نشریه‌ی علمی شهر ایمن
JOURNAL OF RESILIENT CITY
(JRC)

حوزه‌های کاربردی حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند

جواد غریبی[1*]؛ حسین قرایی[2]؛ محمدرضا فرجی‌پور[3]؛ خداداد هلیلی[4]

۱- دانشجوی دکتری، دانشگاه عالی دفاع ملی، تهران (نویسنده مسئول)
۲- دانشیار، مهندسی برق، مرکز تحقیقات مخابرات ایران
۳- استادیار، دانشگاه عالی دفاع ملی، تهران
۴- استادیار، عضو هیات علمی دانشکده کامپیوتر دانشگاه شهید ستاری

دریافت دست‌نوشته: ۱۴۰۲/۰۲/۱۳؛ پذیرش دست‌نوشته: ۱۴۰۲/۰۳/۰۹

واژگان کلیدی

حاکمیت امنیت داده، اینترنت اشیاء، شهر هوشمند

چکیده

شهرهای هوشمند برای بهبود کیفیت زندگی شهروندان به‌شدت به فناوری و داده‌ها متکی هستند. با این حال، این اتکا به فناوری همچنین چالش‌های مهم امنیتی نظیر تهدیدات امنیت سایبری، حریم خصوصی داده‌ها، قابلیت همکاری و فقدان استانداردهای لازم را ایجاد می‌کند. جهت مقابله با این چالش‌ها و همچنین کاهش تقابل‌های امنیت و خدمات اینترنت اشیاء در شهر هوشمند، لازم است ابتکاراتی در نظر گرفته شود. حاکمیت امنیت داده یک فرایند تضمین امنیت داده‌ها در عین حفظ کارایی و عملکرد داده‌ها در حوزه‌های مورد استفاده است. جهت استفاده از حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند لازم است حوزه‌های کاربردی آن شناسایی شود. این حوزه‌ها با در نظر گرفتن ساختار شهر هوشمند، اینترنت اشیاء، ساختار و موضوع داده‌ها و همچنین ذینفعان داده‌ها در شهر هوشمند قابل احصاء است. در این مقاله با مورد مطالعه قرار دادن منابع مختلف و استفاده از ظرفیت نخبگانی ۴ حوزه اصلی و ۱۷ زیرحوزه کاربردی حاکمیت امنیت اینترنت اشیاء در شهر هوشمند شناسایی شده است. همچنین پس از شناسایی حوزه‌ها عوامل مؤثر بر حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند احصاء شده است.

۱- مقدمه و بیان مسئله

معنای شهر هوشمند به معنای ادغام زیرساخت‌های فعلی با فناوری‌های اطلاعاتی و ارتباطی جدید برای ایجاد یک سیستم جامع از خدمات شهری کارآمد است. شهر هوشمند شهری است که زیرساخت‌های فیزیکی، زیرساخت‌های فناوری اطلاعات، زیرساخت‌های اجتماعی و زیرساخت‌های تجاری را برای تقویت هوش جمعی شهر به هم متصل می‌کند. شهر هوشمند فناوری‌های عظیم، پیچیده و وابسته‌ای است که با چالش‌ها و مسائل فنی، اقتصادی، سیاسی و اجتماعی متعددی مواجه است. به‌طورکلی شش حوزه وجود دارد که شهرها می‌توانند در آنها هوشمندتر باشند: دولت هوشمند، افراد هوشمند، اقتصاد هوشمند، حمل‌ونقل هوشمند، محیط‌زیست و سبک زندگی (ما، ۲۰۲۱).

حاکمیت داده فرایندی سازمانی برای مدیریت داده، رسمیت بخشیدن به مجموعه‌ای از سیاست‌ها و فرایندها برای بهبود کیفیت داده و کاهش زائدات داده، حفاظت از داده‌های حساس، حفاظت از داده‌ها و مطلوبیت فناوری با استفاده از قوانین، تشویق استفاده درست از داده و خط‌مشی برای تحلیل داده‌های قوی است (سخایی، ۱۳۹۷). داده‌ها درون شهرهای هوشمند به‌صورت پیوسته جریان دارند و حاکمیت داده تصمیم می‌گیرد که چه داده‌هایی جمع‌آوری

* رایانامه: m.amngh@aut.ac.ir

شوند، توسط چه کسی، به چه روشی و برای چه هدفی استفاده شود؛ از جمله، حقوق دسترسی و یا استفاده از داده‌ها و همچنین قوانینی که برای مدیریت و کنترل کیفیت و کامل بودن داده‌ها (فرانکه و گیلهوفر، ۲۰۲۱). حاکمیت داده با در نظر گرفتن افراد، فرایندها و فناوری‌ها به سازمان کمک می‌کند تا داده به‌صورت کنترل‌شده درآیند و به‌صورت مؤثرتری مورد استفاده قرار گیرند (بروکمن، ۲۰۲۰).

اما نکته‌ای که در بخش امنیت حاکمیت داده وجود دارد این است که حاکمیت داده تنها از نظر دسترسی‌های مجاز به امنیت داده می‌پردازد و جزئیات آن را بررسی نمی‌کند (سینگ، ۲۰۱۹). لذا داده‌های شهر هوشمند از نظر حریم خصوصی و امنیت داده‌ای دارای تهدیدات فراوانی می‌باشند که لازم است تا فرایندهای خاص حاکمیت امنیت داده نیز پیاده‌سازی شوند. حاکمیت امنیت داده فرایند ایجاد و توسعه چارچوب و پشتیبانی ساختار مدیریت است که استراتژی‌های امنیت اطلاعات و اهداف تجاری و کاری سازمان را همسو و هم‌راستا می‌کند. این فرایندها از طریق قوانین و سیاست‌های داخلی صورت می‌پذیرد. مؤسسه گارتنر معتقد است که حاکمیت امنیت داده تنها یک پاسخ با یک سری ویژگی‌ها نیست، بلکه یک زنجیره کامل است که در تمام اجزای سازمان و از سطوح بالای حاکمیتی به سطوح پایین فنی حرکت می‌کند. تمام سطوح یک سازمان باید بر روی اهداف سازمان به توافق برسند و در نهایت از حفاظت از منابع و داده‌ها به بهترین شکل ممکن اطمینان حاصل می‌شود (لوانز و همکاران، ۲۰۱۸).

یکی از چالش‌های مهم اینترنت اشیاء در شهر هوشمند بالا بردن سطح امنیت داده، حفظ اطلاعات، تضمین دسترسی‌های مجاز به داده‌ها در عین حفظ و بهبود خدمات شهر هوشمند می‌باشد (دیلیجنت، ۲۰۱۶). داده‌هایی که در شهر هوشمند وجود دارند دسته‌های زیاد و متفاوتی هستند که هرکدام طبق کاربرد و نوع خود از سطح امنیت متفاوتی برخوردار هستند و هرکدام از داده‌ها تنها باید توسط نهاد مربوط به آن بررسی و اجازه دسترسی داده شود. علاوه بر این، مفهوم شهرهای هوشمند شامل یک سیستم اطلاعاتی است که در همه‌جا وجود دارد و با زیرسیستم‌های به‌هم‌پیوسته توزیع شده است که توسط سازمان‌های مختلف (به‌عنوان‌مثال، حوزه‌های اداری) اداره می‌شوند. حاکمیت امنیت داده باید در شهرهای هوشمند با هدف ایجاد یک محیط محاسباتی قابل اعتماد باشد که از همکاری ایمن بین نهادهای مشارکت کننده در داده‌های تولیدی شهر هوشمند پشتیبانی می‌کند. همچنین از چالش‌های دیگر آن می‌توان به تعاملات و اشتراک‌گذاری داده توسط نهادهایی که لزوماً زیرساخت امنیتی مشترکی ندارد، اشاره کرد. علاوه بر آن، مهم‌ترین چالش آن تفاوت مأموریت و اهداف بخش‌های مختلف شهر هوشمند در فرایند چرخه داده است که می‌تواند موضوعات مهم امنیت داده و کیفیت داده را در تقابل با هم قرار دهد.

در یک شهر هوشمند داده‌های اینترنت اشیاء لازم است مرتباً به اشتراک گذاشته شوند. با توجه به این موضوع، چالش‌هایی نظیر پیچیدگی‌های زیرساختی اشتراک‌گذاری داده، ذینفعان و مشارکت‌های اشتراک‌گذاری داده، تخصیص مسئولیت‌های امنیت اشتراک‌گذاری داده‌ها مطرح می‌شود. این موضوع در کنار مسائل تضمین کیفیت داده، امنیت ذخیره‌سازی و تبادل داده‌های اینترنت اشیاء، حریم خصوصی داده‌ها و همچنین حفظ خدمات شهر هوشمند از چالش‌های اساسی امنیت داده‌های اینترنت اشیاء در شهر هوشمند مطرح می‌شود (کنئی و همکاران، ۲۰۲۲).

با عنایت به مطالب یاد شده فوق، محقق در این تحقیق بر آن است تا با بررسی مبانی و اصول، ارکان جهت‌ساز، قوت‌ها و ضعف‌ها و نیز فرصت‌ها و تهدیدهای پیش رو و همچنین ارائه راهبردها و الزامات اجرایی، نسبت به ارائه طرح راهبردی حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند اقدام نماید تا ضمن بهره‌مند شدن شهر از هوشمندی لازم، از آسیب‌ها و تهدیدات آن نیز مصون بماند؛ بنابراین مسئله اصلی پژوهش حاضر، حفظ امنیت و حریم خصوصی داده‌های اینترنت اشیاء شهر هوشمند در کنار ارائه خدمات بهینه، لحاظ گردیده است.

۱-۱- اهداف تحقیق

۱-۱-۱- هدف اصلی

- حوزه‌های کاربردی حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند

۱-۱-۲- اهداف فرعی

- عوامل مؤثر بر حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند
- شناسایی حوزه‌ها و زیرحوزه‌های کاربردی حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند

۱-۲- سؤالات تحقیق

۱-۲-۱- سؤال اصلی

- حوزه‌های کاربردی حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند کدامند؟

۱-۲-۲- سؤال‌های فرعی

- عوامل مؤثر بر حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند کدامند؟
- حوزه‌های اصلی و زیرحوزه‌های کاربردی حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند کدامند؟

۱-۳- اهمیت و ضرورت تحقیق

۱-۳-۱- اهمیت تحقیق

- با انجام این تحقیق نحوه به‌کارگیری هوشمندانه و پیش‌کنش‌گرایانه حاکمیت امنیت داده در مقابل مخاطرات و چالش‌های امنیتی اینترنت اشیاء در شهر هوشمند تبیین می‌شود.
- تصمیم‌سازان و تصمیم‌گیران ترغیب به به‌کارگیری فناوری‌های نوین در شهر هوشمند شده و با به‌کارگیری سیاست‌ها و راهبردهای مطرح شده، ضمن پایداری مناسب سامانه‌ها، مقابله با تهدیدات و مدیریت بحران تسهیل خواهد شد.

۱-۳-۲- ضرورت تحقیق

- فقدان طرح راهبردی، تعیین اولویت‌ها، پیش‌بینی صحیح در مواجهه با حوادث پیش رو و انفعال در اقدامات را به همراه خواهد داشت.
- بی‌توجهی به تدوین سیاست‌های حاکمیت امنیت داده در شهر هوشمند، علاوه بر نقض حریم خصوصی موجب آسیب‌پذیری زیرساخت‌های حیاتی و خدشه به امنیت ملی و اقتدار کشور خواهد شد.

۲- مبانی نظری و پیشینه‌شناسی

۲-۱- تعاریف، اصطلاحات

- **حاکمیت امنیت داده:** حاکمیت امنیت داده یک فرایند سطح بالای مدیریتی داده به‌منظور پشتیبانی از برنامه‌های امنیت داده در جهت اهداف و چشم‌انداز است (آبراهام و دیگران، ۲۰۱۹).
- **اینترنت اشیاء:** اینترنت اشیاء، اتصال اشیاء و تمام تجهیزات مربوط به شهر هوشمند از طریق شبکه‌های خاص شهر هوشمند مبتنی بر شبکه خارجی و یا داخلی، جهت ایجاد ارتباط، تعامل و اقدام از راه دور است (کومار و دیگران، ۲۰۱۹).
- **شهر هوشمند:** شهر هوشمند یک روند جهانی استراتژی‌های شهری است که با هدف بهبود کیفیت ساکنان مناطق شهری و به‌کارگیری نوآوری و فناوری‌های پیشرفته برای حل مشکلات ناشی از تراکم بالای جمعیت اتخاذ می‌شود (ما، ۲۰۲۱).

۲-۲- پیشینه تحقیق

طبق جدول ۱ شرح پیشینه تحقیق آمده است.

۲-۲-۱-پیشینه‌ها

برابر بررسی به‌عمل‌آمده در پیشینه‌های فوق، هریک از پژوهش‌ها، به جنبه‌ای از مسائل مرتبط با اینترنت اشیاء از قبیل کارکردها، تهدیدها و فرصت‌های مرتبط بر به‌کارگیری، نقاط ضعف و چالش‌های امنیتی و... را مطرح نموده و می‌توان بخشی از ضروری بودن بهره‌مندی از حاکمیت امنیت داده در زمینه بهره‌برداری از اینترنت اشیاء را، از آنها احصاء نمود و مهم‌ترین نتیجه‌ی حاصل از جمع‌بندی پیشینه‌ها مبین این نکته است با وجود مزایای اینترنت اشیاء در شهر هوشمند، لیکن جامعه و سازمان‌ها را با چالش‌هایی از قبیل حفظ حریم خصوصی، تهدیدات امنیتی، مواجهه با داده‌های حجیم، نیاز به مدیریت داده‌های کلان، حفظ امنیت این داده‌ها و... روبرو می‌سازد که نیازمند چاره‌اندیشی می‌باشد.

با بررسی پیشینه‌های ذکر شده، مشخص می‌گردد که

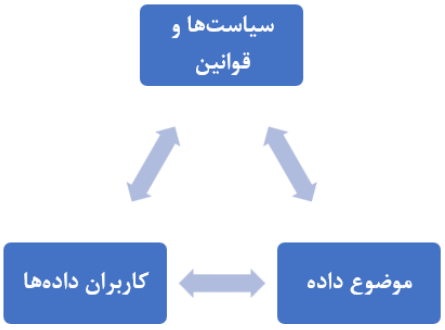
عمده‌ی آنها به مقوله استفاده از اینترنت اشیاء در حوزه‌های شهر هوشمند از یک جنبه خاص و بعضاً با دید فنی و سخت‌افزاری پرداخته‌اند و در هیچ‌یک از آنها، الگو یا طرحی برای استفاده حاکمیت امنیت داده اینترنت اشیاء، ارائه نشده است.

عنوان تحقیق	نتیجه‌گیری
امنیت سایبری در شهرهای هوشمند (افتیمیوپولوس، ۲۰۱۵)	محقق در این تحقیق به ارائه یک طرح پیشنهادی در جهت افزایش امنیت هوشمندسازی شهر دبی می‌پردازد. با توجه به اینکه دبی انتظار داشت تا سال ۲۰۲۰ به یک شهر هوشمند دست پیدا کند، لذا چالش‌های راهبردی مختلفی در این زمینه خواهد داشت. همچنین شهر دبی به یک شهر با اقتصاد جهانی مشهور است. لذا در این طرح از نظر امنیت راهبردی، امنیت شهر در فضای مجازی و همچنین زیرساخت‌های شبکه‌ای هوشمند چالش‌های پیش رو بررسی و تجزیه و تحلیل شدند. همچنین در انتها روش‌های مختلفی در جهت حفظ و افزایش امنیت دیجیتالی شهر ارائه شده است.
بررسی نقش مدیریت امنیت اطلاعات در سازمان‌های شهر هوشمند (حسبینی و همکاران، ۲۰۱۸)	عدم توجه به امنیت در توسعه شهرهای هوشمند نباید با اهداف پایداری و هزینه‌های کمتر توجیه شود. این یک دلیل اصلی برای مشکلاتی خواهد بود که می‌تواند خسارت و تلفات ایجاد کند و بنابراین توسعه شهرهای هوشمند را به‌صورت گسترده به تعویق بیاندازد. حکمرانی هوشمند می‌تواند در پیشبرد سازمان‌ها و کسب‌وکارها به‌صورت مطمئن نقش بزرگی داشته باشد و خطرات و ریسک‌های امنیتی آن را کاهش دهد. در جهت مسائل حاکمیت امنیت اطلاعات برای حل این مسائل نیاز به تحقیقات گسترده‌تری است. در این مقاله، مسائل مدیریت امنیت اطلاعات در شهر هوشمند بحث گردید و همچنین اهمیت مدیریت امنیت اطلاعات در سازمان‌های شهرهای هوشمند بررسی شد. در ادامه نیز عوامل سازمانی مرتبط با ISM (Information Security Management) به صورتی که بیشترین تأثیر را بر عملکرد سازمانی شهرهای هوشمند بگذارد بررسی شد.
طراحی مدلی برای مدیریت اکوسیستم کلان‌داده برای کسب‌وکارهای داده‌محور در جامعه فیزیکی- سایبری با تأکید بر شهر هوشمند (امینی، ۱۳۹۷)	هدف اصلی این پژوهش و تحقیق، طراحی یک مدل برای مدیریت اکوسیستم کلان‌داده برای کسب و کارهای داده محور در جامعه فیزیکی- سایبری با تأکید بر ویژگی‌های شهر هوشمند بوده است. تحلیل‌های این تحقیق نشان می‌دهد که این مدل می‌تواند از ۱۱ لایه تشکیل شود. این لایه‌ها عبارتند از: لایه اصول و ارزش‌های بنیادین، لایه محیط و بافت، لایه هویت، لایه رهبری و استراتژی، لایه سیستم‌ها، لایه منابع و دارایی‌ها، لایه فرایندها و روش‌ها، لایه نحوه مدیریت، لایه قوانین و مقررات، لایه فناوری‌ها، لایه معماری و ساختار می‌باشند. در لایه رهبری و استراتژی مقوله حکمرانی داده‌ها مطرح می‌شود. همچنین انواع مدل حکمرانی شهرها بر پایه داده مورد بررسی قرار گرفته است.
اولویت‌بندی عوامل مؤثر بر امنیت اطلاعات در شهر هوشمند (اکرامی فرد، ۱۳۹۹)	این پژوهش با هدف بررسی و اولویت‌بندی عوامل مؤثر بر امنیت اطلاعات در شهر هوشمند صورت پذیرفته است. جامعه آماری آن شامل کلیه متخصصان، کارشناسان و مدیران آشنا به مسائل امنیت اطلاعات در شرکت‌های منتخب شهر مشهد هستند. نتایج تحقیق نشان می‌دهد که شش معیار: عامل سازمان، توسعه کنترل‌های امنیتی، عدم قطعیت عناصر محیطی، پشتیبانی سازمان، آگاهی سازمانی و مسائل رهبری امنیت اطلاعات به‌عنوان مهم‌ترین معیارها و عوامل مؤثر بر امنیت اطلاعات در شهر هوشمند می‌باشند. با توجه به نتایج به‌دست‌آمده پیشنهاد شده است: حمایت مدیریت ارشد شرکت‌ها از طرح‌ها و پیشنهادها در راستای امنیت اطلاعات باعث پیشرفت سازمان می‌باشد که باعث سرمایه‌گذاری در این زمینه نیز می‌گردد. هر شرکتی به‌ویژه شرکت‌های اطلاعات محور، بودجه‌ای را به‌طور سالانه در جهت پروژه‌های امنیت اطلاعات تخصیص دهند. با همکاری مدیران شرکت و نهادهای ذی‌ربط، فرهنگ امنیت اطلاعات به کارکنان و مدیران میانی و عملیاتی سازمان‌ها از طریق برگزاری کارگاه‌های آموزشی اطلاع‌رسانی و آموزش داده شود تا به ارتقای سطح کیفی امنیت اطلاعات در سازمان بیافزاید.
حاکمیت داده در شهر هوشمند پایدار کراسیمیر (پاسکالوا و همکاران، ۲۰۱۷)	تجزیه و تحلیل‌ها نشان می‌دهد که هوشمندی در حال تبدیل شدن به ابزاری است که برای تحقیق برنامه‌های توسعه پایدار در شهرها تلاش می‌کند. در این بین حاکمیت توسعه پایدار به یکی از اجزای اصلی تبدیل می‌شود. این مقاله به بررسی چگونگی حاکمیت داده در دستور کار شهرهای هوشمند جدید مبتنی بر پایدارسازی می‌پردازد. همچنین ابتکارات پایدار محور شهر هوشمند بیان شده است و سه کشور اروپایی و همچنین نظرسنجی ذینفعان نیز مطرح شده است. در این مقاله چگونگی اینکه مدیریت داده‌ها می‌تواند زیربنای راه‌حل‌های هوشمند سازی و پایدارسازی شهر هوشمند را نشان داده شده است. یافته‌های اساسی این تحقیق نشان می‌دهد که شهرهایی که در تلاش هستند تا به سوی شهرهای هوشمند پایدار بروند نیاز به همکاری و تعامل با ذینفعان برای شناسایی، جمع‌آوری تولید و استفاده از داده‌ها دارند؛ بنابراین پایداری رویکردی تعاملی دارد.

۲-۳- ادبیات تحقیق

یک شهر هوشمند شهری است که با استفاده از تجهیزات فناوری اطلاعات و تجهیزات ارتباطی به بهبود سطح زندگی، کارایی و همچنین پایداری توسعه شهری کمک می‌کند (*Smart Cities Council 2014*) (ارمی، ۲۰۱۷) (*Mircea Eremia, Lucian Toma, Mihai Sanduleac (2017)*). به‌طورکلی می‌توان گفت که مشکلات مربوط به موضوعات سلامت، ترافیک، جمعیت، کمبود منابع، مدیریت پسماندها، مدیریت منابع، ضعف فناوری و... از ادامه توسعه شهری جلوگیری به عمل می‌آورند؛ لذا شهر هوشمند به‌عنوان یک راه‌حل برای توسعه پایدار شهری ارائه می‌شود. موضوع هوشمندی به‌منزله‌ی پایداری و بهینه‌سازی در توسعه مطرح می‌شود (جوشی و دیگران، ۲۰۱۶a).

در حال حاضر، عملکرد توسعه شهری تنها به تجهیزات هوشمند و فناوری اطلاعات بستگی ندارد، بلکه به دسترسی‌پذیری و کیفیت میزان دانش از تجهیزات و ارتباطات نیز بستگی دارد. در شهرهای هوشمند اینترنت اشیاء که موجب اتصال بین تجهیزات و ایجاد شبکه می‌شود نقش کلیدی را دارد (ارمی و همکاران، ۲۰۱۷). هسته اصلی پردازش و فعالیت تجهیزات اینترنت اشیاء داده‌ها هستند که در حجم‌های مختلف، انواع مختلف و با سرعت‌های مختلفی تولید می‌شوند (گررو پرز و همکاران، ۲۰۱۳).



شکل ۱- داده‌های تولیدی شهر هوشمند

به‌صورت کلی می‌توان بخش‌های داده‌های تولیدی در شهرهای هوشمند را به شرح زیر عنوان کرد.

- موضوعات مربوط به داده‌های جمع‌آوری شده (داده‌های شهری و خدمات شهری و...)
- کاربران داده‌های تولید شده و استفاده‌کنندگان آنها (شرکت‌های دولتی، افراد و یا شرکت‌های خصوصی و...)
- سیاست‌های بالادستی دسترسی‌پذیری داده‌ها (چه زمانی؟ چه شخصی؟ چه اطلاعاتی؟ و...)

۲-۳-۱- چالش‌های امنیت داده و حریم خصوصی اینترنت اشیاء در شهر هوشمند

همان‌طور که در قسمت قبل بیان شد داده‌ها در شهر هوشمند به‌صورت پیوسته در حال گردش هستند. با افزایش روند جمعیتی شهرنشینی و هوشمندسازی شهرها قابل پیش‌بینی است که تجهیزات و زیرساخت‌های مورد نیاز برای بخش‌های مختلف شهر هوشمند نظیر حمل‌ونقل هوشمند، دولت هوشمند، سلامت هوشمند، محیط‌زیست، خانه هوشمند و... با رشد زیادی همراه است (سیو، *2018*) (*Lei Cui, Gang Xie, Youyang Qu, Longxiang Gao, Yunyun Yang (2018)*). همچنین افزایش کاربردهای هوشمندی در شهر و هوشمندسازی، ایجاد مشکلات و چالش‌های امنیتی و حریم خصوصی زیادی می‌شود. این مشکلات به دلیل حفره‌های امنیتی در لایه‌های این سیستم می‌باشد. چالش‌هایی نظیر حملات سایبری، دسترسی‌های غیرمجاز، از دسترس خارج شدن سیستم‌ها و... موجب به خطر افتادن کیفیت و قابلیت اطمینان هوشمندی در شهر می‌شود و کاهش اعتماد شهروندان به استفاده از تجهیزات هوشمند می‌شوند (ژانگ، *2017*). (*Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, Xuemin Sherman Shen (2017)*)

یکی از مهم‌ترین چالش‌های مطرح شده در زمینه داده‌های شهر هوشمند، موضوع حریم خصوصی داده‌هاست. امنیت و حریم خصوصی داده اغلب با هم همپوشانی دارند، با این حال این دو چالش از یکدیگر متفاوت هستند. حریم خصوصی مربوط به داده‌های اشخاص و نحوه دسترسی به آن را شامل می‌شود، درحالی‌که امنیت داده از داده‌ها حفاظت می‌کند. حریم خصوصی اطلاعات به حق کنترل بر نحوه جمع‌آوری، ذخیره و استفاده از اطلاعات و داده‌های شخصی می‌پردازد. سازمان‌ها موظفند در مورد اینکه چه داده‌هایی را جمع‌آوری می‌کنند، هدف از جمع‌آوری داده و نحوه به اشتراک‌گذاری داده‌ها شفاف باشند (اکتا، ۲۰۲۲).

۲-۳-۲- ذینفعان مطرح در شهر هوشمند

در مدیریت پروژه‌های شهری و هرگونه قانون‌گذاری بسیار پراهمیت است تا ذینفعان و تأثیرگذاران شهر به‌درستی شناسایی شوند زیرا ذینفعان، در هر بخش از مدیریت حاکمیتی شهر تأثیرگذار هستند (جایاسنا و همکاران، ۲۰۱۹). موضوع مدیریت ذینفعان و بازیگران شهر هوشمند شامل بخش‌های شناسایی، دسته‌بندی، مدیریت ارتباط، تأثیرگذاری، قدرت و کنترل ریسک می‌باشد. یکی از چالش‌های هوشمندسازی شهرها مربوط به اختلاف، تعارض منافع و پیچیدگی برخی از ذینفعان شهر هستند. با شناخت صحیح از تمامی ذینفعان شهر هوشمند می‌توان به حالتی رسید که ذینفعان نیز در جهت رسیدن به اهداف شهر هوشمند پایدار رفتار کنند. شناخت ذینفعان شهر هوشمند باعث می‌شود خواسته‌های آنان به‌درستی مطرح شود و با پاسخ مناسب نیازهایشان مشارکت آنان در مدیریت شهر هوشمند افزایش می‌یابد (رجبلو و همکاران، ۲۰۱۴).

ذینفعان مطرح در شهر هوشمند را می‌توان به دسته‌های زیر تقسیم‌بندی نمود (رجبلو و همکاران، ۲۰۱۴):

- **مراکز آموزشی و بخش آموزش:** یکی از نکات کلیدی شهر هوشمند نوآوری‌هایی است که دائماً در حال توسعه هستند و منبع اصلی نوآوری‌ها در شهر هوشمند به‌شمار می‌روند. با در نظر گرفتن مؤسسات آموزشی، دانشگاه‌ها و پژوهشکده‌ها به‌عنوان یک ذینفع اصلی در شهر هوشمند به پیشرفت فناوری و نوآوری‌های شهر هوشمند کمک شایانی می‌کند.
- **بخش مدیریتی شهری و استانی:** شهرداری‌ها و استانداری‌ها یکی دیگر از ذینفعان اصلی شهرهای هوشمند هستند. خدمات شهری و همچنین ارتباط اصلی شهروندان با بدنه شهر توسط شهرداری‌ها و استانداری‌ها صورت می‌پذیرد؛ لذا در نظر گرفتن بخش مدیریتی شهر به‌عنوان یکی از ذینفعان باعث مشارکت آنها به پیاده‌سازی پروژه‌های شهر هوشمند خواهد شد. همچنین از دیگر نقش‌های آنان می‌توان به تأمین منابع برای پیاده‌سازی پروژه‌ها اشاره کرد. پیاده‌سازی بخش‌های مختلف هوشمندسازی شهرها به تأمین مالی بزرگی احتیاج دارد؛ لذا در نظر گرفتن بخش مدیریت شهری نیز به‌عنوان یکی از مراکز تأمین بودجه (مالیات شهروندان و...) سبب می‌شود از ذینفعان اصلی شهر هوشمند نیز به شمار رود.
- **تأمین‌کنندگان انرژی:** در بسیاری از شهرهای هوشمند به دلیل مسائل محیط‌زیست و همچنین توسعه پایدار رویکرد انرژی سبز پر رنگ است؛ لذا تولید انرژی از بخش دولتی به بخش خصوصی و مردمی منتقل شده و همچنین مشوق‌هایی برای تولید انرژی سبز در نظر گرفته می‌شود. لذا درصورتی‌که تأمین انرژی از سوی شرکت‌های خصوصی و مردمی صورت پذیرد می‌توان این بخش را نیز به‌عنوان یکی از ذینفعان در نظر گرفت.
- **بخش خدمات فناوری اطلاعات:** یکی از کلیدی‌ترین هوشمندی در شهر هوشمند، خدمت‌رسانی تجهیزات فناوری اطلاعات به شهر می‌باشد. بسیاری از شرکت‌های خصوصی، دولتی و زیرساختی هستند که مسئولیت پیاده‌سازی این هوشمندی را در شهر دارند. لذا از مشارکان اصلی شهر هوشمند بخش فناوری اطلاعات و فناوری‌های کامپیوتری می‌باشد.
- **شهروندان:** اصلی‌ترین ذینفع در شهر هوشمند شهروندان هستند. نظرات و نیازهای شهروندان در بالاترین اولویت در مدیریت و حاکمیت شهر هوشمند می‌باشد. همچنین از مباحث مهمی که در این بخش مطرح است شهروندان هوشمند می‌باشد. شهروندان مهم‌ترین نوع مشارکتی را در برنامه‌ریزی شهری دارند و همچنین میزان هوشمندی آنان از مهم‌ترین پارامترهای کلیدی ارزیابی هوشمندی شهر می‌باشد. به‌طور خلاصه مهم‌ترین مؤلفه‌های شهروندان هوشمند می‌توان به تعامل با حاکمیت، خلاقیت و نوآوری، توسعه استعدادها و دسترسی بهینه به آموزش اشاره کرد (کوندپودی، ۲۰۱۶).
- **حاکمیت:** در کشورهای مختلف با توجه به نوع سیاست حاکمیتی، ساختار متفاوتی می‌توان برای بخش حاکمیت آن در نظر گرفت. به‌طورکلی مفهوم حکمروایی شهری که اغلب به‌عنوان جایگزینی برای روش‌های سنتی دولت (متمرکز، سلسه‌مراتبی، از بالا به پایین، بوروکراتیک) در نظر گرفته می‌شود رویکردی بر اساس

مکانیسم‌ها و شبکه‌های عملیاتی عمومی با هدف همکاری، سازمان‌دهی و حتی یکپارچه‌سازی سیستم‌ها و مکانیسم‌های تنوع گسترده سهام‌داران عمومی و خصوصی (چند مرکزی، مبتنی بر شبکه، افقی، متقابل انضباطی، مبتنی بر فرایند، رویکرد از پایین به بالا) است (آرتیوشینا، ۲۰۲۰). یک حاکمیت خوب شهری باعث می‌شود تا مشارکت افراد جامعه در تصمیمات شهری بالا رود و همچنین نیازهای شهروندان به‌صورت مؤثر در نظر گرفته شود.

حاکمیت هوشمند در واقع یکی از بخش‌های اصلی شهر هوشمند می‌باشد که به بخش‌های سیاسی و مشارکتی شهروندان در شهر هوشمند مربوط می‌شود (رولند، ۲۰۱۸). حاکمیت هوشمند می‌تواند از طریق تعامل بین فناوری، مردم، سیاست‌ها، دستورالعمل‌های بهینه، منابع، فرایندهای اجتماعی مرسوم و همچنین اطلاعات از اهداف حاکمیت در شهر هوشمند پشتیبانی کند.

۲-۳-۳- حاکمیت امنیت داده

داده‌های سازمان‌ها و شرکت‌ها به‌صورت افزاینده در حال افزایش می‌باشد. افزایش داده‌ها در جنبه‌های مختلف افزایش منابع تولید داده، حجم داده، کاربردهای داده‌ها و محل داده‌ها اتفاق می‌افتد. به‌ندرت دیگر اتفاق می‌افتد که داده به‌صورت محلی تولید و مصرف شود و یا در درون یک سازمان بماند و در دنیای خارج از آن ارتباطی نداشته باشد. اکنون داده‌ها به‌صورت آزادانه و نامحدود در گردش هستند و نمی‌توان مرز دقیقی برایشان مشخص کرد. با وجود تمام تغییرات و مزیت‌هایی که داده‌ها در اختیار گذاشته‌اند، پس از ایجاد و یا جمع‌آوری، داده‌ها در معرض حمله و یا سوء استفاده قرار می‌گیرند. در ده سال گذشته تعداد گزارش‌های نقض داده‌ها (*Data Breaches*) دو برابر شده است و نیم میلیارد رکورد در سال گذشته ایجاد شده است لذا اعتماد ما به اطلاعات به دلیل فقدان امنیت در معرض تهدید است (دونا دیویس).

اطلاعات و داده‌ها در سیستم فناوری اطلاعات نگه‌داری می‌شوند و ارزش و تصمیمات نهایی سازمان‌ها و دولت‌ها به داده‌ها وابسته است و اهداف سازمانی را می‌توانند محقق سازند. از طرفی همواره داده‌ها از سوی حمله‌ها، دست‌کاری داده‌ها، نقص داده‌ها و... تهدید می‌شوند. لذا لازم است که سازمان‌ها همواره در کارهای روزمره خود امنیت اطلاعات را در نظر بگیرند و ریسک امنیت داده‌ها را در تصمیمات خود در نظر داشته باشند. این تنها در صورتی موفقیت‌آمیز و مؤثر خواهد بود که مدیریت ارشد تهدیدات امنیتی را به‌درستی ارزیابی کند و همچنین سازمان پاسخگوی آن باشد. این همکاری بین امنیت اطلاعات (*Information Security (IS)*) و حاکمیت سازمانی (*Corporate Governance (CG)*) را حاکمیت امنیت اطلاعات (*Information Security Governance (ISG)*) عنوان می‌کنند. حاکمیت امنیت اطلاعات به مسائلی نظیر دارایی‌های امنیت اطلاعات به‌صورت یک موضوع جامع با در نظرگیری ذینفعان سازمان می‌پردازد.

با توجه به مطالبی که عنوان شد می‌توان نتیجه گرفت که حاکمیت امنیت اطلاعات تنها با مسائل فنی امنیت داده‌ها و فناوری اطلاعات سروکار ندارد بلکه موضوعاتی از جنس حاکمیت سازمانی را نیز در نظر می‌گیرد.

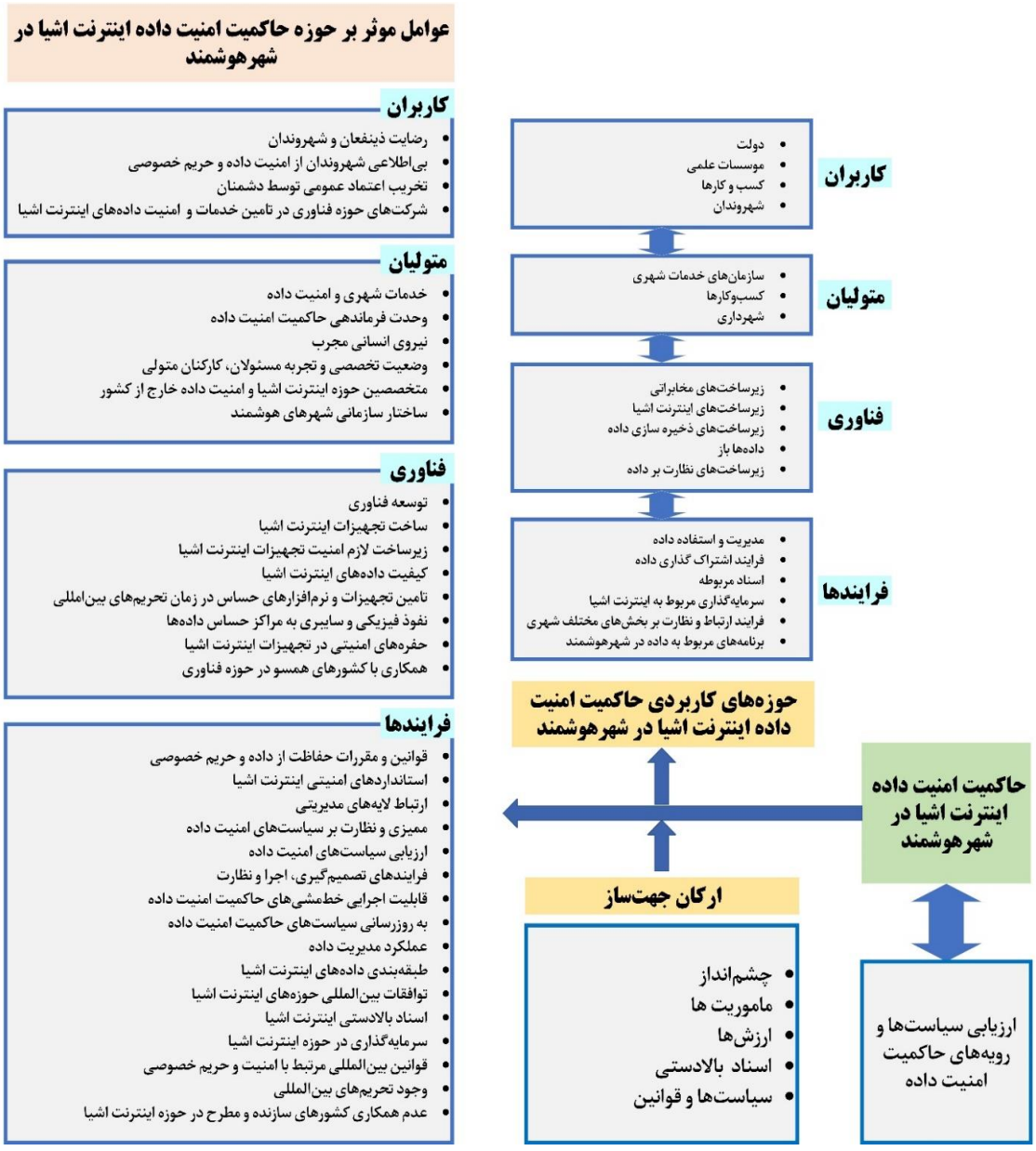
بر اساس مطالعات انجام شده، مدل مفهومی این تحقیق مطابق با شکل ۲ می‌باشد.

۳- روش‌شناسی تحقیق

پژوهش حاضر از لحاظ هدف (نوع تحقیق) در زمره تحقیقات کاربردی دسته‌بندی می‌گردد. همچنین از لحاظ روش تحقیق در زمره تحقیقات توصیفی/تحلیلی با نگاه اکتشافی دسته‌بندی می‌گردد. پژوهش حاضر از نظر موضوع و زمینه علمی به دنبال آن است که با تکیه بر آراء و نظرات خبرگان و بررسی مستندات علمی و قانونی به احصاء حوزه‌های کاربردی حاکمیت امنیت داده در اینترنت اشیاء در حوزه شهر هوشمند برسد. از نظر بعد زمانی، با توجه به تحولات سریع فضای سایبر آینده (میان‌مدت) را شامل خواهد شد. از لحاظ بعد مکانی گستره جغرافیای جمهوری اسلامی ایران مد نظر است. جامعه آماری تحقیق مورد نظر ۴۵ نفر می‌باشد.

در این پژوهش از دو شیوه نمونه‌گیری غیر احتمالی یعنی نمونه‌گیری با استفاده از روش نمونه‌گیری هدفمند (*Purposive Sampling*)/ معیار محور (*Criterion–Based Sampling*) (انتخاب تمام موردها با انتخاب معیار خاص) و نمونه‌گیری با شیوه گلوله برفی (*Snowball*) (انتخاب موردها

با انتخاب محدودی از افراد که پژوهشگر را به افراد دیگر ارجاع می‌دهد) استفاده خواهد شد. تکنیک گردآوری اطلاعات متناسب با روش تحقیق موضوع مورد مطالعه انتخاب می‌شود. در موضوع مورد مطالعه اطلاعات در دو بخش گردآوری می‌شود. بخش اول مربوط به ادبیات موضوع و مبانی نظری (سطح نظری) و بخش دوم مربوط به اخذ نظر صاحب‌نظران و متخصصان (سطح تجربی یا عملی) موضوع تحقیق است، با توجه به اینکه سؤالات پرسشنامه حوزه‌ها و عوامل مؤثر حاکمیت امنیت داده را مورد سؤال قرار می‌دهد روش تحلیل داده‌ها با استفاده از آمار توصیفی و استخراج میانگین پرسش‌ها مربوط به هر یک از اینهاست، ویژگی‌هایی که دارای میانگین ۳ به بالا هستند مورد تأیید خبرگان است و مواردی که زیر این مقدار هستند رد شده‌اند و از این طریق شاخص‌های پیشنهادی مورد ارزیابی قرار می‌گیرد.



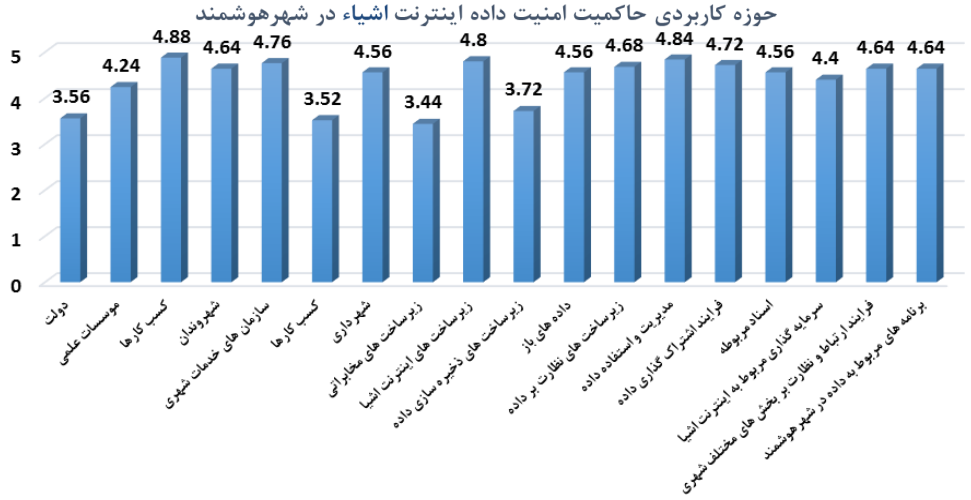
شکل ۲- مدل مفهومی تحقیق.

۴- تجزیه‌وتحلیل یافته‌ها

با توجه به بررسی‌های معلمی و همچنین بررسی‌های میدانی انجام شده بر روی حوزه‌های کاربردی حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند که در فصل دوم نیز به آن پرداخته شد، تعداد ۱۷ حوزه کاربردی متصور برای حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند توسط محقق شناسایی گردید. این حوزه‌ها از طریق پرسشنامه شماره یک مورد ارزیابی و غربالگری خبرگان قرار گرفت و از آنها خواسته شد که میزان موافقت خود را از اعداد ۱ تا ۵ مشخص نمایند. پس از جمع‌آوری پرسشنامه‌ها و بررسی پاسخ‌های خبرگان، تعداد ۱۳ حوزه کاربردی که مقادیر پاسخ آنها بیش از مقدار عددی ۴ بودند، مورد تأیید قرار گرفتند که نتیجه نظرخواهی انجام شده برای ۱۷ حوزه به شرح زیر می‌باشد:

نمودار ۱، مبین این مطلب است که از نظر جامعه خبره، ۱۳ حوزه مؤسسات علمی، کسب‌وکارها، شهروندان، سازمان‌های خدمات شهری، شهرداری، زیرساخت‌های اینترنت اشیاء، داده‌های باز، زیرساخت‌های نظارت بر داده، مدیریت و استفاده داده، فرایند اشتراک‌گذاری داده، اسناد مربوطه، سرمایه‌گذاری مربوط به اینترنت اشیاء، فرایند ارتباط و نظارت بر بخش‌های مختلف شهری، برنامه‌های مربوط به داده در شهر هوشمند، بیشترین و اساسی‌ترین کاربرد را در حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند دارا بوده و دارای امتیاز مساوی یا بالاتر از میانگین ۳ می‌باشند و بنابراین در این رساله فرایند تدوین طرح راهبردی حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند، با در نظر گرفتن این سیزده حوزه صورت خواهد گرفت.

از بین همه عوامل اثرگذار که توسط جامعه آماری و خبره مورد ارزیابی قرار گرفت، پس از تحلیل نرم‌افزاری مشخص گردید که تعداد ۵۸ عامل به شرح جدول ۱ در سطح راهبردی نقش‌آفرینی می‌کنند.



نمودار ۱- انتخاب حوزه‌های اساسی.

جدول ۱- عوامل تأثیرگذار در حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند.

ردیف	عوامل تأثیرگذار در حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند
۱	وجود قوانین و مقررات حفاظت از داده و حریم خصوصی در شهر هوشمند
۲	وجود استانداردهای امنیتی اینترنت اشیاء در سطح شهر هوشمند
۳	گسترش زیرساخت فناوری اطلاعات و ارتباطات کشور
۴	ارتباط پیوسته لایه مدیریت شهری با حاکمیت امنیت داده
۵	استقبال از فناوری‌های نوین
۶	ایجاد فرایند بازرسی و کنترل اجرایی بودن خط‌مشی‌های حاکمیت امنیت داده

ادامه جدول ۱- عوامل تأثیرگذار در حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند.

ردیف	عوامل تأثیرگذار در حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند
۷	انبوه کاربران فضای مجازی
۸	ارزیابی سیاست‌های حاکمیت امنیت داده در شهر
۹	حفظ تسهیل خدمات شهری در کنار امنیت داده‌های شهر هوشمند
۱۰	پیوست امنیت داده در برنامه‌های شهر هوشمند
۱۱	وحدت فرماندهی حاکمیت امنیت داده
۱۲	ارتباط بین حاکمیت با ارکان و دستگاه‌های ذی‌ربط شهر هوشمند
۱۳	برخورداری از نیروی انسانی مجرب در سطح شهر هوشمند
۱۴	در نظرگیری بازیگران متعدد در تصمیم‌گیری و حفظ وحدت فرماندهی
۱۵	کسب رضایت ذینفعان در ارائه خدمات امنیت داده شهر هوشمند
۱۶	راهکارهای افزایش ضریب امنیتی حضور کاربران در بستر اینترنت اشیاء
۱۷	ایجاد برنامه مدون توسعه اینترنت اشیاء با در نظرگیری امنیت داده
۱۸	برنامه‌ریزی، راهبری و پایش و نظارت عالی بر پروژه‌های شهر هوشمند از منظر امنیت داده و ارائه شاخص‌های امنیت
۱۹	برنامه‌های مداوم ممیزی امنیت داده‌های اینترنت اشیاء در شهر
۲۰	عدم چابکی ساختار در فرایند تصمیم‌گیری، اجرا و نظارت بر عملکرد حوزه‌های شهر هوشمند
۲۱	عدم تحلیل ابتدایی داده‌های ورودی لایه حاکمیت
۲۲	عدم قابلیت اجرایی خط‌مشی‌های حاکمیت امنیت داده
۲۳	عدم به‌روزرسانی سیاست‌های حاکمیت امنیت داده مطابق با استانداردهای جهانی
۲۴	عدم‌کفایت وضعیت تخصصی مسئولان و کارکنان متولی شهر هوشمند در حوزه‌های مرتبط با اینترنت اشیاء
۲۵	عدم تجربه متخصصین و مسئولان در حوزه اینترنت اشیاء و شهر هوشمند
۲۶	طولانی بودن زمان تصمیم‌گیری پاسخ‌دهی به تهدیدهای سایبری سامانه‌های اینترنت اشیاء
۲۷	ضعف در عملکرد مدیریت داده
۲۸	ضعف در ساخت تجهیزات اینترنت اشیاء
۲۹	فقدان زیرساخت لازم جهت شناسایی حفره‌های امنیتی
۳۰	ضعف در تأمین شاخص‌ها و استانداردهای فنی مرتبط با اینترنت اشیاء
۳۱	کاهش کیفیت داده‌های اینترنت اشیاء در اثر برنامه‌های امنیت داده
۳۲	فقدان فناوری‌های لازم جهت پاسخ‌دهی به حملات سایبری
۳۳	عدم توجه به تعیین مجوزهای دسترسی سازمان‌ها و شرکت‌ها به داده‌های شهر هوشمند
۳۴	عدم طبقه‌بندی داده‌های اینترنت اشیاء در شهر هوشمند
۳۵	وجود توافقات بین‌المللی مفید در برخی از حوزه‌های اینترنت اشیاء و شهر هوشمند
۳۶	وجود اسناد بالادستی سایر کشورها به‌منظور تدوین سند بالادستی اینترنت اشیاء کشور
۳۷	وجود سرمایه‌گذاران بین‌المللی در برنامه‌های غیر حساس اینترنت اشیاء در شهر هوشمند
۳۸	قوانین بین‌المللی مرتبط با حریم خصوصی و مالکیت داده اینترنت اشیاء در شهر هوشمند
۳۹	امکان الگوبرداری از ساختار سازمانی شهرهای هوشمند در سطح جهانی
۴۰	وجود رقابت در حوزه‌های امنیت داده، اینترنت اشیاء و شهر هوشمند در سطح جهانی
۴۱	سخت شدن شرایط خرید از خارج به‌واسطه اعمال تحریم‌های بین‌المللی و امکان رشد تولید داخلی
۴۲	بهره‌گیری از تجارب سایر کشورها در توسعه بسترهای خدمات‌دهی در اینترنت اشیاء در سطح ملی
۴۳	امکان مشارکت فعال متخصصین حقوقی کشور و مسئولان شهر هوشمند در تدوین قوانین بین‌المللی مربوط به امنیت داده اینترنت اشیاء

جدول ۱- عوامل تأثیرگذار در حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند.

ردیف	عوامل تأثیرگذار در حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند
۴۴	استفاده از ظرفیت متخصصین خارج از کشور
۴۵	امکان صدور دانش و فناوری به کشورهای دوست
۴۶	وجود رقابت سازمان‌ها و شرکت‌های بین‌المللی در ایجاد و توسعه فضای امن اشتراک‌گذاری داده‌های شهر هوشمند
۴۷	عدم همکاری مناسب و سازنده کشورهای دارای فناوری اینترنت اشیاء و شهر هوشمند
۴۸	فقدان نظام حقوق بین‌المللی در حوزه امنیت داده کشورها
۴۹	عدم تأمین تجهیزات و نرم‌افزارهای حساس در زمان تحریم‌های بین‌المللی
۵۰	نفوذ فیزیکی به مراکز حساس داده‌های اینترنت اشیاء
۵۱	تخریب اعتماد شهروندان به برنامه‌های اینترنت اشیاء در شهر هوشمند توسط دشمنان
۵۲	بی‌اطلاعی شهروندان و کاربران از امنیت داده‌ها و حریم خصوصی در بستر اینترنت اشیاء
۵۳	چالش‌های جدید (آسیب‌پذیری) تجهیزات نوظهور اینترنت اشیاء
۵۴	درنظرگیری رقبای قوی در سطح منطقه‌ای و جهانی با انگیزه‌های سیاسی مختلف
۵۵	نفوذ سایبری به مراکز داده جهت سرقت، حذف و یا تغییر داده مربوط به قطعات، تجهیزات، سامانه‌های اینترنت اشیاء و یا اختلال در ارائه خدمات
۵۶	شناسایی مدارات اضافی تعبیه شده در سامانه و تجهیزات اینترنت اشیاء (جهت ردیابی موقعیت مکانی سامانه‌ها، جاسوسی، اعمال اقدامات و سرقت داده‌ها)
۵۷	شناسایی حفره‌های امنیتی و کلیدهای از کار انداز تعبیه شده در ریزتراشه‌ها (کنترل عملیاتی و یا مختل کردن عملکرد تجهیزات)
۵۸	نفوذ سایبری به سامانه‌های اینترنت اشیاء و تزریق داده‌های غلط و گمراه کننده

۵- نتیجه‌گیری

یکی از اساسی‌ترین نیازها برای نیل به پیشرفت و توسعه همه‌جانبه یک کشور، پژوهش است؛ همچنین قدرت و استقلال هر کشوری بر پژوهش و تولید علم استوار است. برای این منظور با توجه به پرسش‌های تحقیق که در ابتدا مطرح شده است، ابتدا حوزه‌های کاربردی اصلی حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند تشریح شد. این چهار حوزه حوزه‌های کاربران، متولیان، فناوری و فرایندها می‌باشد. همچنین در این چهار حوزه اصلی، ۱۷ زیرحوزه شناسایی شده که بر اساس تحقیقات میدانی تعداد ۱۳ زیرحوزه احصاء گردید. همچنین با توجه به حوزه‌ها و زیرحوزه‌های کاربردی حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند، تعداد ۵۶ عامل مؤثر در شهر هوشمند شناسایی گردید.

۶-پیشنهاد

- به‌کارگیری حاکمیت امنیت داده اینترنت اشیاء در شهر هوشمند توسط معاونت‌های ارتباطات و فناوری اطلاعات سازمان‌های خدمات شهری در حوزه‌ها و زیرحوزه‌های معرفی شده
- در نظر گرفتن عوامل مؤثر بر حوزه‌های حاکمیت امنیت داده اینترنت اشیاء به‌منظور تدوین دستورالعمل استانداردسازی نرم‌افزارها، پروتکل‌ها و فرایندهای ارتباط دیجیتالی تجهیزات اینترنت اشیاء توسط سازمان پدافند غیرعامل
- معاونت‌های ارتباطات و فناوری اطلاعات سازمان‌های خدمات شهری و زیر نظر شهرداری‌ها، در خصوص جهت اتخاذ رویکرد حاکمیت امنیت داده اینترنت اشیاء اقدام نمایند.

۷- مراجع

[۱] اکرامی‌فرد، م. (۱۳۹۹). اولویت‌بندی عوامل مؤثر بر امنیت اطلاعات در شهر هوشمند. مؤسسه آموزش عالی اترک.

[۲] امینی، م. (۱۳۹۷). طرحی مدلی برای مدیریت اکوسیستم کلان‌داده برای کسب‌وکارهای داده‌محور در جامعه فیزیکی-سایبری با تأکید بر شهر هوشمند. دانشگاه آزاد اسلامی واحد علوم تحقیقات.

[3] سخایی، م. ج. (۱۳۹۷). مدل‌های بلوغ حاکمیت داده (۱). فابک http://www.fabak.ir/ShowResourceDetailsForPublic.aspx?Side=GgpexOX5EHc=

[4] Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. International Journal of Information Management, 49(January), 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008.

[5] Artyushina, A. (2020). Is civic data governance the key to democratic smart cities? The role of the urban data trust in Sidewalk Toronto. Telematics and Informatics, 55(January), 1–13. https://doi.org/10.1016/j.tele.2020.101456.

[6] Brockman, C. (2020). Data security governance explained. AT&T Business. https://cybersecurity.att.com/blogs/security-essentials/data-governance.at-the-heart-of-security-privacy-and-risk.

[7] Choenni, S., Bargh, M.S., Busker, T., & Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. Journal of Smart Cities and Society, 1(1), 31–51. https://doi.org/10.3233/scs-210119.

[8] Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. IEEE Access, 6(July), 46134–46145. https://doi.org/10.1109/ACCESS.2018.2853985.

[9] Diligent. (2016). Five Best Practices for Information Security Governance terabytes of sensitive data 4, to the Anthem Medical data. 2–5. http://www.businessinsider.com/the-sony-hackers-still-have-a-

[10] Donna Davis. (n.d.). Data Security Governance. IRI-Total Data Management. https://www.iri.com/blog/vldb-operations/data-security-governance.

[11] Efthymiopoulos, M.P. (2015). Cyber-security in smart cities: the case of Dubai. Journal of Innovation and Entrepreneurship, 5(1). https://doi.org/10.1186/s13731-016-0036-x.

[12] Eremia, M., Toma, L., & Sanduleac, M. (2017). The Smart City Concept in the 21st Century. Procedia Engineering, 181, 12–19. https://doi.org/10.1016/j.proeng.2017.02.357.

[13] Franke, J., & Gailhofer, P. (2021). Data Governance and Regulation for Sustainable Smart Cities. Frontiers in Sustainable Cities, 3. https://doi.org/10.3389/frsc.2021.763788.

[14] Guerrero-Pérez, A.D., Huerta, A., González, F., & López, D. (2013). Network Architecture based on Virtualized Networks for Smart Cities. IEEE CCD Smart Cities White Paper, October, 1–6.

[15] Hasbini, M.A., Eldabi, T., & Aldallal, A. (2018). Investigating the information security management role in smart city organisations. World Journal of Entrepreneurship, Management and Sustainable Development, 14(1), 86–98. https://doi.org/10.1108/wjemsd-07-2017-0042.

[16] Jayasena, N.S., Mallawaarachchi, H., & Waidyasekara, K.G.A.S. (2019). Stakeholder Analysis For Smart City Development Project: An Extensive Literature Review. MATEC Web of Conferences, 266(January), 06012. https://doi.org/10.1051/matecconf/201926606012.

[17] Joshi, S., Saxena, S., Godbole, T., & Shreya. (2016). Developing Smart Cities: An Integrated Framework. Procedia Computer Science, 93(September), 902–909. https://doi.org/10.1016/j.procs.2016.07.258.

[18] Kondepudi, S., & Kondepudi, A. (2016). a Step By Step Approach Towards Planning a Smart Sustainable City Using a Strategic Plan. https://doi.org/10.16962/elkapj/si.icssc-2016.1.

[19] Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data, 6(1). https://doi.org/10.1186/s40537-019-0268-2.

[20] Lowans, B., Kish, D., Willemsen, B., & Girard, J. (2018). How to Use the Data Security Governance Framework. Gartner.

[21] Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. Energy Reports, 7, 7999–8012. https://doi.org/10.1016/j.egyr.2021.08.124.

[22] Okta. (2022). Privacy vs. Security: Exploring the Differences & Relationship. Okta. www.okta.com/identity-101/privacy-vs-security.

[23] Paskaleva, K., Evans, J., Martin, C., Linjordet, T., Yang, D., & Karvonen, A. (2017). Data Governance in the Sustainable Smart City. Informatics, 4(4), 41. https://doi.org/10.3390/informatics4040041.

[24] Rajablu, M., Marthandan, G., & Yusoff, W. F. W. (2014). Managing for stakeholders: The role of stakeholder-based management in project success. Asian Social Science, 11(3), 111–125. https://doi.org/10.5539/ass.v11n3p111.

[25] Ruhlandt, R. W. S. (2018). The governance of smart cities: A systematic literature review. Cities, 81(October 2017), 1–23. https://doi.org/10.1016/j.cities.2018.02.014.

[26] Singh, A. (2019). Data Security and Governance (DSG) for Big Data and BI. KuppingerCole Analysts. https://www.kuppingercole.com/blog/singh/data-security-and-governance-dsg-for-big-data-and-bi.

[27] Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. IEEE Communications Magazine, 55(1), 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM.

نشریه‌ی علمی شهر ایمن
JOURNAL OF RESILIENT CITY
(JRC)

Application Areas of Internet of Things Data Security Governance in the Smart City

Javad Gharibi[1*], Hossein Gharaee[2], Mohammad Reza Farajipoor[3], Khodadad Halili[4]

1. Ph.D. Student, Superme National Defence University (Corresponding Author)
2. Associate Professor, ICT Research Institute
3. Assistant Professor, Superme National Defence University
4. Assistant Professor, Superme National Defence University

Abstract:

Smart cities rely heavily on technology and data to improve citizens' quality of life. However, this reliance on technology also creates significant security challenges such as cyber security threats, data privacy, interoperability and lack of necessary standards. In order to deal with these challenges and also to reduce conflicts between security and Internet of Things services in the smart city, it is necessary to consider initiatives. Data security governance is a process of ensuring data security while maintaining the efficiency and performance of the data in the areas of use. In order to use the data security governance of the Internet of Things in Houshmand city, it is necessary to identify its application areas. These areas can be calculated by considering the structure of the smart city, the Internet of Things, the structure and topic of data, as well as the beneficiaries of the data in the smart city. In this article, by studying different sources and using elite capacity, 4 main areas and 17 applied sub-areas of Internet of Things security governance in Houshmand city have been identified. Also, after identifying the areas, the effective factors on data security governance of Internet of Things in Houshmand city have been calculated.

Keywords: Data Security Governance, Internet of Things, Smart City.

* Corresponding author: ***m.amngh@aut.ac.ir***