Scientific Journal of Electronical & Cyber Defence
Vol. 10, No. 3, Autumn 2022, Serial No. 39

A framework for assessing cyber security and privacy threats and investigating their impact on smart city performance

N. Seddighi, M. R. Sanaei*, R. Ehtesham Rasi

*Assistant Professor, Department of Information Technology Management, Faculty of Management and Accounting, Qazvin Branch, Islamic Azad University, Qazvin, Iran

(Received: 18/11/2021, Accepted: 10/01/2022)

ABSTRACT

Today, the world is experiencing the evolution of smart cities. The emergence of such cities stems from the application of information technology innovation, which, despite the creation of numerous economic and social opportunities, has posed citizens with cyber security and privacy threats. The successful transition of cities to smart cities and the optimal performance of smart cities depends on the awareness of these threats and their effectiveness. This study aims to provide a framework for identifying and evaluating cyber security and privacy threats and examining their impact on smart city performance in city. This research is applied in terms of purpose and descriptive survey in terms of the data collection method. In this study, these threats have been identified through in-depth library studies as well as surveys through researcher-made questionnaires using fuzzy Delphi method from academic experts and relevant officials that were selected by purposeful manner and the importance of each threat has been determined using the fuzzy Best-Worst Multi-Criteria method. Then, according to the smart city concepts and theories, the performance of city in the transition to a smart city is described based on five components as smart infrastructure, governance, economy, people, and environment. After that, the hypotheses, described on the impact of these threats on the performance of smart city, have been tested using the Structural Equations Modeling based on Partial Least Squares method. The findings indicated that 11 cyber security threats and 10 privacy challenges existed in the smart city, among which three threats as Legislative challenge, Lack of secure communication, and Insecure APIs and protocols were specified as the key threats. Furthermore, analyzing the fitted model and research hypotheses showed a negative and significant relationship between the variables of cyber security threats and privacy challenges with the smart city performance and a positive and significant relationship between cyber security threats and privacy challenges at a 95% confidence level. Considering the value of the R2 coefficient, it was observed that the variables of cyber security threats and privacy challenges in total, predicted 72.7% of the changes related to the performance variable of smart city, which was remarkable.

Keywords: Smart city, cyber security and privacy threats, fuzzy Delphi method, Fuzzy Best-Worst Multi-Criteria method, Structural Equation Modelling, Partial Least Squares approach.

* Corresponding Author Email: Mohamadrezasanaei44@yahoo.com

نشریه علمی "پدافند الکترونیکی و سایبری"
سال دهم، شماره ۳، پاییز ۱۴۰۱، ص ۹۱- ۷۷

علمی – پژوهشی

ارائه چارچوبی جهت ارزیابی تهدیدهای امنیت سایبری و حریم خصوصی و بررسی تأثیر آن‌ها بر عملکرد شهر هوشمند

نازیلا صدیقی[۱]، محمدرضا ثنایی[۲*]، رضا احتشام راثی[۳]

۱- دانشجوی دکتری مدیریت فناوری اطلاعات، ۲ و ۳- استادیار، گروه مدیریت فناوری اطلاعات،
دانشکده مدیریت و حسابداری، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران

(دریافت: ۱۴۰۰/۰۸/۲۷، پذیرش: ۱۴۰۰/۱۰/۲۱)

چکیده

امروزه جهان در حال تجربه تکامل شهرهای هوشمند است. پیدایش چنین شهرهایی برگرفته از کاربست نوآوری در فناوری اطلاعات بوده که علی‌رغم خلق فرصت‌های اقتصادی و اجتماعی متعدد، شهروندان را با تهدیدهایی در زمینهٔ امنیت سایبری و حریم خصوصی مواجه ساخته است. گذار موفقیت‌آمیز شهرها به‌سوی شهر هوشمند و عملکرد مطلوب شهرهای هوشمند منوط بر آگاهی از این تهدیدها و میزان اثرگذاری آن‌ها است. هدف از این پژوهش، ارائه چارچوبی جهت شناسایی و ارزیابی تهدیدهای امنیت سایبری و حریم خصوصی و بررسی تأثیر آن‌ها بر عملکرد شهر هوشمند در یک شهر است. این پژوهش از نظر هدف، کاربردی و از جنبه شیوه گردآوری داده‌ها، توصیفی- پیمایشی است. در پژوهش حاضر، این تهدیدها با مطالعات عمیق کتابخانه‌ای و نیز نظرسنجی از طریق پرسشنامه‌های محقق‌ساخته به روش دلفی فازی از صاحب‌نظران دانشگاهی و خبرگان سازمان‌های متولی که به شیوه هدفمند قضاوتی انتخاب شدند، شناسایی شده و درجه اهمیت هریک از آن‌ها به روش تصمیم‌گیری چندمعیاره بهترین-بدترین فازی تعیین گردید. در ادامه با استناد بر مفاهیم و نظریات حاکم بر شهر هوشمند، عملکرد آن شهر در گذار به‌سوی شهر هوشمند بر پایه پنج مؤلفه زیرساخت، حاکمیت، اقتصاد، مردم و محیط‌زیست هوشمند تبیین گردیده و آزمون فرضیه‌های مرتبط با تأثیر تهدیدهای مذکور بر عملکرد شهر هوشمند با رویکرد مدل‌سازی معادلات ساختاری مبتنی بر روش حداقل مربعات جزئی انجام گرفت. یافته‌های این پژوهش حاکی از شناسایی ۱۱ تهدید امنیت سایبری و ۱۰ چالش حریم خصوصی در هوشمندسازی آن شهر بود که در میان آن‌ها سه تهدید «چالش قانون‌گذاری»، «فقدان ارتباط امن» و «API ها و پروتکل‌های ناامن» به‌عنوان کلیدی‌ترین تهدیدها تعیین شدند؛ همچنین آزمون مدل برازش‌یافته و فرضیه‌های پژوهش حاکی از وجود رابطه منفی و معنی‌دار میان متغیرهای تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی با متغیر عملکرد شهر هوشمند و نیز رابطه مثبت و معنی‌دار تهدیدهای امنیت سایبری بر چالش‌های حریم خصوصی در سطح اطمینان ۹۵ درصد بود. با توجه به مقدار ضریب تعیین R2، ملاحظه شد که متغیرهای تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی درمجموع، ۷۷/۲ درصد از تغییرات مربوط به متغیر عملکرد شهر هوشمند را پیش‌بینی کرده‌اند که رقم قابل‌توجهی بود.

کلیدواژه‌ها: شهر هوشمند، تهدیدهای امنیت سایبری و حریم خصوصی، روش دلفی فازی، روش بهترین- بدترین فازی، مدل‌سازی معادلات ساختاری، رویکرد حداقل مربعات جزئی

۱- مقدمه

با جنبش جهانی به‌سوی شهرنشینی و استفاده وسیع از فناوری‌های نوین اطلاعات و ارتباطات[1] (ICT)، مفهوم شهرهای هوشمند پدید آمد که توجه بسیاری از محققان را به خود جلب کرده است [۱ و ۲]. شهر هوشمند، شهری است که فناوری‌های مدرن را برای خدمات خودکار و کارآمد یکپارچه می‌سازد تا سبک و کیفیت زندگی شهروندان را بهبود بخشد [۳]. علی‌رغم گرایش شهرها به هوشمندسازی، برنامه‌های کاربردی شهرهای هوشمند نگرانی‌ها و چالش‌هایی از نوع امنیت سایبری و حریم خصوصی برای شهروندان ایجاد می‌نمایند [۴]. ایجاد امنیت سایبری یکی از چالش برانگیزترین و به‌روزترین موضوعات در زمینهٔ شهر هوشمند به‌حساب می‌آید. هزینه کم ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از دولت‌ها، گروه‌های سازمان‌یافته و تروریستی و حتی افراد به فضای شهر هوشمند وارد شده و تهدیدهایی همچون جنگ سایبری، جرائم سایبری، تروریسم سایبری، جاسوسی سایبری و مانند آن‌ها را به وجود آورند [۵]. در کنار تهدیدهای امنیت سایبری، وجود چالش‌های حریم خصوصی نیز معضلی برای

* رایانامه نویسنده مسئول: Mohamadrezasanaei44@yahoo.com

1 Information and Communication Technology

شهروندان در فضای شهر هوشمند محسوب می‌شود. فیشینگ، کلاه‌برداری، حملات به واحد داده‌ها، استراق سمع، حملات به شبکه‌ها و سایت‌ها و غیره ازجمله مصادیق چالش‌ها و تخلفات مربوط به حریم خصوصی می‌باشند [۶]؛ بنابراین شهر هوشمند باید قادر باشد تا از درز اطلاعات، دسترسی‌های غیرمجاز، بروز اختلال و نابودی اطلاعات دفاع کند.

نظر به رشد فزاینده جمعیت در این شهر و آگاهی مسئولان و سیاست‌گذاران شهری از جایگاه فناوری اطلاعات و ارتباطات در تسهیل امور شهروندی در عرصه‌های مختلف، برنامه پنج‌ساله سوم شهرداری در حوزه گذار شهر به‌سوی شهر هوشمند با مجموعه‌ای از واکاوی‌های بین‌المللی و بررسی شهرهای هوشمند سایر کشورها و همچنین بررسی اسناد بالادستی کشور و در نظر گرفتن اولویت‌های شورا و شهرداری در دست تدوین قرار گرفت. به‌کارگیری سازوکارهای سخت‌افزاری و نرم‌افزاری شهر هوشمند برای کشوری چون ایران که شهرهای آن بین مرحله گذار از الگوهای سنتی و مدرن و فرا مدرن سرگردان هستند، الزامی است؛ اما زمینه‌های موجود برای حرکت در این مسیر از نارسایی‌های زیادی برخوردار است که باید ضمن رسیدن به یک آگاهی درست از آن، راهکاریابی سنجیده‌ای را پی گرفت. لازمه گذار موفقیت‌آمیز شهر به‌سوی شهر هوشمند و نیز تدوین خط‌مشی‌ها و راهبردهای مناسب در این مسیر و محافظت از این شهر در مقابل تهدیدات امنیت سایبری و چالش‌های حریم خصوصی، آگاهی برنامه‌ریزان و مسئولان شهری نسبت به این تهدیدها، درجه اهمیت آن‌ها و نیز تأثیرگذاری آن‌ها بر عملکرد شهر هوشمند است. با توجه به تأثیر تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی بر عملکرد شهر هوشمند ، پژوهش حاضر درصدد پاسخ به این سؤال اصلی است که چارچوب مناسب جهت شناسایی و ارزیابی تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی کدام است و تأثیرگذاری این تهدیدها بر عملکرد شهر هوشمند به چه صورت است؟

بر این اساس سایر بخش‌های این مقاله به شرح ذیل سازمان‌دهی شده است. در بخش بعدی، با مروری بر ادبیات و پیشینه پژوهش، تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در شهرهای هوشمند احصاء خواهد شد. سپس روش‌شناسی پژوهش و چارچوب پیشنهادی ارائه می‌شود. در ادامه، چارچوب پیشنهادی برای شناسایی و ارزیابی تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در مسیر هوشمندسازی شهر پیاده‌سازی می‌شود. سپس با نگاشت مدل مفهومی پژوهش و آزمون این مدل، تأثیر متغیرهای تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی بر عملکرد شهر هوشمند موردسنجش قرار خواهد گرفت. در انتها به بحث و نتیجه‌گیری پیرامون یافته‌های پژوهش پرداخته می‌شود.

۲- مروری بر پیشینه پژوهش و چارچوب نظری

حوزه مطالعاتی شهر هوشمند سابقه تاریخی طولانی‌مدتی نداشته و در طی سال‌های اخیر توجه پژوهشگران را به خود جلب نموده است. ازاین‌رو تعداد پژوهش‌های داخلی و خارجی که به‌طور اخص به مطالعه تهدیدهای امنیت سایبری و حریم خصوصی در شهر هوشمند پرداخته باشند بسیار محدود بوده که در ادامه به مهم‌ترین آن‌ها اشاره می‌شود.

نیکوگفتار ناطق [۷] به بررسی حمل‌ونقل عمومی هوشمند در شهرهای هوشمند از دیدگاه امنیت سایبری و تعریف یک مدل معماری جهت طبقه‌بندی حملات و تهدیدات سایبری در این سیستم‌ها و ارائه راهکارهای لازم جهت مصونیت در برابر تهدیدات عمدی پرداخت. او ابتدا ذی‌نفعان اصلی و حوزه‌های تأثیرگذار آن‌ها در زمینهٔ حمل‌ونقل عمومی هوشمند را شناسایی نمود. سپس با بررسی اجمالی الزامات امنیتی، مدل معماری و طبقه‌بندی تهدیدات و حملات پیش‌روی این سیستم‌ها را بررسی کرد. او بین تهدیدات ناشی از حملات عمدی و غیرعمدی تمایز قائل شده و در انتها با نگاه ویژه به تهدیدات عمدی، راهکارهای پیشنهادی متعددی ازجمله استفاده از شبکه‌های خصوصی مجازی، رمزگذاری اطلاعات، استفاده از سیستم‌های تشخیص نفوذ شبکه، حفاظت فیزیکی، کنترل دستی، سیستم‌های نظارتی و اعلان خطر، اجرای سیاست امنیت اطلاعات، ایجاد فایل پشتیبان و بازرسی منظم را ارائه نمود. حمزه و کازرونی [۸] در پژوهشی به تجزیه‌وتحلیل اجزاء اصلی شهر هوشمند و بررسی چالش‌ها و راهبردهای به‌کاربرده شده در این شهر پرداختند. روش پژوهش آن‌ها توصیفی بوده و بر پایه جمع‌آوری اطلاعات اسنادی و متون مرتبط با این حوزه تدوین شد. در همین راستا، در گام نخست با معرفی اجزای اصلی شهر هوشمند، تمامی این اجزاء را مورد آنالیز قرار دادند. سپس، چالش‌های پیش‌رو در اجرای پروژه‌های هوشمندسازی را بررسی کردند. در گام سوم، دو راهبرد مهم همراه با نقاط قوت و ضعف را بررسی کرده و در گام آخر نیز شهرهای هوشمند جهان را با توجه به رتبه‌بندی آن‌ها در هر یک از عوامل تأثیرگذار هوشمندسازی معرفی نمودند. تکلو بیغش و تکلو بیغش [۹] به مطالعه امنیت و حریم خصوصی در برنامه‌های کاربردی شهر هوشمند پرداختند. آن‌ها نخست برنامه‌های کاربردی شهر هوشمند و معماری آن را معرفی کردند. سپس به بحث در خصوص چالش‌های پیرامون حفظ حریم خصوصی و امنیت در این برنامه‌ها پرداختند تا با شناخت و اتخاذ تدابیر سازنده در مواجهه با آن‌ها بتوانند مراقبت‌های بهداشتی هوشمند، حمل‌ونقل و انرژی هوشمند بهبود بخشند. الباسق و همکاران [۱۰] موضوع امنیت سایبری را برای شهرهای هوشمند موردبررسی قرار دادند. آن‌ها نشان دادند که ویژگی‌های خاص شهرهای هوشمند چطور چالش‌های امنیت سایبری را افزایش می‌دهند. به‌علاوه آن‌ها تهدیدهای مختلف مرتبط با شهرهای

هوشمند را موردبررسی قرار داده و در انتها تعدادی از مهم‌ترین راه‌حل‌های امنیت سایبری را برای شهرهای هوشمند ارائه کردند. نویسندگان این مقاله بر این باور بودند که مقابله با چالش‌های امنیتی سایبری از طریق سخت‌کوشی دولت‌ها، توسعه‌دهندگان سخت‌افزار و تجهیزات و شرکت‌های امنیت فناوری اطلاعات امکان‌پذیر است. الدیری [۳] در مطالعه‌ای مروری به بررسی تفصیلی تحقیق‌های مرتبط با چالش‌های امنیتی عمده و راه‌حل‌های جاری در شهرهای هوشمند پرداخته و چندین عامل تأثیرگذار بر ایمنی اطلاعات و داده‌ها در شهرهای هوشمند را معرفی کرد. بر مبنای یافته‌های این نویسنده، آسیب‌پذیری‌ها و ریسک‌های متعددی در زیرساخت فیزیکی-سایبری مورداستفاده در هوشمندسازی شهر وجود دارد که این چالش‌های امنیتی در دوربین‌ها، شبکه‌های ارتباطی، سیستم‌های مدیریت ساختمان، سیستم‌های مدیریت حمل‌ونقل یافت شدند. به‌علاوه چالش‌هایی نیز مربوط به حریم خصوصی شناسایی شدند که در دو دسته چالش‌های حریم خصوصی ارتباطی و کسب‌وکار دسته‌بندی شدند. هاسبینی و همکاران [۱۱] با رجوع به ادبیات تحقیق، اهمیت مدیریت امنیت اطلاعات[1] (ISM) را برای شهرهای هوشمند نشان دادند. سپس بر عوامل برتر سازمانی که بر ISM در سازمان‌های شهر هوشمند اثرگذار بودند تمرکز کردند. یافته‌های آن‌ها حاکی از نیاز مبرم به انجام تحقیقات بیشتر بر روی ISM در حوزه سازمان‌های شهر هوشمند و نیز عوامل سازمانی مرتبط با ISM بود که انتظار می‌رفت بیشترین تأثیر را بر عملکرد سازمانی شهر هوشمند داشته باشند.

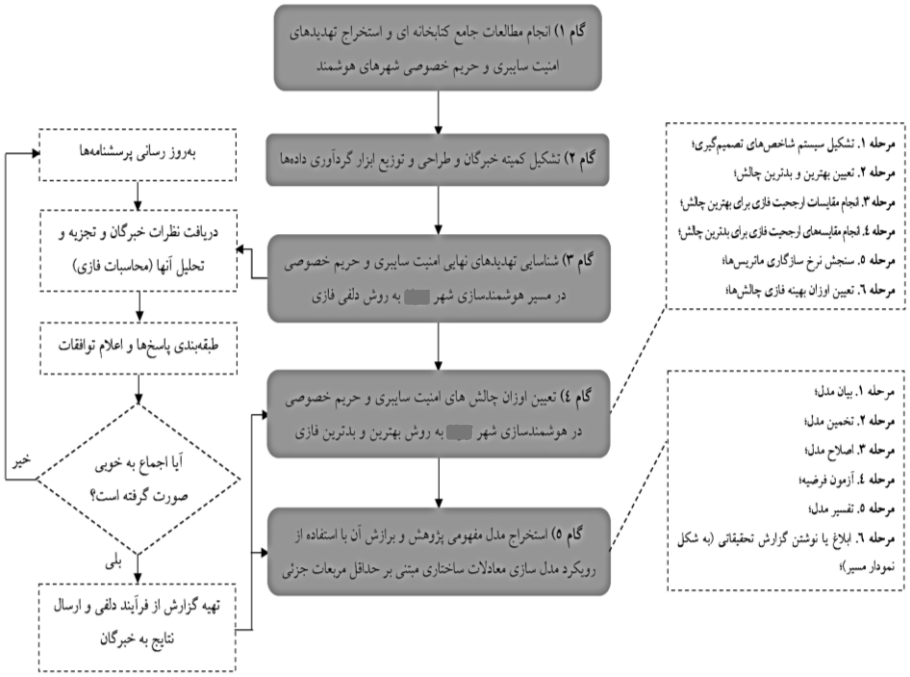
فرحات و همکاران [۱۲] در پژوهشی به بررسی اینترنت اشیا و کاربرد آن در شهرهای هوشمند پرداختند. سپس امنیت اطلاعات و چالش‌های آن را در شهر هوشمند و نیز نحوه حفاظت از داده‌های شهروندان از طریق ایمن‌سازی سیستم انتقال داده‌های مبتنی بر WiFi را تشریح کردند. این سیستم داده‌ها را پیش از انتقال از مبدأ، کدگذاری کرده و آن‌ها را در مقصد رمزگشایی می‌کرد. سیستم پیشنهادی با روش تأیید هویت به افراد مجاز امکان دسترسی به داده‌ها را می‌داد. یافته‌های پژوهش آن‌ها در قالب نمونه اولیه امنیتیِ WiFi با هزینه بسیار کم ارائه شد. روش پیشنهادی رمزنگاری داده‌ها در این پژوهش، برخی از چالش‌های امنیتی را که اینترنت اشیاء به‌ویژه در شهرهای هوشمند با آن مواجه است، حل می‌نمود. سیستم ارائه‌شده در این پژوهش قادر بود ضمن احراز هویت دقیق از کاربران، از نفوذ مهاجمان به داده‌های شخصی شهروندان هر زمان که به‌صورت بی سیم از منبعی به مقصدی انتقال می‌یابد، مقابله نماید. لاوفوس و همکاران [۱۳] در مقاله‌ای مروری و نظام‌مند به بررسی ادبیات پژوهش مرتبط با فناوری‌های جدید امنیت شهر هوشمند پرداخته و نشان دادند که این مداخلات تا چه اندازه با عملیات سنتی مداخلات امنیتی تطابق دارند. آن‌ها با جستجوی گسترده ادبیات، فهرستی از مداخلات امنیتیِ موجود در شهرهای هوشمند را گردآوری کرده و تغییرات متعددی برای وضعیت مفهومی در این حوزه پیشنهاد دادند. سپس این مضامین را به‌تفصیل موردبحث و بررسی قرار داده و اهمیت هر گروه از مداخلات را برای حوزه مدیریت و امنیت شهری ارزیابی کردند. وو و همکاران [۱۴] در پژوهشی به بحث در خصوص مدل خط‌مشی امنیت اطلاعات در شهرهای هوشمند تایوان پرداختند. آن‌ها از روش تحلیل مسیر برای بررسی مشخصه‌های خط‌مشی امنیت اطلاعات در شهرهای هوشمند استفاده کرده و رابطه بین تدوین، پیاده‌سازی، نگهداری و اثربخشی خط‌مشی‌های امنیت اطلاعات را آزمون کردند. همچنین در این پژوهش، تأثیر اثربخشی خط‌مشی های امنیت اطلاعات سازمانی و عملکرد امنیت اطلاعات از جنبه‌هایی چون: مدت‌زمان انتشار خط‌مشی امنیت اطلاعات، مرور خط‌مشی، حمایت از خط‌مشی، توافق با کارکنان، اجرای قانون منصفانه و غیره موردبررسی قرار گرفت که همگی از مظاهر عینی تدوین، پیاده‌سازی و نگهداری مدل‌های خط‌مشی امنیت اطلاعات به شمار می‌رفتند. نویسندگان این مقاله با استفاده از نظرسنجی پرسشنامه‌ای، همبستگی میان مفروضات مختلف و نیز رابطه بین مشخصه‌های امنیت اطلاعات سازمانی، خط‌مشی‌های امنیت اطلاعات و اثربخشی امنیت اطلاعات را یک‌به‌یک در طول اجرای خط‌مشی‌های امنیت اطلاعات تأیید کردند. از میان ۱۱ فرضیه مطروحه در این تحقیق شش فرضیه مورد تأیید قرار گرفتند. یافته‌های این پژوهش نشان داد که در فرآیند ساخت شهر هوشمند، توجه به امنیت اطلاعات از اهمیت وافری برخوردار بوده و این مهم در سطح ملی ضروری می‌باشد. به‌علاوه، برای دستیابی به اهداف امنیت اطلاعات، پیشنهاد شد که شهرهای هوشمند مدل‌های خط‌مشی امنیت اطلاعات[2] (ISP) را ایجاد کرده و با تدوین، پیاده‌سازی، ارزیابی و حفظ این مدل، اثربخشی امنیت اطلاعات را افزایش دهند.

با مروری بر پژوهش‌های پیشین در داخل کشور ملاحظه می‌شود که پژوهش‌های انجام‌گرفته در این حوزه بیشتر تمرکز خود را بر مفاهیم اولیه و گردآوری مطالب در قالب پژوهش نظری قرار داده‌اند. در میان پژوهش‌های خارجی نیز بخشی از پژوهش‌ها تمرکز خود را بر ارائه مطالب نوین در این حوزه و نیز آسیب‌شناسی پیاده‌سازی شهر هوشمند در کشورهای توسعه‌یافته در قالب مطالعه موردی و ارائه درس آموخته‌های آن پرداخته‌اند و بخشی دیگر از پژوهش‌ها صرفاً تا مرحله شناسایی چالش‌های امنیتی شهر هوشمند پیش رفته و بدون ارزیابی و تحلیل دقیق آن‌ها به ارائه راهکارهای پراکنده در جهت مواجهه با این چالش‌ها اکتفا کرده‌اند. این پژوهش در راستای تکمیل پژوهش‌های پیشین و پر کردن خلأ مطالعاتی آن‌ها در نظر دارد تا با مطالعه جامع

[1] Information Security Management

[2] Information Security Policy

پژوهش‌ها و دستاوردهای پژوهشگران در حوزه امنیت سایبری و حریم خصوصی شهر هوشمند، در قالب پژوهشی تحلیلی به شناسایی و دستیابی به اجماع نظر خبرگان در خصوص تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی شهر در گذار به‌سوی شهر هوشمند، تعیین درجه اهمیت این چالش‌ها و تأثیر آن‌ها بر عملکرد شهر هوشمند بپردازد.



شکل (۱). چارچوب متدلوژیک پیشنهادی پژوهش

۳- روش‌شناسی پژوهش و چارچوب متدلوژیک پیشنهادی

پژوهش حاضر از بُعد هدف، کاربردی و بر اساس شیوه گردآوری داده‌ها، توصیفی-پیمایشی است. جامعه آماری این پژوهش در دو بخش قرار می‌گرفت. بخش نخست شامل مدیران عالی و مسئولان ذی‌ربط وزارتخانه ارتباطات و فناوری اطلاعات، سازمان فناوری اطلاعات و ارتباطات شهرداری و پلیس فضای تولید و تبادل اطلاعات بود. بخش دوم شامل صاحب‌نظران دانشگاهی و اساتید متخصص در حوزه مطالعاتی پژوهش حاضر بودند. از بخش نخست، ده خبره سازمانی و از بخش دوم، ۱۷ خبره دانشگاهی به شیوه غیرتصادفی گلوله برفی انتخاب شدند. در این پژوهش برای گردآوری داده‌ها به شیوه میدانی، سه دسته پرسشنامه محقق‌ساخته (پرسشنامه نخست با هدف گردآوری داده‌های موردنیاز در شناسایی تهدیدهای نهایی امنیت سایبری و حریم خصوصی در هوشمندسازی شهر ، پرسشنامه دوم برای تعیین اوزان و درجه اهمیت این تهدیدها و پرسشنامه سوم جهت سنجش متغیرهای مدل مفهومی پژوهش در مقیاس طیف پنج‌بخشی لیکرت) طراحی شد. برای تعیین روایی پرسشنامه‌ها از روش روایی صوری[1] استفاده شد. بدین‌صورت که با ارائه پرسشنامه‌ها به تعدادی از اساتید دانشگاهی و خبرگان سازمانی، اجزاء تشکیل‌دهنده و ساختار پرسشنامه‌ها مورد تأیید قرار گرفت.

در این پژوهش برای سنجش پایایی پرسشنامه نخست، از مقدار آستانه همگرایی نظرات خبرگان (α) که بیانگر اختلاف اجماع نظر خبرگان در دو تکرار متوالی در روش دلفی فازی است، استفاده می‌شود. طبق قرارداد در این پژوهش مقدار آستانه همگرایی نظرات خبرگان به‌صورت α =۰/۱ در نظر گرفته شده است. در پرسشنامه دوم که جهت گردآوری داده‌های موردنیاز برای تعیین اوزان تهدیدهای امنیت سایبری و چالش‌های حریم خصوص به روش تصمیم‌گیری چندمعیاره بهترین و بدترین فازی[2] طراحی شده است، برای سنجش پایایی از روش نسبت سازگاری[3] (CR) استفاده شده است (به‌منظور آشنایی با نحوه محاسبه نسبت سازگاری به پژوهش گوا و ژائو [۱۵] مراجعه شود). برای سنجش پایایی پرسشنامه سوم از ضریب آلفای کرونباخ[4] استفاده شد که مقدار ۰/۷۷۵ برای آن حاصل گردید که حاکی از پایایی این پرسشنامه بود. شکل (۱)، ساختار و مراحل چارچوب متدلوژیک پیشنهادی پژوهش را نمایش می‌دهد.

با توجه به چارچوب پیشنهادی، در این پژوهش برای تجزیه‌وتحلیل داده‌ها در فاز شناسایی و تعیین اوزان تهدیدهای نهایی امنیت سایبری و حریم خصوصی در هوشمندسازی شهر به ترتیب از روش دلفی فازی[5] (FDM) و روش بهترین و بدترین

[1] Facial Validity

[2] Fuzzy Best-Worst Multi-criteria (FBWM) method
[3] Consistency Ratio
[4] Cronbach's alpha
[5] Fuzzy Delphi Method

فازی (F-BWM) گوا و ژائو [۱۵] و نرم‌افزارهای Excel 2013 و GAMS استفاده می‌شود. در پژوهش حاضر روش‌های مطروحه در محیط فازی در قالب تصمیم‌گیری گروهی انجام می‌گیرد. راهبرد تصمیم‌گیری گروهی از سوگیری نتایج جلوگیری کرده و با تمکین به خرد جمعی، بر افزایش دقت تصمیم‌گیری خواهد افزود. پیاده‌سازی روش‌های مذکور در محیط فازی این امکان را فراهم می‌سازد که با استفاده از تخمین‌های سه‌نقطه‌ای و در نظر گرفتن توابع امکان برای نظرات خبرگان از عدم قطعیت قضاوت‌های ذهنی آن‌ها کاسته و دقت تصمیم‌گیری را افزایش دهد. به‌علاوه در این پژوهش برای مدل‌سازی تأثیر تهدیدهای مذکور بر عملکرد شهر هوشمند و برازش مدل و آزمون فرضیات پژوهش از رویکرد مدل‌سازی معادلات ساختاری مبتنی بر حداقل مربعات جزئی (PLS-SEM) در نرم‌افزارهای SPSS V.16 و SMART PLS بهره گرفته خواهد شد.

چارچوب متدلوژیک پیشنهادی، مراحل و گام‌های پیاده‌سازی روش‌های مطروحه را با هدف شناسایی و ارزیابی تهدیدهای امنیت سایبری و حریم خصوصی و تأثیر آن بر عملکرد شهر هوشمند به‌صورت شماتیک و شفاف نشان می‌دهد. به‌منظور راستی آزمایی و نمایش قابلیت این چارچوب، در بخش بعدی مقاله به پیاده‌سازی آن جهت شناسایی و ارزیابی تهدیدهای امنیت سایبری و حریم خصوصی شهر در مسیر هوشمندسازی و نیز بررسی تأثیر این تهدیدها بر عملکرد این شهر پرداخته می‌شود.

۴- نتایج پژوهش

به‌منظور نمایش قابلیت چارچوب پیشنهادی، در این بخش به پیاده‌سازی این چارچوب برای شناسایی و ارزیابی تهدیدهای امنیت سایبری و حریم خصوصی در هوشمندسازی شهر و بررسی تأثیر آن‌ها بر عملکرد شهر هوشمند پرداخته می‌شود.

با مروری جامع بر پژوهش‌های انجام‌گرفته در بخش پیشینه پژوهش و نیز مطالعه سایر پژوهش‌های مرتبط، فهرستی از تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در شهرهای هوشمند که برگرفته از ترکیب یافته‌های این پژوهش‌ها و مبتنی بر تکرار آن‌ها در مقالات بود احصاء گردید. ازآنجاکه ارزیابی صحیح تهدیدهای هوشمندسازی شهر منوط به تناسب‌بخشی و بومی‌سازی تهدیدهای مستخرج از ادبیات تحقیق با فضای اجتماعی، اقتصادی، فرهنگی، سیاسی، قانونی (حقوقی) و زیرساخت‌های فناوری حاکم در این شهر است، لذا این تهدیدها از سوی کمیته ۱۰ نفره از خبرگان سازمانی طی چهار راند روش دلفی فازی مطابق با جدول (۱) مورد پایش و بازنگری قرار گرفته و تهدیدهایی که در راندهای دوم، سوم یا چهارم به اجماع نظر رسیده‌اند (حد آستانه کمتر از ۰/۱) برجسته شدند. طبق نظرات خبرگان، تهدیدهایی که مقدار میانگین فازی‌زدایی شده آن‌ها در راندی که به اجماع رسیده‌اند بیشتر از ۵ بود به‌عنوان تهدیدهای نهایی در مسیر هوشمندسازی آن شهر تعیین شده و در غیر این صورت از نظرسنجی خارج می‌شوند. نتایج تحلیل نظرات خبرگان طی چهار راند دلفی فازی به‌صورت جدول (۲) احصاء گردید.

جدول (۱). نظرسنجی تهدیدهای امنیت سایبری و حریم خصوصی مستخرج از ادبیات پژوهش از خبرگان سازمانی در هوشمندسازی شهر

ابعاد	تهدیدها	مراجع	میانگین نظرات در مرحله اول	میانگین نظرات در مرحله دوم	اختلاف نظرات در مراحل اول و دوم	میانگین نظرات در مرحله سوم	اختلاف نظرات در مراحل دوم و سوم	میانگین نظرات در مرحله چهارم	اختلاف نظرات در مراحل سوم و چهارم
تهدیدهای امنیت سایبری	افزایش حجم تبادلات دیجیتال	[۱؛ ۳؛ ۱۶؛ ۱۷؛ ۱۸؛ ۱۹؛ ۲۰؛ ۲۱؛ ۲۲؛ ۲۳؛ ۲۴]	۶/۳۳	۶/۵	۰/۱۷	۶/۳	۰/۲۰	۶/۳۸	۰/۰۸
	افزایش برنامه‌های کاربردی و ارتباطات از طریق تلفن همراه		۶/۷۳	۶/۹۳	۰/۲۰	۶/۹۸	۰/۰۵		
	افزایش میزان استفاده از هوش مصنوعی در شبکه‌های دیجیتال و ارتباطات ماشین به ماشین		۵/۸۸	۵/۷۳	۰/۱۵	۴/۸۳	۰/۹۰	۴/۸۳	۰/۰۰
	وجود محصولات نرم‌افزاری و سخت‌افزاری با آسیب‌پذیری‌های امنیتی		۶/۹۳	۶/۹۵	۰/۰۲				
	جنگ و تروریسم سایبری		۴/۷۵	۴/۸۳	۰/۰۸				
	جاسوسی سایبری		۵/۹۳	۶/۰۵	۰/۱۲	۶/۳	۰/۲۵	۶/۲۵	۰/۰۵

جدول (۱). نظرسنجی تهدیدهای امنیت سایبری و حریم خصوصی مستخرج از ادبیات پژوهش از خبرگان سازمانی در هوشمندسازی شهر

ابعاد	تهدیدها	مراجع	میانگین نظرات در مرحله اول	میانگین نظرات در مرحله دوم	اختلاف نظرات در مراحل اول و دوم	میانگین نظرات در مرحله سوم	اختلاف نظرات در مراحل دوم و سوم	میانگین نظرات در مرحله چهارم	اختلاف نظرات در مراحل سوم و چهارم
	دست‌کاری در داده‌ها و حملات تصنعی		۴/۶۸	۴/۴۵	۰/۲۳	۴/۴۸	۰/۰۳		
	از بین رفتن داده‌ها		۵/۴۸	۴/۸۵	۰/۶۳	۴/۸	۰/۰۵		
	نفوذ ویروس و بدافزار به سیستم‌های شهر هوشمند		۶/۵	۵/۷۳	۰/۷۷	۵/۵۳	۰/۲۰	۵/۶	۰/۰۷
	چالش قانون‌گذاری		۶/۷۵	۶/۹۵	۰/۲۰	۷/۱۸	۰/۲۳	۷/۱۳	۰/۰۵
	سرقت داده‌ها و اطلاعات و دستگاه‌های فیزیکی		۴/۶	۴/۸۸	۰/۲۸	۴/۸۳	۰/۰۵		
	ناکارایی سخت‌افزاری و نرم‌افزاری		۴/۴۳	۴/۸۸	۰/۴۵	۴/۸۳	۰/۰۵		
	چالش در دسترسی داده‌ها		۵/۴۸	۴/۴۵	۱/۰۳	۴/۴۳	۰/۰۲		
	APIها و پروتکل‌های ناامن		۶/۰۸	۶/۱	۰/۰۲				
	حملات ناشی از عدم پذیرش سرویس DoS		۵/۱	۵/۴۵	۰/۳۵	۵/۶۸	۰/۲۳	۵/۶۸	۰/۰۰
	خرابی حسگرها		۴/۰۵	۴/۲۵	۰/۲۰	۴/۲۳	۰/۰۲		
	فقدان ارتباط امن		۵/۵۳	۵/۰۳	۰/۵۰	۵/۰۳	۰/۰۰		
	چالش مدیریت و ذخیره‌سازی داده‌ها		۴/۸۸	۴/۸۵	۰/۰۳				
	اختلال در زیرساخت‌های مهم		۵/۶۸	۵/۸۵	۰/۱۷	۵/۸۵	۰/۰۰		
	امنیت فضای ابری		۵/۸۸	۵/۸۵	۰/۰۳				
	تهدیدهای هوش مصنوعی		۴/۷	۴/۲۵	۰/۴۵	۴/۲۵	۰/۰۰		
چالش‌های حریم خصوصی	تهدیدهای حریم خصوصی در داده‌کاوی و به اشتراک‌گذاری داده‌ها	[۳؛ ۱۶؛ ۲۰،۲۱؛ ۲۲، ۲۵]	۶/۵	۶/۴۸	۰/۰۲				
	تهدیدهای حریم خصوصی در داده‌های Mashup		۵/۸۸	۵/۸۳	۰/۰۵				
	استراق سمع		۶/۱۳	۶/۴۵	۰/۳۲	۶/۲۸	۰/۱۷	۶/۳	۰/۰۲
	چالش دسترسی به داده‌ها		۴/۶۵	۴/۶	۰/۰۵				
	خطر محرمانگی و یکپارچگی		۶/۰۸	۶/۰۸	۰/۰۰				
	خطر کلاه‌برداری و درز داده‌ها		۶/۱۸	۶/۰۵	۰/۱۳	۶/۰۵	۰/۰۰		
	جعل هویت		۴/۹	۵/۲	۰/۳۰	۵/۲۳	۰/۰۳		
	اطلاعات ساختگی		۵/۹	۵/۸۵	۰/۰۵				
	حملات کانال جانبی		۵/۳	۴/۸	۰/۵۰	۴/۸۵	۰/۰۵		
	استفاده ثانویه از داده‌های جمع‌آوری‌شده		۵/۶۸	۵/۶۳	۰/۰۵				
	جعل آدرس اینترنتی		۵/۵۵	۵/۶۳	۰/۰۸				
	حمله به یکپارچگی داده‌ها		۵/۱۵	۵/۲۳	۰/۰۸				

جدول (۲). تهدیدهای نهایی امنیت سایبری و حریم خصوصی در هوشمندسازی شهر

ابعاد	تهدیدهای نهایی
تهدیدهای امنیت سایبری	افزایش حجم تبادلات دیجیتال (CS1)، افزایش برنامه‌های کاربردی و ارتباطات از طریق تلفن همراه (CS2)، وجود محصولات نرم‌افزاری و سخت‌افزاری با آسیب‌پذیری‌های امنیتی (CS3)، جاسوسی سایبری (CS4)، نفوذ ویروس و بدافزار به سیستم‌های شهر هوشمند (CS5)، چالش قانون‌گذاری (CS6)، API ها و پروتکل‌های ناامن (CS7)، حملات ناشی از عدم پذیرش سرویس DoS (CS8)، فقدان ارتباط امن (CS9)، اختلال در زیرساخت‌های مهم (CS10)، امنیت فضای ابری (CS11)
چالش‌های حریم خصوصی	تهدیدهای حریم خصوصی در داده‌کاوی و به اشتراک‌گذاری داده‌ها (P1)، تهدیدهای حریم خصوصی در داده‌های Mashup (P2)، استراق سمع (P3)، خطر محرمانگی و یکپارچگی (P4)، خطر کلاه‌برداری و درز داده‌ها (P5)، جعل هویت (P6)، اطلاعات ساختگی (P7)، استفاده ثانویه از داده‌های جمع‌آوری‌شده (P8)، جعل آدرس اینترنتی (P9)، حمله به یکپارچگی داده‌ها (P10)

نظر به آن‌که تهدیدهای نهایی امنیت سایبری و حریم خصوصیِ شناسایی‌شده از درجه اهمیت یکسانی در بروز مخاطره برای شهر هوشمند برخوردار نبودند، لذا در فاز بعدی به‌منظور محاسبه اوزان این تهدیدها از روش تصمیم‌گیری چندمعیاره بهترین-بدترین فازی، بهره گرفته شد. مطابق با الگوریتم این روش و ضمن نظرسنجی از اعضاء کمیته خبرگان، «چالش قانون‌گذاری (CS6)» و «جعل آدرس اینترنتی (P9)» به ترتیب به‌عنوان بهترین و بدترین تهدید تعیین گردیدند. در این مقاله منظور از بهترین و بدترین تهدید، مهم‌ترین و کم‌اهمیت‌ترین تهدید از منظر خبرگان می‌باشد. به عبارتی تهدیدی که آثار زیان بار فراوانی داشته باشد به‌عنوان مهم‌ترین (بهترین) تهدید و تهدیدی که آثار زیان‌بار کمتری داشته باشد به‌عنوان کم‌اهمیت‌ترین (بدترین) تهدید شناخته می‌شود. سپس بردار ارجحیت مهم‌ترین تهدید نسبت به دیگر تهدیدها و نیز ارجحیت تهدیدها نسبت به بدترین تهدید تعیین شد. برای تعیین این بردار از خبرگان خواسته شد تا ارجحیت مهم‌ترین تهدید را نسبت به سایر تهدیدها و نیز ارجحیت تهدیدها نسبت به بدترین تهدید در هوشمندسازی شهر را با استفاده از جدول راهنمای (۳) مشخص کنند.

جدول (۳). واژه‌های کلامی و اعداد فازی متناظر [۱۵]

واژه‌های کلامی	عدد فازی متناظر
اهمیت برابر (EI)	(1, 1, 1)
اهمیت ضعیف (WI)	(2/3, 1, 3/2)
نسبتاً مهم (FI)	(3/2, 2, 5/2)
خیلی مهم (VI)	(5/2, 3, 7/2)
کاملاً مهم (AI)	(7/2, 4, 9/2)

پس از گردآوری نظرات خبرگان و محاسبه میانگین نظرات، نتایج به‌صورت جدول (۴) حاصل گردید.

جدول (۴). میانگین نظرات خبرگان پیرامون ارجحیت تهدیدهای نهایی در هوشمندسازی شهر

ابعاد	تهدیدها	بهترین تهدید (CS6)	بدترین تهدید (P9)
تهدیدهای امنیت سایبری	افزایش حجم تبادلات دیجیتال (CS1)	(۱/۷۳,۲/۲,۲/۷)	(۲/۱۷,۲/۶,۳/۰۵)
	افزایش برنامه‌های کاربردی و ارتباطات از طریق تلفن همراه (CS2)	(۱/۸۳,۲/۳,۲/۸)	(۲/۲۵,۲/۷,۳/۲)
	وجود محصولات نرم‌افزاری و سخت‌افزاری با آسیب‌پذیری‌های امنیتی (CS3)	(۲/۱۲,۲/۶,۳/۱)	(۲/۳,۲/۷,۳/۱)
	جاسوسی سایبری (CS4)	(۳,۳/۵,۴)	(۲/۹,۳/۴,۳/۹)
	نفوذ ویروس و بدافزار به سیستم‌های شهر هوشمند (CS5)	(۲/۶۲,۳/۱,۳/۶)	(۲/۹۲,۳/۴,۳/۹)
	چالش قانون‌گذاری (CS6)	(۱,۱,۱)	(۳/۰۵,۳/۵,۳/۹۵)
	APIها و پروتکل‌های نا امن(CS7)	(۲/۰۳,۲/۵,۳)	(۲/۴۵,۲/۹,۳/۳۵)
	حملات ناشی از عدم پذیرش سرویس DoS (CS8)	(۱/۸۳,۲/۳,۲/۸)	(۲/۵۲,۳,۳/۵)
	فقدان ارتباط امن (CS9)	(۲/۱۲,۲/۵,۲/۹)	(۲/۶۵,۳/۱,۳/۵۵)
	اختلال در زیرساخت‌های مهم (CS10)	(۲/۷,۳/۲,۳/۷)	(۲/۶۷,۳/۱,۳/۵۵)
	امنیت فضای ابری (CS11)	(۲/۴۷,۲/۹,۳/۳۵)	(۲/۸,۳/۳,۳/۸)
چالش‌های حریم خصوصی	تهدیدهای حریم خصوصی در داده‌کاوی و به اشتراک‌گذاری داده‌ها (P1)	(۲/۲۳,۲/۷,۳/۲)	(۲/۱۷,۲/۶,۳/۰۵)
	تهدیدهای حریم خصوصی در داده‌های Mashup (P2)	(۱/۶۵,۲/۱,۲/۶)	(۱/۷۷,۲/۲,۲/۶۵)
	استراق سمع (P3)	(۲/۲۲,۲/۷,۳/۲)	(۲/۲۲,۲/۷,۳/۲)
	خطر محرمانگی و یکپارچگی (P4)	(۲/۷,۳/۲,۳/۷)	(۲/۷۲,۳/۲,۳/۷)
	خطر کلاه‌برداری و درز داده‌ها (P5)	(۲/۱۲,۲/۶,۳/۱)	(۲/۳۵,۲/۸,۳/۲۵)
	جعل هویت (P6)	(۲/۴۲,۲/۹,۳/۴)	(۲/۵۵,۳,۳/۴۵)
	اطلاعات ساختگی (P7)	(۲,۲/۵,۳)	(۲/۱۲,۲/۶,۳/۱)
	استفاده ثانویه از داده‌های جمع‌آوری‌شده (P8)	(۱/۹۷,۲/۴,۲/۸۵)	(۲/۰۷,۲/۵,۲/۹۵)
	جعل آدرس اینترنتی (P9)	(۳/۰۵,۳/۵,۳/۹۵)	(۱,۱,۱)
	حمله به یکپارچگی داده‌ها (P10)	(۲/۰۲,۲/۵,۳)	(۲/۲۲,۲/۷,۳/۲)

با جایگذاری مقادیر حاصله در مدل پایه برنامه‌ریزی خطی روش FBWM، مدل بسط‌یافته از ۶۳ متغیر و ۱۸۴ محدودیت در نرم‌افزار GAMS وارد شد. با حل مدل، مقدار بهینه بردار اوزان تهدیدها و تابع هدف به‌صورت $(W_1^*, W_2^*, \dots, W_n^*)$ و ξ^* در جدول (۵) گردید. با توجه به آن‌که طبق استاندارد، شاخص سازگاری (CI) برای $\tilde{a}_{BW} = (2/5, 3, 3/5)$، مقدار ۶/۶۹ و برای $\tilde{a}_{BW} = (3/5, 4, 4/5)$ مقدار ۸/۰۴ در نظر گرفته شده است و ازآنجاکه در این پژوهش $\tilde{a}_{BW} = (3/05, 3/5, 3/95)$ حاصل گردید، لذا با قطعی سازی این عدد، مقدار $a_{BW} = 3/5$ حاصل گردید که با محاسبه مقدار میانگین ۶/۶۹ و ۸/۰۴، مقدار شاخص سازگاری ۷/۳۶ حاصل گردید که حاکی از سازگاری بالای نتایج و پایایی پرسشنامه دوم است. $\tilde{a}_{BW}$ بیانگر ارجحیت فازی بهترین تهدید نسبت به بدترین تهدید است.

جدول (۵). اوزان نهایی تهدیدهای امنیت سایبری و حریم خصوصی شهر در گذار به‌سوی شهر هوشمند

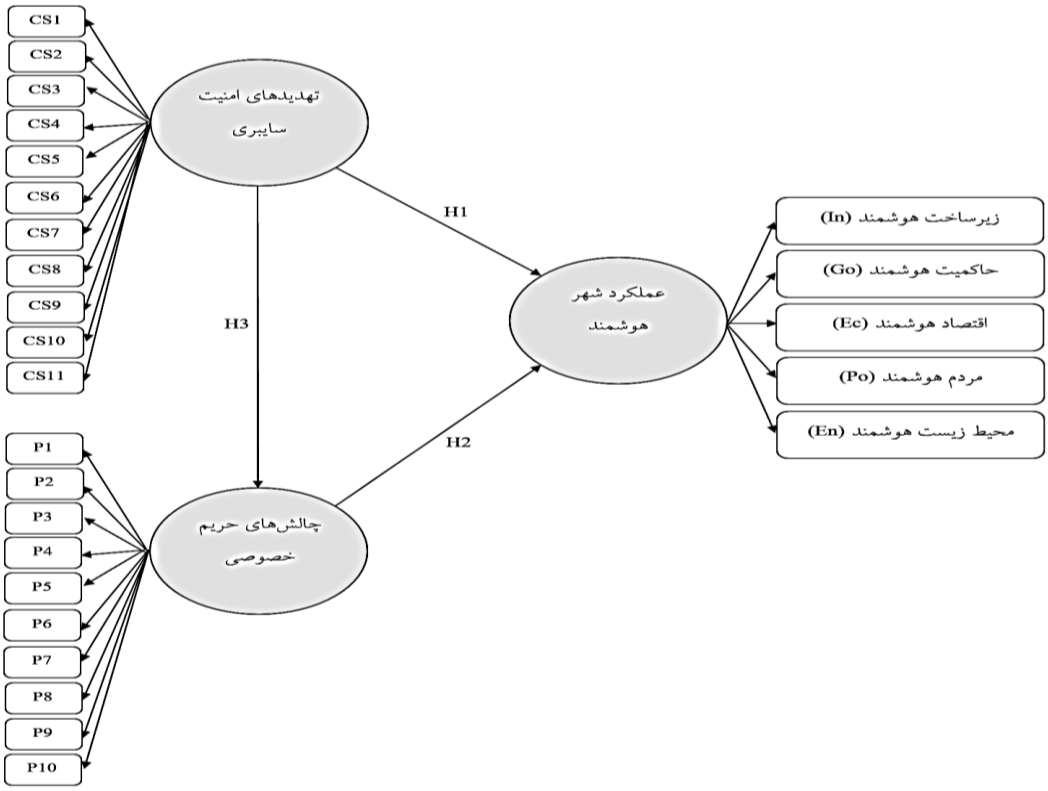
تهدیدها	$\tilde{w}_j^*$	w_j^*
افزایش حجم تبادلات دیجیتال (CS1)	(۰/۰۳۳,۰/۰۴۳,۰/۰۶۲)	۰/۰۴۴۵
افزایش برنامه‌های کاربردی و ارتباطات از طریق تلفن همراه (CS2)	(۰/۰۳۴,۰/۰۴۴,۰/۰۶۳)	۰/۰۴۵۵
وجود محصولات نرم‌افزاری و سخت‌افزاری با آسیب‌پذیری‌های امنیتی (CS3)	(۰/۰۳۶,۰/۰۴۷,۰/۰۶۴)	۰/۰۴۸۰
جاسوسی سایبری (CS4)	(۰/۰۳۵,۰/۰۴۲,۰/۰۵۱)	۰/۰۴۲۳
نفوذ ویروس و بدافزار به سیستم‌های شهر هوشمند (CS5)	(۰/۰۳۸,۰/۰۴۶,۰/۰۶)	۰/۰۴۷۰
چالش قانون‌گذاری (CS6)	(۰/۰۹,۰/۰۹۴,۰/۰۹۸)	۰/۰۹۴۰
APIها و پروتکل‌های ناامن(CS7)	(۰/۰۳۶,۰/۰۵۱,۰/۰۶۹)	۰/۰۵۱۵
حملات ناشی از عدم پذیرش سرویس (CS8) DoS	(۰/۰۳۸,۰/۰۴۷,۰/۰۶۸)	۰/۰۴۹۰
فقدان ارتباط امن (CS9)	(۰/۰۳۹,۰/۰۵۳,۰/۰۷۱)	۰/۰۵۳۷
اختلال در زیرساخت‌های مهم (CS10)	(۰/۰۳۳,۰/۰۴۲,۰/۰۵۶)	۰/۰۴۲۸
امنیت فضای ابری (CS11)	(۰/۰۳۸,۰/۰۴۸,۰/۰۶۶)	۰/۰۴۹۳
تهدیدهای حریم خصوصی در داده‌کاوی و به اشتراک‌گذاری داده‌ها (P1)	(۰/۰۳۴,۰/۰۴۴,۰/۰۶۱)	۰/۰۴۵۲
تهدیدهای حریم خصوصی در داده‌های Mashup (P2)	(۰/۰۳۵,۰/۰۴۴,۰/۰۵۷)	۰/۰۴۴۷
استراق سمع (P3)	(۰/۰۳۵,۰/۰۴۵,۰/۰۶۲)	۰/۰۴۶۲
خطر محرمانگی و یکپارچگی (P4)	(۰/۰۳۴,۰/۰۴۳,۰/۰۵۷)	۰/۰۴۳۸
خطر کلاه‌برداری و درز داده‌ها (P5)	(۰/۰۳۳,۰/۰۴۷,۰/۰۶۶)	۰/۰۴۷۸
جعل هویت (P6)	(۰/۰۳۴,۰/۰۴۴,۰/۰۵۹)	۰/۰۴۴۸
اطلاعات ساختگی (P7)	(۰/۰۳۱,۰/۰۴۷,۰/۰۶۳)	۰/۰۴۷۰
استفاده ثانویه از داده‌های جمع‌آوری‌شده (P8)	(۰/۰۳۸,۰/۰۴۵,۰/۰۵۹)	۰/۰۴۶۲
جعل آدرس اینترنتی (P9)	(۰/۰۱۹,۰/۰۲,۰/۰۲۱)	۰/۰۲۰۰
حمله به یکپارچگی داده‌ها (P10)	(۰/۰۳۷,۰/۰۴۸,۰/۰۶۴)	۰/۰۴۸۸
مقدار ξ^*	۱/۲۸۶	
شاخص سازگاری	۷/۳۶	
نرخ سازگاری	۰/۱۷۵	

با توجه به نتایج حل مدل برنامه‌ریزی خطی روش بهترین بدترین، ملاحظه شد که سه تهدید چالش قانون‌گذاری (CS6)، فقدان ارتباط امن (CS9) و APIها و پروتکل‌های ناامن (CS7) به‌عنوان مهم‌ترین تهدیدها در هوشمندسازی شهر تعیین شدند. همان‌طور که ملاحظه می‌شود، این سه شاخص متعلق به بُعد «تهدیدهای امنیت سایبری» بوده که حاکی از اهمیت این بُعد از منظر خبرگان در پیاده‌سازی موفقیت‌آمیز زیرساخت‌ها و نظام شهر هوشمند در است. در میان چالش‌های حریم خصوصی نیز «حمله به یکپارچگی داده‌ها (P10)» به‌عنوان چالشی مهم در هوشمندسازی شهر شناسایی شد.

با توجه به مفاهیم مطروحه پیرامون موضوعات هوشمندسازی شهری، امنیت و تهدیدهای سایبری و حریم خصوصی در فضای شهر هوشمند و نیز نظریات پژوهشگران پیرامون این حوزه، چالش‌های امنیت سایبری به‌عنوان متغیر برون‌زا و حریم خصوصی در شهر هوشمند به‌عنوان متغیر درون‌زای متأثر از امنیت سایبری ملاک مطالعه بر روی متغیر وابسته عملکرد شهر هوشمند قرار گرفتند. ضمن بررسی‌های به‌عمل‌آمده از مطالعات پیشین و جمع‌بندی آن‌ها، ملاحظه شد که اغلب این مطالعات مصادیق سنجش عملکرد شهر هوشمند را در مؤلفه‌هایی (یا به بیان دیگر، فناوری‌ها یا برنامه‌های کاربردی) چون زیرساخت هوشمند، حاکمیت هوشمند، اقتصاد هوشمند، مردم هوشمند و محیط‌زیست هوشمند مدنظر قرار می‌دادند [۱۶، ۳۲-۲۵]. با استناد بر این مؤلفه‌ها، متغیرهای آشکار این سازه از مدل مفهومی نیز احصاء گردید. متغیرهای آشکار دو سازه تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در مسیر هوشمندسازی شهر نیز در جدول (۲) به دست آمد. بدین ترتیب مدل مفهومی مفروض این پژوهش در سنجش تأثیر تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی بر روی عملکرد شهر هوشمند به‌صورت شکل (۲) حاصل گردید. در این مدل، متغیر «تهدیدهای امنیت سایبری» به‌عنوان متغیر پنهان برون‌زا (متغیر مستقل) و متغیر «چالش‌های حریم خصوصی» و «عملکرد شهر هوشمند» به‌عنوان متغیر پنهان درون‌زا (متغیر وابسته) فرض شده است. این مدل برگرفته از سه فرضیه اصلی و سه فرضیه فرعی به شرح ذیل است:

- فرضیه اصلی ۱ (H1): در گذار آن شهر به‌سوی شهر هوشمند، «تهدیدهای امنیت سایبری» بر «عملکرد شهر هوشمند» تأثیر منفی و معنی‌داری دارد.
- فرضیه اصلی ۲ (H2): در گذار آن شهر به‌سوی شهر هوشمند، «چالش‌های حریم خصوصی» بر «عملکرد شهر هوشمند» تأثیر منفی و معنی‌داری دارد.

- فرضیه اصلی ۳ (H3): در گذار آن شهر به‌سوی شهر هوشمند، «تهدیدهای امنیت سایبری» بر «چالش‌های حریم خصوصی» تأثیر مثبت و معنی‌داری دارد.
- فرضیه فرعی ۱: در گذار آن شهر به‌سوی شهر هوشمند، گویه‌های (CS1) تا (CS11) متغیرهای آشکار «تهدیدهای امنیت سایبری» را تبیین می‌کنند.
- فرضیه فرعی ۲: در گذار آن شهر به‌سوی شهر هوشمند، گویه‌های (P1) تا (P10) متغیرهای آشکار «چالش‌های حریم خصوصی» را تبیین می‌کنند.
- فرضیه فرعی ۳: در گذار آن شهر به‌سوی شهر هوشمند، «زیرساخت هوشمند، حاکمیت هوشمند، اقتصاد هوشمند، مردم هوشمند و محیط‌زیست هوشمند» متغیرهای آشکار «عملکرد شهر هوشمند» را تبیین می‌کنند.



شکل (۲). مدل مفهومی پژوهش

به‌منظور آزمون مدل مفهومی مفروض، در این پژوهش از رویکرد مدل‌سازی معادلات ساختاری به شرح ذیل استفاده شده و تحلیل‌های لازم در سه بخش ۱) برازش مدل‌های اندازه‌گیری، ۲) برازش مدل ساختاری و ۳) برازش کلی مدل (اندازه‌گیری و ساختاری) انجام گرفته است. به‌این‌ترتیب که ابتدا، از صحت روابط موجود در مدل‌های اندازه‌گیری با استفاده از معیارهای پایایی و روایی اطمینان حاصل کرده و سپس به بررسی و تفسیر روابط موجود در بخش ساختاری پرداخته و در مرحله پایانی نیز برازش کلی مدل پژوهش بررسی می‌شود.

به‌منظور پیش‌آزمون داده‌های گردآوری‌شده پیرامون سنجش نرمال بودن آن‌ها در برازش مدل، آزمون کلوموگروف-اسمیرنوف پیاده‌سازی شد. نتایج این آزمون حاکی از حصول میزان معنی‌داری کمتر از ۰/۰۵ برای تمامی گویه‌های پرسشنامه سوم بود که فرض صفر در خصوص نرمال بودن داده‌ها را رد کرده و غیر نرمال بودن داده‌ها را نشان داد. لذا روش حداقل مربعات جزئی در مدل‌سازی معادلات ساختاری این پژوهش که قابلیت پیاده‌سازی برای نمونه آماری با اندازه کوچک و داده‌های غیر نرمال داشت، استفاده شد.

در ادامه، در برازش مدل‌های اندازه‌گیری، پایایی و روایی سازه‌های پژوهش بر اساس سه معیار ۱) پایایی هریک از گویه‌ها، ۲) پایایی ترکیبی[1] هریک از سازه‌ها و ۳) میانگین واریانس استخراج شده[2] (AVE) موردبررسی قرار گرفت و نتایج به‌صورت جداول (۶) و (۷) حاصل گردید.

[1] Composite Reliability
[2] Average Variance Extracted

جدول (۶). مقادیر بارهای عاملی متغیرهای آشکار (گویه‌ها) در مدل اندازه‌گیری

متغیرهای آشکار	تهدیدهای امنیت سایبری	چالش‌های حریم خصوصی	عملکرد شهر هوشمند
CS1	۰/۶۹	...	...
CS2	۰/۵۰	...	...
CS3	۰/۴۵	...	...
CS4	۰/۹۰	...	...
CS5	۰/۷۰	...	...
CS6	۰/۹۱	...	...
CS7	۰/۷۲	...	...
CS8	۰/۷۱	...	...
CS9	۰/۵۹	...	...
CS10	۰/۴۵	...	...
CS11	۰/۷۵	...	...
Ec	...	...	۰/۹۳
En	...	...	۰/۳۶
Go	...	...	۰/۵۲
In	...	...	۰/۹۴
Po	...	...	۰/۵۰
P1	...	۰/۹۲	...
P2	...	۰/۵۸	...
P3	...	۰/۸۰	...
P4	...	۰/۶۱	...
P5	...	۰/۵۸	...

نتایج حاصل از تحلیل عاملی تأییدی و بررسی ضرایب بارهای عاملی در جدول بالا نشان می‌دهد که اغلب متغیرهای آشکار (گویه‌ها) با سطح همبستگی بالا و تعداد معدودی نیز با سطح همبستگی متوسط رو به بالا به‌خوبی متغیرهای پنهان را اندازه‌گیری می‌کنند. برای تعیین پایایی هریک از سازه‌ها، علاوه بر معیار سنتی آلفای کرونباخ، از معیار مدرن‌تر پایایی ترکیبی نیز استفاده شد. برتری این معیار نسبت به ضریب آلفای کرونباخ این است که پایایی سازه‌ها نه به‌صورت مطلق بلکه با توجه به همبستگی شاخص‌هایشان با یکدیگر محاسبه می‌شود. لذا برای سنجش بهتر پایایی، هردو معیار به کار برده شد. مقدار پایایی ترکیبی بالای ۰/۷ برای هر سازه، نشان از پایداری درونی مناسب برای مدل‌های اندازه‌گیری داشته و مقدار کمتر از ۰/۶ عدم وجود پایایی را نشان می‌دهد. همان‌طور که در جدول (۷) ملاحظه می‌شود، مقادیر پایایی ترکیبی برای سازه‌های مدل مفهومی بالاتر از ۰/۸ به دست آمده است. پس از بررسی معیار پایایی، دومین معیار برازش مدل‌های اندازه‌گیری روایی همگرا است. معیار میانگین واریانس استخراج‌شده (AVE) که میزان همبستگی هر سازه از مدل مفهومی را با گویه‌های (متغیرهای آشکار) مربوط به خود بررسی می‌کند، معرف روایی همگرا است. طبق تجربه و اظهارات پژوهشگران، مقدار ۰/۴ به بالای این معیار، کافی محسوب می‌شود (جدول ۷).

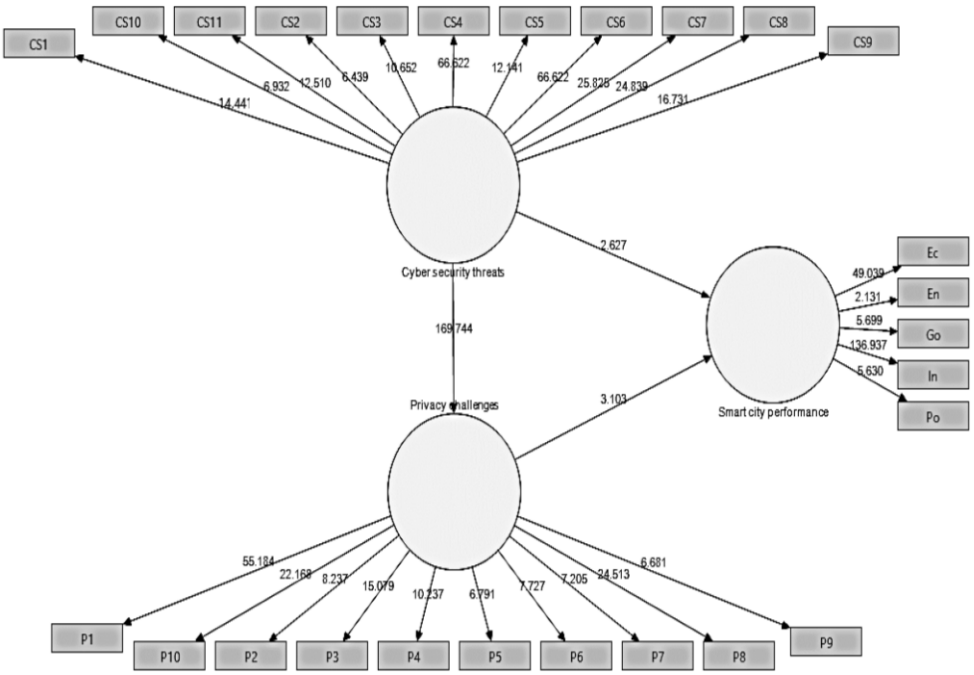
جدول (۷). معیارهای کلی کیفیت برازش مدل اندازه‌گیری

متغیرهای پنهان	عملکرد شهر هوشمند	چالش‌های حریم خصوصی	تهدیدهای امنیت سایبری
میانگین واریانس استخراجی	۰/۴۸	۰/۴۵	۰/۴۷
پایایی ترکیبی	۰/۸	۰/۷۹	۰/۸۶
ضریب تعیین (R^2)	۰/۷۲۷	۰/۹۲۵	...
آلفای کرونباخ	۰/۷۵	۰/۷۴	۰/۷۹
مقادیر اشتراکی	۰/۴۸	۰/۴۵	۰/۴۷
افزونگی	۰/۳۵	۰/۴۱	...

با حصول نتایج مقادیر بارهای عاملی و ضرایب آلفای کرونباخ، پایایی ترکیبی و AVE از طریق تحلیل‌ها و خروجی نرم‌افزار و ازآنجاکه مقادیر هریک از معیارهای مذکور برای هریک از متغیرهای پنهان بیشتر از حدنصاب و آستانه تعریف شده است؛ بنابراین، می‌توان مناسب بودن وضعیت پایایی و روایی همگرای مدل پژوهش را تأیید کرد. سومین معیار سنجش برازش مدل‌های اندازه‌گیری در تحلیل‌های PLS، روایی واگرا است که با روش بارهای عاملی متقابل[1] و آزمون فورنل و لارکر[2] بررسی می‌شود. ازآنجاکه مقادیر همبستگی بین بارهای عاملی اغلب گویه‌های (شاخص‌های) مربوط به هریک از سازه‌های تهدیدهای امنیت سایبری، چالش‌های حریم خصوصی و عملکرد شهر هوشمند با یکدیگر بیشتر از میزان همبستگی آن شاخص با سازه دیگری غیر از سازه خود بود؛ بنابراین، این امر واگرایی مناسب مدل را با استفاده از روش اول نشان داد. در روش دوم بررسی روایی واگرایی، میزان رابطه یک سازه با شاخص‌هایش در مقایسه رابطه آن سازه با سایر سازه‌هاست؛ به‌طوری‌که روایی واگرای قابل‌قبول یک مدل حاکی از آن است که یک سازه در مدل تعامل بیشتری با شاخص‌های خود دارد تا با سازه‌های دیگر. با بررسی موارد مطروحه، روایی واگرایی مدل اندازه‌گیری تأیید شد.

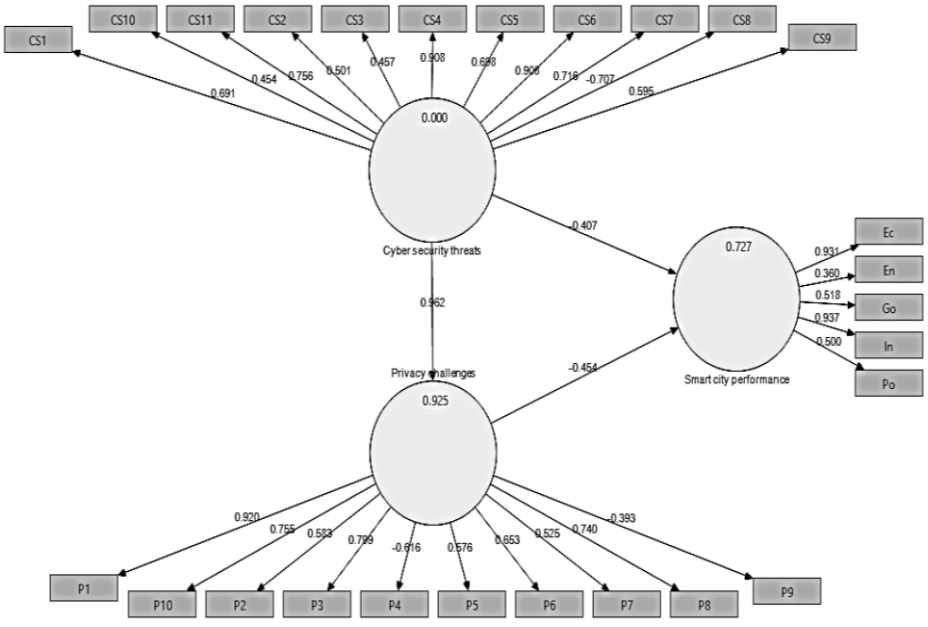
در ادامه، مدل ساختاری روابط بین متغیرهای پنهان بررسی شده و معیارهای ضرایب معناداری t-values، معیار مجذور R یا R^2 و معیار استون-گیزر[3] (Q^2) برای برازش مدل ساختاری تعیین شدند. در شکل (۳) مقادیر t برای ارزیابی بخش ساختاری مدل نشان داده شده است. با توجه به این‌که تمام اعداد واقع بر مسیرها بالاتر از ۱/۹۶ هستند، این مطلب حاکی از معنادار بودن مسیرها، مناسب بودن مدل ساختاری و تأیید تمام فرضیه‌های اصلی پژوهش است.

1. Cross-Loadings
2. Fornell and Larcker
3. Stone-Geisser Criterion



شکل (۳). مقادیر معناداری t برای ارزیابی بخش ساختاری مدل مفهومی پژوهش

با توجه به مفاد جدول (۷) و نیز شکل (۴) مقدار ضریب تعیین نیز برای هریک از متغیرهای پنهان محاسبه گردید. با توجه به این‌که مقدار R^2 برای سازه‌های چالش‌های حریم خصوصی و عملکرد شهر هوشمند به ترتیب ۰/۹۲۵ و ۰/۷۲۷ است؛ لذا مناسب بودن برازش مدل ساختاری تأیید می‌شود.



شکل (۴). ضرایب مسیر، مقادیر بارهای عاملی و R^2

در ادامه، معیار استون-گیزر (Q^2) که قدرت پیش‌بینی مدل را مشخص می‌سازد محاسبه شد. مقدار Q^2 در مورد سازه‌های درون‌زای مدل پژوهش یعنی سازه تهدیدهای امنیت سایبری مقدار ۰/۳۷۵، سازه چالش‌های حریم خصوصی مقدار ۰/۳۲۸ و برای عملکرد شهر هوشمند مقدار ۰/۲۹ حاصل گردید که بیانگر روابط مناسب میان سازه‌های درون‌زای مدل با یکدیگر است. در نهایت برای بررسی برازش مدل کلی که هر دو بخش مدل اندازه‌گیری و ساختاری را کنترل می‌کند، معیار نیکویی برازش[1] (GoF) موردسنجش قرار گرفت و مقدار آن، ۰/۵۰۶ حاصل گردید که این عدد نشان از برازش کلی قوی مدل دارد.

[1] Goodness of Fit

با بررسی ضرایب معناداری t هریک از مسیرها و نیز ضرایب استانداردشده بار عاملی مربوط به مسیرها، فرضیه‌های تحقیق آزموده می‌شوند. با توجه به اینکه مقدار t ضرایب هریک از مسیرها در شکل (۳) بیشتر از ۱/۹۶ بود؛ بنابراین، در سطح اطمینان ۹۵ درصد، مسیرهای پیش‌بینی‌شده تهدیدهای امنیت سایبری عملکرد شهر هوشمند، چالش‌های حریم خصوصی-عملکرد شهر هوشمند و تهدیدهای امنیت سایبری-چالش‌های حریم خصوصی معنا دارند. جدول (۸) نتایج آزمون مدل ساختاری پژوهش را به‌تفصیل نشان می‌دهد. با توجه به شکل (۴) و جدول (۸) ملاحظه می‌شود که تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی هر دو دارای تأثیر معنادار و منفی بر عملکرد شهر هوشمند هستند به‌عبارت‌دیگر افزایش این تهدیدها و چالش‌ها، عملکرد شهر هوشمند را به مخاطره خواهد انداخت. از سوی دیگر تهدیدهای امنیت سایبری دارای تأثیر مثبت و معناداری بر چالش‌های حریم خصوصی است به‌عبارت‌دیگر این تهدیدها می‌تواند زمینه‌ساز به خطر افتادن حریم خصوصی و تقویت چالش‌های آن شود. مقادیر مربوط به ضریب مسیرها در مدل نهایی تحقیق نشان می‌دهد که تهدیدهای امنیت سایبری، ۴۰/۷ درصد و چالش‌های حریم خصوصی، ۴۵/۴ درصد از تغییرات مربوط به متغیر عملکرد شهر هوشمند را به‌طور مستقیم تبیین می‌کنند. از سوی دیگر، ضریب ۰/۹۶۲ نیز نشان می‌دهد که متغیر تهدیدهای امنیت سایبری به‌طور غیرمستقیم و از طریق متغیر میانجی چالش‌های حریم خصوصی نیز به میزان ۴۳/۶ درصد بر متغیر وابسته عملکرد شهر هوشمند تأثیر دارد. از سوی دیگر با توجه به مقدار ضریب تعیین R^2، ملاحظه می‌شود که متغیرهای تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی درمجموع، ۷۲/۷ درصد از تغییرات مربوط به متغیر وابسته عملکرد شهر هوشمند را پیش‌بینی کرده و مابقی آن، یعنی ۲۷/۳ درصد تغییرات، مربوط به سایر عواملی است که در این پژوهش بررسی نشده‌اند.

جدول (۸). نتایج آزمون مدل پژوهش

	مسیر	ضریب مسیر	مقدار معناداری t	نتیجه فرضیه
فرضیه‌های اصلی	تهدیدهای امنیت سایبری---> عملکرد شهر هوشمند	-۰/۴۰۷	۲/۶۲۷	تأیید
	چالش‌های حریم خصوصی---> عملکرد شهر هوشمند	-۰/۴۵۴	۳/۱۰۳	تأیید
	تهدیدهای امنیت سایبری---> چالش‌های حریم خصوصی	۰/۹۶۲	۱۶۹/۷۴۴	تأیید

	متغیر پنهان	متغیر آشکار	مقدار معناداری t	نتیجه فرضیه
فرضیه‌های فرعی	تهدیدهای امنیت سایبری	CS1	۱۴/۴۴	تأیید
		CS2	۶/۴۳۹	تأیید
		CS3	۱۰/۶۵۲	تأیید
		CS4	۶۶/۶۲۲	تأیید
		CS5	۱۲/۱۴۱	تأیید
		CS6	۶۶/۶۲۲	تأیید
		CS7	۲۵/۸۲۵	تأیید
		CS8	۲۴/۸۳۹	تأیید
		CS9	۱۶/۷۳۱	تأیید
		CS10	۶/۹۳۲	تأیید
		CS11	۱۲/۵۱	تأیید
	چالش‌های حریم خصوصی	P1	۵۵/۱۸۴	تأیید
		P2	۸/۲۳۷	تأیید
		P3	۱۵/۰۷۹	تأیید
		P4	۱۰/۲۳۷	تأیید
		P5	۶/۷۹۱	تأیید
		P6	۷/۷۲۷	تأیید
		P7	۷/۲۰۵	تأیید
		P8	۲۴/۵۳۱	تأیید
		P9	۶/۶۸۱	تأیید
		P10	۲۲/۱۶۸	تأیید
	عملکرد شهر هوشمند	Ec	۴۹/۰۳۹	تأیید
		En	۲/۱۳۱	تأیید
		Go	۵/۶۹۹	تأیید
		In	۱۳۶/۹۳۷	تأیید
		Po	۵/۶۳	تأیید

۵- بحث و نتیجه‌گیری

پژوهش حاضر با هدف ارائه چارچوبی جهت شناسایی و ارزیابی تهدیدهای امنیت سایبری و حریم خصوصی و بررسی تأثیر آن‌ها بر عملکرد شهر هوشمند در آن شهر نگارش یافت. صرف‌نظر از قابلیت‌های شهر هوشمند و تسهیلاتی که برای شهروندان به ارمغان می‌آورد، تهدیدهای امنیت سایبری و حریم خصوصی، ازجمله نگرانی‌های کلیدی در فضای این شهرها هستند که مطالعه و بررسی جامع‌نگر و کارشناسی را برای مواجهه با آن‌ها می‌طلبد. امنیت سایبری شهر هوشمند مسئله مهمی است که با دغدغه‌های امنیتی در خصوص فناوری، کاربردها، زیرساخت و داده‌ها یا اطلاعات گره خورده است. چالش‌های حریم خصوصی نیز معضلی دیگر برای شهروندان در فضای شهر هوشمند محسوب می‌شود. با مروری بر پژوهش‌های پیشین داخلی ملاحظه شد که تعداد محدود پژوهش‌های انجام شده در این حوزه بیشتر تمرکز خود را بر مفاهیم اولیه و گردآوری مطالب در قالب پژوهش مروری قرار داده‌اند. در میان پژوهش‌های خارجی نیز بخشی از

پژوهش‌ها تمرکز خود را بر ارائه مطالب نوین در این حوزه و نیز آسیب‌شناسی پیاده‌سازی شهر هوشمند در کشورهای توسعه‌یافته در قالب مطالعه موردی و ارائه درس آموخته‌های آن پرداخته‌اند و بخشی دیگر از پژوهش‌ها نیز صرفاً تا مرحله شناسایی چالش‌های امنیتی شهر هوشمند پیش رفته و بدون ارزیابی و تحلیل دقیق آن‌ها به ارائه راهکارهای پراکنده در جهت مواجهه با این چالش‌ها اکتفا کرده‌اند. نوآوری پژوهش حاضر از نظر موضوعی و ارتباط با نیاز جامعه دانشگاهی و اولویت‌های پیش‌بینی‌شده در اسناد بالادستی نظام و نیز از نظر روش‌شناسی پژوهش و ابزار تحلیل داده‌ها قابل‌توجه است. در این پژوهش، الگوی ارزیابی و آسیب‌شناسی تهدیدهای امنیت سایبری و حریم خصوصی در قالب روشی آمیخته از رویکرد تصمیم‌گیری فازی و نیز مدل‌سازی معادلات ساختاری انجام گرفت که به‌نوبه خود منحصربه‌فرد است. یافته‌های این پژوهش حاکی از شناسایی ۱۱ تهدید امنیت سایبری و ۱۰ چالش حریم خصوصی در گذار آن شهر به‌سوی شهر هوشمند بود که از میان آن‌ها چالش قانون‌گذاری، فقدان ارتباط امن و APIها و پروتکل‌های ناامن به‌عنوان مهم‌ترین تهدیدهای امنیت سایبری و حمله به یکپارچگی داده‌ها به‌عنوان مهم‌ترین چالش حریم خصوصی شهروندان تعیین شدند. یافته‌های مذکور حاکی از آن بود که توجه صرف به تهدیدها و چالش‌های متداول در فرآیند هوشمندسازی شهری (که غالباً مبتنی بر مؤلفه‌های اقتصادی هستند) به‌تنهایی تحلیل دقیق و جامع‌نگری را ارائه نمی‌نماید. به‌علاوه، تعیین تهدیدهای مطروحه به‌عنوان مهم‌ترین تهدیدهای امنیت سایبری و حریم خصوصی در هوشمندسازی آن شهر، دال بر بی‌اهمیتی سایر تهدیدها نبوده، بلکه هر تهدید حسب اوزان حاصله از درجه اهمیت متفاوتی در بروز چالش در مسیر هوشمندسازی آن شهر برخوردار بود. یافته‌های این پژوهش در شناسایی و اولویت‌بندی دقیق تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی پیش روی هوشمندسازی آن شهر ، ضمن گشایش دریچه تحقیقاتی جدید برای پژوهشگران در افزایش ابعاد عملکردی شهر هوشمند (مانند بررسی زندگی هوشمند، تحرک هوشمند، بهداشت و درمان هوشمند و غیره) و تکمیل و بالندگی سایر وجوه پژوهش حاضر، در ایجاد آگاهی و بینش لازم برای سیاست‌گذاران، در اتخاذ راهبردها و تصمیمات مقتضی مرتبط با پیاده‌سازی پروژه هوشمندسازی آن شهر نیز الهام‌بخش است.

ضمن مطالعه و آسیب‌شناسی به‌عمل‌آمده پیرامون تأثیر تهدیدهای امنیت سایبری و حریم خصوصی بر عملکرد شهر هوشمند ملاحظه شد که تهدیدهای امنیت سایبری زمینه‌ساز به مخاطره افتادن حریم خصوصی شهروندان و تضعیف عملکرد شهر هوشمند در پنج بخش زیرساخت هوشمند، حاکمیت هوشمند، اقتصاد هوشمند، مردم هوشمند و محیط‌زیست هوشمند می‌باشند. وجود چالش در حریم خصوصی شهروندان نیز به‌نوبه خود تقویت‌کننده تضعیف عملکرد شهر هوشمند بود. لذا مسئولان ذی‌ربط و سازمان‌های متولی امر لازم است در مسیر هوشمندسازی آن شهر با توجه به ضرایب عاملی حاصله برای هریک از تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی، تدابیر لازم فنی، مدیریتی، مالی، فکری و انسانی را برای مواجهه با آن‌ها اتخاذ نموده و برنامه مدیریت ریسک جامعی را در این خصوص تدوین نمایند. راه‌حل بسیاری از این چالش‌های امنیت سایبری و حریم خصوصی به در طرح‌ریزی پروفایل ریسک شهر هوشمند، مدل‌های امنیتی لایه‌ای، تکنیک‌های رمزنگاری، شفافیت داده‌ها و برنامه‌های اقدامات اضطراری قرار دارد. این راه‌حل‌ها، زمانی مؤثرتر واقع می‌شوند که از رویکرد جامعی برای امنیت و حریم خصوصی بهره ببرند. شهرهای هوشمند از انبوهی دستگاه به‌هم‌پیوسته تشکیل شده است، لذا لازم است که راه‌حل‌های امنیتی و حریم خصوصی به‌جای مجموعه برنامه‌های دفاعی مجزا، حول یک نظام دفاعی متمرکز شوند. از منظر فنی نیز متخصصین، تکنسین‌ها، برنامه نویسان و کارشناسان مجرب در حوزه شبکه، فناوری اطلاعات و ارتباطات و علوم کامپیوتری لازم است در مقابله با تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی اقدامات فنی چون: ارائه امنیت فیزیکی برای تجهیزات، کابل شبکه و سرورها، رمزگذاری ترافیک شبکه با الگوریتم‌های متقارن پایدار، استفاده از ارتباطات ایمن چون VPN برای دسترسی از راه دور، ایمن‌سازی شبکه‌های بی‌سیم با پروتکل‌های WPA2، استفاده از سرورهای متمرکز تأیید اعتبار و صدور مجوز، استقرار فایروال‌ها در هر نقطه انتقال و استفاده از روش‌های احراز هویت قوی مانند کارت‌های بیومتریک یا کارت‌های هوشمند در فهرست برنامه خود قرار دهند. وجود سیستم‌های آسیب‌پذیر امنیتی شهر هوشمند که می‌تواند در دسترس کاربران ناآگاه قرار داشته باشد، از فقدان بسترهای موردنیاز قانونی و حقوقی نشئت می‌گیرد. وجود خلأ قانونی و نبود قانون و آئین‌نامه‌های نظارتی در حوزه اقدامات خرابکارانه سایبری (همچون جنگ سایبری) به‌طور محسوس وجود دارد. ترتیب اثر مثبت در این حوزه، نیازمند راهبرد کلان و جامعی است که بتواند اقدامات هماهنگ دولت، بخش خصوصی و شهروندان را تحت پوشش قرار دهد. از سوی دیگر، فرهنگ‌سازی در رعایت جنبه‌های قانونی امنیت، به‌کارگیری استانداردهای ایمنی و پیروی از توصیه‌های آژانس‌های امنیت سایبری ملی و بازیگردانان امنیت فناوری اطلاعات و ترویج شیوه‌های مناسب استفاده از فناوری‌های اطلاعات و ارتباطات و تدوین استانداردهای عملکردی ازجمله

راهکارها و راهبردهای مؤثر در قانون‌گذاری در این فضاست. رشد فزاینده داده‌ها و دستگاه‌ها در شهرهای هوشمند، مسائل زیادی را برای حریم خصوصی شهروندان ایجاد کرده‌اند. مهاجمان داخلی با نفوذ به داده‌های بزرگ قادرند تا حریم خصوصی صاحبان داده را استنباط و نقض نمایند. برای شناسایی آن‌ها لازم است تا قابلیت ردیابی را افزایش داده و به نهاد ثالث معتمدی را به‌عنوان ناظر و حسابرس اتخاذ کرد. در این راستا، اهتمام و همکاری میان شهرداری‌ها، نهادهای قانون‌گذار، صنعت، دانشگاه و کسب‌وکارها برای تنظیم سیاست‌ها و آئین‌نامه‌های حریم خصوصی ضروری هستند. به‌علاوه، حفظ حریم خصوصی داده‌ها، دسترس‌پذیری و مدیریت باید به‌طور هم‌زمان انجام گیرند.

در انجام پژوهش حاضر پژوهشگر با محدودیت‌هایی مواجه بود که مهم‌ترین آن دشواری‌های موجود در گردآوری داده‌های پژوهش به‌واسطه شیوع ویروس کرونا بود. با عنایت به اینکه مؤلفه‌های مدل ارائه‌شده، ۷۲/۷ درصد تغییرات مربوط به متغیر وابسته عملکرد شهر هوشمند را تبیین و ۲۷/۳ درصد مابقی مربوط به سایر عوامل و مؤلفه‌هایی است که بررسی نشده‌اند، لذا، پیشنهاد می‌شود در پژوهش‌های آتی لازم است عوامل دیگری نیز موردمطالعه و شناسایی قرار گیرند. همچنین، با توجه به فقدان پشتوانه نظری برای حمایت از پژوهش عملکرد شهر هوشمند، انجام مطالعات کیفی مبتنی بر رویکرد نظریه داده بنیان در این حوزه کاملاً احساس می‌شود. بااین‌حال، نتایج و یافته‌های پژوهش حاضر و مواردی ازاین‌دست می‌تواند گام نخست برای ساخت نظریه در زمینهٔ عملکرد شهر هوشمند به شمار آیند.

۶- مراجع

[1] R. Khatoun, & S. Zeadally, "Cybersecurity and privacy solutions in smart cities," IEEE Communications Magazine, Vol. 55, No. 3, pp. 51-59, 2017.

[2] A. Meijer, & M. P. R. Bolívar, "Governing the smart city: a review of the literature on smart urban governance," International Review of Administrative Sciences, Vol. 82, No. 2, pp. 392-408, 2016.

[3] A. AlDairi, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies," Procedia Computer Science, Vol. 109, pp. 1086-1091, 2017.

[4] M. Benkő, & T. Germán, "Crime prevention aspects of public space renewal in Budapest," Journal of Place Management and Development, Vol. 9, No. 2, pp. 191-209, 2016.

[5] K. M. Lord, & T. Sharp, "America's Cyber Future: Security and Prosperity in the Information Age," Washington, DC: Center for a New American Security, Vol. 1, 2011.

[6] S. Ijaz, M. A. Shah, A. Khan, & M. Ahmed, "Smart cities: A survey on security concerns," International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, pp. 612-625, 2016.

[7] M. Nikoo Goftar Nategh, "A Cyber Security Architecture Model for Intelligent Public Transportation Systems in Smart Cities," 16th International Conference on Transportation and Traffic Engineering, Tehran, 2016. (In Persian)

[8] A. M. Hamzeh, & M. A. Kazeruni, "Smart Cities: Component Analysis, Challenges and Strategies Review," 3rd International Conference on Applied Research in Structural Engineering and Construction Management, Tehran, 2019. (In Persian)

[9] A. Taklo Bighash, & M. Shayan Fard, "Challenges and Strategies for Security and Privacy in Smart City Applications," Fourth National Conference on New Ideas in Engineering, Rasht, 2019. (In Persian)

[10] A. Alibasic, R. Al Junaibi, Z. Aung, W. L. Woon, & M. A. Omar, "Cybersecurity for Smart Cities: A Brief Review," In International Workshop on Data Analytics for Renewable Energy Integration, pp. 22-30, 2016.

[11] M. A. Hasbini, T. Eldabi, & A., Aldallal, "Investigating the information security management role in smart city organisations," World Journal of Entrepreneurship, Management and Sustainable Development, Vol. 14, No. 1, pp. 86-98, 2018.

[12] I. S. Farahat, A. S. Tolba, M. Elhoseny, & W. Eladrosy, "Data Security and Challenges in Smart Cities". In Security in Smart Cities: Models, Applications, and Challenges, pp. 117-142, 2019.

[13] J. Laufs, H. Borrion, & B. Bradford, "Security and the smart city: A systematic review," Sustainable Cities and Society, Vol. 169, pp. 1-18, 2020.

[14] Y. C. Wu, R. Sun, & Y. J. Wu, "Smart city development in Taiwan: From the perspective of the information security policy," Sustainability, Vol. 12, No. 7, pp. 1-18, 2020.

[15] S. Guo, & H. Zhao, "Fuzzy best-worst multi-criteria decision-making method and its applications," Knowledge-Based Systems, Vol. 121, pp. 23-31, 2017.

[16] M. Shah Mohammadi Ardabili, H. Hamidi, & M. H. Zahedi, "A Review of Challenges, Risks and Cyber Security in Smart Cities," 2nd International Conference on New Developments in Management, Economics and Accounting, Tehran, 2018. (In Persian)

[17] A. Khalilipour Roknabadi, & Y. Noor Ali Vand, "Cyber threats and their impact on national security," Quarterly Journal of Strategic Studies,

Vol. 56, No. 15, 196-167, 2012. (In Persian)

[18] S. Alromaihi, W. Elmedany, & C. Balakrishna, "Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications," 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 140-145, 2018.

[19] A. R. Berkel, P. M. Singh, & M. J. van Sinderen, "An Information Security Architecture for Smart Cities," In International Symposium on Business Modeling and Software Design, pp. 167-184, 2018.

[20] T, Braun, B. C. Fung, F. Iqbal, & B. Shah, "Security and privacy challenges in smart cities," Sustainable cities and society, Vol. 39, pp. 499-507, 2018.

[21] Z. A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, ..., and N. Syed, "Future challenges for smart cities: Cyber-security and digital forensics," Digital Investigation, Vol. 22, pp. 3-13, 2017.

[22] V. L. Thing, "Cyber security for a smart nation. In Computational Intelligence and Computing Research (ICCIC)," IEEE International Conference on, pp. 1-3, 2014.

[23] A. Arabo, "Cyber security challenges within the connected home ecosystem futures," Procedia Computer Science, Vol. 61, pp. 227-232, 2015.

[24] J. N. Pelton, & I. B. Singh, "Cyber Defense in the Age of the Smart City," In Smart Cities of Today and Tomorrow, pp. 67-83, 2019.

[25] S. Soltani, H. Mahroghi, & S. A. Hosseini Sano, "Introducing smart city technologies and examining their cyber security challenges," the first national smart city conference, Qom, 2016. (In Persian)

[26] P. Sanati, "Security and Privacy in Smart City Applications: Challenges and Solutions," International Congress of Engineering Sciences and Sustainable Urban Development, Danish Polytechnic University, Denmark, 2018. (In Persian).

[27] V. Albino, U. Berardi, and R. M. Dangelico, "Smart cities: Definitions, dimensions, performance, and initiatives," Journal of urban technology, Vol. 22, No. 1, pp. 3-21, 2015.

[28] L. Shen, Z. Huang, S. W. Wong, S. Liao, and Y. Lou, A "holistic evaluation of smart city performance in the context of China," Journal of Cleaner Production, Vol. 200, pp. 667-679, 2018.

[29] M. Airaksinen, I.P., Seppä, A. Huovila, H. M. Neumann, B. Iglar, & P. Bosch, "Smart city performance measurement framework CITYkeys," In 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC), pp. 718-723, 2017.

[30] P. Lombardi, S. Giordano, H. Farouh, & W. Yousef, "Modelling the smart city performance," Innovation: The European Journal of Social Science Research, Vol. 25, No. 2, pp. 137-149, 2012.

[31] R. Wall, S. Stavropoulos, J. Edelenbos, & F. Pajević, "Evaluating the performance of smart cities in the global economic network," In Transforming city governments for successful smart cities, No. 8, pp. 87-113, 2015.

[32] S. Chauhan, N. Agarwal, & A. K. Kar, "Addressing big data challenges in smart cities: a systematic literature review," Info, Vol. 18, No. 4, pp. 73-90, 2016.