فصلنامه علمی امنیت ملی
سال چهاردهم، شماره پنجاه و سوم، پائیز ۱۴۰۳
مقاله پنجم از صفحات ۱۷۶-۱۴۳

مقاله پژوهشی: ارائه طرح راهبردی حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند

جواد غریبی[۱] حسین قرایی[۲] محمدرضا فرجی پور[۳] و خداداد هلیلی[۴]

تاریخ دریافت: ۱۴۰۱/۰۹/۰۸ تاریخ پذیرش: ۱۴۰۲/۰۳/۰۸

چکیده

دستیابی موثر به اهداف شهرهوشمند بدون اطمینان از امنیت این حجم از داده میسر نخواهد بود. چالش‌هایی نظیر امنیت داده، حریم خصوصی داده‌ها، کیفیت داده، دسترسی داده‌ها، درنظر گرفتن منافع ذینفعان به‌طور هم‌زمان و بسیاری از موضوعات دیگر دستیابی به اهداف هوشمند شهر را مشکل می‌کنند. جهت مقابله با این تهدیدات و همچنین کاهش تقابل‌های امنیت و خدمات اینترنت اشیا در شهرهوشمند، نیاز به «راهبردهای حاکمیت امنیت داده‌های اینترنت اشیا در شهرهوشمند» است که در این تحقیق به عنوان هدف اصلی مطرح گردیده و بر این اساس محقق به دنبال پاسخ به این سوال بوده که «راهبردهای حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند چیست؟» پس از بررسی اسناد بالادستی، نسبت به شناخت محیط داخل و خارج و تجزیه و تحلیل آن‌ها اقدام و بر اساس نظرات خبرگان، راهبردهای مربوطه تدوین گردید. سپس بر اساس محاسبه مطلوبیت‌ها اولویت‌بندی شدند. همچنین تاثیر هریک از راهبردهای مذکور بر تحقق اهداف کلان تعیین گردید. این راهبردها با قابلیت پیاده‌سازی و اجرای همسو با سایر حوزه‌ها ارائه شده است و با تبدیل این راهبردها به برنامه‌های اجرایی و پیاده‌سازی آن‌ها، می‌توان موانع بهره‌مندی داده‌های اینترنت اشیا در شهرهوشمند را برطرف کرده و باتوجه به چرخه داده‌ها در شهرهوشمند چالش‌های اساسی امنیت داده‌های اینترنت اشیا را تا حد قابل قبولی برطرف کرد.

کلیدواژه‌ها: طرح راهبردی، حاکمیت امنیت داده، اینترنت اشیا، شهرهوشمند.

[۱] دانش آموخته مقطع دکتری دانشگاه عالی دفاع ملی، رایانامه: j.gharibi@sndu.ac.ir
[۲] دانشیار پژوهشگاه ارتباطات و فناوری اطلاعات (نویسنده مسئول)، رایانامه: gharaee@itrc.ac.ir
[۳] مدرس دانشگاه دفاع ملی، رایانامه: mrfaraji@ihu.ac.ir
[۴] استادیار دانشکده کامپیوتر، دانشگاه شهید ستاری، رایانامه: halili@chmail.ir

۱. مقدمه و بیان مسئله:

امروزه با پیشرفت فناوری در هر سازمان تجاری تحول یافته‌ای استفاده از اطلاعات در کسب‌کار و تجارت بسیار پراهمیت واقع شده است. این اطلاعات در سیستم‌های فناوری اطلاعات ذخیره و مربوط می‌شوند اما با پیشرفت فناوری هم‌زمان خطرات امنیتی و تهدیدات در برابر این اطلاعات نیز بیشتر می‌شود. لذا یکی از چالش‌های هوشمند شدن بر پایه اطلاعات، اطمینان حاصل کردن از حفظ سه‌گانه امنیت (دسترسی‌پذیری، محرمانگی و یکپارچگی) است. هم‌زمان با پیاده‌سازی فناوری اطلاعات در سازمان‌ها، نمی‌توان در تصمیمات سازمانی بخش فناوری اطلاعات را نادیده گرفت. چالش‌هایی نظیر پیشرفته شدن روزافزون هوشمندی، پیچیده شدن تهدیدات هوشمندی، کمبود آگاهی فناوری اطلاعات و امنیت اطلاعات در افراد ذی‌ربط، سرمایه‌گذاری نامناسب برای بخش امنیت اطلاعات، نبود حاکمیت سازمانی در بخش امنیت اطلاعات از جمله چالش‌های امروزه هوشمند شدن سازمان‌ها می‌باشد (بولنگیر، ۲۰۲۰).[۱]

فضای سایبر به‌شدت آسیب‌پذیر است و در سطح ملی می‌تواند از سوی عوامل بیرونی یا درونی مورد تهدید جدی قرار گرفته و صدمه ببیند که این خسارت متوجه حاکمیت، سازمان‌ها و نهادهای دولتی، موسسه‌ها، بانک‌ها و در نهایت شهروندان خواهد گردید؛ بنابراین امنیت فضای سایبری یکی از مولفه‌های امنیت ملی است که باید به‌طور جدی مورد توجه قرار گیرد (سعادتمند، ۱٤۰۰). سازمان استاندارد جهانی[۲] در سال ۲۰۱۳ استاندارد مربوط به حاکمیت امنیت اطلاعات را در بخشی از سری استانداردهای ۲۷۰۰۰ منتشر کرد. این استاندارد شامل راهنمایی‌هایی برای موضوع حاکمیت امنیت اطلاعات است که فعالیت‌های امنیت اطلاعات را با راهبردهای سازمان به‌وسیله ارائه شش سطح اصولی، همسو می‌کند. این استاندارد پنج فعالیت مشخص را برای حاکمیت امنیت اطلاعات درنظر

---

[۱] Kevin Bollengier
[۲] ISO/IEC

می‌گیرد: ارزیابی، دستور و راهنمایی، مانیتور، ارتباط و ممیزی که نیاز است در سطوح بدنه حاکمیت و مدیریت اجرایی اجرا شود. از طرفی تولید اطلاعات از طرق مختلف نیز از مواردی است که موضوع امنیت اطلاعات را بیشتر مورد توجه قرار می‌دهد. از جمله موضوع شهر هوشمند است که با ایجاد تسهیلات و کاربرد سیستم‌ها، تولید حجم زیاداطلاعات در آن شکل ویژه‌ای خواهد داشت. معنای شهرهوشمند به‌معنای ادغام زیرساخت‌های فعلی با فناوری‌های اطلاعاتی و ارتباطی جدید برای ایجاد یک سیستم جامع از خدمات شهری کارآمد می‌باشد. شهرهوشمند شهری است که زیرساخت‌های فیزیکی، زیرساخت‌های فناوری اطلاعات، زیرساخت‌های اجتماعی و زیرساخت‌های تجاری را برای تقویت هوش جمعی شهر به هم متصل می‌کند. شهرهوشمند فناوری‌های عظیم، پیچیده و وابسته‌ای می‌باشد 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، محیط زیست و سبک زندگی (ما، ۲۰۲۱).[1]

برای ایجاد نظامی که بتواند حوزه‌های فوق را هماهنگ و مدیریت نماید، ساختاری مورد نیاز است که با رسمیت بخشی به سیاست‌ها و رفتارهای مربوط به انسجام و محافظت از داده‌ها اقدام نماید. لذا نیازمندی به کاربرد مفهوم حاکمیت داده ضرورت می‌یابد. 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 شوند، توسط چه‌کسی، به چه روشی و برای چه هدفی استفاده شود. از جمله مثال، حقوق دسترسی و یا استفاده از داده‌ها و همچنین قوانینی که برای مدیریت و کنترل

[1] Chen Ma

کیفیت و کامل بودن داده‌ها (فرانک و گالوفر[۱] ۲۰۲۱). حاکمیت داده با درنظر گرفتن افراد، فرایندها و فناوری‌ها به سازمان کمک می‌کند تا داده به‌صورت کنترل‌شده درآیند و بصورت موثرتری مورد استفاده قرار گیرند (بروکمن[۲] ۲۰۲۰) اما نکته موجود در بخش امنیت حاکمیت داده، این است که حاکمیت داده تنها از نظر دسترسی‌های مجاز به امنیت داده می‌پردازد و جزئیات آن را بررسی نمی‌کند (سینگ[۳] ۲۰۱۹). لذا داده‌های شهرهوشمند از نظر حریم خصوصی و امنیت داده‌ای دارای تهدیدات فراوانی می‌باشند که لازم است تا فرایندهای خاص حاکمیت امنیت داده نیز پیاده‌سازی شوند. به اعتقاد موسسه گارتنر؛ حاکمیت امنیت داده تنها یک پاسخ با یک سری ویژگی‌ها نیست، بلکه یک زنجیره کامل 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 درنهایت از حفاظت از منابع و داده‌ها به بهترین شکل ممکن اطمینان حاصل می‌شود (لوانز[٤] ۲۰۱۸).

به‌طور کلی اهداف حاکمیت امنیت داده در شهرهوشمند، بالابردن سطح امنیت و حفظ اطلاعات است و با استفاده از سیاست‌های تعریف شده توسط بدنه حاکمیت سازمان، تضمین می‌کند که فقط افراد مجاز به دسته‌های مختلف داده‌ها دسترسی دارند (دیلیجنت، ۲۰۱٦)[٥] همچنین می‌توان به همسوسازی اهداف تجاری با اهداف امنیت اطلاعات، بهره‌مندی ذی‌نفعان و بدنه حاکمیت از ارزش و منفعت و همچنین تضمین مورد توجه قرار دادن ریسک اطلاعات، اشاره کرد (ایزو ۲۷۰۱٤، ۲۰۲۰)[٦] داده‌های موجود در شهرهوشمند دسته‌های متفاوتی دارند که هرکدام طبق کاربرد و نوع خود از سطح امنیت متفاوتی برخوردارند. هر کدام از داده‌ها تنها توسط نهاد مربوطه بررسی و اجازه دسترسی داده شود.

---

[۱] Johannes Franke, Peter Gailhofer

[۲] Carisa Brockman

[۳] Anmol Singh

[٤] Brian Lowans, Deborah Kish, Bart Willemsen, John Girard

[٥] Diligent

[٦] ISO 27014

علاوه بر این، مفهوم شهرهای هوشمند شامل یک سیستم اطلاعاتی است که در همه جا وجود دارد و با زیرسیستم‌های به‌هم پیوسته توزیع شده که توسط سازمان‌های مختلف اداره می‌شوند. حاکمیت امنیت داده باید در شهرهای هوشمند با هدف ایجاد یک محیط محاسباتی قابل اعتماد که از همکاری ایمن بین نهادهای مشارکت کننده در داده‌های تولیدی شهرهوشمند پشتیبانی می‌کند، باشد. همچنین از چالش‌های دیگر آن می‌توان به تعاملات و اشتراک‌گذاری داده توسط نهادهایی که لزوما زیرساخت امنیتی مشترکی ندارد، اشاره کرد. علاوه‌بر آن، مهم‌ترین چالش آن تفاوت ماموریت و اهداف بخش‌های مختلف شهرهوشمند در فرایند چرخه داده است که می‌تواند موضوعات مهم امنیت داده و کیفیت داده را در تقابل با هم قرار دهد.

به‌منظور دستیابی به برنامه حاکمیت امنیت داده در شهرهوشمند، لازم است تا چشم‌انداز موردنظر با ماموریت‌ها متصل شود. یک طرح راهبردی موثر با طرح‌ریزی و مشخص کردن ماموریت‌ها، چشم‌انداز و برنامه لازم برای دستیابی به آن می‌تواند دستیابی به یک برنامه حاکمیت امنیت داده را بهبود و تسهیل بخشد (فرنسی، ۲۰۱۹).[۱] از دیگر مزیت‌های طرح راهبردی در شهرهوشمند می‌توان به درنظرگرفتن تمامی ذینفعان و عوامل موثر در شهر هوشمند اشاره و همچنین تاثیرات بلندمدت و کوتاه‌مدت آنها را مشخص وسیاست‌های لازم را اتخاذ نمود. شواهد و مطالعات میدانی حاکی است که تاکنون در راستای بهره‌گیری از حاکمیت امنیت داده اقدامی در حوزه داده‌های اینترنت اشیا و شهرهوشمند نشده و قوت‌ها، فرصت‌ها، چالش‌ها و تهدیدهای آن در این حوزه تبیین نشده است.

در شهر هوشمند، با به‌کارگیری حسگرهای محیطی داده‌های متنوع و حجیم، دریافت شده و به‌منظور ذخیره و پردازش آنها از تجهیزات اینترنت اشیاء، استفاده می‌شود. حفاظت، دسترسی مجاز و امنیت این داده‌ها، با تعریف سیاست‌های حاکمیت انجام می‌شود که در قالب حاکمیت امنیت داده‌های اینترنت اشیاء قابل بررسی است.

---

[۱] Amanda Ferenczy

این تحقیق پس از بررسی اصول و مبانی اینترنت اشیا، حاکمیت امنیت داده و شهر هوشمند، حوزه‌های کاربرد حاکمیت امنیت داده در شهرهوشمند به‌ویژه کاردبردهای آن در حوزه داده‌های اینترنت اشیا تشریح و در ادامه فرصت‌ها، چالش‌ها و تهدیدات به‌کارگیری حاکمیت امنیت داده اینترنت اشیا در شهر هوشمند بیان خواهد شد. باتوجه به اینکه تحقیق حاضر در حوزه کاربردی اینترنت اشیا در شهرهوشمند است، در بخش محیط‌شناسی، محیط داخلی و خارجی با رویکرد به‌کارگیری حاکمیت امنیت داده بررسی شده و نقاط قوت، ضعف، فرصت‌ها و تهدیدات به‌کارگیری حاکمیت امنیت داده اینترنت اشیا در حوزه شهرهوشمند احصاء می‌شود. در نهایت پس از تجزیه و تحلیل داده‌ها، طرح راهبردی به-کارگیری حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند ارایه خواهد شد.

با عنایت به مطالب فوق، این تحقیق بر آن است تا با بررسی مبانی و اصول، ارکان جهت‌ساز، قوت‌ها و ضعف‌ها و نیز فرصت‌ها و تهدیدهای پیش‌رو و همچنین ارایه راهبردها و الزامات اجرایی به‌کارگیری این فناوری در حوزه نظامی، نسبت به ارایه طرح راهبردی حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند اقدام نماید تا ضمن بهره‌مندی شهر از هوشمندی لازم، از آسیب‌ها و تهدیدات آن نیز مصون بماند. بنابراین مساله اصلی پژوهش حاضر، حفظ امنیت و حریم خصوصی داده‌های اینترنت اشیا شهرهوشمند در کنار ارائه خدمات بهینه، لحاظ گردیده است.

اهداف تحقیق عبارتند از: هدف اصلی این تحقیق دستیابی به طرح راهبردی حاکمیت امنیت داده اینترنت اشیا در شهر هوشمند می‌باشد. همچنین از اهداف فرعی این تحقیق می‌توان اهداف تعیین ارکان جهت‌ساز (اصول، چشم‌انداز، ماموریت و اهداف کلان) حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند، احصاء نقاط قوت، ضعف، فرصت‌ها و تهدیدات حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند و همچنین تعیین راهبردهای حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند را نام برد.

سوالات تحقیق تحقیق: باتوجه به اهداف، سوال اصلی، طرح راهبردی حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند می‌باشد. همچنین باتوجه به اهداف فرعی اولین سوال فرعی به‌صورت «ارکان جهت‌ساز (اصول، چشم‌انداز، ماموریت و اهداف کلان) حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند کدامند؟». سوال دوم، «نقاط قوت، ضعف، فرصت‌ها و تهدیدات حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند کدامند؟» و سوال سوم نیز، «راهبردهای حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند کدامند؟» می‌باشد.

۱,۱ اهمیت و ضرورت تحقیق

اهمیت تحقیق: ۱- با انجام این تحقیق نحوه مواجهه هوشمندانه و پیش‌کنش‌گرایانه با مخاطرات و چالشهای امنیتی اینترنت اشیاء در شهر هوشمند تبیین می‌شود. ۲- تصمیم-سازان 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.

ضرورت تحقیق: ۱- فقدان طرح راهبردی، تعیین اولویت‌ها، پیش‌بینی صحیح در مواجهه با حوادث پیش رو و انفعال در اقدامات را به همراه خواهد داشت. ۲- بی‌توجهی به تدوین سیاست‌های حاکمیت امنیت داده در شهر هوشمند، علاوه‌بر نقض حریم خصوصی موجب آسیب‌پذیری زیرساخت‌های حیاتی و خدشه به امنیت ملی و اقتدار کشور خواهد شد.

۲. مبانی نظری و پیشینه شناسی

۲,۱ تعاریف، اصطلاحات

- طرح راهبردی: طرح راهبردی طرحی است جامع، منسجم و انعطاف‌پذیر که علاوه بر ارایه راهبردهای مناسب جهت نیل به هدف، الزامات اجرایی و مسیر رسیدن به هدف را نیز مشخص می‌کند (دفتر استراتژی دانشگاه شریف, ۱۳۹۸).
- حاکمیت امنیت داده: حاکمیت امنیت داده یک فرایند مدیریتی فعال داده به‌منظور حمایت از برنامه‌های امنیت داده جهت نیل به راهبرد و چشم انداز است.

تضمین محرمانگی و امنیت داده مهم‌ترین رکن حاکمیت امنیت داده و شامل ابعاد، مشخص کردن نقش‌ها، نظارت، فرایند مدیریت داده، استانداردسازی، سیاست‌های امنیت داده و ارزیابی سیاست‌ها است (آبراهام و دیگران، ۲۰۱۹).

- اینترنت اشیا: اینترنت اشیا، اتصال اشیاء و تمام تجهیزات مربوط به شهرهوشمند از طریق شبکه‌های خاص شهرهوشمند مبتنی بر اینترنت و اینترانت، جهت ایجاد ارتباط، تعامل و اقدام از راه دور است (کومار و دیگران، ۲۰۱۹).
- شهر هوشمند: شهر هوشمند یک روند جهانی راهبردهای شهری است که با هدف بهبود کیفیت زندگی ساکنان مناطق شهری و به‌کارگیری نوآوری و فناوری‌های پیشرفته برای حل مشکلات ناشی از تراکم بالای جمعیت اتخاذ می‌شود. به حل مشکلات شهری‌سازی به‌خصوص آلودگی محیطی، مصرف زمین، انبساط شهری[۱] تراکم حمل و نقل، نیازهای انرژی، مشکلات دسترسی به خدمات عمومی و همچنین مجموعه‌ای متنوع از ابتکارات عمومی: ایجاد سیستم‌های حمل‌ونقل بهتر برای حمایت از نوآوری خلاق، دانش برای طراحی سیاست‌های صرفه‌جویی کمک می‌کند (ما، ۲۰۲۱).
- حاکمیت امنیت اطلاعات: بدنه حاکمیت امنیت اطلاعات با همراستا کردن اقدامات امنیتی اطلاعات و افزایش سطح امنیت اطلاعات سازمان و همچنین اهداف تجاری سازمان، ارزش آفرینی می‌کند. بدنه حاکمیت با درنظر گرفتن راهبردها و دستورالعمل‌هایی به‌دنبال مشخص کردن اهداف، فرایندها وظایف هر بخش است (ایزو ۲۷۰۰۱، ۲۰۱۳). حاکمیت امنیت اطلاعات بالاترین بدنه امنیتی سازمان است که با دادن دستورالعمل‌ها و سیاست‌های لازم به بخش مدیریت امنیت اطلاعات سازمان و همچنین بخش اجرایی و عملیاتی سازمان به پیاده-سازی و دستیابی به اهداف تجاری در عین حفظ امنیت اطلاعات و دارایی‌های

[۱] urban sprawl

سازمان می‌پردازد. امروزه هر شهری نیازمند شاخص‌های اندازه‌گیری عملکرد آن است. شاخص‌های کنونی به‌طور کلی در طول زمان استانداردسازی، سازگار یا قابل مقایسه نشدند. استاندارد ایزو ۳۷۱۲۰ شهر هوشمند مجموعه‌ای از شاخص‌های استاندارد شده است که یک دیدگاه یکنواخت را برای آنچه اندازه‌گیری شده و نحوه اندازه‌گیری آن تضمین می‌کند. در کل ایزو ۳۷۱۲۰، ۱۰۰ شاخص عملکردی مورد نیاز یا پیشنهاد شده شهر هوشمند را تعیین می‌کند و همچنین شامل ٤٦ هسته و ٥٤ شاخص پشتیبانی گزارش است.

۲,۲ پیشینه تحقیق

جدول ۱ پیشینه تحقیق

عنوان تحقیق	مقایسه مدل‌ها و چارچوب‌های حاکمیت داده با هدف دستیابی به پیش-نیازها، موانع و مولفه‌های یک برنامه حاکمیت داده برای داده‌های حوزه سلامت (سامنی و دیگران، ۱۳۹۸)
نتیجه‌گیری	بیمارستان‌ها و سایر سازمان‌های سلامت باوجود واحدهای سازمانی و وظایف متنوع از مهم‌ترین سازمان‌ها در هر جامعه محسوب می‌شوند. این اختلاف، باعث ایجاد ناهماهنگی و ناهمگونی در بین واحدهای سازمانی و داده‌های جمع‌آوری شده توسط آن‌ها می‌شود. علاوه‌بر این، سازمان‌های سلامت حجم زیادی از اطلاعات را جمع‌آوری، ذخیره و پردازش می‌کنند، بنابراین آنها با چالش‌های زیادی در ارتباط با داده روبه‌رو هستند.
عنوان تحقیق	حاکمیت داده برای امنیت در اینترنت اشیا و محیط‌های ابری همگرا (الرویث، ۲۰۱٦)
نتیجه‌گیری	در این تحقیق فرض شده‌است که با افزایش نوآوری‌ها و رشد شهرهای هوشمند حجم عظیمی از داده‌ها تولید می‌شود که نیاز به محاسبات ابری و پردازش داده‌های حجیم دارد. لذا این تحقیق به بررسی چالش‌های اینترنت اشیا می‌پردازد که یکی از چالش‌های کلان داده‌ها می‌باشد.
عنوان تحقیق	چالش‌ها و مولفه‌های مهم حاکمیت امنیت اطلاعات: مرور مقالات (القدمی، ۲۰۲۰) [۲]
نتیجه‌گیری	مرور ادبیات سیستماتیک ارائه شده در این مقاله با هدف معرفی امنیت اطلاعات به عنوان یک راه‌حل جامع برای همسویی بین سیاست‌های امنیت اطلاعات و اهداف سازمان است. این تحقیق نیاز به ایجاد یک چارچوب

[۱] Majid Al-Ruithe, Siyakha Mthunzi, Elhadj Benkhelifa

[۲] Sultan AlGhamdi, Khin Than Win, Elena Vlahu-Gjorgievska

	جامع برای حکمرانی امنیت اطلاعات را مشخص می‌کند که ۱) اهداف سازمان و حفاظت از آن را متصل می‌کند، ۲) هر جنبه‌ای از راهبرد، کنترل و مقررات را مورد بررسی قرار می‌دهد، ۳) با سیاست‌ها، رعایت روش‌ها و دستورالعمل‌ها را تضمین و (٤) ارزیابی و انطباق مستمر را تضمین می‌کند.
عنوان تحقیق	طرح داده شهر: مفهوم‌سازی یک ابزار سیاست برای حاکمیت داده در شهرهای هوشمند (لوپی، ۲۰۱۹)[۱]
نتیجه‌گیری	این مقاله مفهوم برنامه راهبردی داده شهری به‌عنوان یک ابزار سیاست حکمرانی داده‌ها ارائه می‌دهد که قصد دارد تولید و استفاده از داده‌های شهری را در یک راهبرد بلندمدت جامع و تکاملی با اهداف توسعه شهر پیوند دهد. مفهوم طرح داده‌های شهر با درنظر گرفتن مسائل جاری مربوط به حریم خصوصی و دستکاری داده‌ها در شهرهای هوشمند تدوین شد. نتیجه این فرایند تحلیلی تدوین طرح کلی داده‌های شهر به‌عنوان یک ابزار سیاست حکمرانی داده‌ها برای حمایت از مذاکرات مداوم بین نمونه‌های تولیدکنندگان داده و کاربران داده برای ایجاد بینش مشترک شهرهای هوشمند است.
عنوان تحقیق	یک چارچوب مفهومی برای حاکمیت داده در اکوسیستم‌های دیجیتال IS با قابلیت IoT(داسگوپتا، ۲۰۱۹)[۲]
نتیجه‌گیری	این مقاله چارچوب چهار بعدی که به تازگی توسعه یافته‌است و می‌تواند پوشش حکمرانی را در چرخه داده‌ها در اکوسیستم دیجیتال امنیت اطلاعات با قابلیت اینترنت اشیا را فراهم کند، مورد بحث قرار می‌دهد. چارچوب چهار بعدی از طریق تجزیه تحلیل و مرور ادبیات علمی و عملی موجود در زمینه فناوری اطلاعات، داده‌ها و حاکمیت سازمانی در زمینه اکوسیستم اینترنت اشیا و دیجیتال امنیت اطلاعات توسعه می‌یابد. مباشران داده[۳] می‌توانند از چارچوب پیشنهادی برای مدیریت و تعریف دستورالعمل‌های کل شرکت، قوانین شرکت و دارایی‌های داده برای ارائه حکمرانی و کیفیت ضروری داده‌ها استفاده کنند.
عنوان تحقیق	چالش‌های امنیت و حریم خصوصی در شهرهای هوشمند (براون، ۲۰۱۸) [٤]
نتیجه‌گیری	شهرهای هوشمند باید از حریم خصوصی و امنیت فردی برای اطمینان از مشارکت شهروندان خود اطمینان حاصل کنند. اگر شهروندان تمایلی به مشارکت نداشته باشند، مزایای اصلی شهرهوشمند از بین می‌رود. این مقاله به امید پیش‌بینی اختلالات بی‌ثبات کننده و پرهزینه، راه‌حل‌های ممکن را برای پنج چالش شهرهوشمند ارائه می‌دهد. این چالش‌ها شامل حفظ حریم‌خصوصی با داده‌های ابعادی بالا، ایمن سازی یک شبکه با سطح حمله بزرگ، ایجاد شیوه‌های اشتراک‌گذاری داده‌های قابل اعتماد، استفاده

[۱] Lucia, Lupi

[۲] Avirup Dasgupta, Asif Gill, Farookh Hussain

[۳] Data stewards

[٤] Trevor Braun, Benjamin C.M. Fung, Farkhund Iqbal, Babar Shah

	صحیح از هوش مصنوعی و کاهش خرابی‌ها در شبکه هوشمند است.
عنوان تحقیق	یک چارچوب پیشنهادی بهترین عملکرد برای حاکمیت امنیت اطلاعات (گشگری[۱] ۲۰۱۷)
نتیجه‌گیری	در این مقاله سعی شده تا بر پایه‌ی سطوح بالای فاکتورهای اساسی موفقیت به مفهوم امنیت اطلاعات بپردازد. مقاله همچنین چارچوب حاکمیتی امنیت اطلاعات را بر قوانین و سیاست‌های مطرح شده در استانداردهای کوبیت[۲] و ایزو۲۷۰۱٤ پیاده‌سازی نموده است.

برابر بررسی به‌عمل آمده در پیشینه‌های فوق، هریک از پژوهش‌ها، به جنبه‌ای از مسایل 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 الزامات ارایه یک طرح راهبردی در زمینه بهره‌برداری از اینترنت اشیاء را، از آن‌ها احصاء نمود و مهم‌ترین نتیجه‌ی حاصل از جمع‌بندی پیشینه‌ها مبین این نکته است باوجود مزایای اینترنت اشیا در شهرهوشمند، 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 بعضا با دید فنی و سخت افزاری پرداخته و در هیچ‌یک، الگو یا طرحی برای استفاده از اینترنت اشیاء در حوزه کلان کشوری با هدف مدیریت و حاکمیت داده و امنیت داده، ارائه نشده است. در صورت وجود الگوی راهبردی آن مطابق با ارزش‌ها و ساختار جمهوری اسلامی ایران نیست همچنین دیدگاه‌های ارایه شده جامعیت کافی برای استفاده در این پژوهش را ندارد.

مهم‌ترین نوآوری این پژوهش: ۱- حاکمیت امنیت داده در اینترنت اشیاء در شهرهوشمند و اینکه به‌صورت یک طرح راهبردی تدوین شود. ۲- تلاش در جهت تدوین و تشخیص مناسب بودن روش‌ها و برنامه‌های توسعه مفهوم اینترنت اشیاء درشهرهوشمند و کمک به

---

[۱] Ghada Gashgari, Robert Walters, Gary Wills

[۲] COBIT

تصمیم‌گیری درست در این حوزه، ۳- بهره برداری از فناوری اینترنت اشیا در محیط رایانش ابری با لحاظ کردن امنیت کلان داده حوزه شهرهوشمند می‌باشد.

۲,۳ ادبیات تحقیق

شهرهوشمند شهری است که بااستفاده از تجهیزات فناوری‌اطلاعات و تجهیزات ارتباطی به بهبود سطح زندگی، کارایی و همچنین پایداری توسعه شهری کمک می‌کند[۱] (ارمی، ۲۰۱۷).[۲] درحال‌حاضر، 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 اشیا که موجب اتصال بین تجهیزات و ایجاد شبکه می‌شود نقش کلیدی را دارد (ارمی، ۲۰۱۷).[۳] هسته اصلی پردازش و فعالیت تجهیزات اینترنت اشیا داده‌ها هستند که در حجم‌های مختلف، انواع مختلف و با سرعت‌های مختلفی تولید می‌شوند (گوئر-پرز، ۲۰۱۳).[٤] این داده‌های حجیم تولید شده در یک شهرهوشمند پتانسیل زیادی برای ایجاد ارزش و بهره‌وری در شهرهای هوشمند ایجاد می‌کنند. یک شهرهوشمند نقش انتقال دهنده داده‌ها در محیط‌های زندگی شهروندان و همچنین محل‌های تولید داده نظیر حمل‌ونقل، بخش سلامت، انرژی و آموزش را دارد. برای مثال داده‌های هواشناسی با سرعت بسیار زیادی در حال تولید هستند، لذا تشخیص و بهره‌برداری از این داده‌ها در بخش کشاورزی بسیار مفید خواهد بود. همچنین این اطلاعات به برنامه‌ریزی‌های روزانه شهروندان بسیار یاریگر خواهد بود (جوشی، ۲۰۱٦).[٥]

تجهیزات اینترنت اشیا و فناوری‌اطلاعات در شهرهوشمند موجب ذخیره‌سازی و پردازش داده‌ها برای تولید داده‌هایی هستند که موجب بهبود عملکرد سرویس‌های مختلف در

---

[۱] Smart Cities Council

[۲] Mircea Eremia, Lucian Toma, Mihai Sanduleac

[۳] Mircea Eremia, Lucian Toma, Mihai Sanduleac

[٤] Guerrero-Pérez, Huerta, González, López

[٥] Sujata Joshi, Saksham Saxena, Tanvi Godbole, Shreya

شهرهوشمند می‌شوند. از کاربردهای داده‌ها در شهرهای هوشمند می‌توان به‌صورت کلی به بخش‌های شبکه هوشمند، سلامت هوشمند، حمل‌ونقل هوشمند و حاکمیت هوشمند اشاره کرد. در عملکردهای اشاره شده می‌توان داده‌های تولیدی شهرهوشمند را به دسته‌های مختلفی تقسیم کرد. یک دسته داده‌های مربوط به زیرساخت‌های خدمات شهری است که توسط حسگر درون شهر تولید و بلافاصله در دسترس برای استفاده‌های مختلف قرار می‌گیرند (داده‌های عملیاتی شهری) (لوپی، ۲۰۱۹).[۱] دسته دیگری از داده‌ها، داده‌های مربوط به شبکه‌های اجتماعی می‌باشد که اطلاعات زیادی را در مورد نظرات افراد و نیازهای روز جامعه بیان می‌کنند (آرتیوشینا، ۲۰۲۰).[۲] دسته‌های دیگری از داده‌ها علاوه بر دو دسته ذکر شده نیز وجود دارند.

۲،۳،۱چالش‌های امنیت داده اینترنت اشیا در شهرهوشمند

همان‌طور که در قسمت قبل بیان شد داده‌ها در شهرهوشمند به‌صورت پیوسته در حال گردش هستند. با افزایش روند جمعیتی شهرنشینی و هوشمندسازی شهرها قابل پیش‌بینی است، که تجهیزات و زیرساخت‌های موردنیاز برای بخش‌های مختلف شهرهوشمند نظیر، حمل‌نقل هوشمند، دولت هوشمند، سلامت هوشمند، محیط زیست، خانه هوشمند و ... با رشد زیادی همراه است (سیو، ۲۰۱۸).[۳] همچنین افزایش کاربردهای هوشمندی در شهر و هوشمندسازی، موجب مشکلات و چالش‌های امنیتی و حریم خصوصی زیادی می‌شود. این مشکلات به‌دلیل حفره‌های امنیتی در لایه‌های این سیستم می‌باشد. چالش‌هایی نظیر حملات سایبری، دسترسی‌های غیرمجاز، از دسترسی خارج شدن سیستم‌ها و... موجب به خطر افتادن کیفیت و قابلیت اطمینان هوشمندی در شهر و کاهش اعتماد شهروندان به استفاده از تجهیزات هوشمند می‌شوند (ژانگ، ۲۰۱۷).[۴]

---

[۱] Lucia Lupi

[۲] Anna Artyushina

[۳] Lei Cui, Gang Xie, Youyang Qu, Longxiang Gao, Yunyun Yang

[۴] Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, Xuemin Sherman Shen

بسیاری از روش‌های حفاظت داده (نظیر، رمزگذاری، بایومتریک و..) به‌صورت گسترده در کاربردهای مختلف بیان شده ولی متاسفانه این روش‌ها در شهرهوشمند به‌دلیل چالش محیطی آن قابل پیاده‌سازی نیست. دلیل اصلی آن این است که حسگرها و تجهیزات توان محاسباتی کمی دارند و لذا تنها می‌توان الگوریتم‌های ساده‌ای به‌صورت مستقیم پیاده‌سازی نمود (آلومایر و پووندران، ۲۰۱٤)[۱] برای درست روشن شدن موضوع چالش‌های امنیت داده‌ها، ابتدا لازم است معماری اینترنت اشیا در شهرهوشمند را بررسی نمود.

۲,۳,۲ اینترنت اشیا

اینترنت اشیا مفهومی جدید در دنیای فناوری و ارتباطات است که در آن برای هر موجودی (انسان، حیوان و یا شیء) قابلیت ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترانت، فراهم می‌گردد (آلام، ۲۰۲۰)[۲].

۲,۳,۲,۱ معماری اینترنت اشیا در شهرهوشمند

در راستای توسعه شهرهای هوشمند، معماری‌های مختلفی در این‌خصوص طراحی شده است. معماری ارائه شده در این قسمت معماری شناخته شده ٤ لایه می‌باشد (آنگریشی، ۲۰۱۷)[۳] این معماری را می‌توان به ٤ لایه ادراک[٤]، لایه شبکه[٥]، لایه پشتیبانی[٦]، لایه کاربرد[۷]تقسیم کرد که در شکل ۱ نمایش داده شده است. ۱- لایه ادراک: به عنوان لایه لبه و یا لایه حسگر نامیده می‌شود و پایین‌ترین لایه این معماری می‌باشد. ۲- لایه شبکه: لایه اصلی در معماری اینترنت اشیا است که به شبکه‌های اساسی مانند اینترنت، شبکه حسگر بسیم‌ها و شبکه‌های مخابراتی بستگی دارد. ۳- لایه پشتیبان: بسیار شبیه لایه کابرد

---

[۱] Basel Alomair, Radha Poovendran

[۲] Mansaf Alam, Kashish Ara Shakil, Samiya Khan

[۳] Kishore Angrishi

[٤] Perception Layer

[٥] Network Layer

[٦] Support Layer

[۷] Application Layer

کار می‌کند. این لایه پشتیبانی از نیازهای برنامه‌های متنوعی را از طریق تکنیک‌های هوشمند محاسباتی فراهم می‌کند. ٤- لایه کاربرد: به عنوان لایه بالایی، مسئولیت فراهم-سازی هوشمندی و خدمات کاربردی و یا برنامه‌ها را به کاربران دارد و برپایه شخصی-سازی کاربران می‌باشد.

شکل ۱ معماری برپایه اینترنت اشیا در شهرهوشمند (آنگریشی، ۲۰۱۷)[۱]

۲،۳،۳ حاکمیت امنیت داده

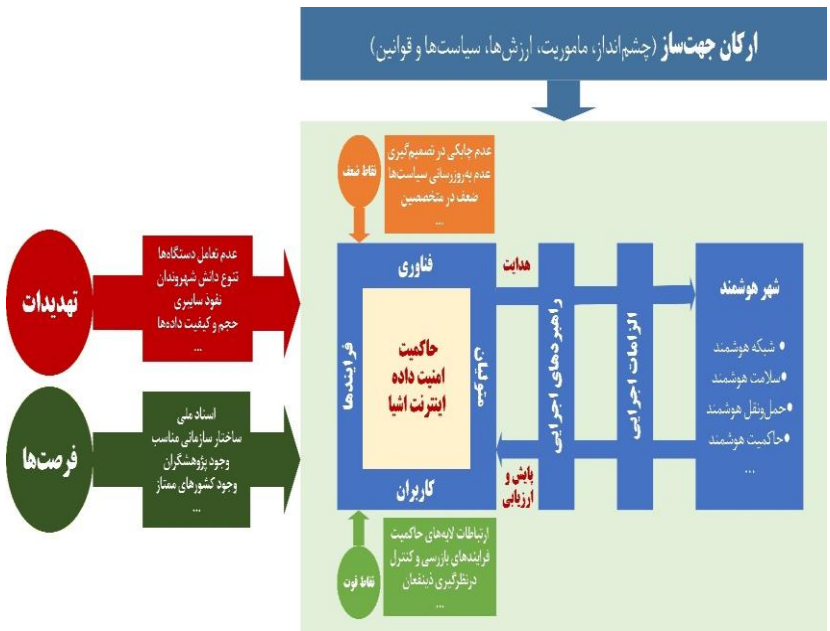
حاکمیت مفهوم تازه‌ای نیست. درحقیقت از زمانی که مفهوم شهروند و مردم وجود داشته، مفهوم حاکمیت نیز تعریف شده است. حاکمیت در حقیقت فرایند تصمیم‌سازی است و همچنین فرایند اینکه کدام تصمیم‌ها پیاده‌سازی بشوند یا نشوند. حاکمیت دو بخش اصلی عملکرد[۲] و انطباق‌پذیری[۳] دارد. عملکرد یک سری رویدادهایی است که با برنامه‌ریزی شروع می‌شود. یک سری گزارشات را پشت سر گذاشته و با بازخورد به اوج خود می‌رسد. انطباق به انجام الزامات و سیاست‌ها، قراردادها و موارد دیگر اشاره دارد. یک برنامه حاکمیت خوب[٤]اجزای مختلفی (انتخاب اهداف مشخص، شفافیت و مسئولیت‌ها، برنامه‌ریزی راهبردی، مدیریت ریسک، مسئولیت‌های تصمیم‌گیری، بررسی و نظارت بر عملکردها، تدوین استانداردهای و سیاست‌ها) دارد. یک برنامه حاکمیت خوب امنیت را

[۱] Kishore Angrishi
[۲] Performance
[۳] Compliance
[٤] Good Governance

برای کلیه ذینفعان سازمان و جوامع مانند کارمندان، سرمایه‌گذاران، طلبکاران، مشتریان، مردم و.. فراهم می‌کند و در شکل شماره دو مشاهده می‌شود (کپینگ، ۲۰۱۸).[۱]

شکل ۲ برنامه حاکمیت (کپینگ، ۲۰۱۸)

براساس مطالعات انجام شده، مدل مفهومی این تحقیق مطابق با شکل ۳ می‌باشد.



شکل ۳ مدل مفهومی تحقیق

[۱] Yu Keping

۳. روش تحقیق

پژوهش از لحاظ هدف (نوع تحقیق) در زمره تحقیقات کاربردی دسته‌بندی می‌گردد. این پژوهش به این دلیل کاربردی است که یافته‌های آن به متولیان حوزه شهرهای‌هوشمند در کشور در بهره‌برداری از اینترنت اشیاء کمک خواهد نمود و باعث ارتقاء، توانمندی و افزایش مهارت‌های راهبردی متولیان در بهره‌گیری از فرصت‌ها و مقابله با تهدیدهای اینترنت اشیاء خواهد شد. همچنین از لحاظ روش تحقیق در زمره تحقیقات توصیفی/تحلیلی با نگاه اکتشافی دسته‌بندی می‌گردد. از نظر موضوع و زمینه علمی به‌دنبال آن است که با تکیه برآراء ونظرات خبرگان و بررسی مستندات علمی و قانونی به طرح راهبردی حاکمیت امنیت داده در اینترنت اشیا در حوزه شهرهوشمند برسد. از نظر بعد زمانی، با توجه به تحولات سریع فضای سایبر آینده (میان مدت) را شامل خواهد شد. از لحاظ بعد مکانی به گستره جغرافیای جمهوری اسلامی ایران نظر دارد. جامعه آماری این تحقیق ۴۵ نفر می‌باشد. از دو شیوه نمونه‌گیری غیر احتمالی یعنی نمونه‌گیری با استفاده از روش نمونه‌گیری هدفمند[۱]/ معیار محور[۲](انتخاب تمام موردها با انتخاب معیار خاص) و نمونه‌گیری با شیوه گلوله برفی [۳]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 سئوالات پرسشنامه شاخص‌ها و راهبردهای حاکمیت امنیت داده را مورد سئوال قرار می دهد روش تحلیل داده‌ها با استفاده از آمار توصیفی و استخراج میانگین پرسش‌ها مربوط به هر یک از این‌ها است، ویژگی‌های دارای

---

[۱] purposive Sampling

[۲] Criterion –Based Sampling

[۳] Snowball

میانگین ۳ به بالا که مورد تایید خبرگان است و مواردی که زیر این مقدار هستند رد شده‌اند؛ از این طریق شاخص‌های پیشنهادی مورد ارزیابی قرار می‌گیرد.

۳,۱ تدوین راهبردها

در این مقاله «روش تدوین راهبرد داعا» به‌کار گرفته شد، زیرا روش ارائه شده توسط دانشگاه عالی دفاع ملی، معایب روش دیوید را پوشش داده و در تدوین راهبردها، به‌خوبی به موضوع تهدیدات می‌پردازد، بنابراین در موضوعات مرتبط با حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند، روش مناسبی برای تدوین راهبرد می‌باشد. خلاصه مراحل تدوین راهبردها که در این تحقیق استفاده شده، به شرح ذیل می‌باشد:

۱) مطالعه اکتشافی براساس فرمایشات مقام معظم رهبری(مدظله‌العالی)، اسناد بالادستی، مدارک موجود و تحقیقات پیشین در راستای موضوع تحقیق
۲) مطالعه مبانی نظری اعم از تئوری‌ها، الگوها، راهبردهای موجود، مدل‌ها و... .
۳) تعیین چارچوب نظری (بر اساس مفاد اسناد بالادستی و مبانی نظری تحقیق).
٤) بررسی تخصصی موضوع (متغیرهای تحقیق) و احصاء عوامل تاثیرگذار مربوط از درون آن.
۵) مطالعه تطبیقی چند کشور و احصاء عوامل تاثیرگذار مربوطه ناشی از مطالعه تطبیقی.
٦) مطالعه محیط داخلی و خارج و احصاء عوامل تاثیرگذار مربوطه.
۷) انجام مصاحبه‌های خبرگی جهت تولید ادبیات تکمیلی با توجه به جدید بودن موضوع تحقیق.
۸) احصاء و تجمیع عوامل تاثیرگذار که از مطالعات فوق و ادبیات تکمیلی حاصل شده‌اند.
۹) تعیین اصول و ارزش‌ها، چشم‌انداز و اهداف کلان حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند براساس اسناد بالادستی، فرمایشات مقام معظم رهبری(مدظله‌العالی)، مصاحبه‌های تکمیلی انجام شده و با استفاده از روش نخبگی.

۱۰) تفکیک عوامل تاثیرگذار به عوامل داخلی و خارجی با استفاده از پرسشنامه‌های محقق‌ساخته و پس از اخذ نظر از خبرگان.

۱۱) وزن‌دهی به عوامل محیط داخلی و خارجی براساس نظر خبرگان.

۱۲) ساخت یا معرفی ابزار سنجش وضع موجود محیط داخل و خارج.

۱۳) ارزیابی وضع موجود عوامل محیط داخلی و محیط خارج.

۱٤) تعیین ضرایب اهمیت هر عامل در محیط داخل و خارج.

۱۵) تقسیم عوامل داخلی به دو دسته قوت‌ها و ضعف‌ها و عوامل خارجی به دو دسته فرصت‌ها و تهدیدها.

۱٦) تشکیل ماتریس‌های کمی ارزیابی عوامل داخلی و خارجی.

۱۷) تعیین موقعیت راهبردی (تعیین وضع موجود و مطلوب) بر روی محور مختصات دکارتی براساس داده‌های حاصل از ارزیابی عوامل داخلی و خارجی.

۱۸) محاسبه زاویه بین بردار وضع موجود و وضع مطلوب و تعیین میزان چرخش راهبردی.

۱۹) تعیین درصد تخصیص منابع در جهت تقویت نقاط قوت، رفع نقاط ضعف، استفاده از فرصت‌ها و کاهش تهدیدها.

۲۰) انتخاب راهبردهای خرد براساس عوامل محیطی چهارگانه، اختلاف زاویه وضع موجود و وضع مطلوب و درنظر گرفتن درصد تخصیص منابع و تدوین آنها. جهت این امر، گزاره‌های راهبردی با استفاده از روش داده‌بنیاد، از طریق خبرگی و انجام جلسات طوفان فکری استخراج و تدوین گردیدند.

۲۱) تدوین راهبردهای ترکیبی با استفاده از ترکیب راهبردهای خرد (ماتریس بهبود یافته) و با نگاه به اهداف کلان.

۲۲) ارزیابی راهبردهای ترکیبی. به منظور اطمینان از مناسب بودن راهبردهای تدوین شده، با استفاده از پرسشنامه محقق ساخته و براساس تلاقی هر یک از راهبردها با عوامل

داخلی و خارجی، میزان تاثیر هر یک از راهبردها بر عوامل مذکور مورد سنجش قرار گرفت.

۲۳) تشکیل ماتریس ارزیابی راهبردها که براساس نتایج حاصل از ارزیابی راهبردها انجام می‌پذیرد.

۲٤) محاسبه و تعیین میزان مطلوبیت راهبردهای ترکیبی با استفاده از تکنیک «انتخاب برترین پیشنهاد از طریق تشابه به راه حل ایده‌آل».

۲۵) اولویت‌بندی (رتبه‌بندی) راهبردهای ترکیبی براساس میزان مطلوبیت آنها.

۲٦) ارزیابی راهبردهای اولویت‌بندی شده بر مبنای اهداف کلان حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند با استفاده از روش نخبگی و جلسات طوفان مغزی.

٤. تجزیه و تحلیل یافته‌ها

٤,۱ ارکان جهت‌ساز

براساس اسناد بالادستی، ارکان جهت‌ساز حاکم بر حوزه حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند به‌روش نخبگی و برگزاری جلسات طوفان فکری، در جدول ۲ آمده است:

جدول ۲ ارکان جهت‌ساز

ردیف	ارکان جهت‌ساز	توضیحات
۱	اصول	اصل چند بعدی بودن، اصل خودحفاظتی، اصل رصد دائمی تهدیدات، اصل پیشگیری، اصل مسئولیت‌پذیری، اصل خلاقیت و نوآوری، اصل مشارکت، اصل خدمات‌دهی، اصل پایداری
۲	ارزش	ارتقاء امنیت و خدمات‌دهی اینترنت اشیا در شهرهوشمند با رویکرد حاکمیت امنیت داده
۳	چشم انداز	تحقق توسعه امن و پایدار اینترنت اشیا در شهرهوشمند با بهره‌گیری از قابلیت‌های حاکمیت امنیت داده به‌منظور همراستاسازی امنیت داده اینترنت اشیا و خدمات‌دهی شهرهوشمند با ویژگی‌های نیروی انسانی توانمند، ساختار چابک و پویا، برخورداری از دانش بومی، دارای تجهیزات پیشرفته امن و پایدار.
٤	ماموریت	حفظ امنیت و حریم خصوصی داده، کنترل و نظارت بر جریان داده‌ها، تسهیل خدمات داده‌ها و همچنین بهبود کیفیت داده‌های

		اینترنت اشیا در شهرهوشمند
۵	هدف کلان	مصون‌سازی شهرهوشمند از خطرات امنیتی داده‌های اینترنت اشیا، حفظ حریم خصوصی داده‌های اینترنت اشیا در شهرهوشمند، دستیابی به سطح بالایی از خدمات‌دهی اینترنت اشیا در شهرهوشمند، همراستاسازی امنیت داده‌های اینترنت اشیا و خدمات‌دهی آن در شهرهوشمند، دستیابی به دانش و فناوری بومی جهت تولید تجهیزات و برنامه‌های کاربردی اینترنت اشیا با درنظرگیری سطح حساسیت، بهره‌گیری از نیروی انسانی توانمند، آموزش‌دیده، با انگیزه در سطوح مختلف

٤,٢ استخراج عوامل محیطی داخلی و خارجی

در این مرحله در خصوص ۵۸ عامل داخلی و خارجی ، ابتدا طی پرسش‌نامه شماره دو از جامعه خبره نظرخواهی گردید که نتیجه به دست آمده شامل تعیین عوامل محیط داخل (قوت و ضعف)، عوامل محیط خارج (فرصت، تهدید)، میزان اهمیت و امتیاز وضع موجود و مطلوب هر یک از عوامل از منظر خبرگان می‌باشد. نتایج و جمع‌بندی مربوطه و همچنین فهرست مربوطه به شرح ذیل می‌باشد:

جدول ۳ عوامل محیطی داخلی و خارجی

عوامل محیطی	شرح
قوت‌ها	۱- وجود قوانین و مقررات حفاظت از داده و حریم خصوصی در شهرهوشمند، ۲- وجود استانداردهای امنیتی اینترنت اشیا در سطح شهرهوشمند، ۳- گسترش زیرساخت فناوری اطلاعات و ارتباطات کشور، ٤- ارتباط پیوسته لایه مدیریت شهری با حاکمیت امنیت داده، ٥- استقبال از فناوری‌های نوین، ٦- ایجاد فرایند بازرسی و کنترل اجرایی بودن خط‌مشی‌های حاکمیت امنیت داده، ۷- انبوه کاربران فضای مجازی، ۸- ارزیابی سیاست‌های حاکمیت امنیت داده در شهر، ۹- حفظ و تسهیل خدمات شهری در کنار امنیت داده‌های شهرهوشمند، ۱۰- پیوست امنیت داده در برنامه‌های شهرهوشمند، ۱۱- وحدت فرماندهی حاکمیت امنیت داده، ۱۲- ارتباط بین حاکمیت با ارکان و دستگاه‌های ذی‌ربط شهرهوشمند، ۱۳- برخورداری از نیروی انسانی مجرب در سطح شهرهوشمند، ١٤- درنظرگرفتن بازیگران متعدد در تصمیم‌گیری و حفظ وحدت فرماندهی، ۱۵- کسب رضایت ذینفعان در ارائه خدمات امنیت داده شهرهوشمند، ١٦- راهکارهای افزایش ضریب امنیتی حضور کاربران در بستر اینترنت اشیا، ۱۷- ایجاد برنامه مدون توسعه اینترنت اشیا با درنظرگیری امنیت داده، ۱۸- برنامه‌ریزی، راهبری و پایش و نظارت عالی بر پروژه‌های شهرهوشمند از منظر امنیت داده و ارائه شاخص‌های امنیت، ۱۹- برنامه‌های مداوم ممیزی امنیت داده‌های اینترنت اشیا در شهر.

ضعف‌ها[1]	
فرصت‌ها	۱- وجود توافقات بین‌المللی مفید در برخی از حوزه‌های اینترنت اشیا و شهرهوشمند، ۲- وجود اسناد بالادستی سایرکشورها به منظور تدوین سند بالادستی اینترنت اشیا کشور، ۳- وجود سرمایه‌گذاران بین‌المللی در برنامه‌های غیرحساس اینترنت اشیا در شهرهوشمند، ٤- قوانین بین‌المللی مرتبط با حریم خصوصی و مالکیت داده اینترنت اشیا در شهرهوشمند، ٥- امکان الگوبرداری از ساختار سازمانی شهرهای هوشمند در سطح جهانی، ٦- وجود رقابت در حوزه‌های امنیت داده، اینترنت اشیا و شهرهوشمند در سطح جهانی، ۷- سخت شدن شرایط خرید از خارج در اثر اعمال تحریم‌های بین‌المللی و امکان رشد تولید داخلی، ۸- بهره‌گیری از تجارب سایر کشورها در توسعه بسترهای خدمات‌دهی در اینترنت اشیا در سطح ملی، ۹- امکان مشارکت فعال متخصصین حقوقی کشور و مسئولان شهرهوشمند در تدوین قوانین بین‌المللی مربوط به امنیت داده اینترنت اشیا، ۱۰- استفاده از ظرفیت متخصصین خارج از کشور، ۱۱- امکان صدور دانش و فناوری به کشورهای دوست، ۱۲- وجود رقابت سازمان‌ها و شرکت‌های بین‌المللی در ایجاد و توسعه فضای امن اشتراک‌گذاری داده‌های شهرهوشمند.
تهدیدات	۱- عدم همکاری مناسب و سازنده کشورهای دارای فناوری اینترنت اشیا و شهرهوشمند، ۲- فقدان نظام حقوق بین‌المللی در حوزه امنیت داده کشورها، ۳- عدم تامین تجهیزات و نرم‌افزارهای حساس در زمان تحریم‌های بین‌المللی، ٤- نفوذ فیزیکی به مراکز حساس داده‌های اینترنت اشیا، ٥- تخریب اعتماد شهروندان به برنامه‌های اینترنت اشیا در شهرهوشمند توسط دشمنان، ٦- بی‌اطلاعی شهروندان و کاربران از امنیت داده‌ها و حریم خصوصی در بستر اینترنت اشیا، ۷- چالش‌های جدید (آسیب‌پذیری) تجهیزات نوظهور اینترنت اشیا، ۸- درنظرگیری رقبای قوی در سطح منطقه‌ای و جهانی با انگیزه‌های سیاسی مختلف، ۹- نفوذ سایبری به مراکز داده جهت سرقت، حذف و یا تغییر داده مربوط به قطعات، تجهیزات، سامانه‌های اینترنت اشیا و یا اختلال در ارائه خدمات، ۱۰- شناسایی مدارات اضافی تعبیه شده در سامانه و تجهیزات اینترنت اشیا (جهت ردیابی موقعیت مکانی سامانه‌ها، جاسوسی، اعمال اقدامات و سرقت داده‌ها)، ۱۱- شناسایی حفره‌های امنیتی و کلیدهای از کارانداز تعبیه شده در ریزتراشه‌ها (کنترل عملیاتی و یا مختل کردن عملکرد تجهیزات)، ۱۲- نفوذ سایبری به سامانه‌های اینترنت اشیا و تزریق داده‌های غلط و گمراه کننده.

٤,۳ ارزیابی عوامل داخلی و خارجی

با محاسبه صورت گرفته و میانگین عوامل خارجی و از طرفی با توجه به جمع امتیازات موزون محاسبه شده در بالا (مجموع حاصل‌ضرب میانگین امتیاز وضع موجود در وزن

[1] جهت کسب اطلاعات بیشتر به دفتر فصلنامه مراجعه شود.

نرمال‌شده عوامل)، این‌طور استنباط می‌گردد که؛ جامعه از نظر عوامل خارجی با تهدیدهایی مواجه است و از نظر عوامل داخلی نیز در موضع ضعف می‌باشد.

جدول ٤ جمع نمرات موزون وضعیت موجود

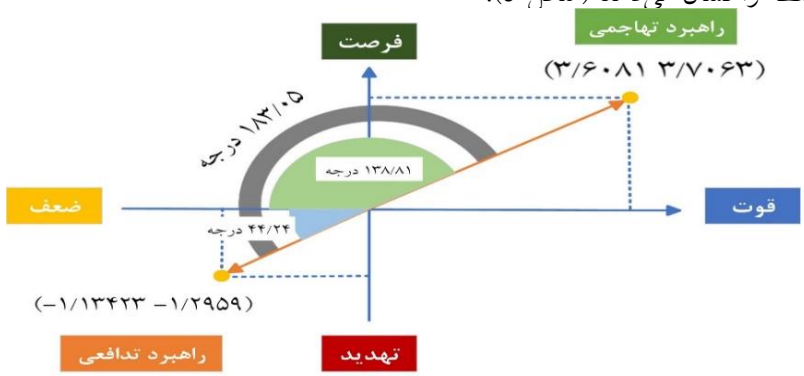
قوت	۱/۸۱۱٤ (+)	X^+
ضعف	۳/۱۰۷۳ (–)	X^-
فرصت	۲/۰۷۳۱۷ (+)	Y^+
تهدید	۳/۲۰۷٤ (–)	Y^-

جدول ٥ جمع نمرات موزون وضعیت مطلوب

قوت	٤/۲٦۸۲ (+)	X^+
ضعف	۰/٦٦۰۱ (–)	X^-
فرصت	٤/۱٦۳۸۱ (+)	Y^+
تهدید	۰/٤٥۷٤٤ (–)	Y^-

٤,٤ تعیین موقعیت و تحلیل شکاف راهبردی

اگر چهار گروه قوت‌ها، ضعف‌ها، فرصت‌ها و تهدیدها را طوری بر روی محورهای مختصات قرار دهیم که فرصت‌ها Y مثبت، تهدیدها Y منفی، قوتها X مثبت و ضعف‌ها X منفی درنظر گرفته شوند، جمع جبری X ها طول یک نقطه و جمع جبری Y ها عرض همان نقطه را نشان می‌دهد (شکل ٤).



شکل ٤ مشخصات منطقه راهبردی حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند

- عدد حاصل از جمع جبری دو عامل قوت و ضعف (در وضعیت موجود) برابر است با: $X1 = 1.8114 - 3.0966 = -1.2959$

- عدد حاصل از جمع جبری دو عامل فرصت و تهدید و برابر(در وضعیت موجود) است با: $Y_1 = 0.6449 - 1.8772 = -1.13423$
- عدد حاصل از جمع جبری دو عامل قوت و ضعف (در وضعیت مطلوب) برابر است با: $X_2 = 4.2682 - 0.5294 = 3.7063$
- عدد حاصل از جمع جبری دو عامل فرصت و تهدید (در وضعیت مطلوب) برابر است با: $Y_1 = 4.1452 - 0.5532 = 3.6081$

اعداد به‌دست آمده در شکل ٤، مختصات نقاط X و Y را در نمودار ارزیابی موقعیت و اقدام راهبردی را نشان می‌دهند که نقطه مذکور را روی محور مختصات مشخص و از مبدا مختصات پاره خطی به آن رسم می‌شود بیانگر وضع موجود که نشان دهنده تدافعی بودن راهبرد سازمان است.

٤,٥ تدوین راهبردها

باتوجه به تجزیه‌وتحلیل راهبردی انجام شده، راهبردهای حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند، براساس اصول و ارکان جهت‌ساز تدوین گردید. این راهبردها با استفاده از عوامل برترساز (قوت‌ها و فرصت‌ها) به منظور رفع ضعف‌ها و پاسخ به تهدیدات، به روش نخبگی تدوین گردیدند که در نهایت تعداد ۱۰ راهبرد ارائه شده‌است.

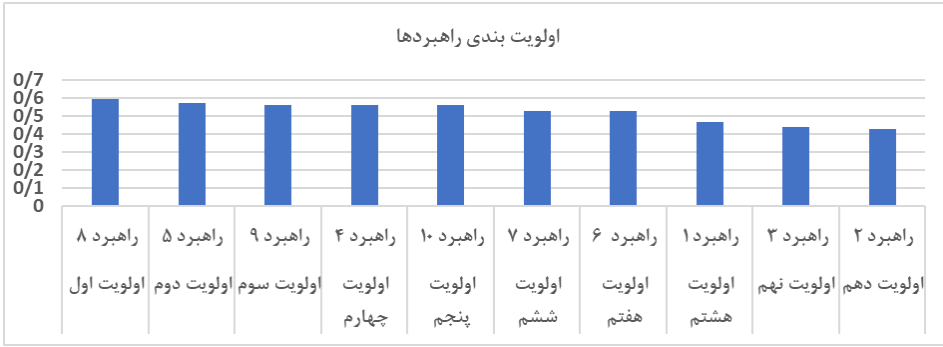
جدول ٦ جدول راهبردهای خروجی ماتریس SWOT

ردیف	شرح راهبرد
۱	بومی‌سازی تجهیزات و برنامه‌های کاربردی اینترنت اشیا با بهره‌گیری از متخصصین داخلی و ظرفیت دانشگاهی با درنظرگیری سطح حساسیت و شرایط تحریمی
۲	ایجاد زیرساخت‌ها و رویه‌های فنی و امنیتی با بهره‌گیری از فناوری‌های بومی و متخصصین داخلی جهت شناسایی حفره‌های امنیتی تجهیزات اینترنت اشیا در شهرهوشمند
۳	ایجاد بستر اجرایی برنامه‌های حاکمیت امنیت داده به کمک اسناد ملی اینترنت اشیا با درنظرگیری مولفه‌های تنوع دانش شهروندان، تخصیص اعتبارات ملی، نوع عملکرد مدیران مرتبط با شهرهوشمند و بازیگران مرتبط با داده‌های اینترنت اشیا به منظور پیاده‌سازی موثر راهبردها و سیاست‌های حاکمیت امنیت داده
٤	تدوین و به‌روزرسانی شاخص‌ها و استانداردهای فنی مربوط به امنیت و کیفیت داده‌های اینترنت اشیا جهت بهبود کیفیت و امنیت داده‌های اینترنت اشیا در شهرهوشمند با بهره‌گیری از اسناد مرتبط کشورهای دیگر و مشارکت فعال متخصصین فنی مرتبط با امنیت داده‌های اینترنت اشیا

۵	طبقه‌بندی داده‌های اینترنت اشیا در شهرهوشمند و ایجاد رقابت میان سازمان‌ها و شرکت‌های خدمات شهری به کمک تسهیل مجوزهای دسترسی به داده‌های باز اینترنت اشیا با درنظرگیری امنیت و حریم خصوصی داده‌ها
٦	ایجاد ساختار پویا و چابک در بدنه حاکمیت و سازمان‌های مرتبط با حاکمیت امنیت داده‌های اینترنت اشیا در شهرهوشمند به منظور بهبود تصمیم‌گیری، تعامل و ارتباط با نهادها و ارگان‌های ملی و شهری
۷	نظارت و پایش مداوم امنیت تجهیزات، داده‌های اینترنت اشیا و همچنین دسترسی‌های سازمان‌ها و شرکت‌ها به داده‌های حساس با بهره‌گیری از سیستم‌ها و قوانین نظارتی به منظور تضمین امنیت و حریم خصوصی داده‌های اینترنت اشیا
۸	ایجاد برنامه‌های آموزشی مرتبط با امنیت داده‌های اینترنت اشیا با درنظرگیری سطوح مدیران، متخصصین و شهروندان شهرهوشمند با بهره‌گیری از متخصصین داخلی به منظور ارتقای سطح عملی امنیت داده
۹	ایجاد برنامه‌های توسعه امن اینترنت اشیا در شهرهوشمند با بهره‌گیری از سند الزامات ملی پیاده‌سازی اینترنت اشیا و متخصصین حقوقی مرتبط با امنیت داده‌های اینترنت اشیا
۱۰	کسب اعتماد و رضایت شهروندان و ذینفعان شهرهوشمند با نظارت و کنترل برنامه‌های حاکمیت امنیت داده‌های اینترنت اشیا

٤,٦ الویت‌بندی راهبردها

باتوجه به محدودیت‌های موجود در تامین منابع مختلف مادی و معنوی (از ساختار و سازمان، نیروی انسانی، زمان، بودجه، تجهیزات، امکانات، فرآیندهای اجرایی و...) اجرای تمامی راهبردها به‌ویژه در سال اول برنامه امکان‌پذیر نمی‌باشد. لذا لازم است که راهبردها، اولویت‌بندی گردند. بنابراین با استفاده از «تکنیک تعیین رجحان ترتیبی به‌وسیله شباهت به جواب ایده‌آل» نسبت به تعیین مطلوبیت راهبردها اقدام گردید و سپس راهبردهای مذکور براساس مقادیر مطلوبیت‌های محاسبه شده، اولویت‌بندی گردیدند. به‌طوری‌که راهبرد با بالاترین مقدار مطلوبیت دارای بالاترین اولویت اجرا باشد. نمودار مطلوبیت راهبردهای اساسی طبق نمودار ۱ است.



نمودار ۱ مقادیر مطلوبیت راهبردها به ترتیب اولویت

٤,۷ تعیین تاثیر راهبردها در تحقق اهداف کلان

از آنجاکه راهبردهای حاکمیت امنیت دادههای اینترنت اشیا در شهرهوشمند، باید در راستای تحقق اهداف کلان باشد و باتوجه به اینکه راهبردهای مذکور در راستای اهداف ذکر شده تدوین شده است، لذا بهمنظور تعیین تاثیر راهبردهای تدوین شده بر این اهداف، از طریق پرسشنامه، راهبردهای تعیین شده، و تاثیر هر یک از این راهبردها بر اهداف کلان را مشخص شد که در نهایت نتایج ذیل حاصل گردید:

جدول ٦ تعیین تاثیر راهبردهای ارائه شده بر تحقق اهداف کلان

اولویت	شماره راهبرد	تاثیر راهبرد بر تحقق هر یک از اهداف کلان (درصد ٪)					
		هدف کلان ۱	هدف کلان ۲	هدف کلان ۳	هدف کلان ٤	هدف کلان ٥	هدف کلان ٦
هشتم	راهبرد ۱	۲۷/۷۸	٥/٥٦	۲۲/۲۲	٥/٥٦	۲۷/۷۸	۱۱/۱۱
نهم	راهبرد ۲	۳۱/۲٥	۱۲/٥	۱۲/٥	۳۱/۲٥	٦/۲٥	٦/۲٥
دهم	راهبرد ۳	۲۳/٥۳	۱۷/٦٥	۲۳/٥۳	۱۷/٦٥	٥/۸۸	۱۱/۷٦
چهارم	راهبرد ٤	۲۲/۲۲	۱۱/۱۱	٥/٥٦	۲۷/۷۸	۱۱/۱۱	۲۲/۲۲
دوم	راهبرد ٥	۱۷/٦٥	۱۱/۷٦	۲۳/٥۳	۲۳/٥۳	۱۷/٦٥	٥/۸۸
هفتم	راهبرد ٦	۷/٦۹	۰/۰	۳۸/٤٦	۳۸/٤٦	۷/٦۹	۷/٦۹
ششم	راهبرد ۷	۳۰/۷۷	۷/٦۹	۱٥/۳۸	۳۰/۷۷	۷/٦۹	۷/٦۹
اول	راهبرد ۸	۲۳/٥۳	٥/۸۸	۲۳/٥۳	۱۱/۷٦	۱۱/۷٦	۲۳/٥۳
سوم	راهبرد ۹	۲۳/٥۳	۱۷/٦٥	٥/۸۸	۲۳/٥۳	۲۳/٥۳	٥/۸۸
پنجم	راهبرد ۱۰	۳۰/۷۷	۳۰/۷۷	۷/٦۹	۷/٦۹	۷/٦۹	۱٥/۳۸

۵ .نتیجه‌گیری

یکی از اساسی‌ترین نیازها برای نیل به پیشرفت و توسعه همه‌جانبه یک کشور، پژوهش می‌باشد؛ همچنین قدرت و استقلال هر کشوری بر پژوهش و تولید علم استوار است. برای این‌منظور باتوجه به پرسش‌های تحقیق، ابتدا ارکان جهت‌ساز پنج‌گانه به‌صورت زیر احصاء شده است:

الف- اصول: ۱- اصل چند بعدی بودن ۲- اصل خودحفاظتی ۳- اصل رصد دائمی تهدیدات ٤- اصل پیشگیری ٥- اصل مسئولیت‌پذیری ٦- اصل خلاقیت و نوآوری ۷- اصل مشارکت ۸- اصل خدمات‌دهی ۹- اصل پایداری.

ب-ارزش: ارتقاء امنیت و خدمات‌دهی اینترنت اشیا در شهرهوشمند با رویکرد حاکمیت امنیت داده.

ج- چشم انداز: تحقق توسعه امن و پایدار اینترنت اشیا در شهرهوشمند با بهره‌گیری از قابلیت‌های حاکمیت امنیت داده به‌منظور همراستاسازی امنیت داده اینترنت اشیا و خدمات‌دهی شهرهوشمند با ویژگی‌های نیروی انسانی توانمند، ساختار چابک و پویا، برخورداری از دانش بومی، دارای تجهیزات پیشرفته امن و پایدار.

د- ماموریت: حفظ امنیت و حریم خصوصی داده، کنترل و نظارت بر روی جریان داده‌ها، تسهیل خدمات داده‌ها و همچنین بهبود کیفیت داده‌های اینترنت اشیا در شهرهوشمند

ه- هدف کلان :۱- مصون‌سازی شهرهوشمند از خطرات امنیتی داده‌های اینترنت اشیا ۲- حفظ حریم خصوصی داده‌های اینترنت اشیا در شهرهوشمند ۳- دستیابی به سطح بالایی از خدمات دهی اینترنت اشیا در شهرهوشمند ٤- همراستاسازی امنیت داده‌های اینترنت اشیا و خدمات‌دهی آن در شهرهوشمند ٥- دستیابی به دانش و فناوری بومی جهت تولید تجهیزات و برنامه‌های کاربردی اینترنت اشیا با درنظرگیری سطح حساسیت ٦- بهره‌گیری از نیروی انسانی توانمند، آموزش‌دیده، با انگیزه در سطوح مختلف

در ادامه با بررسی محیطی و انجام مصاحبه با خبرگان سایبری، عوامل تاثیرگذار در حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند احصاء و جهت مشخص نمودن نقاط

قوت، ضعف، فرصت، تهدید و همچنین میزان اهمیت، امتیاز وضع موجود و مطلوب طی پرسشنامه‌هایی در اختیار خبرگان قرار گرفت. در این‌خصوص براساس چهار حوزه اصلی کاربردی حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند، عوامل تاثیرگذار داخلی و خارجی شناسایی شد. عوامل تاثیر گذار داخلی بر اساس نقاط ضعف و قوت و عوامل تاثیرگذار خارجی بر اساس فرصت و تهدید در بخش ٤,٢ تشریح گردید. سپس بر اساس تجزیه و تحلیل نتایج به‌دست آمده و با استفاده از ابزارهای ریاضی و در دستگاه مختصات دکارتی، جمع جبری ارزش‌ها، تشخیص منابع، جدول SWOT، ماتریس بهبودیافته، راهبردهای مناسب، راهکارهای اساسی و الزامات اجرایی راهبردها پیشنهاد گردید. بر این اساس راهبردهای ده‌گانه ارائه شده به‌صورت زیر می‌باشد.

۱- بومی‌سازی تجهیزات و برنامه‌های کاربردی اینترنت اشیا با بهره‌گیری از متخصصین داخلی و ظرفیت دانشگاهی با درنظرگیری سطح حساسیت و شرایط تحریمی

۲- ایجاد زیرساخت‌ها و رویه‌های فنی و امنیتی با بهره‌گیری از فناوری‌های بومی و متخصصین داخلی جهت شناسایی حفره‌های امنیتی تجهیزات اینترنت اشیا در شهرهوشمند

۳- ایجاد بستر اجرایی برنامه‌های حاکمیت امنیت داده به کمک اسناد ملی اینترنت اشیا با درنظرگیری مولفه‌های تنوع دانش شهروندان، تخصیص اعتبارات ملی، نوع عملکرد مدیران مرتبط با شهرهوشمند و بازیگران مرتبط با داده‌های اینترنت اشیا به منظور پیاده‌سازی موثر راهبردها و سیاست‌های حاکمیت امنیت داده

٤- تدوین و به‌روزرسانی شاخص‌ها و استانداردهای فنی مربوط به امنیت و کیفیت داده‌های اینترنت اشیا جهت بهبود کیفیت و امنیت داده‌های اینترنت اشیا در شهرهوشمند با بهره‌گیری از اسناد مرتبط کشورهای دیگر و مشارکت فعال متخصصین فنی مرتبط با امنیت داده‌های اینترنت اشیا

۵- طبقه‌بندی داده‌های اینترنت اشیا در شهرهوشمند و ایجاد رقابت میان سازمان‌ها و شرکت‌های خدمات شهری به کمک تسهیل مجوزهای دسترسی به داده‌های باز اینترنت اشیا با درنظرگیری امنیت و حریم خصوصی داده‌ها

٦- ایجاد ساختار پویا و چابک در بدنه حاکمیت و سازمان‌های مرتبط با حاکمیت امنیت داده‌های اینترنت اشیا در شهرهوشمند به منظور بهبود تصمیم‌گیری، تعامل و ارتباط با نهادها و ارگان‌های ملی و شهری

۷- نظارت و پایش مداوم امنیت تجهیزات، داده‌های اینترنت اشیا و همچنین دسترسی‌های سازمان‌ها و شرکت‌ها به داده‌های حساس با بهره‌گیری از سیستم‌ها و قوانین نظارتی به منظور تضمین امنیت و حریم خصوصی داده‌های اینترنت اشیا

۸- ایجاد برنامه‌های آموزشی مرتبط با امنیت داده‌های اینترنت اشیا با درنظرگیری سطوح مدیران، متخصصین و شهروندان شهرهوشمند با بهره‌گیری از متخصصین داخلی به منظور ارتقای سطح عملی امنیت داده

۹- ایجاد برنامه‌های توسعه امن اینترنت اشیا در شهرهوشمند با بهره‌گیری از سند الزامات ملی پیاده‌سازی اینترنت اشیا و متخصصین حقوقی مرتبط با امنیت داده‌های اینترنت اشیا

۱۰- کسب اعتماد و رضایت شهروندان و ذینفعان شهرهوشمند با نظارت و کنترل برنامه‌های حاکمیت امنیت داده‌های اینترنت اشیا

ارزیابی ۱۰ راهبرد ارائه شده نشان می‌دهد که می‌توان علاوه بر تحقق اهداف کلان، بر چالش‌های حاکمیت امنیت داده اینترنت اشیا در شهرهوشمند نیز فائق آمد. باتوجه به پرسش اصلی تحقیق، طرح راهبردی حاکمیت امنیت داده اینترنت اشیا در شهر هوشمند مطابق شکل شماره ۵ خواهد بود.

شکل ۵ طرح راهبردی حاکمیت امنیت داده اینترنت اشیا در شهر هوشمند

٦ .پیشنهاد

۱- به‌کارگیری راهبردهای مطرح شده توسط معاونت‌های ارتباطات و فناوری اطلاعات سازمان‌های خدمات شهری

۲- استفاده از راهبردهای احصاء شده به‌منظور تدوین دستورالعمل استانداردسازی نرم‌افزارها، پروتکل‌ها وفرایندهای ارتباط دیجیتالی تجهیزات اینترنت اشیا توسط سازمان پدافند غیر عامل

۳- تدوین دستورالعمل استانداردسازی نرم‌افزارها، پروتکل‌ها وفرایندهای ارتباط دیجیتالی تجهیزات اینترنت اشیا با بهره‌گیری از متخصصین داخلی به منظور ارتقای سطح عملی امنیت داده

٤- معاونت‌های ارتباطات و فناوری اطلاعات سازمان‌های خدمات شهری و زیرنظر شهرداری‌ها، درخصوص اتخاذ رویکرد حاکمیت امنیت داده اینترنت اشیا اقدام نمایند.

۵- معاونت‌های آموزشی سازمان پدافند غیر عامل و شهرداری کلان‌شهرها نسبت به تدوین راهبردهای امنیت داده‌های اینترنت اشیا در شهرهوشمند با رویکرد راهبردهای ارائه شده درخصوص حاکمیت امنیت داده اقدام نماید.

فهرست منابع ومآخذ

الف. منابع فارسی

- سامنی، سارا؛ نصیری، رامین و محسن‌زاده، مهران. (۱۳۹۸)، ***مقایسه مدلها و چارچوب های حاکمیت داده با هدف دستیابی به پیش نیازها، موانع و مولفه های یک برنامه حاکمیت داده برای داده های حوزه سلامت***. ششمین کنفرانس بین المللی فناوری اطلاعات، کامپیوتر و مخابرات.
- سخایی، محمدجواد. (۱۳۹۷)، ***مدل های بلوغ حاکمیت داده (۱)***. فابک، http://www.fabak.ir
- سعادتمند، امیر مسعود؛ کریمی قهرودی، محمدرضا و محمدی، حافظ و بابک، محمد. (۱٤۰۰)، ***تعیین شاخص‌های ارزیابی امنیت سایبری به روش مطالعه تطبیقی***، فصلنامه امنیت ملی، دوره ۱۱، شماره ٤۰، ۳۷-٦٦

- دفتر استراتژی دانشگاه شریف. (۱۳۹۸). ***تعریف دقیق راهبرد و مدیریت راهبردی چیست؟*** https://sharifstrategy.org/strategic-management-2/#tryf_rahbrd_chyst.

ب. منابع انگلیسی

- 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
- Alam, M., Shakil, K. A., & Khan, S. (2020). ***Internet of Things (IoT)***. Springer International Publishing. https://doi.org/10.1007/978-3-030-37468-6
- AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). ***Information security governance challenges and critical success factors: Systematic review***. Computers and Security, 99. https://doi.org/10.1016/j.cose.2020.102030
- Alomair, B., & Poovendran, R. (2014). ***Efficient Authentication for Mobile and Pervasive Computing***. IEEE Transactions on Mobile Computing, 13(3), 469–481. https://doi.org/10.1109/TMC.2012.252
- Al-Ruithe, M., Mthunzi, S., & Benkhelifa, E. (2016***). Data governance for security in IoT & cloud converged environments***. Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA, 0. https://doi.org/10.1109/AICCSA.2016.7945737
- Angrishi, K. (2017). ***Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets***. 1–17. http://arxiv.org/abs/1702.03681
- 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
- Bollengier, K., Viable, O., & Security, I. (2020). ***Organizing Viable Information Security Governance and Management***: July. https://doi.org/10.5281/zenodo.3960147
- Braun, T., Fung, B. C. M., Iqbal, F., & Shah, B. (2018). ***Security and privacy challenges in smart cities***. Sustainable Cities and Society, 39, 499–507. https://doi.org/10.1016/j.scs.2018.02.039
- 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
- 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
- Dasgupta, A., Gill, A., & Hussain, F. (2019). ***A conceptual framework for data governance in IoT-enabled digital IS ecosystems***. DATA 2019 - Proceedings of the 8th International Conference on Data Science, Technology and Applications, Data, 209–216. https://doi.org/10.5220/0007924302090216

- Diligent. (2016). ***Five Best Practices for Information Security Governance terabytes of sensitive data***, business insider, http://www.businessinsider.com/the-sony-hackers-still-have-a-
- 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
- Ferenczy, A. (2019). ***3 Reasons Why Corporate Strategic Planning is Important***. AchieveIt, https://www.achieveit.com/resources/blog/3-reasons-corporate-strategic-planning-important
- 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
- Gashgari, G., Walters, R., & Wills, G. (2017). ***A proposed best-practice framework for information security governance***. IoTBDS 2017 - Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, IoTBDS, 295–301. https://doi.org/10.5220/0006303102950301
- 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.
- ISO 27014. (2020). ***INTERNATIONAL STANDARD ISO / IEC Information security, cybersecurity and privacy protection Governance of information security***, (ISO/IEC 27014:2020).
- Joshi, S., Saxena, S., Godbole, T., & Shreya. (2016). ***Developing Smart Cities: An Integrated Framework***. Procedia Computer Science, 93, 902–909. https://doi.org/10.1016/j.procs.2016.07.258
- Keping, Y. (2018). ***Governance and Good Governance: A New Framework for Political Analysis***. Fudan Journal of the Humanities and Social Sciences, 11(1). https://doi.org/10.1007/s40647-017-0197-4
- 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
- Lowans, B., Kish, D., Willemsen, B., & Girard, J. (2018). ***How to Use the Data Security Governance Framework***. Gartner.
- Lupi, L. (2019). ***City Data Plan: The Conceptualisation of a Policy Instrument for Data Governance in Smart Cities***. Urban Science, 3(3), 91. https://doi.org/10.3390/urbansci3030091
- 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
- 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
- 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.