# برنامه‌های کاربردی شهر هوشمند

## مبتنی بر امنیت و حریم خصوصی


**سید فرزین موسوی‌تبار کانی و دیگران ***

**F.Musavi546541@gmail.com**

* سایر نویسندگان: فرزاد حسین‌زاده، آذر قناتی و فریده ده‌حقی. این مقاله، توسط هیئت تحریریه فصلنامه، تلخیص و ویرایش شده است.

**اشاره**

با شکوفایی و رشد اینترنت اشیا، شهر هوشمند به یک پارادایم نوظهور تبدیل شده است که شامل: سنجش همه جا حاضر، زیرساختارهای شبکه‌ای ناهمگن و سیستم‌های کنترل و پردازش اطلاعات هوشمند است. یک شهر هوشمند، می‌تواند دنیای فیزیکی را در زمان واقعی نظارت کند و سرویس‌های هوشمندی برای ساکنان محلی و مسافران ارائه نماید؛ خدماتی چون: حمل و نقل، بهداشت و درمان، محیط، سرگرمی و انرژی. بااین‌حال، نگرانی‌هایی در مورد امنیت و حفظ حریم خصوصی به‌وجود می‌آیند؛ زیرا برنامه‌های کاربردی شهر هوشمند، نه تنها طیف گسترده‌ای از اطلاعات حساس به حریم خصوصی را برای مردم و محافل اجتماعی جمع وری می‌کنند، بلکه امکانات شهر را کنترل می‌نمایند و زندگی مردم را تحت تأثیر قرار می‌دهند. در این مقاله، به بررسی امنیت و حریم خصوصی در برنامه‌های کاربردی شهرستان هوشمند می‌پردازیم.

به طور خاص در ابتدا، برنامه‌های کاربردی امیدوارکننده شهر هوشمند و معماری آن را معرفی می‌کنیم. سپس، چالش‌های

حفظ حریم خصوصی و امنیت را در این برنامه‌های کاربردی مورد بحث قرار می‌دهیم. برخی از تلاش‌های تحقیقاتی انجام

شده‌اند تا به این چالش‌های حریم خصوصی و امنیت برای مراقبت‌های بهداشتی هوشمند، حمل و نقل، انرژی هوشمند بپردازند. در نهایت، به برخی از مسائل باز برای تحقیقات آینده نیز اشاره خواهیم کرد.

**کلیدواژگان:** شهر هوشمند، اینترنت، برنامه‌های کاربردی شهر، حفظ حریم خصوصی، امنیت.

## برنامه‌های کاربردی شهر هوشمند و معماری

یک شهر هوشمند، جهان فیزیکی و جهان اطلاعاتی را به هم متصل می‌کند و بسیاری از برنامه‌های کاربردی هوشمند، از محلی تا جهانی از سنجش تا کنترل ظاهر می‌شوند. در این بخش، برنامه‌های کاربردی شهر هوشمند و معماری ناهمگن را معرفی می‌کنیم.

## الف. برنامه‌های کاربردی شهر هوشمند

برنامه‌های کاربردی شهر هوشمند، از جنبه‌های مختلف برای افراد و شهر سودمند است؛ انرژی، محیط، صنعت، زندگی و خدمات. ما برنامه‌های کاربردی متعدد را به شرح زیر معرفی می‌نماییم:

**ـ انرژی هوشمند**

بهره‌برداری گسترده از حسگرهایی که به طور گسترده برای نظارت بر تولید انرژی، انتقال، توزیع و مصرف و انرژی هوشمند و کاربرد سودمند، شارژ وسایل الکتریکی و شبکه هوشمند و غیره به‌کار گرفته شده‌اند، نه تنها این روند می‌تواند مصرف انرژی را در ابعاد مختلف کاهش دهد، بلکه می‌تواند مانع از قطع شبکه توان و شکست در کاربردی انرژی شود.

**ـ محیط زیست هوشمند**

محیط زیست هوشمند، به گونه‌ای ارتقا یافته است که از محیط زیست پایدار و آب‌وهوای مناسب برای شهر هوشمند حمایت کند. روند مدیریت آب‌وهوای هوشمند و سنجش همه جا حاضر به طور مشترک برای برنامه‌های کاربردی محیط هوشمند استفاده می‌شوند. به این ترتیب، می‌توان بر گاز پسماند، گاز گلخانه‌ای و سروصدای شهر، آلودگی آب‌وهوا و شرایط جنگل و غیره نظارت کرد و در نهایت، از عهده توسعه پایدار و هوشمند برآمد.

**ـ صنعت هوشمند**

با وجود محرک اصلی توسعه پایدار صنعتی در شهر هوشمند، صنعت هوشمند به گونه‌ای توسعه یافته است تا تولید صنعتی و ساخت‌وساز را بهینه‌سازی کند و در عین حال، به کارایی و استحکام و قدرت مناسب دست یابد. از یک سو، این روش باعث می‌شود مصرف منابع و مواد در طی فرآیندهای صنعتی محدود شوند و از سوی دیگر، مانع از انتشار بیش از حد و اتلاف گاز و گرمای صنعتی می‌شود. هر دو روند کنترل و سنجش، به میزان برابری در صنعت هوشمند مفید هستند و به عملیات دقیق و بازخورد بلادرنگ مناسبی نیاز دارند. در نهایت، دستگاه‌های Servo و موتورها و ربات‌ها استفاده شده‌اند، تا کنترل دقیق و عملیات نهایی را در صنعت هوشمند ارائه نمایند.

**ـ زندگی هوشمند**

در ناحیه خانه، زندگی هوشمند مدیریت هوشمند دستگاه‌ها و امکانات مختلف را ارائه می‌کند و خانه‌های راحتی به‌وجود می‌آورد و به طور هم‌زمان، بهره‌وری انرژی را بهبود می‌بخشد. همچنین، این روند می‌تواند کنترل از راه دور لوازم خانه، تنظیمات آب‌وهوا، صرفه‌جویی در انرژی، نظارت و سرگرمی و آموزش و پرورش را نیز لحاظ کند. در جامعه [یا ساختمان]، برنامه‌های کاربردی زندگی هوشمند، به طور هوشمندانه‌ای، بازیافت زباله، شبکه‌های اجتماعی و پارکینگ را مدیریت می‌کند و یک جامعه هوشمند [با ساختمان هوشمند] با زندگی راحت، خدمات صمیمی، تجارب فوق‌العاده و محیط زیست و انرژی پایدار ایجاد می‌کند.

**ـ خدمات هوشمند**

خدمات هوشمند، باعث می‌شوند سرویس‌ها و امکانات عمومی در طیف وسیعی از جنبه‌ها به مردم سود برسانند؛ برای مثال، حمل‌ونقل

**اجزای سنجش و بررسی، از دستگاه‌های پوشیدنی، سنسورهای صنعتی و دستگاه‌های هوشمند بهره می‌گیرند تا اطلاعات دنیای فیزیکی را اندازه‌گیری و سنجش کنند و این اطلاعات را برای تصمیم‌گیری به واحد پردازش ارسال نمایند؛ به عبارت دیگر، اجزای سنجش و اندازه‌گیری، مانند پلی هستند که جهان اطلاعات و فیزیکی را به هم متصل می‌سازند. دستگاه‌های سنجش، توسط دولت‌ها، ادارات و شرکت‌ها مستقر شده‌اند و یا توسط کاربران به‌کار گرفته شده‌اند**

هوشمند می‌تواند به ساکنان محلی و مسافران کمک کند تا از تراکم ترافیک‌های جاده‌ای اجتناب کنند و ناوبری جاده انجام دهند و نقاط مورد نظر را شناسایی نمایند و برنامه‌ریزی سفر را مدیریت کنند و غیره. با استفاده از حسگرهای استقراریافته، دوربین‌های تقاطع‌ها، GPS و گوشی‌های هوشمند افراد داخل جاده، می‌توان اطلاعاتی لازم در این حوزه مانند ترافیک جاده‌ای را به‌دست آورد. مرکز کنترل، برنامه‌های جاده‌ای مسافران را تنظیم می‌کند و به گوشی‌های هوشمند و یا GPSهای آنها بازخورد می‌دهد. علاوه بر این، با مدیریت چراغ‌های راهنمایی و ابزارهای حمل‌ونقل عمومی، مانند: اتوبوس، قطار و دوچرخه‌های اشتراکی نیز می‌توان ترافیک جاده‌ای را تنظیم کرد. به منظور ارائه مراقبت‌های بهداشتیِ باکیفیت، باید رویکردهای مراقبت‌های بهداشتی هوشمند، نظارت پیوسته‌ای بر سلامت داشته باشند و تشخیص به‌موقع را برای افراد یک شهر هوشمند انجام دهند. این روند، می‌تواند متکی بر دستگاه‌های پوشیدنی و حسگرهای پزشکی باشد که شرایط سلامت کاربران را اندازه‌گیری و سنجش می‌کنند و اطلاعات مربوط به سلامت آنها را به واحد پردازش می‌فرستند تا پزشکان به تشخیص آن بپردازند. همچنین، دسترسی آسان به اطلاعات جامع بهداشت و سلامت قبلی کاربر فراهم می‌آورد و به طور قابل توجهی، احتمال تشخیص بیماری‌های عفونی و یا مزمن را در مراحل اوّلیه افزایش می‌دهد. علاوه بر این، مراقبت‌های بهداشتی هوشمند، شامل برنامه‌های کاربردی مربوط به سلامت متنوعی هستند؛ مانند مراقبت در منزل، هشدار اورژانس و تناسب اندام و آموزش هوشمند.

**ب. معماری شهر هوشمند**

برای اینکه به مدیریت دقیق شهری و سنجشِ همه‌جاحاضر دست یابیم، شهر هوشمند، اطلاعات به‌دست‌آمده از جهان فیزیکی و اطلاعات انتقال‌یافته در جهان ارتباطاتی و اطلاعات پردازش‌شده در جهان اطلاعاتی برای سرویس‌های هوشمند را تغییر می‌دهد. شهر هوشمند، از اجزای سنجش، زیرساخت‌های شبکه ناهمگن، واحدهای پردازش و مؤلفه‌های عملیات و کنترل استفاده می‌کند.

**اجزای سنجش و بررسی**

اجزای سنجش و بررسی، از دستگاه‌های پوشیدنی، سنسورهای صنعتی و دستگاه‌های هوشمند بهره می‌گیرند تا اطلاعات دنیای فیزیکی را اندازه‌گیری و سنجش کنند و این اطلاعات را برای تصمیم‌گیری به واحد پردازش ارسال نمایند؛ به عبارت دیگر، اجزای سنجش و اندازه‌گیری، مانند پلی هستند که جهان اطلاعات و فیزیکی را به هم متصل می‌سازند. دستگاه‌های سنجش، توسط دولت‌ها، ادارات و شرکت‌ها مستقر شده‌اند و یا توسط کاربران به‌کار گرفته شده‌اند. علاوه بر این، با توجه به محدودیت‌های اندازه دستگاه، باتری و قابلیت‌های پردازش، این دستگاه‌های سنجش با منابع محدود معمولاً داده‌های ریزدانه و بلادرنگ را پیش‌پردازش و یا فشرده می‌کنند و آن را به شبکه می‌فرستند.

**۱. شبکه‌های ناهمگن**

با همزیستی دستگاه‌های سنجش عظیم و برنامه‌های کاربردی مختلف، اطلاعات سنجش به شیوه‌های گوناگون جمع‌آوری شده‌اند که در آن زیرساخت‌های شبکه‌های ناهمگن، نقش اصلی را در پشتیبانی از شهرهای هوشمند ایفا می‌کنند. شبکه‌های ناهمگن، شبکه‌های سلولی، شبکه‌های ناحیه محلی بی‌سیم (WLAN) و شبکه‌های ناحیه‌گسترده (WAN) و ارتباطات دستگاه‌به‌دستگاه (D2D) و ارتباطات موج

میلی‌متری و شبکه‌های حسگر و غیره را با هم ترکیب می‌کند و سوئیچینگ بدوی مشکلی در میان انواع مختلف شبکه‌ها ایجاد می‌کند. شبکه‌های ناهمگن، جهان ارتباطی در شهر هوشمند را نشان می‌دهند و جهان اطلاعاتی و فیزیکی را به هم متصل می‌کنند.

**۲. واحد پردازش**

واحد پردازش، از سِرورهای محاسبات ابری قدرتمند و پایگاه داده‌های فراوان و سیستم‌های کنترل اختصاصی برای تحلیل و پردازش اطلاعات سنجشِ جمع‌آوری‌شده از جهان فیزیکی، برای تصمیم‌گیری استفاده می‌کند. واحد پردازش، جهان اطلاعاتی در شهر هوشمند را مدیریت می‌کند. اشخاص مجاز، مانند: دولت، بیمارستان‌ها، کارخانه‌ها و کاربران، امتیازات و مجوزهای خاصی دارند تا به اطلاعات جمع‌آوری‌شده دسترسی یابند. آنها می‌توانند الزامات و یا سیاست‌های تصمیم‌گیری و کنترل شهر هوشمند را تعیین نمایند.

**۳. مؤلفه‌های عملیاتی و کنترل**

با تنظیم روند بهینه‌سازی و تصمیمات واحد پردازش، یک شهر هوشمند به گونه‌ای بازخورد می‌دهد که جهان فیزیکی، از طریق و گوشی‌های هوشمند، تغییر کند؛ مانند مؤلفه‌های servo و گوشی‌های هوشمند. این مؤلفه‌های عملیاتی و کنترل، تنظیماتی را در محیط فیزیکی به‌وجود می‌آورند؛ به گونه‌ای که کیفیت زندگی را بالا ببرند که این روند در شهر هوشمند پیشنهاد شده است. آنها همچنین، جریان دوطرفه شهر هوشمند را پیاده‌سازی می‌کنند. نه تنها این جریانِ دومسیره می‌تواند دانشی در مورد جهانِ فیزیکی به‌دست آورد، بلکه می‌تواند هر دستگاه و یا مؤلفه را در شهر هوشمند مدیریت و نظارت نماید؛ به‌طوری‌که آن دستگاه از نظر عملیاتی، خوب و هوشمند کار کند.

## مسائل حریم خصوصی و امنیت در شهر هوشمند

با وجود اینکه شهرها به دنبال هوشمندتر شدن هستند، برنامه‌های کاربردی شهرهای هوشمند، نگرانی‌ها و چالش‌هایی از نظر امنیت و حریم خصوصی ایجاد می‌کنند. به عنوان یک پارادایم شبکه‌بندی و اطلاعاتی، شهر هوشمند باید بتواند از اطلاعات به‌دست‌آمده در برابر دسترسی‌های غیرمجاز، افشا، اختلال و اصلاح و بازرسی و نابودی دفاع کند. الزامات اساسی امنیت و حفظ حریم خصوصی، از جمله محرمانگی و یکپارچگی و عدم انکار و دسترس‌پذیری و کنترل دسترسی و حفظ حریم خصوصی، باید در جهان فیزیکی، ارتباطی و اطلاعاتی ارضا شوند. علاوه بر این الزامات کلی، تأمین امنیت یک شهر هوشمند، با مجموعه‌ای از چالش‌های منحصربه‌فرد روبه‌روست.

از یک سو، شهر هوشمند، اطلاعات حساس به حریم خصوصی و مقیاس ریزدانه را از محیط اطراف و زندگی خصوصی افراد جمع‌آوری می‌کند و از سوی دیگر، این اطلاعات را پردازش می‌نماید و بر زندگی افراد اثر می‌گذارد و یا شاید آنها را تغییر می‌دهد. با توجه به این ویژگی‌های منحصربه‌فرد، مسائل امنیت و حفظ حریم خصوصی، چالش‌برانگیز بوده و مانع از این می‌شوند که شهر هوشمند برای استفاده مناسب، وسوسه‌انگیزتر شود.

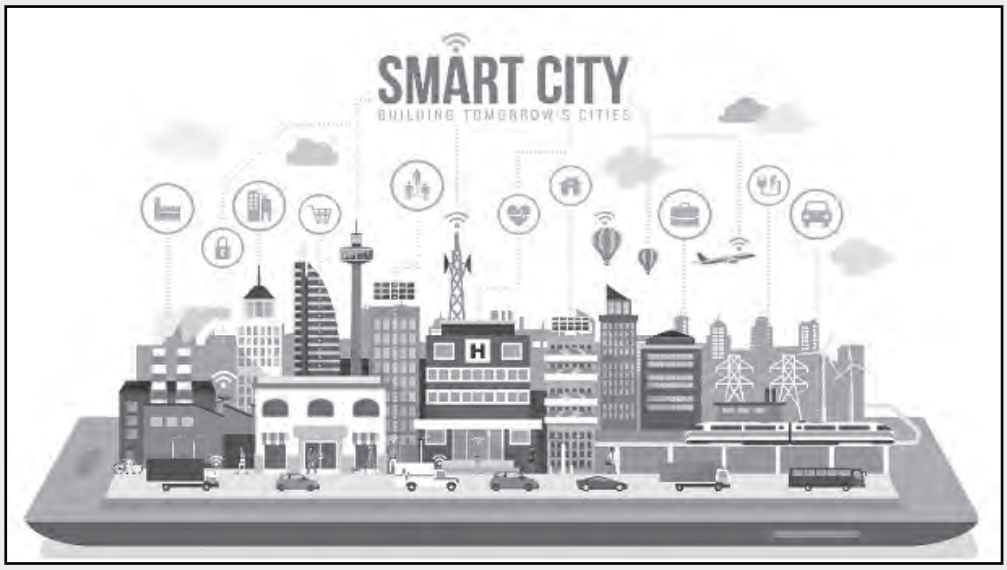
## نشت حریم خصوصی در سنجش داده‌ها

یک شهر هوشمند، نسبت به نشت حریم خصوصی و اطلاعاتِ استنتاج‌شده توسط مهاجمان خارجی، آسیب‌پذیر است؛ زیرا

اطلاعات خصوصی، جمع‌آوری شده، انتقال یافته و پردازش شده است. حفظ حریم خصوصیِ افشاشده در شهر هوشمند، ممکن است شامل هویت و موقعیت کاربر در حمل‌ونقل، شرایط سلامت در بهداشت و درمان و شیوه زندگی استنباط شده از نظارت هوشمند، انرژی هوشمند و خانه و اجتماع باشد. این روند، می‌تواند نظارت خوبی برای اینکه از افشای اطلاعات حساس به حریم خصوصی برای اشخاص غیرقابل اطمینان و یا غیرمجاز در دو جهان فیزیکی و ارتباطی، جلوگیری شود. برای حفظ حریم خصوصی کاربر در طی سنجش داده‌ها، می‌توان از برخی روش‌های جدید حریم خصوصی و امنیت، مانند: رمزنگاری، گمنامی و کنترل دسترسی استفاده کرد. مارتینز و همکاران، یک مجموعه مفاهیم حریم خصوصی و الزامات حریم خصوصی عمومی برای برنامه‌های کاربردی شهر هوشمند معرفی کردند. حفظ حریم خصوصی هویت، پرس‌وجو، محل، ردّ پا و مالک با برخی از ایده‌های اساسی، مشخص و تعیین شده‌اند تا مسائل کلی را حل کنند؛ با این حال، ممکن است این مسئله به طور ناخودآگاه آشکار شود که بخشی از اطلاعات خصوصی را نمی‌توان برای افراد غیرقابل اطمینان فاش کرد؛ برای مثال، نظارت هوشمند می‌تواند نکات مهم زندگی روزمره ساکنان، سبک زندگی آنان و یا حتی حریم خصوصی را به‌دست دهد؛ با وجود اینکه این روش در اصل برای نظارت بر رفتارهای جنایتکارانه در دنیای سایبری و واقعی طراحی شده بود. به طور مشابه، یک خانه هوشمند می‌تواند از دوربین نظارت برای تشخیص سرقت و یا رویدادهای غیرطبیعی استفاده کند. مهاجمان مزاحم در خانه هوشمند، ممکن است اطلاعات شخصی در مورد محیط خانه به‌دست آورند که حریم خصوصی محل اقامت را به خطر اندازد. بسیاری از رویکردهای حفاظت از امنیت و حریم خصوصی در برابر حملات و استراق سمع‌های خارجی، توسعه یافته‌اند؛ اما مهاجمان داخلی بالقوه، مانند: عاملان، کارکنان و نیروهای امنیتی که می‌توانند به مدارک نظارتی دسترسی یابند، ممکن است اطلاعات و داده‌های کاربران را به سرقت ببرند و یا شکافی برای مهاجمان خارجی ایجاد کنند. علاوه بر این، داده‌های شهر هوشمند، در مقیاس ریزدانگی بالایی قرار دارند و انواع متفاوتی دارند؛ به گونه‌ای که الزامات حفظ حریم خصوصی، با هم متفاوت است. این مسئله نیز چالش‌برانگیز است که چگونه مکانیزیم‌های حفاظت از حریم خصوصی مناسبی در شهر هوشمند را توسعه دهیم که تعادلی بین حریم خصوصی و بهره‌وری ایجاد شود.

یک شهر هوشمند، از مزیت‌های نسبی سِرورهای ابری قدرتمند برای ذخیره‌سازی داده و پردازش در جهان اطلاعات استفاده می‌کند و با توجه به سِرورهای ابری غیرقابل اطمینان، با تهدیدهای امنیتی روبه‌رو می‌شود. اگر داده‌های شهر هوشمند در طی ذخیره‌سازی و پردازش در متن واضحی هستند، آنها را می‌توان به سِرور ابری نشان داد. یک روش جایگزین، می‌تواند رمزی کردن داده‌های شهر هوشمند و ارسال متن‌های رمزی به سِرور ابری برای ذخیره‌سازی و پردازش باشد. اگرچه این روش مانع از این می‌شود که سِرورهای ابری نامطمئن، به‌طورکامل به داده‌های جمع‌آوری‌شده دسترسی داشته باشند، اما سِرور ابری نمی‌تواند داده‌های رمزگذاری‌شده را پردازش کند و عملیات تحلیلی مؤثری برای برنامه‌های کاربردی شهر هوشمند

**با وجود اینکه شهرها به دنبال هوشمندتر شدن هستند، برنامه‌های کاربردی شهرهای هوشمند، نگرانی‌ها و چالش‌هایی از نظر امنیت و حریم خصوصی ایجاد می‌کنند. به عنوان یک پارادایم شبکه‌بندی و اطلاعاتی، شهر هوشمند باید بتواند از اطلاعات به‌دست‌آمده در برابر دسترسی‌های غیرمجاز، افشا، اختلال و اصلاح و بازرسی و نابودی دفاع کند. الزامات اساسی امنیت و حفظ حریم خصوصی، از جمله محرمانگی و یکپارچگی و عدم انکار و دسترس‌پذیری و کنترل دسترسی و حفظ حریم خصوصی، باید در جهان فیزیکی، ارتباطی و اطلاعاتی ارضا شوند**




انجام دهد. آخرین دستاوردهای رمزگذاری هومومرفیک، روند پردازش را روشن کرده است؛ مانند جمع و مقایسه داده‌های رمزگذاری‌شده. سربارهای محاسباتی از نظر بهره‌وری نیز با چالش روبه‌رو هستند؛ به‌خصوص زمانی‌که داده‌های عظیم در شهر هوشمند وجود دارند.

یکی دیگر از مسائل چالش‌برانگیز مربوط به شهر هوشمند، اشتراک‌گذاری داده‌ها و کنترل دسترسی است؛ برای مثال، داده‌های ترافیک جادهای را می‌توان با استقرار دوربین‌ها و یا گوشی‌های هوشمند مسافران و GPS، به شیوه‌ای مناسب جمع‌آوری کرد. در طی برنامه‌ریزی جاده‌های جهانی، تعریف سیاست‌های دسترسی، چالش‌برانگیز است و اینکه چگونه داده‌ها را با حفظ حریم خصوصی، در میان همکاران به اشتراک بگذاریم. بنابراین، ذخیره‌سازی داده‌های شهر هوشمند و یا به اشتراک‌گذاری آنها، به تلاش‌های تحقیقاتی گسترده‌ای در این باره نیاز دارد.

### کنترل وابسته و قابل اعتماد

یک شهر هوشمند، یک جریان کنترل دومسیره دارد که متکی بر سیستم کنترل و محرک‌هایی است که بتواند عملیات تعیین‌شده توسط مرکز کنترل را تحقق بخشد. سیستم‌های کنترل و بازخورد، در جهان فیزیکی و به طور خاص زیرساخت‌های صنعتی و عمومی، به اهداف بسیار جذابی برای مهاجمان، جنایتکاران و حتی تروریست‌ها تبدیل شده‌اند. حملات انکار خدمات، حملات جعل، تزریق داده‌های مخرب و غیره، همگی باعث مختل شدن شهر هوشمند خواهند شد؛ به گونه‌ای که مدیریت، کنترل و عملیات آن یا مغرضانه و نادرست و یا غیرفعال می‌شود. بسیاری از این حملات مخرب و سوء رفتارها، بر اساس بازرسی‌ها و حسابرسی‌های شخص ثالث، تشخیص داده می‌شوند. قابلیت یکپارچگی داده‌ها و امضای دیجیتال، در نرم‌افزارهایی به‌کار گرفته شده که شبکه‌هایی را برای دستیابی به یکپارچگی داده‌ها، کنترل دسترسی و غیره تعریف می‌کنند. در همین حال، محاسبات قابل اعتماد، یک راه‌حل جدید است که با استفاده از آن، می‌توان در برابر تغییرات چارچوب نرم‌افزار و سیستم عملیاتی مقاومت کرد؛ با این حال، این طرح‌ها تأخیر زیاد و نرخ منفی بالایی دارند تا بتوانند حملات هوشمند را در شهر هوشمند تشخیص دهند. ازآنجاکه قابلیت اعتماد کنترل، به عنوان بالاترین اولویت در شهر هوشمند در نظر گرفته شده، تشخیص سریع و کارآمد حملات مخرب و سوء رفتارها، به مسئله‌ای چالش‌برانگیز تبدیل شده است و به تلاش‌های همکارانه‌ای در میان احزاب و ذی‌نفعان متعدد نیاز دارد تا به هدف اصلی دست یابند.

### راه‌حل‌های امنیت برای پارادایم‌های شهر هوشمند

برای تحقق مفهوم امنیت و حریم خصوصی در شهر هوشمند، راه‌حل‌های متعادل و عملی مورد نظر هستند. در این بخش،

طرح‌های حفاظت از حریم خصوصی و امنیت جدید را برای چندین پارادایم شهر هوشمند نوظهور معرفی می‌کنیم؛ از جمله: مراقبت‌های بهداشتی هوشمند، حمل‌ونقل هوشمند و شبکه‌های هوشمند.

### تحلیل گسترش عفونت با حفظ حریم خصوصی برای حوزه مراقبت‌های بهداشتی هوشمند

مراقبت‌های بهداشتی هوشمند که با حسگرهای پزشکی متصل، ذخیره‌سازی

**یک شهر هوشمند، از مزیت‌های نسبی سِرورهای ابری قدرتمند برای ذخیره‌سازی داده و پردازش در جهان اطلاعات استفاده می‌کند و با توجه به سِرورهای ابری غیرقابل اطمینان، با تهدیدهای امنیتی روبه‌رو می‌شود. اگر داده‌های شهر هوشمند در طی ذخیره‌سازی و پردازش در متن واضحی هستند، آنها را می‌توان به سِرور ابری نشان داد. یک روش جایگزین، می‌تواند رمزی کردن داده‌های شهر هوشمند و ارسال متن‌های رمزی به سِرور ابری برای ذخیره‌سازی و پردازش باشد**

داده‌های سلامت و واحدهای سلامت در نظر

گرفته شده است، خدمات بهداشتی تسکینی، درمانی و پیشگیرانه فراهم می‌کند و می‌تواند طیف وسیعی از اطلاعات سلامت زمان واقعی را از کاربران جمع‌آوری کند و آنها را تحلیل نماید و از مسائل شدید و مهم مراقبت‌های بهداشتی در سطح شهر، مانندگسترش بیماری‌های عفونی، دفاع کند.

بیماری‌های عفونی، مانند: ابولا، آنفولانزا و عفونت حاد تنفسی، می‌توانند به‌سرعت از طریق تماس انسان به انسان شیوع پیدا کنند؛ به‌خصوص زمانی که بیماران آلوده، در جمعیت سرفه و یا عطسه می‌کنند. افرادی که تماس‌های مکرر و یا روابط اجتماعی زیادی با بیمار دارند، معمولاً از دیدگاه زیست‌پزشکی و جامعه‌شناسی آسیب‌پذیرند. یک رویکرد پیشگیری قدیمی از این بیماری، این است که افراد مستعد را برای دوره‌ای مشخص از افراد دیگر جدا کنیم. با این حال، این روش شرایط سلامتی و حساسیت و آسیب‌پذیری آنها را از جنبه‌های منفی در نظر نمی‌گیرد؛ از جمله: هزینه بهداشت و درمان بالا، مشکلات اقتصادی افراد منزوی‌شده و ترس و یا اضطراب در میان جامعه. برای مقابله با مشکل گسترش عفونت، مراقبت‌های بهداشتی هوشمند، هشدارهای تشخیص کارآمد و یا شرایط سلامت [یا اضطراری] مناسبی ایجاد می‌کنند؛ به این صورت که در زمان واقعی، روند عفونت را در طی فصل شیوع بیماری تحلیل می‌نمایند. به طور کلی، گسترش بیماری‌های عفونی، به تماس‌های اجتماعی کاربران و شرایط سلامتی آنها بستگی دارد. به طور خاص، این فرآیند شیوع، تحت تأثیر چند عامل اصلی عفونی است که از جمله آنها، آسیب‌پذیری بیمار آلوده، قدرت ایمنی کاربری که با آنها تماس دارند و مدت زمان تماس و روابط اجتماعی است.

تلفیقی از داده‌های شبکه‌های اجتماعی و داده‌های زمان واقعی سلامت افراد، امکانی را فراهم می‌آورد که پارادایم جدید تحلیل عفونت ساده شود. از یک سو، شبکه اجتماعی، انواع برنامه‌های کاربردی را برای تماس اجتماعی افراد معدن در طی تعاملات اجتماعی آنها در نظر می‌گیرد؛ برای مثال، برنامه دوست‌یابی وی‌چت می‌تواند دوستان در یک مجاورت فیزیکی را پیدا کند و تعاملات اجتماعی آنها را ثبت نماید؛ چنانکه روش‌های تشخیص گفتار می‌تواند سرفه و یا عطسه افراد را تشخیص دهد و تابع تگ کردن صورت، می‌تواند تصاویر کاربر را از میان تصاویر شناسایی کند.

از سوی دیگر، دستگاه‌های پوشیدنی و حسگرهای پزشکی، می‌توانند شرایط سلامتی زمان واقعی کاربر را اندازه‌گیری کنند. با این حال، داده‌های شبکه‌های اجتماعی و سلامتی، توسط چندین ارائه‌دهنده خدمات مستقل، مانند فروشندگان شبکه‌های اجتماعی و بیمارستان‌ها جمع‌آوری شده‌اند. همکاری این ارائه‌دهندگان خدمات، چالش اصلی این تحلیل عفونی است و یک سری مسائل امنیتی را در پی دارد. هر دو سِرورهای ابر سلامت و اجتماعی، به‌عنوان موجودیت‌های صادق، اما کنجکاو در برنامه‌های کاربردی مراقبت از بهداشت هوشمند در نظر گرفته شده‌اند. برای حفظ حریم خصوصی داده‌های کاربر و دستیابی به دسترس‌پذیری داده، رمزنگاری هومومورفیک را می‌توان مورد استفاده قرار داد تا شبکه‌های اجتماعی و داده‌های سلامت را برای سِرورهای ابر نامطمئن، غیرقابل رؤیت کرد.

همکاری سِرورهای مختلف ابری نامطمئن، از

طریق موجودیت‌های مجاز صورت می‌گیرد؛ با این حال، زمانی که بیمارستان، داده‌های بیماران آلوده را در سِرور ابر اجتماعی مورد جست‌وجو قرار می‌دهد، سِرور ابر اجتماعی ممکن است نتیجه بگیرد که کاربر مورد جست‌وجو، آلوده شده است؛ حتی اگر محتوای مورد جست‌وجو هنوز هم نامرئی باشد. علاوه بر این، هر نهاد بدون مجوز مالکِ داده نباید بتواند داده‌های مالک را مورد کاوش قرار دهد. روش‌های حفاظت از حریم خصوصی و امنیت فعلی، برای مراقبت‌های بهداشتی هوشمند ضروری هستند. بدون وجود حمایت مؤثر، کاربران مایل نیستند که داده‌های سلامت و اجتماعی خود را با دیگران به اشتراک بگذارند؛ به گونه‌ای که تحلیل عفونت صورت نگیرد.

برای این منظور، پروتکل‌های انتقال با دقتِ کم مشروط برای پرس‌وجوهای داده‌های با حفظ حریم خصوصی، توسعه یافته‌اند. از یک سو به نهاد مجاز مانند دکتر اجازه می‌دهد که به داده‌های شبکه اجتماعی بیمار از سِرور ابر اجتماعی دسترسی یابد و از سوی دیگر، مانع از این می‌شود که سِرور ابر اجتماعی به داده‌ها دسترسی یابد و هرگونه اطلاعاتی را در مورد پرس‌وجو استنباط کند؛ مانند هویت بیمار. صاحبان داده و یا کاربران، می‌توانند به نهاد مورد اعتماد قبل از پرس‌وجو، مجوز اعطا کنند.

هر نهاد، بدون اجازه کاربر نمی‌تواند هر داده‌ای را جست‌وجو کند. علاوه بر این، محاسبات چندجانبه امن مبتنی بر رمزنگاری هوموفیک، برای جلوگیری از این مسئله استفاده می‌شود که ابرهای سلامت نامطمئن از داده‌های سلامت و اجتماعی خصوصی یاد بگیرند.

## ناوبری ایمن برای حمل‌ونقل هوشمند

یک شهر هوشمند، سرویس‌های حمل‌ونقل هوشمند را برای ساکنان و بازدیدکنندگان محلی از جنبه‌های مختلف ارائه می‌دهد؛ از جمله تنظیم ترافیک جاده، ناوبری، نقطه توصیه‌شده مورد نظر، پارکینگ و غیره. ناوبری، به‌عنوان بخش جدایی‌ناپذیر موجود، توجه زیادی را به خود جلب کرده است. دستگاه‌های GPS موجود، می‌توانند ناوبری استاتیک فراهم کنند و مسیر را روی نقشه‌های از پیش دانلودشده نشان دهند؛ با این حال، فاقد تنظیمات ترافیک جاده‌ای در زمان واقعی هستند؛ به گونه‌ای که سریع‌ترین مسیرِ محاسبه‌شده، ممکن است با ازدحام پویا کمی با تأخیر روبه‌رو شود. روش‌های ناوبری پویا از هوش انسانی استفاده می‌کنند و ترافیک جاده‌ای پویا را از مسافران جاده و یا واحدهای کنار جاده‌ای (RSU)، به شیوه‌ای مناسب مورد سنجش قرار می‌دهند.

## مدیریت تطبیقی، کلیدی برای شبکه هوشمند

شبکه هوشمند، بر میلیون‌ها معیار هوشمند تکیه می‌کند تا مصرف برق زمان واقعی را در مناطق مسکونی و یا ساختمان‌ها

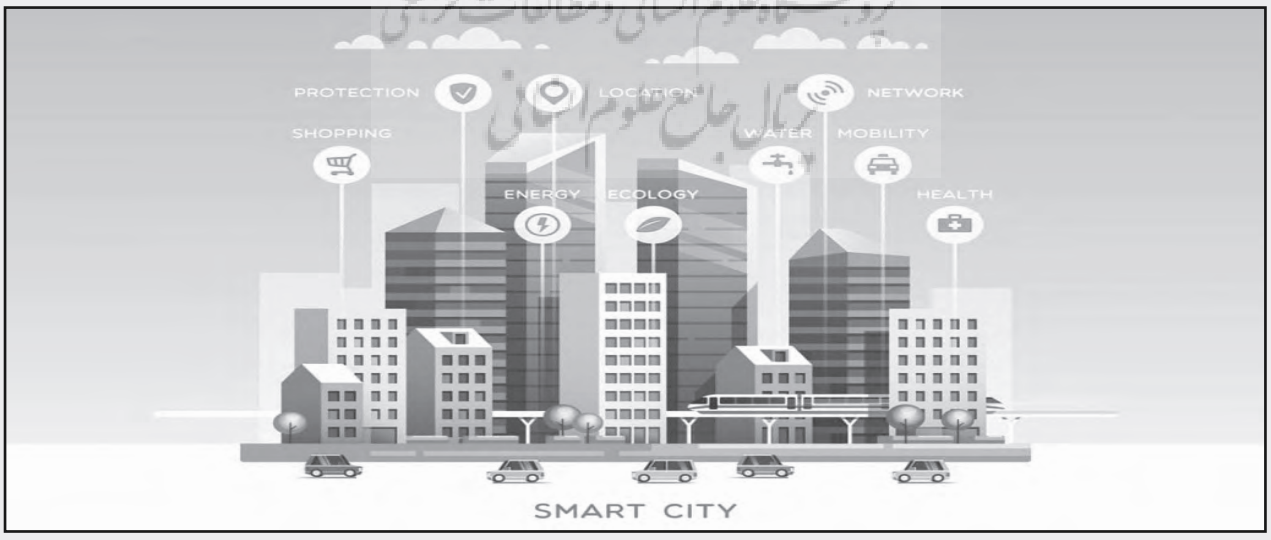
اندازه‌گیری کند. این داده‌های معیار، اندازه‌گیری می‌شوند تا مرکز را به گونه‌ای کنترل کنند که توزیع توان بهینه‌سازی شود؛ با این حال، یک‌سری از تلاش‌های حمله برای دستکاری رکوردهای معیارهای هوشمند و داده‌های اصلاحی ارسال‌شده به مرکز کنترل نیز انجام شده است. علاوه بر این، فزونی حجم اطلاعات داده‌های اندازه‌گیری، مسئله چالشی جدیدی در رابطه با مدیریت کلیدهای مخفی برای هر دستگاه فراهم آورده است.

عمدتاً یکپارچگی داده‌ها و احراز هویت، باید در طی جمع‌آوری معیارهای هوشمند انجام

**یکی دیگر از مسائل چالش‌برانگیز مربوط به شهر هوشمند، اشتراک‌گذاری داده‌ها و کنترل دسترسی است؛ برای مثال، داده‌های ترافیک جاده‌ای را می‌توان با استقرار دوربین‌ها و یا گوشی‌های هوشمند مسافران و GPS، به شیوه‌ای مناسب جمع‌آوری کرد. در طی برنامه‌ریزی جاده‌های جهانی، تعریف سیاست‌های دسترسی، چالش‌برانگیز است و اینکه چگونه داده‌ها را با حفظ حریم خصوصی، در میان همکاران به اشتراک بگذاریم. بنابراین، ذخیره‌سازی داده‌های شهر هوشمند و یا به اشتراک‌گذاری آنها، به تلاش‌های تحقیقاتی گسترده‌ای در این باره نیاز دارد**

شود. علاوه بر این، داده‌های اندازه‌گیری ناحیه خانه، می‌تواند شیوه زندگی ساکنان و شرایط زندگی و اولویت‌ها را نشان دهد. اگر افراد جمع‌آوری‌کننده غیرقابل اعتماد این اطلاعات، اطلاعات خصوصی را یاد بگیرند و آشکار کنند، حریم خصوصی ساکنان به خطر می‌افتد و اُفت اقتصادی ایجاد می‌شود. ژانگ و همکاران، یک طرح جمع‌آوری با حفظ حریم خصوصی پیشنهاد کردند (PARK) که بهره‌وری محاسباتی را بهبود بخشند و از داده‌های معیار هوشمند حفاظت کنند تا برای افراد جمع‌آوری‌کننده غیرقابل اعتماد، فاش نشود. یک طرح مدیریت کلیدی سازگار، بر اساس زنجیره هَش (Hash) دوطرفه توسعه یافته و کلیدهای رمزنگاری، برای هر معیار هوشمند در طول هر دوره تولید می‌کند. موجودیت‌های مورد اعتماد، کلید رمزگشایی را برای جمع‌آوری‌کننده محاسبه می‌کنند که مجموع متن رمزشده از گروه، N معیار هوشمند است. این مسئله، تنها زمانی صورت می‌گیرد که تمام N متن رمزشده در اختیار باشد و فرد جمع آوری کننده می‌تواند مجموع N معیار هوشمند را رمزگشایی کند. اگر معیار هوشمند، رویکرد شبکه هوشمند را برآورده نکند و یا اصلاً در شبکه هوشمند وجود نداشته باشد، هر کلید رمزنگاری معیار هوشمند، به طور خودکار به‌روز می‌گردد. کلید رمزگشایی جمع‌آوری‌کننده نیز به طور هم‌زمان به‌روزرسانی می‌شود.

قدرت‌های مورد اعتماد، طول زنجیره هَش



را تعیین می‌کنند که نشان‌دهنده اعتبار معیار هوشمند است. یک معیار با شهرت بالا، کلیدی را با زمان انقضای طولانی دریافت می‌کند. زمانی که برخی از معیارها به شبکه هوشمند می‌پیوندند و یا از آن خارج می‌شوند، قدرت‌های مورد اعتماد، تنها باید کلید رمزگشایی جمع‌آوری‌کننده را به‌روز کنند. سربار ابطال، از توزیع مجدد کلید رمزگشایی به‌دست می‌آید.

## جهت‌گیری تحقیقات آینده

ازآنجاکه راه‌حل‌های امنیت و حریم خصوصی محصولی، تمام چالش‌های موجود در شهر هوشمند را در نظر نمی‌گیرند، ما تنها برخی از جهت‌گیری‌های باز تحقیقاتی را مورد بحث قرار می‌دهیم؛ از جمله اینکه در ابتدا، روند سنجش جمعیت یا crowdsens-ing که دستگاه‌های سنجش هوشمند ساکنان محلی را استفاده می‌کند، می‌تواند قابلیت سنجش بهبودیافته برای شهر هوشمند ارائه کند؛ به جای اینکه تنها بر حسگرهای ثابت از پیش استقراریافته تکیه نماید؛ با این حال، دقت سنجش جمعیت ممکن است با توجه به دانش مشارکت‌کننده و یا خودخواهی و ترجیحات او تغییر نماید. یک ایده اوّلیه از تحریک شهروندان برای همکاری و یا سنجش جمعیت، این است که مشوق‌هایی برای آنها ایجاد کنیم. علاوه بر این، موفقیت و قابلیت اعتماد نیز در هنگام طراحی طرح‌های تشویقی باید لحاظ شود. علاوه بر این، حریم خصوصی مشارکت کنندگان سنجش جمعیت، ممکن است توسط مهاجمان هوشمندتر به خطر بیفتد. به طور خاص، زمانی که مشارکت کنندگان متعددی، نتایج سنجش را در کنار یکدیگر قرار می‌دهند، اطلاعات خصوصی مشارکت‌کننده به احتمال زیاد به طور مشارکتی توسط دیگران استنباط می‌شود.

**شهر هوشمند، نسبت به تزریق داده‌های نادرست، در فازهای کنترل و سنجش، آسیب‌پذیر است. روش‌های امضای دیجیتال، نمی‌توانند مانع از دستکاری داده از منشأ شوند. یک دیدگاه برای تشخیص تزریق داده‌های غلط، این است که روش‌های یادگیری ماشین و داده‌کاوی را به‌کار بگیریم تا با مرز داده‌های سنجش معقول، مقابله کنیم. روش‌های تشخیص غیرطبیعی، می‌تواند جایگزینی برای شناسایی داده‌های نادرست باشد**

بنابراین، اینکه چگونه به انگیزه و حریم خصوصی دست یابیم، به‌عنوان چالشی برای سنجش جمعیت در شهر هوشمند باقی می‌ماند.

ضمن اینکه شهر هوشمند، نسبت به تزریق داده‌های نادرست، در فازهای کنترل و سنجش، آسیب‌پذیر است. روش‌های امضای دیجیتال، نمی‌توانند مانع از دستکاری داده از منشأ شوند. یک دیدگاه برای تشخیص تزریق داده‌های غلط، این است که روش‌های یادگیری ماشین و داده‌کاوی را به‌کار بگیریم تا با مرز داده‌های سنجش معقول، مقابله کنیم. روش‌های تشخیص غیرطبیعی، می‌تواند جایگزینی برای شناسایی داده‌های نادرست باشد؛ با این حال، حلّ این مسئله، به دانش چندرشته‌ای و تلاش‌هایی نیاز دارد.

در نهایت، حجمِ همیشه در حالِ رشد داده‌ها و دستگاه‌ها در شهرهای هوشمند، مشکلات بسیاری برای حریم خصوصی و خدمات هوشمند ایجاد کرده‌اند. مهاجمان داخلی، از هوش انسانی بهره‌برداری کرده‌اند و به داده‌های بزرگ دسترسی پیدا کرده‌اند؛ به‌گونه‌ای‌که حریم خصوصی صاحبان داده، ممکن است استنباط و نقض شود؛ حتی طرح‌های رمزنگاری سنّتی نیز برای داده‌های بزرگ اِعمال شده‌اند. یک جایگزین برای تشخیص این مهاجمان داخلی، این است که قابلیت ردیابی را افزایش دهیم و به شخص ثالثِ موردِ اعتماد، این اجازه را بدهیم که به نظارت و حسابرسی بپردازد. در همین حال، به تلاش‌های همکارانه در میان شهرداری‌ها، بخش مقررات و صنعت و دانشگاه و شرکت‌های کسب‌وکار، برای تنظیم سیاست‌ها و مقررات حریم خصوصی، نیازمندیم. علاوه بر این، حفظ حریم خصوصی داده‌ها، دسترس‌پذیری و مدیریت، باید به طور هم‌زمان به‌وجود آید.■