های IT برای هوشمندسازی هر گونه خدمات شهری بهره می‌گیرد. این یکپارچه‌سازی مبرم در فن آوری‌ها به دلیل عدم توجه به آزمون‌های امنیتی فناوری‌های جدید بکار گرفته شده و همچنین عدم مشارکت سایر بخشهای سیستمی در رویدادهای امنیتی به دلیل ارتباطات عظیم، با چالش‌های امنیتی متعددی مواجه است. از سوی دیگر، وجود پیچیدگی بالا و وابستگی شدید و ارتباطات متمرکز می‌تواند منجر به سطح نامحدودی از حملات و مسائل مرتبط با رمزنگاری شود. در این مقاله ما قصد داریم که بازنگری دقیقی را بر مبنای مطالب مربوط به معضلات مهم امنیتی شهرهای هوشمند و راهکارهای کنونی ارائه دهیم. علاوه براین، چندین مورد از عوامل مؤثری را که بر امنیت داده‌ها و اطلاعات در شهرهای هوشمند تأثیر می‌گذارند، معرفی می‌کنیم.

واژگان کلیدی: فناوری‌های شهرهای هوشمند، رایانش ابری، دستگاه‌های موبایل، امنیت سایبری.

مجله‌ی علمی پژوهش در علوم رایانه، شماره ۳۱، پاییز ۱۴۰۲، ص ۱۵- ۸

ISSN: 2745-3673
http://www.Rcsj.ir

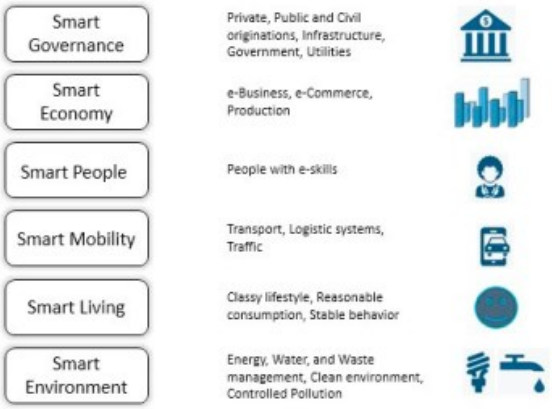
مقدمه

هیچ تعریف خاص و جامعی برای مفهوم شهر هوشمند وجود ندارد، به طوریکه کشورها و دولتهایشان، با توجه به تمایل خود برای تغییر، محدودیت‌های منابع و وضعیت مالی، تعیین می‌کنند که برای هوشمندسازی چقدر باید تلاش کنند[1]. با اینحال، ما به طور کلی از مفهوم شهر هوشمند برای یکپارچه سازی زیرساختهای سنتی و آخرین فن‌آوریهای اطلاعات و ارتباطات استفاده می‌کنیم تا سیستم کاملی را برای سرویسهای مرتبط با منابع کارآمد و شهرهای واقعی در محیطهای شهری ایجاد نماییم.

پنج عامل اصلی اساساً برای یک شهر هوشمند مورد نیاز هستند: فن آوری اطلاعات و ارتباطات مدرن، ساختمان‌ها، امکانات و زیرساختها، مدیریت حمل و نقل و ترافیک و خود شهر[2]. از نظر فنی، شهر هوشمند در صدد ایجاد همکاری بین نهادهای حکومتی و مؤسسات دولتی و خصوصی به منظور پیاده سازی و گسترش پلتفرمهای رایانه‌ای بلندمدتی است که از فن آوریهای مدرن از جمله رایانش ابری متحرک[3]، اشیاء الکترونیکی، شبکه‌ها و متدولوژیهای تصمیم گیری هوشمند بهره می‌گیرند. به طور کل، هدف شهرهای هوشمند در سراسر جهان، رسیدگی به چالش‌های اصلی پیش روی جهان حاضر است که عبارتند از تغییرات آب و هوایی، محدودیت منابع ، شهرنشینی و افزایش رشد جمعیت. علاوه بر این، هدف شهرهای هوشمند حفظ رقابت اقتصادی در محیط های شهری، و فراهم آوردن شیوه‌های زندگی برتر برای شهروندان است[4]. مفاهیم هوشمند نیز به اندازه خود شهرها، مختلف و متمایز هستند. به طور کلی، شش بعد یا حوزه وجود دارد که در آن شهرها می‌توانند هوشمندتر شوند: حاکمیت هوشمند، اقتصاد هوشمند، افراد هوشمند، تحرک هوشمند، زندگی و محیط زیست هوشمند[5] (شکل ۱).

شهر هوشمند نه تنها در صدد استفاده از پلتفرم‌های هوشمند برای اجرای مؤثر خدمات شهری است، بلکه این یک مفهوم گسترده است که اشیاء فیزیکی و الکترونیکی را که از طریق شبکه‌های باسیم و بیسیم با یکدیگر تعامل و ارتباط برقرار می‌کنند را شامل می‌شود.

از سوی دیگر، شهر هوشمند پیرامون علوم متعدد مرتبط با کامپیوتر است که در کنار فرآیند هوشمندسازی کلی مانند هوش مصنوعی، رایانش ابری، رایانش جاسازی شده و بیومتریک مورد استفاده قرار می‌گیرد. علاوه بر فن آوریهای مدرن به کار گرفته شده که به عنوان محور اصلی مقررات کلی شهر هوشمند در نظر گرفته می‌شوند، مانند RFID (سیستم شناسایی فرکانس رادیویی) و دستگاه‌های دستی هوشمند (تلفن‌ها، لپ تاپها، تبلت ها و غیره)، بدیهی است که شهرهای هوشمند، سیستم‌های پیچیده، عظیم و به هم وابسته‌ای هستند که این امر مشکلات و چالشهای متعدد سیاسی، اجتماعی، اقتصادی و فنی را بوجود می‌آورد. هزینه‌ها و تأمین بودجه ، نیازهای روزافزون و همواره متغیر جمعیت، همکاری بین ذینفعان، رابطهای کاربری عامه پسند، تعامل پذیری، امنیت و حریم خصوصی نمونه‌هایی از مسائل پیش روی شهرهای هوشمند هستند. ما در این مقاله، بر امنیت و حفظ حریم خصوصی شهرهای هوشمند تمرکز می‌کنیم، زیرا امنیت اطلاعات و حفظ حریم خصوصی داده‌ها، چالش‌های مهمی هستند که در صورت عدم توجه به آنها، آسیب‌های جدی را بوجود می‌آورند.



شکل ۱. ابعاد شهرهای هوشمند

مجله‌ی علمی پژوهش در علوم رایانه، شماره ۳۱، پاییز ۱۴۰۲، ص ۱۵- ۸

ISSN: 2745-3673
http://www.Rcsj.ir

تضمین امنیت در شهرهای هوشمند نشاندهنده حفاظت از داده‌ها، اطلاعات و شبکه‌ها در برابر هر گونه حملات و فعالیتهای مخرب است. با این حال، برخی چالشهای امنیتی وجود دارند که دستیابی به کمال امنیت را در شهرهای هوشمند پیچیده می‌سازند. سخت افزارها و نرم افزارهای به کارگرفته شده در شهرهای هوشمند، بطور معمول بدون بررسی و آزمایش مناسب و کافی از نظر امنیت سایبری از سوی فروشندگان به فروش می‌رسند. استفاده از این محصولات ناامن می‌تواند موجب هک شدن و ورود داده‌ها و اطلاعات جعلی به سیستم‌ها و در نتیجه خاموشی آنها و قطع سرویس گردد. ما برای ارزیابی چگونگی هوشمندسازی یک شهر، به سطح اتوماسیون و سیستم‌های رایانه‌ای که از آن استفاده می‌کنند و همچنین یکپارچگی بین سیستم‌های آن توجه می‌کنیم. این یکپارچگی بالا، منجر به ایجاد وابستگیهای عملیاتی از مهم‌ترین سیستم‌ها تا ساده‌ترین آن‌ها می‌شود که می‌توانند حملات آبشاری عظیمی را ایجاد کند که منجر به آسیبهایی در زیرساختها و ارتباطات کلی آن‌ها می‌شود. از سوی دیگر، شهرهای هوشمند در ارزیابی آسیب پذیریها و برنامه‌های واکنشی و بازیابی با مسائلی مواجه می‌شوند. در نهایت، توجه به امنیت مستلزم هزینه بالایی بوده و به بودجه مناسبی برای فرآیند طولانی در بخش‌های دولتی نیاز دارد.

در مجموع، مسائل مرتبط با امنیت در شهرهای هوشمند، مسائلی واقعی و رایجی هستند و مستلزم تحلیل و بررسی فوری می‌باشند. بنابراین، امنیت، حفظ حریم خصوصی و مسائل مرتبط با آن، عناوین داغی هستند به خصوص اینکه فن آوریها و سیستمهای شهر هوشمند برای بهینه سازی شهرها و بهبود کیفیت زندگی بسیار مهم هستند. ما در این مقاله چندین مورد از نگرانیهای امنیتی و حفظ حریم خصوصی در شهرهای هوشمند را مورد توجه قرار می‌دهیم. منظور ما از امنیت داده‌ها و اطلاعات، این است که این پتانسیل وجود دارد که داده‌ها و اطلاعات به طور تصادفی یا تعمدی تحت تأثیر شکستهای فنی ناشی از حملات یا فعالیتهای مخرب قرار بگیرند؛ و همچنین منظور ما از حفظ حریم خصوصی داده‌ها، توانایی محافظت از داده‌ها در برابر دسترسیهای غیرمجاز یا استفاده مجدد از آنها و نیز حفظ فرایندهای جمع آوری داده‌ها و اجرای همه عملیات و فرایندها بر روی آن می‌باشد.

کارهای مرتبط

امنیت و حریم خصوصی همیشه عناوین داغی برای بحث کردن هستند. برای شهر هوشمند، نگرانی‌های امنیتی و حفظ حریم خصوصی حتی مهمتر از هر گونه پدیده تکنولوژیکی دیگر است، زیرا تعداد شهرهای هوشمند بسرعت در سراسر جهان در حال افزایش است. بنابراین، محققان باید توجه بیشتری به مسائل مربوط به امنیت و حفظ حریم خصوصی در شهرهای هوشمند معطوف نمایند تا مطالبی غنی از تحقیقات و مطالعات بیشتر را در این زمینه فراهم آورند. ما در این مقاله، به بررسی چندین تحقیق ارزشمند که در مورد چالشهای امنیتی و حفظ حریم خصوصی و مسائل مرتبط با آن بحث می‌کنند، پرداخته‌ایم.

در[۶]، نویسندگان شهرهای هوشمند را در به عنوان گردآوری اطلاعات و فناوریهای ارتباطات مطابق با آخرین پیشرفت‌های علمی می‌دانند و به بحث در مورد مسائل کنونی شهری و فن‌آوریهای مدرن شهری می‌پردازند. علاوه براین، آن‌ها ریسک‌ها وابهامات کنونی در شهرهای هوشمند را با تعریف شش سناریوی شهرهای معروف به شهر هوشمند تصریح می‌کنند. این مقاله در [۷]، اطلاعاتی را در مورد الزامات، مزایا و چالشهای موجود در حوزه‌های پژوهشی شهر هوشمند فراهم می‌آورد. همچنین در مورد نسخه تازه‌ای از ابر اشیا (CoT) بحث می‌کند که تلفیقی از فن آوری اینترنت اشیا و علم رایانش ابری CC است و بحثهایی را در رابطه با نحوه ارائه این خدمات شهرهای هوشمند بر مبنای ابر اشیا ارائه می‌دهد.

در[۹]، نویسندگان از طریق ارائه مدلی که عوامل اصلی شهرهای هوشمند (سرورها، افراد و اشیاء) و تعامل بین آنها را نشان می‌دهد، به بررسی نگرانیهای امنیتی و حفظ حریم خصوصی می‌پردازند. این نویسندگان در[۱۰]، در مورد مقررات مربوط به نقض امنیت و حریم خصوصی بحث می‌کنند و اظهار می‌دارند که این مقررات با اهمیت و ضرورت مسائل امنیتی و حفظ حریم خصوصی تناسبی ندارد.

بدیهی است که شهرهای هوشمند مزایای هنگفتی را برای کاربران به همراه دارند، اما در عین حال کاربران نگران حفظ حریم خصوصی داده‌های خود هستند که از طریق کانالهای نا امن منتقل می‌شوند. بنابراین کانالهای ارتباطی باید به منظور فراهم آوردن رسانه‌های امن برای انتقال داده‌ها به خصوص از طریق شبکه‌های بی سیم ایمن سازی شوند [۱۱،۱۲]. در[۱۳]، نویسندگان

ISSN: 2745-3673
http://www.Rcsj.ir

درباره توازن حریم خصوصی با شهر هوشمند به بحث می‌پردازند. آن‌ها در مورد جوانب منفی که ممکن است شهرهای هوشمند در زندگی ما در خصوص نقض حریم خصوصی بوجود آورند گفتگو می‌کنند. کاربران باید توجه زیادی به آنچه به اشتراک می‌گذارند داشته باشند و باید بدانند زمانیکه هر بخشی از داده‌های شخصی خود را به اشتراک بگذارند، این داده‌ها آشکار خواهند بود. طراحان و تحلیلگران باید در مورد ضرورت تفکر در مورد حفاظت از داده‌ها در مقابل آسیب‌پذیری‌های امنیتی در طی طراحی شهر هوشمند آگاه باشند. فن آوریهای زیرساختی-سایبری باید در طی فرآیند طراحی به منظور پیش بینی عملکرد شهر هوشمند مشخص شوند.

امنیت در شهر هوشمند

ما عنوان کرد ایم که به کمال رساندن یک شهر خاص و تبدیل آن به یک شهر هوشمند، یک فرایند کاملاً ماهرانه، چالش برانگیز و هوشمندانه است، به طوریکه مستلزم سطح وابستگی و ارتباط بالایی در سراسر لایه‌های مختلف آن (داده‌ها، اطلاعات، فن آوری، کاربردها و زیرساختها) می‌باشد. در این بخش، ما چالشهای مهم امنیتی و تخلفات مرتبط با آن را که می‌توانند در هر لایه از هوشمندسازی یک شهر صورت بگیرند، ارائه می‌دهیم.

امنیت زیرساخت

آسیب پذیریها و ریسکهای متعددی پیش روی زیرساختهای فیزیکی سایبری مورد استفاده در هوشمندسازی شهرها وجود دارند. با این وجود، این سیستم‌های زیرساخت‌های فیزیکی سایبری مدرن به طور گسترده‌ای مورد استفاده قرار می‌گیرند، اما هیچ دیدگاه رضایت بخشی در مورد آسیب پذیریها و تهدیدات آنها ارائه نمی‌شود. به طور کلی تهدیدات تعمدی یا تصادفی در مورد امنیت زیرساختهای شهر هوشمند، پیامدهای جدی مختلفی را بر کمال و هوشمندی یک شهر در پی دارد. از این رو ما تهدیدات و چالشهای مهم پیش روی امنیت زیرساختها را ارائه می‌کنیم. زیرساخت‌های شهری مانند تأمین برق، توزیع آب، خیابان‌ها، ساختمان‌ها و موارد دیگر با تهدیدات خاص امنیتی در سیستمها و اجزای فیزیکی سایبری مواجه هستند که عبارتند از:

- دوربین‌ها: شهرها پر از دوربینهای خصوصی و عمومی هستند که هر دوی اینها با استفاده از حفاظت رمزگذاری، و حفاظت از نام کاربری/ رمز عبور، بطور متفاوتی محافظت می‌شوند. گسترش این دوربینهای خصوصی و عمومی و دسترسی به آن‌ها می‌تواند موجب نقض حریم خصوصی افراد شده و به عنوان جاسوسی محسوب شود و به نگرانیهای حکومتی بینجامد.
- شبکه‌های ارتباطات: اشیاء فیزیکی سایبری در یک شهر هوشمند با استفاده از فن آوریهای مختلف ارتباطات مانند وای فای، 4G, RFID, GSM و موارد دیگر به یکدیگر متصل می‌شوند. هر یک از این‌ها نگرانی‌های امنیتی مختص خودشان را دارند که باید در طی گسترش و استفاده از فن آوریهای ارتباطات مورد توجه قرار گیرند.
- ایجاد سیستمهای مدیریت: طراحان و توسعه دهندگان چنین سیستمهایی، معمولاً بر سرویسهای ارائه شده متمرکز هستند و مسائل مربوط به امنیت سایبری را نادیده می‌گیرند. بنابراین، تولیدکنندگان این سیستمها هرگز با گزینه‌های پیامهای هشدار دهنده به کاربران در مورد تخلفات امنیتی از آنها پشتیبانی نمی‌کنند و نسبت به این آسیب پذیریها پاسخگو نیستند که این امر منجر به ایجاد سیستمهای مدیریتی ناامن و ضعیفی می‌شود.
- سیستم‌های مدیریت حمل ونقل: این سیستم‌ها با مهمترین موارد هک (سرقت اطلاعات) مواجه می‌شوند، به طوریکه می‌توانند فجایعی را به ویژه در سیستمهای ترافیک هوایی یا کنترل قطار به بار آورند. علاوه براین، ترافیک‌های سنگینی را به وجود می‌آورند که ممکن است با هک سیستمهای کنترل بر چراغهای راهنما و تابلوهای راهنمایی رانندگی و تابلوهای حد سرعت مجاز، تا چندین ساعت به طول انجامند.

اساساً زیرساختهای شهری، ترکیبی از سیستمهای فیزیکی سایبری هستند که با اجزای مستقل فیزیکی ادغام شده‌اند. CPSها شامل اشیاء فیزیکی به هم متصل مانند حسگرها، عوامل محاسباتی، اشیاء شبکه و ... می‌باشند. در شهرهای هوشمند، CPSها باید سه وظیفه مهم را به انجام برسانند که عبارتند از جمع آوری داده‌ها، تصمیم گیری در مورد اجرای فرآیندهای مؤثر

مجله‌ی علمی پژوهش در علوم رایانه، شماره ۳۱، پاییز ۱۴۰۲، ص ۱۵- ۸

ISSN: 2745-3673
http://www.Rcsj.ir

و کنترل اجزای فیزیکی. در ادامه، ما به طور خلاصه به تهدیدات مهم پیش روی یکپارچه سازی زیرساختهای شهری اشاره می‌کنیم:

استراق سمع : قرار دادن ابزار استراق سمع در شبکه خاصی به منظور جاسوسی در کانالهای ارتباطاتی و دستیابی به نحوه ترافیک شبکه و نقشه آن. استراق سمع تهدید خطرناکی است که منجر به از بین رفتن یکپارچگی و حریم خصوصی شده و می‌تواند شکستهای مالی و شخصی را به بار آورد.

سرقت : این آیتم با سرقت اشیاء نامحسوس مانند داده‌ها و اطلاعات حساس، گواهی نامه‌ها، کلیدهای رمزنگاری و نرم افزاری؛ و همچنین سرقت اشیای فیزیکی محسوس مانند دستگاههای دستی مثل تلفنهای هوشمند، لپ تاپها و تبلتها و ...) و سایر تجهیزات تکنولوژیکی، زیرساخت‌های شهری را تحت تأثیر قرار می‌دهد. این امر می‌تواند در دسترس پذیری و محرمانگی سیستمها اختلال ایجاد کند و موجب مشکلات مالی و از بین رفتن اعتبار شود.

ممانعت از سرویسDoS: این آیتم به سر ریز ارتباطات تا مسدود شدن سرویسها و دستگاههای مبتنی بر این ارتباطات اشاره دارد. حملات DoS دسترس پذیری سیستمها یا ارتباطات را تحت تأثیر قرار می‌دهد.

تهدیدات دیگر می‌توانند به دلیل شکستهای سخت افزاری، اشکالات نرم افزاری، عملکرد محیطی و طبیعی و همچنین خاتمه پشتیبانی فروشندگان و تولیدکنندگان ایجاد شوند. چنین تهدیداتی می‌توانند بر دسترس پذیری و یکپارچه سازی سیستمهای زیرساختی تأثیر بگذارند و موجب اشکالاتی در ارائه خدمات و امر تولید شوند.

حریم خصوصی اطلاعات/ داده‌ها در شهرهای هوشمند

شهرهای هوشمند با حجم عظیمی از داده های واقعی و فن آوریهای مرتبط سر و کار دارند که فن آوریهای داده محوری هستند که بر فرایند ایجاد، پردازش، اجرا و تولید داده‌ها تأثیر می‌گذارند. شهرهای هوشمند، دارای منابع زیادی برای تولید داده‌های مختلف می‌باشند. در بین این منابع، سیستم‌هایی قرار دارند که بطور پیوسته داده‌های منحصربفرد و مناسبی را ایجاد می‌کنند. این سیستمها در شهرهای هوشمند متداول بوده و داده‌هایی که تولید می‌کنند داده‌های بزرگ نامیده می‌شوند[۱۴،۱۵]. سیستم‌های دیگر نیز داده‌های سنتی و کوچک را به مجموعه دادههای زیرساخت انتقال می‌دهند که به چند طریق مورد استفاده قرار می‌گیرند. سیستم‌هایی وجود دارند که داده‌های قفل شده را به صورت داده‌های باز در دسترس عموم قرار می‌دهند. یکی از سیستمهای دیگر، سیستم‌های مرتبط با یادگیری ماشین است که داده‌های و تجزیه و تحلیل داده‌ها را توسعه می‌دهد. همه این داده‌های شهری برای اجرای فن آوریهای شهر هوشمند مورد استفاده قرار می‌گیرند ، بنابراین ایمن نگه داشتن حجم گسترده این داده‌ها و اطلاعات اهمیت دارد. علاوه براین، حفظ حریم خصوصی داده‌های قفل شده و داده‌های شخصی و همچنین حصول اطمینان از عدم دسترسی تصادفی یا عمدی به آنان حائز اهمیت است. حفظ حریم شخصی با محافظت از ۵ مسئله مرتبط در این حوزه، تضمین می‌شود: حفاظت از هویتها: که حفاظت از دادههای شخصی و محرمانه پرسنل را نشان می‌دهد. حفاظت از حوزه‌های افراد: که حفاظت از مکان و سرمایه هر شخص را نشان می‌دهد، حفاظت از موقعیتهای مکانی: که جلوگیری از ردیابی مکانی را نشان می‌دهد، حفاظت از ارتباطات: که از استراق سمع هر گونه مکالمات جلوگیری می‌کند و در نهایت حفاظت از تراکنشها: که از هر گونه خرید، مبادله و جستار محافظت می‌کند. مسائل مربوط به حریم خصوصی را می‌توان به سه دسته تقسیم نمود: حریم خصوصی ارتباطات، فردی و کسب وکار[۱۶] (جدول ۱).

جدول ۱. چالش‌ها و تخلفات مربوط به حریم خصوصی

دسته بندی	چالش‌های مرتبط با حریم خصوصی	تخلفات	توصیف
حریم خصوصی ارتباطات	ارتباط M2M ارتباط شهروندان با شهر هوشمند	استراق سمع	جاسوسی کردن از همه مکالمات و رکوردها و گوش دادن به کانالهای ارتباطاتی؛ و یا بازخوانی داده ها با استفاده از ریدرهای غیرمجاز [۱۷]
		DOS	مسدود کردن همه عملیات سیستم با استفاده از سیگنالهای

ISSN: 2745-3673
http://www.Rcsj.ir

			رادیویی برای دستگاههای پخش به منظور اهداف مخرب؛ و یا اصطلاحاً کور کردن شهرهای هوشمند [۱۸]
		حمله مردی در میان	جدا کردن کانالهای ارتباطی برای دستکاری داده‌های انتقال یافته و اقدامات اپراتورهای جعلی [۱۹]
		حملات کانال کناری	استفاده از هرگونه اطلاعات در مورد پیاده سازی فیزیکی امور محاسباتی مانند مصرف انرژی و زمان اجرا [۱۹،۲۰]
		احراز هویت	مرتبط ساختن داده‌ها و اطلاعات با کسی که به آن تعلق دارند
		استفاده ثانویه	استفاده از داده‌ها و اطلاعات جمع آوری شده بر اساس مجوز و استفادهٔ خاص آن برای اهداف غیر مجاز دیگر
حریم خصوصی کسب و کار	بانکداری تجارت الکترونیک	فیشینگ	جعل کردن هویت طرف مشهور و مورد اعتماد به منظور کسب اطلاعات مهم مانند رمز عبور یا شماره کارتهای اعتباری او از طریق ایمیل و پیامک [۲۱]
		اسپوفینگ (حملات جعل)	تکثیر داده‌ها توسط عامل مخرب سوم و ارسال آن به خواننده پس از فاش سازی پروتکل امنیتی [۱۶]
		حمله به یکپارچگی داده‌ها	دریافت اطلاعات در مورد مشتریان و شبکه‌ها و تزریق اطلاعات کاذب به مرکز نظارت بر سیستم [۲۲]

نتیجه گیری

امنیت سایبری شهر هوشمند، مسئله مهمی است که با نگرانیهای امنیتی در خصوص فن آوری، کاربردها، زیرساخت‌ها و دادهها / اطلاعات همراه می‌باشد. امنیت سایبری عمدتاً تحت تأثیر یکپارچه سازی مبرم فن آوریها و ارتباطات فشرده حاصل از آن، پیچیدگی و وابستگی بالا قرار دارد که منجر به سطح نامحدودی از حملات و مسائل مرتبط با رمزنگاری می‌شود. امنیت سایبری شهرهای هوشمند، مسئله مهمی است که مستلزم همکاری بین المللی کارشناسان از سراسر جهان می‌باشد.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] SIEMENS. Available from: <http://www.siemens.com/innovation/en/home/pictures-of-the-future/infrastructureand-finance/smart-cities-facts-and-forecasts.html>. [Jan 2017]
[2] FORBES. Available from: < http://www.forbes.com/sites/peterhigh/2015/03/09/the-top-five-smart-cities-in-theworld/#5715497d5a0e> [Dec 2016]
[3] Tawalbeh LA, Alassaf N, Bakheder W, Tawalbeh A. Resilience Mobile Cloud Computing: Features, Applications and Challenges. In 2015 Fifth International Conference on e-Learning (econf) 2015 Oct 18 (pp. 280-284). IEEE.
[4] Lo'ai AT, Basalamah A, Mehmood R, Tawalbeh H. Greener and smarter phones for future cities: Characterizing the impact of GPS signal strength on power consumption. IEEE Access. 2016;4:858-68.
[5] Vanolo A. Smartmentality: The smart city as disciplinary strategy. Urban Studies. 2013 Jul 11:0042098013494427.
[6] Batty M, Axhausen KW, Giannotti F, Pozdnoukhov A, Bazzani A, Wachowicz M, Ouzounis G, Portugali Y. Smart cities of the future. The European Physical Journal Special Topics. 2012 Nov 1;214(1):481-518.
[7] Petrolo R, Loscrì V, Mitton N. Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms. Transactions on Emerging Telecommunications Technologies. 2015 Feb 1.
[8] Tawalbeh LA, Haddad Y, Khamis O, Aldosari F, Benkhelifa E. Efficient software-based mobile cloud computing framework. InCloud Engineering (IC2E), 2015 IEEE International Conference on 2015 Mar 9 (pp. 317-322). IEEE.
[9] Elmaghraby AS, Losavio MM. Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of advanced research.2014 Jul 31;5(4):491-497.
[10] Bartoli A, Hernandez-Serrano J, Soriano M, Dohler M, Kountouris A, Barthel D. On the Ineffectiveness of Today's Privacy Regulations for Secure Smart City Networks. Smart Cities Council, Washington, DC. 2012 Nov.
[11] Sklavos N, Zhang X. Handbook of Wireless Security: From Specifications to Implementations. CRC-Press, A Taylor and Francis Group, ISBN X. 2007;84938771:2007.
[12] Moh'd A, Aslam N, Marzi H, Tawalbeh LA. Hardware implementations of secure hashing functions on FPGAs for WSNs. InProceedings of the 3rd International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2010 Jul.
[13] Ahmed KB, Bouhorma M, Ahmed MB. Age of big data and smart cities: privacy trade-off. arXiv preprint arXiv:1411.0087. 2014 Nov
[14] Lo'ai AT, Bakheder W, Song H. A mobile cloud computing model using the cloudlet scheme for big data applications. InConnected Health: Applications, Systems and Engineering Technologies (CHASE), 2016 IEEE First International Conference on 2016 Jun 27 (pp. 73-77). IEEE.
[15] Lo'ai AT, Mehmood R, Benkhlifa E, Song H. Mobile cloud computing model and big data analysis for healthcare applications. IEEE Access. 2016;4:6171-80.
[16] Ijaz, Sidra, Munam Ali Shah, Abid Khan, and Mansoor Ahmed. "Smart Cities: A Survey on Security Concerns." INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS 7, no. 2 (2016): 612-625.
[17] Cédric, LÉVY-BENCHETON, Eleni DARRA, Daniel Bachlechner, Michael Friedewald, Timothy MITCHENER-NISSEN, Monica LAGAZIO, and K. U. N. G. Antonio. "Cyber Security for Smart Cities-an Architecture Model for Public Transport. pdf." (2015).
[18] Oliveira LM, Rodrigues JJ, Sousa AF, Lloret J. Denial of service mitigation approach for IPv6-enabled smart object networks. Concurrency and Computation: Practice and Experience. 2013 Jan 1;25(1):129-42
[19] Lo'ai AT, Somani TF. More Secure Internet of Things Using Robust Encryption Algorithms Against Side Channel Attacks.

ISSN: 2745-3673
http://www.Rcsj.ir

[20] Lo'ai AT, Somani TF, Houssain H. Towards secure communications: Review of side channel attacks and countermeasures on ECC. In Internet Technology and Secured Transactions (ICITST), 2016 11th International Conference for 2016 Dec 5 (pp. 87-91). IEEE

[21] TechTarget. Available from < http://searchsecurity.techtarget.com/definition/phishing> [Jan 207]

[22] Nanni G. (2013/. Transformational ‘smart cities’: cyber security and resilience. Symantec, Mountain View, CA.