Journal of Business Intelligence Management Studies
Vol. 10, No.38, Winter 2022
ims.atu.ac.ir
DOI: 10.22054/ims.2021.59476.1925

ATU PRESS

Original Research
Received: 2021-03-02 Revised: 2021-08-17 Accepted: 2021-09-17
ISSN: 1735/112X eISSN: 2538-2527

Identification and Assessment of Cyber Security and Privacy Challenges in the Transition of Tehran Metropolis to Smart City under Uncertainty

Nazila Seddighi — Ph.D. student, Information Technology Management, Faculty of Management and Accounting, Qazvin Islamic Azad University, Qazvin, Iran

Mohammad Reza Sanaei * — Assistant Professor, Department of Information Technology Management, Faculty of Management and Accounting, Qazvin Islamic Azad University, Qazvin, Iran

Reza Ehtesham Rasi — Assistant Professor, Department of Industrial Management, Faculty of Management and Accounting, Qazvin Islamic Azad University, Qazvin, Iran

Abstract

The growing trend of the world towards new technologies and the formation of smart cities, despite their capabilities and benefits, has raised serious concerns about cyber security threats and citizens' privacy challenges. Tehran is no exception to this rule in the transition to a smart city. The present paper, in a descriptive survey study, aims to provide a framework for managing cyber security and privacy challenges in the transition of Tehran to a smart city. In this research, these challenges are identified by in-depth library studies as well as the implementation of fuzzy Delphi method among a sample of organizational experts (including ten senior managers and relevant officials of the Ministry of Communication and Information Technology, Tehran Municipality Information and Communication Technology Organization, and cyber police). Moreover, the degree of importance (weight) of each challenge is determined by the Fuzzy Best-Worst method (FBWM). The findings of this study indicated the high

* Corresponding Author: mohamadrezasanaei44@yahoo.com

How to Cite: Seddighi, N., Sanaei, M. R., Ehtesham Rasi, R. (2022). Identification and Assessment of Cyber Security and Privacy Challenges in the Transition of Tehran Metropolis to Smart City under Uncertainty, *Journal of Business Intelligence Management Studies*, 10(38), 109-136.

capability of the proposed framework in identifying and accurately weighting these challenges under uncertainty.

Keywords: Smart City, Cyber security, Privacy, Fuzzy Delphi Method, Fuzzy Best-Worst Method.

مقاله پژوهشی
تاریخ ارسال: ۱۳۹۹/۱۲/۱۲
تاریخ بازنگری: ۱۴۰۰/۰۵/۲۶
تاریخ پذیرش: ۱۴۰۰/۰۶/۲۶
ISSN: 1735/112X
eISSN: 2538-2527

مطالعات مدیریت کسب و کار هوشمند
سال دهم، شماره ۳۸، زمستان ۱۴۰۰، ص ۱۰۹ تا ۱۳۶
ims.atu.ac.ir
DOI: 10.22054/ims.2021.59476.1925

شناسایی و ارزیابی چالش‌های امنیت سایبری و حریم خصوصی در گذار کلان‌شهر تهران به‌سوی شهر هوشمند تحت شرایط عدم قطعیت

نازیلا صدیقی — دانشجوی دکتری مدیریت فناوری اطلاعات، دانشگاه آزاد اسلامی واحد قزوین، قزوین، ایران.

محمدرضا ثنائی * — استادیار گروه مدیریت فناوری اطلاعات، دانشگاه آزاد اسلامی واحد قزوین، قزوین، ایران.

رضا احتشام راثی — استادیار گروه مدیریت صنعتی، دانشگاه آزاد اسلامی واحد قزوین، قزوین، ایران.

چکیده

گذار موفقیت‌آمیز کلان‌شهر تهران به‌سوی شهر هوشمند درگرو شناسایی و ارزیابی تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی و اتخاذ تدابیر مقتضی در قبال چالش‌های اولویت‌دار است. این مقاله در قالب پژوهشی توصیفی-پیمایشی و با هدف ارائه چارچوبی جهت مدیریت چالش‌ها و تهدیدهای مذکور در مسیر هوشمندسازی شهر تهران نگارش یافته است. در پژوهش حاضر، این چالش‌ها با مطالعات عمیق کتابخانه‌ای و نیز نظرسنجی به روش دلفی فازی از خبرگان سازمانی، که به شیوه هدفمند انتخاب شدند، شناسایی شده و درجه اهمیت هریک از آن‌ها به روش بهترین-بدترین فازی تعیین می‌گردد. یافته‌های پژوهش حاکی از قابلیت بالای چارچوب پیشنهادی در شناسایی و ارزیابی دقیق این چالش‌ها و نیز تعیین سه چالش «چالش قانون‌گذاری»، «فقدان ارتباط امن» و «API ها و پروتکل‌های ناامن» به‌عنوان کلیدی‌ترین چالش‌های امنیت سایبری و حریم خصوصی در مسیر هوشمندسازی شهر تهران بود که به‌تناسب، اقدامات پیشگیرانه و اصلاحی در خصوص هریک از آن‌ها ارائه شد.

کلیدواژه‌ها: شهر هوشمند، امنیت سایبری، حریم خصوصی، روش دلفی فازی، روش بهترین-بدترین فازی.

* نویسنده مسئول: mohamadrezasanaei44@yahoo.com

مقدمه

با جنبش جهانی به‌سوی شهرنشینی و استفاده گسترده از فناوری‌های اطلاعات، مفهوم شهرهای هوشمند به وجود آمد که توجه زیادی از پژوهشگران را در سال‌های اخیر به خود جلب کرده است (Khatoun & Zeadally, 2017; Meijer & Bolívar, 2016). هدف نخست شهرهای هوشمند اصلاح و بهبود سبک زندگی مردم، تشویق توسعه بدون تأثیر بر منابع نسل‌های آینده (توجه به توسعه پایدار) و ایجاد پیشرفت در کارکردهای شهری است (Manchanda et al., 2020). شهرهای هوشمند علی‌رغم مزایا، دارای خطرات پنهان ازجمله درز اطلاعات، تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی و حملات سایبری مخرب هستند (Chen et al., 2020). با توجه به عدم قطعیت‌های موجود در دنیای واقعی و اهمیت شناسایی حملات سایبری، امنیت سایبری شهرهای هوشمند آینده و شبکه‌های هوشمند آن‌ها بسیار حیاتی است (Mohammadpourfard et al., 2021). توسعه امنیت سایبری فعلی، همگام با پذیرش مشتاقانه فناوری‌های شهرهای هوشمند نبوده، لذا طراحی صحیح مبتنی بر روش‌های یادگیری عمیق برای حفاظت از خطرات سایبری شهرهای هوشمند الزامی است (Chen et al., 2020). در کنار موضوع امنیت سایبری، مسائل مربوط به حریم خصوصی را می‌توان به سه دسته ارتباطات، فردی و کسب‌وکار تقسیم نمود. 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 (Ijaz et al., 2016).

شهر تهران نیز در مسیر هوشمندشدن از این موارد مستثنا نیست. تأمین امنیت در شهر هوشمند درگرو شناسایی و ارزیابی تهدیدات و چالش‌ها و اتخاذ تدابیر و راهکارهای مقتضی در قبال چالش‌های اولویت‌دار است. با توجه به تأثیر تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در کاهش کارایی هوشمندسازی شهر تهران پژوهش حاضر درصدد ارائه چارچوبی متدلوژیک جهت شناسایی و تحلیل تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در گذار کلان‌شهر تهران به‌سوی شهر هوشمند است. بر این

اساس، سایر بخش‌های این مقاله به شرح ذیل سازمان‌دهی شده است. در بخش بعدی، مروری بر پیشینه پژوهش انجام گرفته و چارچوب نظری اولیه چالش‌ها احصاء خواهد شد. سپس روش‌شناسی پژوهش و چارچوب متدلوژیک پیشنهادی ارائه می‌شود. در ادامه، چارچوب پیشنهادی جهت شناسایی و ارزیابی تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در مسیر هوشمندسازی شهر تهران پیاده‌سازی می‌شود. بخش پایانی مقاله نیز به بحث و نتیجه‌گیری اختصاص یافته است.

مروری بر پیشینه پژوهش و چارچوب نظری

با توجه به نوپا بودن حوزه مطالعاتی پژوهش حاضر و علی‌رغم قابلیت‌ها و کارکردهای منحصربه‌فرد شهرهای هوشمند، تعداد پژوهش‌های داخلی و خارجی که به‌طور اخص به بررسی پیاده‌سازی موفق شهر هوشمند و چالش‌های پیش روی آن پرداخته باشد، محدود بوده که در ادامه مهم‌ترین آن‌ها معرفی می‌شوند. شاه‌محمدی اردبیلی و همکاران (۱۳۹۷) در پژوهشی، تحلیلی جامع از آسیب‌پذیری‌ها و چشم‌انداز خطرات مربوط به چهار بخش اصلی شهر هوشمند مشتمل بر شبکه‌های هوشمند، سیستم‌های خودکار ساختمان، وسایل نقلیه هوایی بدون سرنشین، وسایل نقلیه هوشمند با قابلیت فنّاوری حسگر اینترنت اشیاء و فضای ابری ارائه کردند و مطالبی نیز راجع به فناوری‌ها و پلتفرم‌ها مطرح نمودند. تکلو بیغش و شایان فرد (۱۳۹۸) به بررسی امنیت و حریم خصوصی در برنامه‌های کاربردی شهر هوشمند پرداختند. بدین‌صورت که ابتدا برنامه‌های کاربردی امیدوارکننده شهر هوشمند و معماری آن را معرفی کردند. سپس چالش‌های حفظ حریم خصوصی و امنیت در این برنامه‌های کاربردی را مورد بحث قرار دادند تا با شناخت و اتخاذ تدابیر سازنده در مواجهه با آن‌ها به بهبود مراقبت‌های بهداشتی هوشمند، حمل‌ونقل، انرژی هوشمند پرداخته شود. الروماهی و همکاران[1] (۲۰۱۸) موضوع امنیت و حریم خصوصی در حوزه شهر هوشمند را برای برنامه‌های مراقبت بهداشتی مورد تجزیه‌وتحلیل قرار دادند. در این راستا، از یک‌سو

1. Alromaihi et al.

مروری بر برنامه‌های کاربردی مختلف اینترنت اشیاء و آسیب‌پذیری‌های سایبری آن‌ها انجام دادند و از سوی دیگر، ارزیابی جامعی بر رویکردهای مقابله با مشکل حملات سایبری ارائه کردند. سپس فنونی را برای مقابله با حملات سایبری در تجهیزات اینترنت اشیاء مربوط به مراقبت‌های بهداشتی در شهر هوشمند ارائه نموده و انواع مختلفی از حملات و نیازهای امنیتی مرتبط با آن‌ها را تشریح نمودند. برکل و همکاران[1] (۲۰۱۸) در پژوهش خود به تلفیق تحلیل تهدیدها و مدل‌سازی معماری سازمانی و بررسی و کاهش این چالش‌ها با نگاه جامع‌نگرانه پرداختند. آن‌ها معماری امنیت اطلاعات را ارائه نمودند که می‌توانست به ذی‌نفعان پروژه‌های شهر هوشمند برای ساخت شهرهای هوشمند ایمن‌تر کمک نماید. گوندوز و دس[2] (۲۰۲۰) تهدیدها و راه‌حل‌های احتمالی شبکه هوشمندِ مبتنی بر اینترنت اشیاء را مورد تجزیه‌وتحلیل قرار دادند. آن‌ها بر انواع حملات سایبری تمرکز کرده و با ژرف‌نگری به بررسی وضعیت امنیت سایبری شبکه هوشمند پرداخته و به بحث و بررسی آسیب‌پذیری شبکه، اقدامات متقابل علیه حملات و الزامات امنیتی متمرکز شدند. ژائو و همکاران[3] (۲۰۲۱) مطالعه مروری نظام‌مندی روی پژوهش‌های انتشاریافته در بازه زمانی سال‌های ۲۰۰۰ تا ۲۰۱۹ در حوزه شهرهای هوشمند انجام دادند. هدف مطالعه آن‌ها، ایجاد تصویری جامع از پیشرفت‌های پژوهشی در حوزه شهرهای هوشمند و نیز تعیین مسائل مهم و شناسایی خلأهای پژوهشی بود.

با بررسی پژوهش‌های پیشین داخلی، ملاحظه می‌شود که تعداد محدود پژوهش‌های انجام‌شده 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 صرفاً تا مرحله شناسایی چالش‌های امنیتی شهر هوشمند پیش

1. Berkel et al.
2. Gunduz & Das
3. Zhao et al.

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 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 تهران در گذار به‌سوی شهر هوشمند و نیز تعیین درجه اهمیت این چالش‌ها بپردازد. با مروری بر پژوهش‌های مرتبط فهرست تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در شهرهای هوشمند که برگرفته از ترکیب یافته‌های پژوهش‌های پیشین و مبتنی بر تکرار آن‌ها در مقالات بود به‌صورت جدول ۱ احصاء گردید.

جدول ۱. چارچوب نظری اولیه تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی شهرهای هوشمند

ابعاد	تهدیدها و چالش‌ها	مراجع
تهدیدهای امنیت سایبری	۱. افزایش حجم تبادلات دیجیتال ۲. افزایش برنامه‌های کاربردی و ارتباطات از طریق تلفن همراه ۳. افزایش میزان استفاده از هوش مصنوعی در شبکه‌های دیجیتال و ارتباطات ماشین به ماشین ۴. وجود محصولات نرم‌افزاری و سخت‌افزاری با آسیب‌پذیری‌های امنیتی ۵. جنگ و تروریسم سایبری ۶. جاسوسی سایبری ۷. دست‌کاری در داده‌ها و حملات تصنعی ۸. از بین رفتن داده‌ها ۹. نفوذ ویروس و بدافزار به سیستم‌های شهر هوشمند ۱۰. چالش قانون‌گذاری ۱۱. سرقت داده‌ها و اطلاعات و دستگاه‌های فیزیکی ۱۲. ناکارایی سخت‌افزاری و نرم‌افزاری	Khatoun & Zeadally, 2017; Aldairi, 2017; Alromaihi et al., 2018; Berkel et al., 2018; Braun et al., 2018; Baig et al., 2017; Thing, 2014; Arabo, 2015; Pelton & Singh, 2019; شاه‌محمدی اردبیلی و همکاران، ۱۳۹۷؛ خلیلی‌پور رکن‌آبادی و نورعلی وند، ۱۳۹۱

ابعاد	تهدیدها و چالش‌ها	مراجع
	۱۳. چالش در دسترسی داده‌ها ۱۴. API ها و پروتکل‌های ناامن ۱۵. حملات ناشی از عدم پذیرش سرویس DoS ۱۶. خرابی حس‌گرها ۱۷. فقدان ارتباط امن ۱۸. چالش مدیریت و ذخیره‌سازی داده‌ها ۱۹. اختلال در زیرساخت‌های مهم ۲۰. امنیت فضای ابری ۲۱. تهدیدهای هوش مصنوعی	
چالش‌های حریم خصوصی	۱. تهدیدهای حریم خصوصی در داده‌کاوی و به اشتراک‌گذاری داده‌ها ۲. تهدیدهای حریم خصوصی در داده‌های Mashup ۳. استراق سمع ۴. چالش دسترسی به داده‌ها ۵. خطر محرمانگی و یکپارچگی ۶. خطر کلاه‌برداری و درز داده‌ها ۷. جعل هویت ۸. اطلاعات ساختگی ۹. حملات کانال جانبی ۱۰. استفاده ثانویه از داده‌های جمع‌آوری‌شده ۱۱. جعل آدرس اینترنتی ۱۲. حمله به یکپارچگی داده‌ها	Aldairi, 2017; Braun et al., 2018; Baig et al., 2017; Thing, 2014; شاه‌محمدی اردبیلی و همکاران، ۱۳۹۷؛ سلطانی و همکاران، ۱۳۹۵

روش‌شناسی پژوهش و چارچوب متدلوژیک پیشنهادی

پژوهش حاضر ازنظر هدف در زمره پژوهش‌های کاربردی و بر اساس شیوه گردآوری داده‌ها از نوع پژوهش‌های توصیفی- پیمایشی است. جامعه آماری این پژوهش شامل مدیران عالی و مسئولان ذی‌ربط وزارتخانه ارتباطات و فناوری اطلاعات، سازمان فناوری اطلاعات و ارتباطات شهرداری تهران و پلیس فضای تولید و تبادل اطلاعات است. از آن‌جاکه تصمیم‌گیری در خصوص ارزیابی شهر هوشمند و چالش‌های امنیتی این شهر در

سطح راهبردی این ارگان‌ها است و پیش‌بینی می‌شود که داده‌های موردنیاز این پژوهش در اختیار تعداد معدودی از مدیران و کارشناسان سازمانی باشد، لذا ده خبره سازمانی به شیوه نمونه‌گیری هدفمند قضاوتی انتخاب شدند. اطلاعات جمعیت‌شناختی گروه خبرگان این پژوهش در جدول ۲ ارایه شده است.

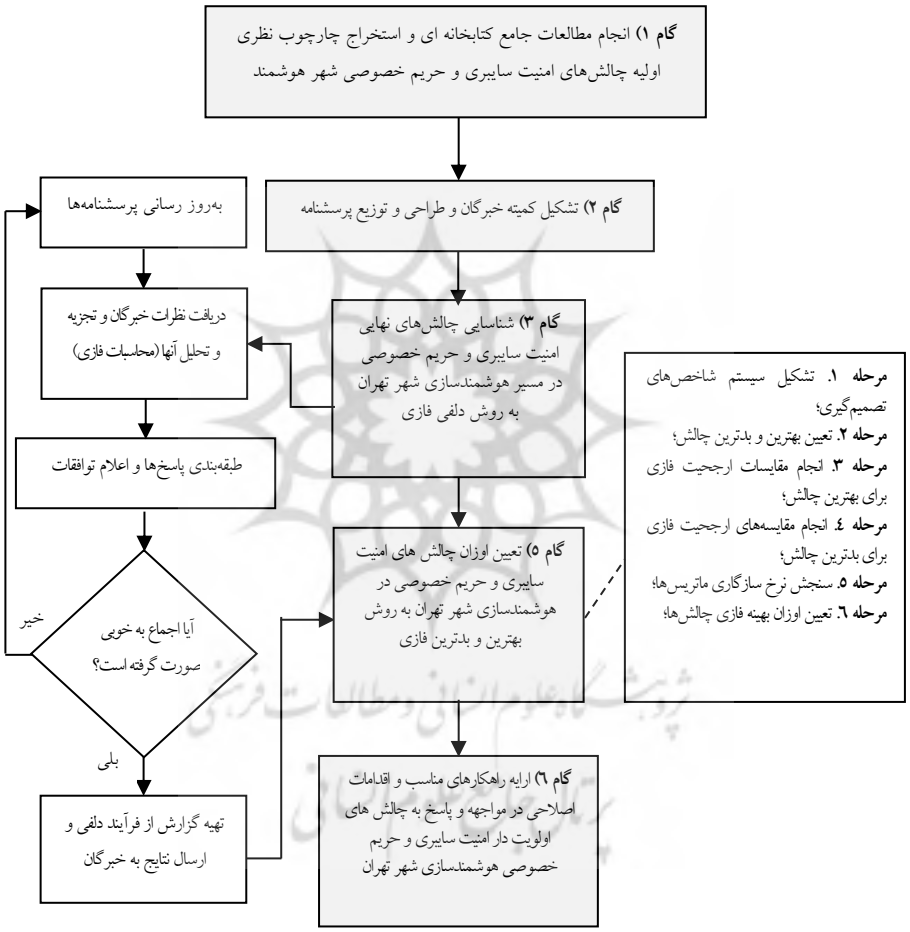
جدول ۲. اطلاعات جمعیت‌شناختی اعضاء پنل خبرگان

خبرگان	میزان تحصیلات	سازمان	سابقه
۱	دکتری	وزارتخانه ارتباطات و فناوری اطلاعات	۹ سال
۲	کارشناسی ارشد		۱۵ سال
۳	کارشناسی		۸ سال
٤	کارشناسی ارشد		۱۰ سال
٥	دانشجوی دکتری		۷ سال
٦	دانشجوی دکتری	سازمان فناوری اطلاعات و ارتباطات شهرداری تهران	۱۲ سال
۷	کارشناسی ارشد		٦ سال
۸	کارشناسی		١٦ سال
۹	کارشناسی ارشد	پلیس فضای تولید و تبادل اطلاعات	۱۱ سال
۱۰	دکتری		۲۰ سال

در این پژوهش، برای گردآوری داده‌ها دودسته پرسشنامه محقق‌ساخته جهت گردآوری داده‌ها طراحی شده است. برای تعیین روایی پرسشنامه‌ها از روش روایی محتوا[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. 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

1. Content Validity

اوزان تهدیدهای امنیت سایبری و چالش‌های حریم خصوص به روش بهترین و بدترین فازی[1] طراحی شده است، برای سنجش پایایی از روش نسبت سازگاری[2] استفاده می‌شود (به‌منظور آشنایی با نحوه محاسبه نسبت سازگاری به پژوهش گو و ژائو[3] (۲۰۱۷) مراجعه شود). شکل ۱، ساختار و مراحل چارچوب متدلوژیک پیشنهادی را به‌صورت شماتیک نمایش می‌دهد.



شکل ۱. چارچوب متدلوژیک پیشنهادی

1. Fuzzy Best Worst Multi-Criteria (F-BWM) method
2. Consistency Ratio (CR)
3. Guo & Zhao

با توجه به چارچوب متدلوژیک پیشنهادی، در این پژوهش برای تجزیه‌وتحلیل داده‌ها در فاز شناسایی و تعیین اوزان چالش‌های امنیت سایبری و حریم خصوصی در هوشمندسازی شهر تهران به ترتیب از روش دلفی فازی[1] و روش بهترین و بدترین فازی و نرم‌افزارهای اکسل و گمز 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.

روش بهترین- بدترین نخستین بار از سوی رضایی[2] (۲۰۱۶) معرفی شد. در این روش، بهترین و بدترین شاخص توسط تصمیم‌گیرنده مشخص می‌شود و مقایسه زوجی بین هر یک از این دو شاخص (بهترین و بدترین) و دیگر شاخص‌ها صورت می‌گیرد؛ سپس یک مسئله حداکثر حداقل برای مشخص کردن وزن شاخص‌های مختلف فرموله و حل می‌شود؛ همچنین در این روش فرمولی برای محاسبه نرخ سازگاری (مطابق با آنچه در بخش ارزیابی پایایی پرسشنامه دوم عنوان شد) به‌منظور بررسی اعتبار مقایسات در نظر گرفته شده است. ازجمله ویژگی‌های برجسته این روش نسبت به سایر روش‌های تعیین وزن مبتنی بر ماتریس‌های مقایسات زوجی می‌توان به نیاز کمتر این روش به داده‌های مقایسه‌ای و حصول مقایسه استوارتر و درنتیجه کسب پاسخ‌های قابل‌اطمینان‌تر به کمک این روش، اشاره کرد. با توجه به کاستی‌های موجود در روش بهترین و بدترین قطعی در مواجهه با عدم قطعیت موجود در قضاوت‌های خبرگان پیرامون مقایسات زوجی ابعاد و شاخص‌های ارزیابی پایداری، گو و ژائو[3] (۲۰۱۷) در مقاله‌ای روش بهترین و بدترین فازی را معرفی کردند. روش بهترین و بدترین فازی، ویژگی‌های برجسته روش قطعی بهترین و

1. Fuzzy Delphi Method (FDM)
2. Rezaei, J.
3. Guo & Zhao

بدترین را به ارث می‌برد و علاوه بر آن، می‌تواند وزن‌های حاصل از شاخص‌ها را به‌جای اعداد قطعی با اعداد فازی به دست آورد. بر مبنای روش پیشنهادی این دو پژوهشگر، الگوریتم حل مسئله تعیین وزن شاخص‌ها شامل پنج گام اصلی مشتمل بر: ۱) تشکیل سیستم شاخص‌های تصمیم‌گیری، ۲) تعیین بهترین (مهم‌ترین) و بدترین (کم‌اهمیت‌ترین) شاخص، ۳) انجام مقایسات ارجحیت فازی برای بهترین شاخص، ۴) انجام مقایسه‌های ارجحیت فازی برای بدترین شاخص، ۵) سنجش نرخ سازگاری ماتریس‌ها و ۶) تعیین اوزان بهینه فازی شاخص‌ها می‌شود (به منظور آشنایی جزئیات این مراحل به پژوهش گو و ژائو[1] (۲۰۱۷) مراجعه شود).

تجزیه‌وتحلیل داده‌ها

با انجام مطالعات کتابخانه‌ای و احصاء چالش‌های امنیت سایبری و حریم خصوصی در جدول ۱، به منظور تناسب‌بخشی و بومی‌سازی چارچوب نظری اولیه مطابق با فضای اجتماعی، اقتصادی، فرهنگی، سیاسی، قانونی (حقوقی) و زیرساخت‌های فناوری حاکم در شهر تهران روش دلفی فازی اتخاذ شد. روش دلفی فازی که تلفیقی از روش دلفی و منطق فازی است، نخستین بار از سوی کافمن و گوپتا[2] در دهه ۱۹۸۰ معرفی گردید که در آن خبرگان با استفاده از اعداد فازی تخمین‌های سه‌نقطه‌ای از پدیده‌ها می‌زدند (Kuo & Chen, 2008; Cheng & Lin, 2002). در این روش، توابع درجه عضویت برای ارائه دیدگاه‌های خبرگان استفاده می‌شود. این امر باعث می‌شود خبرگان مجبور به اصلاح دائمی نقطه‌نظرات خود نباشند. به‌علاوه، ازآنجاکه تمامی دیدگاه‌ها در قالب درجه‌های عضویت تشریح می‌شوند؛ لذا، هیچ اطلاعات مفیدی از دست نخواهد رفت.

با توزیع پرسشنامه نخست، نظرات خبرگان طی راندهای مختلف این روش بر روی تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی، ارائه و تجزیه‌وتحلیل شد. با این توضیح که بر اساس دیدگاه خبرگان سازمانی، سطح پذیرش هر چالش پس از اجماع نظر،

1. Guo & Zhao
2. Kaufman & Gupta

عدد ۵ در نظر گرفته‌شده است و سطح آستانه اختلاف میان دو مرحله نظرسنجی که بیانگر شرط توقف الگوریتم روش دلفی فازی است، ۰/۱ منظور شده است. پس از ارسال پرسشنامه دلفی فازی به خبرگان و تکمیل آن با استفاده از جدول راهنمای ۳، نتایج شمارش نقطه‌نظرات آن‌ها جمع‌آوری شد. با توجه به دیدگاه ۱۰ خبره، دیدگاه تجمیعی آن‌ها با استفاده از میانگین حسابی محاسبه و سپس فازی‌زدایی شد. نتایج نظرات خبرگان در خصوص تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در مسیر گذار شهر تهران به‌سوی شهر هوشمند در مرحله نخست نظرسنجی در جدول ۴ ارائه شده است.

جدول ۳. عبارات کلامی میزان توافق بر وجود تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در هوشمندسازی شهر تهران و اعداد فازی مثلثی متناظر

عبارت کلامی	عدد فازی مثلثی متناظر
خیلی کم	(۳، ۱، ۱)
کم	(۵، ۳، ۱)
متوسط	(۷، ۵، ۳)
زیاد	(۹، ۷، ۵)
خیلی زیاد	(۱۰، ۹، ۷)

جدول ٤. میانگین نظرات خبرگان در مرحله نخست نظرسنجی

بُعد	تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی	میانگین نظرات	میانگین فازی‌زدایی‌شده نظرات
امنیت سایبری	افزایش حجم تبادلات دیجیتال	(۷/۸,۲/۷,۲/۵)	۶/۳۳
	افزایش برنامه‌های کاربردی و ارتباطات از طریق تلفن همراه	(۱/۹,۶/۷,۶/۵)	۶/۷۳
	افزایش میزان استفاده از هوش مصنوعی در شبکه‌های دیجیتال و ارتباطات ماشین به ماشین	(۵/۸,۸/۶,۸/۴)	۵/۸۸
	وجود محصولات نرم‌افزاری و سخت‌افزاری با آسیب‌پذیری‌های امنیتی	(۳/۹,۸/۷,۸/۵)	۶/۹۳
	جنگ و تروریسم سایبری	(۴/۷,۶/۵,۴)	۴/۷۵
	جاسوسی سایبری	(۵/۸,۸/۶,۵)	۵/۹۳

بُعد	تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی	میانگین نظرات	میانگین فازی‌زدایی‌شده نظرات
	دست‌کاری در داده‌ها و حملات تصنعی	(۵/۷,۶/۵,۸/۳)	۴/۶۸
	از بین رفتن داده‌ها	(۱/۸,۴/۶,۴/۴)	۵/۴۸
	نفوذ ویروس و بدافزار به سیستم‌های شهر هوشمند	(۹,۴/۷,۴/۵)	۶/۵
	چالش قانون‌گذاری	(۹,۶/۷,۶/۵)	۶/۷۵
	سرقت داده‌ها و اطلاعات و دستگاه‌های فیزیکی	(۶/۷,۶/۵,۶/۳)	۴/۶
	ناکارایی سخت‌افزاری و نرم‌افزاری	(۳/۷,۴/۵,۴/۳)	۴/۴۳
	چالش در دسترسی داده‌ها	(۱/۸,۴/۶,۴/۴)	۵/۴۸
	API ها تا و پروتکل‌های ناامن	(۷/۸,۷,۵)	۶/۰۸
	حملات ناشی از عدم پذیرش سرویس DoS	(۸/۷,۶,۲/۴)	۵/۱
	خرابی حس‌گرها	(۷,۵,۲/۳)	۴/۰۵
	فقدان ارتباط امن	(۱/۸,۴/۶,۶/۴)	۵/۵۳
	چالش مدیریت و ذخیره‌سازی داده‌ها	(۵/۷,۸/۵,۸/۳)	۴/۸۸
	اختلال در زیرساخت‌های مهم	(۳/۸,۶/۶,۶/۴)	۵/۶۸
	امنیت فضای ابری	(۵/۸,۸/۶,۸/۴)	۵/۸۸
	تهدیدهای هوش مصنوعی	(۴/۷,۶/۵,۸/۳)	۴/۷
حریم خصوصی	تهدیدهای حریم خصوصی در داده‌کاوی و به اشتراک‌گذاری داده‌ها	(۹,۴/۷,۴/۵)	۶/۵
	تهدیدهای حریم خصوصی در داده‌های Mashup	(۵/۸,۸/۶,۸/۴)	۵/۸۸
	استراق سمع	(۸۵,۷,۵)	۶/۱۳
	چالش دسترسی به داده‌ها	(۴/۷,۶/۵,۶/۳)	۴/۶۵
	خطر محرمانگی و یکپارچگی	(۷/۸,۷,۵)	۶/۰۸
	خطر کلاه‌برداری و درز داده‌ها	(۵/۸,۷,۲/۵)	۶/۱۸
	جعل هویت	(۶/۷,۸/۵,۴)	۴/۹
	اطلاعات ساختگی	(۴/۸,۸/۶,۸/۴)	۵/۹
	حملات کانال جانبی	(۸,۲/۶,۴/۴)	۵/۳
	استفاده ثانویه از داده‌های جمع‌آوری‌شده	(۳/۸,۶/۶,۶/۴)	۵/۶۸
	جعل آدرس اینترنتی	(۸,۴/۶,۶/۴)	۵/۵۵
	حمله به یکپارچگی داده‌ها	(۶/۷,۶,۲/۴)	۵/۱۵

در مرحله دوم نظرسنجی، پس از به‌روزرسانی پرسشنامه نخست و اعمال‌نظر هریک از خبرگان در کنار میانگین نظرات، این امکان برای خبرگان مهیا شد تا در صورت صلاحدید بر دیدگاه پیشین خود تجدیدنظر نمایند. مطابق با مرحله نخست، پس از شمارش نتایج نظرات جدید خبرگان، میانگین نظرات محاسبه و فازی زدایی شد. درنهایت، اختلاف میانگین نظرات در این دو مرحله مطابق با جدول ۵ محاسبه شده و شاخص‌هایی که در آن‌ها اختلاف بین میانگین این دو مرحله کمتر از حد آستانه (۰/۱) بود از فرآیند نظرسنجی خارج شده یا در غیر این صورت وارد مرحله سوم نظرسنجی خواهند شد.

جدول ۵. اختلاف دیدگاه خبرگان در مرحله اول و دوم نظرسنجی

بُعد	تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی	میانگین نظرات در مرحله ۱	میانگین نظرات در مرحله ۲	اختلاف نظرات در مراحل ۱ و ۲
امنیت سایبری	افزایش حجم تبادلات دیجیتال	۶/۳۳	۶/۵	۰/۱۷
	افزایش برنامه‌های کاربردی و ارتباطات از طریق تلفن همراه	۶/۷۳	۶/۹۳	۰/۲۰
	افزایش میزان استفاده از هوش مصنوعی در شبکه‌های دیجیتال و ارتباطات ماشین به ماشین	۵/۸۸	۵/۷۳	۰/۱۵
	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
	دست‌کاری در داده‌ها و حملات تصنعی	۴/۶۸	۴/۴۵	۰/۲۳
	از بین رفتن داده‌ها	۵/۴۸	۴/۸۵	۰/۶۳
	نفوذ ویروس و بدافزار به سیستم‌های شهر هوشمند	۶/۵	۵/۷۳	۰/۷۷
	چالش قانون‌گذاری	۶/۷۵	۶/۹۵	۰/۲۰
	سرقت داده‌ها و اطلاعات و دستگاه‌های فیزیکی	۴/۶	۴/۸۸	۰/۲۸
	ناکارایی سخت‌افزاری و نرم‌افزاری	۴/۴۳	۴/۸۸	۰/۴۵

بُعد	تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی	میانگین نظرات در مرحله ۱	میانگین نظرات در مرحله ۲	اختلاف نظرات در مراحل ۱ و ۲
	چالش در دسترسی داده‌ها	۵/۴۸	۴/۴۵	۱/۰۳
	API ها و پروتکل‌های ناامن	۶/۰۸	۶/۱	۰/۰۲
	حملات ناشی از عدم پذیرش سرویس DoS	۵/۱	۵/۴۵	۰/۳۵
	خرابی حس‌گرها	۴/۰۵	۴/۲۵	۰/۲۰
	فقدان ارتباط امن	۵/۵۳	۵/۰۳	۰/۵۰
	چالش مدیریت و ذخیره‌سازی داده‌ها	۴/۸۸	۴/۸۵	۰/۰۳
	اختلال در زیرساخت‌های مهم	۵/۶۸	۵/۸۵	۰/۱۷
	امنیت فضای ابری	۵/۸۸	۵/۸۵	۰/۰۳
	تهدیدهای هوش مصنوعی	۴/۷	۴/۲۵	۰/۴۵
حریم خصوصی	تهدیدهای حریم خصوصی در داده‌کاوی و به اشتراک‌گذاری داده‌ها	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
	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
	جعل هویت	۴/۹	۵/۲	۰/۳۰
	اطلاعات ساختگی	۵/۹	۵/۸۵	۰/۰۵
	حملات کانال جانبی	۵/۳	۴/۸	۰/۵۰
	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

با توجه به نتایج حاصله ملاحظه می‌شود که کمیته خبرگان در ۱۳ چالش که میزان اختلاف‌نظر آن‌ها در راندهای اول و دوم نظرسنجی کمتر از حد آستانه (۰/۱) است، به اجماع نظر رسیده‌اند (چالش‌هایی که در جدول فوق به رنگ تیره نشان داده شده‌اند). لذا فرآیند نظرسنجی برای این چالش‌ها متوقف می‌شود. در میان این چالش‌ها، سه چالش

«جنگ و تروریسم سایبری»، «چالش مدیریت و ذخیره‌سازی داده‌ها» و «چالش دسترسی به داده‌ها»، سطح پذیرش کمتر از ۵ داشته، لذا از چارچوب نظری نهایی تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در مسیر هوشمندسازی شهر تهران خارج شده و ۱۰ چالش دیگر وارد چارچوب نظری نهایی می‌شوند. با تکرار فرآیند نظرسنجی تا چهار مرحله، اجماع نظر بر روی کلیه چالش‌ها شکل گرفت و چارچوب نظری نهایی تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در گذار شهر تهران به سمت شهر هوشمند به‌صورت جدول ۶ حاصل گردید.

جدول ٦. چارچوب نظری نهایی تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در گذار شهر تهران به‌سوی شهر هوشمند

ابعاد	تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی
چالش‌های 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)

ابعاد	تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی
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)

در ادامه، برای تعیین اوزان این تهدیدها و چالش‌ها به روش تصمیم‌گیری چندشاخصه بهترین-بدترین فازی، نخست، پرسشنامه‌ای محقق‌ساخته طراحی و میان اعضاء کمیته خبرگان سازمانی توزیع گردید. در این پرسشنامه به‌منظور تعیین بهترین و بدترین شاخص، هم‌زمان مقدار میانگین پذیرش این شاخص‌ها در روش دلفی فازی و نیز نقطه‌نظر مستقیم اعضاء کمیته خبرگان، ملاک نظر قرار گرفته و دو چالش «چالش قانون‌گذاری (CS6)» و «جعل آدرس اینترنتی (P9)» به ترتیب به‌عنوان بهترین و بدترین شاخص تعیین شدند. سپس بردار ارجحیت مهم‌ترین شاخص نسبت به دیگر شاخص‌ها و نیز ارجحیت شاخص‌ها نسبت به بدترین شاخص تعیین شد. درنهایت از داده‌های جمع‌آوری‌شده میانگین گرفته شد و نتایج به‌صورت جدول ۷ حاصل گردید.

جدول ۷. میانگین نظرات خبرگان پیرامون ارجحیت بهترین (مهم‌ترین) چالش «چالش قانون‌گذاری (CS6)» نسبت به سایر چالش‌ها و سایر چالش‌ها نسبت به بدترین (کم‌اهمیت‌ترین) چالش «جعل آدرس اینترنتی (P9)»

ابعاد	شاخص‌ها	بهترین شاخص	بدترین شاخص
تهدیدهای امنیت سایبری	CS1	(۷/۲,۲/۲,۷۳/۱)	(۰۵/۳,۶/۲,۱۷/۲)
	CS2	(۸/۲,۳/۲,۸۳/۱)	(۲/۳,۷/۲,۲۵/۲)
	CS3	(۱/۳,۶/۲,۱۲/۲)	(۱/۳,۷/۲,۳/۲)

ابعاد	شاخص‌ها	بهترین شاخص	بدترین شاخص
	CS4	(۴,۵/۳,۳)	(۹/۳,۴/۳,۹/۲)
	CS5	(۶/۳,۱/۳,۶۲/۲)	(۹/۳,۴/۳,۹۲/۲)
	CS6	(۱,۱,۱)	(۹۵/۳,۵/۳,۰۵/۳)
	CS7	(۳,۵/۲,۰۳/۲)	(۳۵/۳,۹/۲,۴۵/۲)
	CS8	(۸/۲,۳/۲,۸۳/۱)	(۵/۳,۳,۵۲/۲)
	CS9	(۹/۲,۵/۲,۱۲/۲)	(۵۵/۳,۱/۳,۶۵/۲)
	CS10	(۷/۳,۲/۳,۷/۲)	(۵۵/۳,۱/۳,۶۷/۲)
	CS11	(۳۵/۳,۹/۲,۴۷/۲)	(۸/۳,۳/۳,۸/۲)
چالش‌های حریم خصوصی	P1	(۲/۳,۷/۲,۲۳/۲)	(۵./۳,۶/۲,۱۷/۲)
	P2	(۶/۲,۱/۲,۶۵/۱)	(۶۵/۲,۲/۲,۷۷/۱)
	P3	(۲/۳,۷/۲,۲۲/۲)	(۲/۳,۷/۲,۲۲/۲)
	P4	(۷/۳,۲/۳,۷/۲)	(۷/۳,۲/۳,۷۲/۲)
	P5	(۱/۳,۶/۲,۱۲/۲)	(۲۵/۳,۸/۲,۳۵/۲)
	P6	(۴/۳,۹/۲,۴۲/۲)	(۴۵/۳/۳,۵۵/۲)
	P7	(۳,۵/۲,۲)	(۱/۳,۶/۲,۱۲/۲)
	P8	(۸۵/۲,۴/۲,۹۷/۱)	(۹۵/۲,۵/۲,۰۷/۲)
	P9	(۹۵/۳,۵/۳,۰۵/۳)	(۱,۱,۱)
	P10	(۳,۵/۲,۰۲/۲)	(۳۲,۷/۲,۲۲/۲)

با جایگذاری مقادیر حاصله در مدل برنامه‌ریزی خطی مدل بسط‌یافته از **۶۳** متغیر و **۱۸۴** محدودیت در نرم‌افزار گمز وارد شد. با حل مدل، مقدار بهینه بردار اوزان چالش‌ها و تابع هدف به‌صورت $(W_1^*, W_2^*, \dots, W_n^*)$ و ξ^* در جدول ۸ 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.

جدول ۸. اوزان نهایی تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی شهر تهران در گذار به‌سوی شهر هوشمند

چالش‌ها	$\widetilde{w}_j^*$	w_j^*
CS1	(۰۶۲/۰,۰۴۳/۰,۰/۰۳۳)	۰۴۴۵/۰
CS2	(۰۶۳/۰,۰۴۴/۰,۰۳۴/۰)	۰۴۵۵/۰
CS3	(۰۶۴/۰,۰۴۷/۰,۰۳۶/۰)	۰۴۸۰/۰
CS4	(۰۵۱/۰,۰۴۲/۰,۰۳۵/۰)	۰۴۲۳/۰
CS5	(۰۶/۰,۰۴۶/۰,۰۳۸/۰)	۰۴۷۰/۰
CS6	(۰۹۸/۰,۰۹۴/۰,۰۹/۰)	۰۹۴۰/۰
CS7	(۰۶۹/۰,۰۵۱/۰,۰۳۶/۰)	۰۵۱۵/۰
CS8	(۰۶۸/۰,۰۴۷/۰,۰۳۸/۰)	۰۴۹۰/۰
CS9	(۰۷۱/۰,۰۵۳/۰,۰۳۹/۰)	۰۵۳۷/۰
CS10	(۰۵۶/۰,۰۴۲/۰,۰۳۳/۰)	۰۴۲۸/۰
CS11	(۰۶۶/۰,۰۴۸/۰,۰۳۸/۰)	۰۴۹۳/۰
P1	(۰۶۱/۰,۰۴۴/۰,۰۳۴/۰)	۰۴۵۲/۰
P2	(۰۵۷/۰,۰۴۴/۰,۰۳۵/۰)	۰۴۴۷/۰
P3	(۰۶۲/۰,۰۴۵/۰,۰۳۵/۰)	۰۴۶۲/۰
P4	(۰۵۷/۰,۰۴۳/۰,۰۳۴/۰)	۰۴۳۸/۰
P5	(۰۶۶/۰,۰۴۷/۰,۰۳۳/۰)	۰۴۷۸/۰
P6	(۰۵۹/۰,۰۴۴/۰,۰۳۴/۰)	۰۴۴۸/۰
P7	(۰۶۳/۰,۰۴۷/۰,۰۳۱/۰)	۰۴۷۰/۰
P8	(۰۵۹/۰,۰۴۵/۰,۰۳۸/۰)	۰۴۶۲/۰
P9	(۰۲۱/۰,۰۲/۰,۰۱۹/۰)	۰۲۰۰/۰
P10	(۰۶۴/۰,۰۴۸/۰,۰۳۷/۰)	۰۴۸۸/۰
مقدار $\bar{\xi}^*$	۱/۲۸۶	
شاخص سازگاری	۷/۳۶	
نرخ سازگاری	۰/۱۷۵	

با توجه به نتایج حل مدل برنامه‌ریزی خطی، ملاحظه شد که پنج شاخص چالش قانون‌گذاری (CS6)، فقدان ارتباط امن (CS9)، APIها و پروتکل‌های ناامن (CS7)،

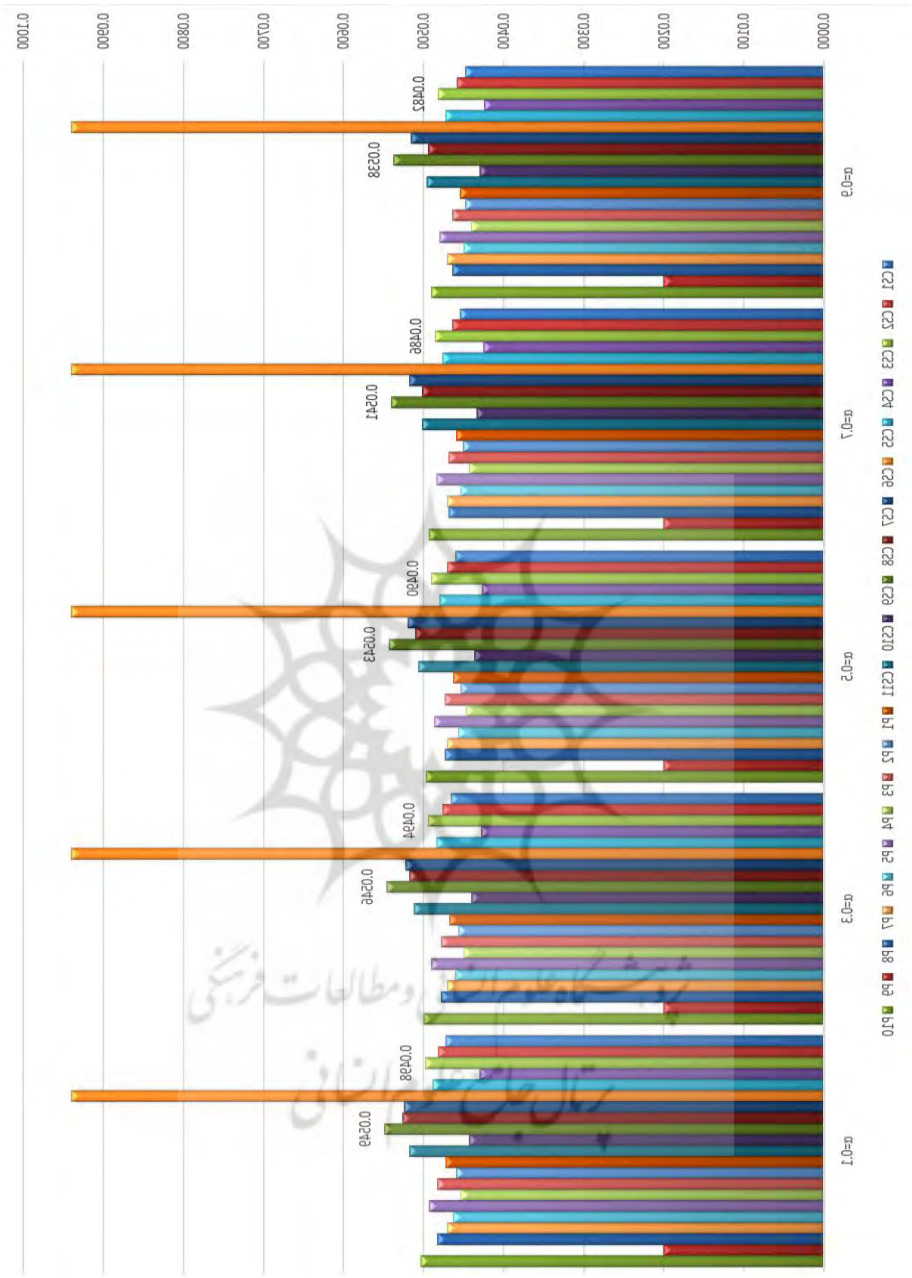
امنیت فضای ابری (CS11) و حملات ناشی از عدم پذیرش سرویس DoS (CS8) به‌عنوان مهم‌ترین چالش‌ها در هوشمندسازی شهر تهران تعیین شدند. این پنج شاخص متعلق به بُعد «تهدیدهای امنیت سایبری» بود که حاکی از اهمیت این بُعد از منظر خبرگان در پیاده‌سازی موفقیت‌آمیز زیرساخت‌ها و نظام شهر هوشمند در تهران است. در میان چالش‌های حریم خصوصی نیز «حمله به یکپارچگی داده‌ها (P10)» به‌عنوان چالشی مهم در هوشمندسازی شهر تهران شناسایی شد. تعیین شاخص‌های مطروحه، دال بر بی‌اهمیتی سایر شاخص‌ها نبوده، بلکه هر شاخص حسب اوزان حاصله از درجه اهمیت متفاوتی در بروز چالش در مسیر هوشمندسازی شهر تهران برخوردار است. به‌علاوه نتایج حاصله برای نرخ سازگاری حاکی از سازگاری بالای نتایج و پایایی پرسشنامه این گام از متدلوژی است.

نظر به آن‌که، تعیین درجه اهمیت تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی به قضاوت‌های ذهنی و ارجحیت‌های اعلامی از سوی اعضاء کمیته خبرگان در فضای عدم قطعیت، وابسته است، لذا، پیش‌بینی رفتار سطح ریسک‌پذیری خبرگان با رویکرد برش آلفا در نتایج حاصله برای اوزان این تهدیدها و چالش‌ها می‌تواند زمینه را برای تحلیل حساسیت این موضوع فراهم نماید. به‌عبارت‌دیگر، این رویکرد مشخص خواهد کرد که افزایش یا کاهش سطح ریسک‌پذیری خبرگان در ارائه قضاوت‌های خود در خصوص ارجحیت نسبی شاخص‌ها نسبت به یکدیگر، چه تأثیری بر روی تغییر اوزان حاصله برای این شاخص‌ها خواهد داشت. هر مجموعه فازی به‌صورت کامل و منحصربه‌فرد با برش‌های آلفای آن تعریف می‌شود. برش‌های آلفای هر عدد فازی، به ازای هر مقدار آلفا در بازه [۰،۱]، بازه‌ای بسته از اعداد حقیقی هستند. هرچه برش‌های آلفا در بازه مطروحه به صفر نزدیک‌تر شود، سطح ریسک‌پذیری خبرگان در ارائه قضاوت‌های خود نسبت به شاخص‌ها کاهش می‌یابد. نتایج پیش‌بینی تحلیل حساسیت نظرات خبرگان پیرامون ارجحیت نسبی شاخص‌ها در سطوح مختلف برش آلفا به‌صورت جدول ۹ حاصل گردید.

جدول ۹. پیش‌بینی و تحلیل حساسیت نظرات خبرگان و اوزان نهایی تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در هوشمند سازی شهر تهران

شاخص	سطوح برش آلفا									
	==1	α=099	α=088	α=077	α=066	α=055	α=044	α=033	α=0/2	α=0/1
CS1	۰۴۴۵/۰	۰۴۴۸/۰	۰۴۵۱/۰	۰۴۵۴/۰	۰۴۵۷/۰	۰۴۶۰/۰	۰۴۶۳/۰	۴۶۶/۰	۰۴۶۹/۰	۰۴۷۲/۰
CS2	۰۴۵۵/۰	۰۴۵۸/۰	۰۴۶۱/۰	۰۴۶۴/۰	۰۴۶۷/۰	۰۴۷۰/۰	۰۴۷۳/۰	۰۴۷۶/۰	۰۴۷۹/۰	۰۴۸۲/۰
CS3	۰۴۸۰/۰	۰۰۴۸۲	۰۴۸۴/۰	۰۴۸۶/۰	۰۴۸۸/۰	۰۴۹۰/۰	۰۴۹۲/۰	۰۴۹۴/۰	۰۴۹۶/۰	۰۴۹۸/۰
CS4	۰۴۲۳/۰	۰۴۲۴/۰	۰۴۲۵/۰	۰۴۲۵/۰	۰۴۲۶/۰	۰۴۲۷/۰	۰۴۲۷/۰	۰۴۲۸/۰	۰۴۲۹/۰	۰۴۲۹/۰
CS5	۰۴۷۰/۰	۰۴۷۲/۰	۰۴۷۴/۰	۰۴۷۶/۰	۰۴۷۸/۰	۰۴۸۰/۰	۰۴۸۲/۰	۰۴۸۴/۰	۰۴۸۶/۰	۰۴۸۸/۰
CS6	۰۹۴۰/۰	۰۹۴۰/۰	۰۹۴۰/۰	۰۹۴۰/۰	۰۹۴۰/۰	۰۹۴۰/۰	۰۹۴۰/۰	۰۹۴۰/۰	۰۹۴۰/۰	۰۹۴۰/۰
CS7	۰۵۱۵/۰	۰۵۱۶/۰	۰۵۱۷/۰	۰۵۱۸/۰	۰۵۱۹/۰	۰۵۲۰/۰	۰۵۲۱/۰	۰۵۲۲/۰	۰۵۲۳/۰	۰۵۲۴/۰
CS8	۰۴۹۰/۰	۰۴۹۴/۰	۰۴۹۸/۰	۰۵۰۲/۰	۰۵۰۶/۰	۰۵۱۰/۰	۰۵۱۴/۰	۰۵۱۸/۰	۰۵۲۲/۰	۰۵۲۶/۰
CS9	۰۵۳۷/۰	۰۵۳۸/۰	۰۵۳۹/۰	۰۵۴۱/۰	۰۵۴۲/۰	۰۵۴۳/۰	۰۵۴۵/۰	۰۵۴۶/۰	۰۵۴۷/۰	۰۵۴۹/۰
CS10	۰۴۲۸/۰	۰۴۳۰/۰	۰۴۳۲/۰	۰۴۳۳/۰	۰۴۳۵/۰	۰۴۳۷/۰	۰۴۳۸/۰	۰۴۴۰/۰	۰۴۴۲/۰	۰۴۴۳/۰
CS11	۰۴۹۳/۰	۰۴۹۶/۰	۰۴۹۹/۰	۰۵۰۱/۰	۰۵۰۴/۰	۰۵۰۷/۰	۰۵۰۹/۰	۰۵۱۲/۰	۰۵۱۵/۰	۰۵۱۷/۰
P1	۰۴۵۲/۰	۰۴۵۴/۰	۰۴۵۶/۰	۰۴۵۹/۰	۰۴۶۱/۰	۰۴۶۳/۰	۰۴۶۶/۰	۰۴۶۸/۰	۰۴۷۰/۰	۰۴۷۳/۰
P2	۰۴۴۷/۰	۰۴۴۸/۰	۰۴۴۹/۰	۰۴۵۱/۰	۰۴۵۲/۰	۰۴۵۳/۰	۰۴۵۵/۰	۰۴۵۶/۰	۰۴۵۷/۰	۰۴۵۹/۰
P3	۰۴۶۲/۰	۰۴۶۴/۰	۰۴۶۶/۰	۰۴۶۹/۰	۰۴۷۱/۰	۰۴۷۳/۰	۰۴۷۶/۰	۰۴۷۸/۰	۰۴۸۰/۰	۰۴۸۳/۰
P4	۰۴۳۸/۰	۰۴۴۰/۰	۰۴۴۲/۰	۰۴۴۳/۰	۰۴۴۵/۰	۰۴۴۷/۰	۰۴۴۸/۰	۰۴۵۰/۰	۰۴۵۲/۰	۰۴۵۳/۰
P5	۰۴۷۸/۰	۰۴۸۰/۰	۰۴۸۲/۰	۰۴۸۳/۰	۰۴۸۵/۰	۰۴۸۷/۰	۰۴۸۸/۰	۰۴۹۰/۰	۰۴۹۲/۰	۰۴۹۳/۰
P6	۰۴۴۸/۰	۰۴۵۰/۰	۰۴۵۲/۰	۰۴۵۳/۰	۰۴۵۵/۰	۰۴۵۷/۰	۰۴۵۸/۰	۰۴۶۰/۰	۰۴۶۲/۰	۰۴۶۳/۰
P7	۰۴۷۰/۰	۰۴۷۰/۰	۰۴۷۰/۰	۰۴۷۰/۰	۰۴۷۰/۰	۰۴۷۰/۰	۰۴۷۰/۰	۰۴۷۰/۰	۰۴۷۰/۰	۰۴۷۰/۰
P8	۰۴۶۲/۰	۰۴۶۴/۰	۰۴۶۶/۰	۰۴۶۹/۰	۰۴۷۱/۰	۰۴۷۳/۰	۰۴۷۶/۰	۰۴۷۸/۰	۰۴۸۰/۰	۰۴۸۳/۰
P9	۰۲۰۰/۰	۰۲۰۰/۰	۰۲۰۰/۰	۰۲۰۰/۰	۰۲۰۰/۰	۰۲۰۰/۰	۰۲۰۰/۰	۰۲۰۰/۰	۰۲۰۰/۰	۰۲۰۰/۰
P10	۰۴۸۸/۰	۰۴۹۰/۰	۰۴۹۲/۰	۰۴۹۳/۰	۰۴۹۵/۰	۰۴۹۷/۰	۰۴۹۸/۰	۰۵۰۰/۰	۰۵۰۲/۰	۰۵۰۳/۰

شکل ۲ پیش‌بینی تغییر اوزان تهدیدهای امنیت سایبری و چالش‌های حریم خصوص در هوشمندسازی شهر تهران را به ازای میزان سطح ریسک‌پذیری خبرگان در قضاوت‌های ذهنی خود در خصوص ارجحیت نسبی شاخص‌ها نشان می‌دهد.



شکل ۲. پیش‌بینی اوزان تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در هوشمندسازی شهر تهران برحسب سطح ریسک‌پذیری خبرگان در قضاوت‌ها

همان‌طور که ملاحظه می‌شود با کاهش سطح ریسک‌پذیری خبرگان در قضاوت‌های خود پیرامون اهمیت نسبی تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی (کاهش سطح برش آلفا)، وزن اختصاص‌یافته به آن تهدید و چالش افزایش یافته است. نظر به آن‌که توابع امکان فازی تمامی چالش‌ها یکسان در نظر گرفته شده است (به‌عبارت‌دیگر، یال‌های توابع مثلثی آن‌ها به‌صورت خطی منظور شده است)، لذا رفتار افزایشی وزن تهدیدها و چالش‌ها به‌واسطه کاهش سطح برش آلفا، حسب شیب خط یال مثلث آن شاخص، با ضریب مشخصی انجام گرفته است.

بحث و نتیجه‌گیری

با عنایت بر این که، پیاده‌سازی موفق پروژه شهر هوشمند در تهران درگرو شناسایی و ارزیابی تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی و ارائه برنامه‌ای مدوّن در جهت مقابله با تهدیدها و چالش‌های اولویت‌دار است، پژوهش حاضر با هدف ارائه الگوی تحلیل تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در گذار کلان‌شهر تهران به‌سوی شهر هوشمند نگارش یافت. نوآوری پژوهش حاضر ازنظر موضوعی و ارتباط با نیاز جامعه دانشگاهی و اولویت‌های پیش‌بینی‌شده در اسناد بالادستی نظام و نیز ازنظر روش‌شناسی پژوهش و ابزار تحلیل داده‌ها قابل توجه است. در این پژوهش، الگوی ارزیابی تهدیدهای امنیت سایبری و چالش‌های حریم خصوصی در قالب روشی آمیخته از رویکرد تصمیم‌گیری فازی انجام گرفت که به‌نوبه خود منحصربه‌فرد است. در اختیار داشتن برنامه‌ای برای رفع تهدیدها، موانع و چالش‌های امنیت سایبری و حریم خصوصی گامی مهم در جهت پیاده‌سازی موفق پروژه هوشمندسازی شهر تهران، است. با توجه به یافته‌های پژوهش، راهبردها و برنامه‌های عملیاتی ذیل جهت مواجهه با تهدیدها و چالش‌های شناسایی‌شده در مسیر پیشبرد پروژه هوشمندسازی شهر تهران پیشنهاد می‌شود:

–وجود سیستم‌های آسیب‌پذیر امنیتی شهر هوشمند که می‌تواند در دسترس کاربران ناآگاه قرار داشته باشد، از فقدان بسترهای موردنیاز قانونی و حقوقی نشأت می‌گیرد. ترتیب اثر مثبت در این حوزه، نیازمند استراتژی 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. 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.

–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 بستن راه‌های نفوذ با ایجاد پروتکل‌های امن، ارائه امنیت فیزیکی برای تجهیزات، کابل شبکه و سرورها، رمزگذاری ترافیک شبکه با الگوریتم‌های متقارن پایدار، تقویت امنیت فضای ابری، استفاده از ارتباطات ایمن چون VPN برای دسترسی از راه دور، ایمن‌سازی شبکه‌های بی‌سیم با پروتکل‌های WPA2، استقرار فایروال‌ها در هر نقطه انتقال و غیره را در فهرست برنامه‌های خود قرار دهند.

تعارض منافع

در پژوهش حاضر تعارض منافعی وجود ندارد.

ORCID
Nazila Seddighi **http://orcid.org/0000-0003-0624-7293**
Mohammad Reza Sanaei **http://orcid.org/0000-0001-8787-5421**
Reza Ehtesham Rasi **http://orcid.org/0000-0003-3853-5097**

منابع

آقایی، رضا، آقایی، اصغر و محمدحسینی ناجی زاده، رامین. (۱۳۹۴). شناسایی و رتبه بندی شاخص‌های کلیدی مؤثر بر نگهداری و تعمیرات چابک با استفاده از رویکرد دلفی فازی و دیمتل فازی (مطالعهٔ موردی: صنعت خودروسازی ایران)، *نشریهٔ مدیریت صنعتی*، ۷(۴)، ۶۴۱-۶۷۲. Doi: 10.22059/imj.2015.57420

تکلو بیغش، ابوالفضل و شایان فرد، محسن. (۱۳۹۸). چالش ها و راهکارهای امنیت و حریم خصوصی در برنامه های کاربردی شهر هوشمند، *چهارمین کنفرانس ملی ایده های نوین در فنی و مهندسی*، رشت.

خلیلی‌پور رکن‌آبادی، علی و نورعلی وند، یاسر. (۱۳۹۱). تهدیدات سایبری و تأثیر آن بر امنیت ملی، *فصلنامه مطالعات راهبردی*، ۱۵(۵۶)، ۱۹۶-۱۶۷.

سلطانی، سمیه، محروقی، حمیدرضا و حسینی سنو، سید امین. (۱۳۹۵). معرفی تکنولوژی‌های شهر هوشمند و بررسی چالش‌های امنیت سایبری آن‌ها، *اولین کنفرانس ملی شهر هوشمند*، قم.

شاه محمدی اردبیلی، مرجان، حمیدی، حجت اله و زاهدی، محمدهادی. (۱۳۹۷). مروری بر چالش‌ها، خطرات و امنیت سایبری در شهرهای هوشمند، *دومین کنفرانس بین المللی تحولات نوین در مدیریت ، اقتصاد و حسابداری*، تهران.

References

AlDairi, A. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science*, 109, 1086-1091. DOI: 10.1016/j.procs.2017.05.391.

Alromaihi, S., Elmedany, & W., Balakrishna, C. (2018). Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications. *6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. 140-145. IEEE. DOI**:** 10.1109/W-FiCloud.2018.00028

Arabo, A. (2015). Cyber security challenges within the connected home ecosystem futures. *Procedia Computer Science*, 61, 227-232. DOI: 10.1016/j.procs.2015.09.201

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., ..., & Syed, N. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, 22, 3-13. DOI: 10.1016/j.diin.2017.06.015

Berkel, A. R., Singh, P. M., & van Sinderen, M. J. (2018). An Information Security Architecture for Smart Cities. *In International Symposium on Business Modeling and Software Design*. 167-184. Springer, Cham.

DOI: 10.1007/978-3-319-94214-8_11

Braun, T., Fung, B. C., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable cities and society*, 39: 499-507. DOI: 10.1016/j.scs.2018.02.039

Chen, D., Wawrzynski, P., & Lv, Z. (2020). Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Society*, 102655. DOI: 10.1016/j.scs.2020.102655

Cheng, C. H. & Lin, Y. (2002). Evaluating the best main battle tank using fuzzy decision theory with linguistic criteria evaluation. *European Journal of Operational Research*, 142(1), 174-186. DOI: 10.1016/S0377-2217(01)00280-6

Gunduz, M. Z. & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, 107094. DOI: 10.1016/j.comnet.2019.107094

Guo, S. & Zhao, H. (2017). Fuzzy best-worst multi-criteria decision-making method and its applications. *Knowledge-Based Systems*, 121, 23-31. DOI:10.1016/j.knosys.2017.01.010

Ijaz, S., Shah, M. A., Khan, A., & Ahmed, M. (2016). Smart cities: A survey on security concerns. *International Journal of Advanced Computer Science and Applications*, 7(2), 612-625.

Khatoun, R. & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, 55(3), 51-59. DOI:10.1109/MCOM.2017.1600297CM

Kuo, Y. F. & Chen, P. C. (2008). Constructing performance appraisal indicators for mobility of the service industries using Fuzzy Delphi Method. *Expert Systems with Applications*, 35(4), 1930-1939. DOI:10.1016/j.eswa.2007.08.068

Manchanda, C., Sharma, N., Rathi, R., Bhushan, B., & Grover, M. (2020). Neoteric security and privacy sanctuary technologies in smart cities. In *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 236-241). IEEE. DOI:10.1109/CSNT48778.2020.9115780

Meijer, A. & Bolívar, M. P. R. (2016). Governing the smart city: a review of the literature on smart urban governance. *International Review of Administrative Sciences*, 82(2), 392-408. DOI: 10.1177/0020852314564308

Mohammadpourfard, M., Khalili, A., Genc, I., & Konstantinou, C. (2021). Cyber-Resilient Smart Cities: Detection of Malicious Attacks in Smart Grids. *Sustainable Cities and Society*, 103116. DOI: 10.1016/j.scs.2021.103116

Pelton, J. N. & Singh, I. B. (2019). Cyber Defense in the Age of the Smart City. *In Smart Cities of Today and Tomorrow*. 67-83. Copernicus, Cham. DOI: 10.1007/978-3-319-95822-4_4

Rezaei, J. (2016). Best-worst multi-criteria decision-making method: Some properties and a linear model. *Omega*, 64, 126-130. DOI: 10.1016/j.omega.2015.12.001

Thing, V. L. (2014). Cyber security for a smart nation. *In Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on*. 1-3. IEEE. DOI: 10.1109/ICCIC.2014.7238277

Zhao, F., Fashola, O. I., Olarewaju, T. I., & Onwumere, I. (2021). Smart city research: A holistic and state-of-the-art literature review. *Cities*, *119*, 103406. DOI: 10.1016/j.cities.2021.103406

References [In Persian]

Aghaei, R., Aghaei, A., & Mohammad Hosseini Najizadeh, R. (2015). Identification and ranking of key indicators affecting agile maintenance using the fuzzy Delphi and fuzzy DEMATEL approaches (Case study: Iranian automotive industry), *Journal of Industrial Management*, 7 (4), 641-672. Doi: 10.22059/imj.2015.57420 [In Persian]

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

Khalilipour Roknabadi, A., & Noor Ali Vand, Y. (2012). Cyber Threats and Their Impact on National Security, *Strategic Studies Quarterly*, 15 (56), 196-167. [In Persian]

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

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

استناد به این مقاله: صدیقی، نازیلا.، ثنائی، محمدرضا.، احتشام رائی، رضا. (۱۴۰۰). شناسایی و ارزیابی چالش‌های امنیت سایبری و حریم خصوصی در گذار کلان‌شهر تهران به‌سوی شهر هوشمند تحت شرایط عدم قطعیت، *مطالعات مدیریت کسب وکار هوشمند*، ۱۰(۳۸)، ۱۰۹-۱۳۶.

DOI: 10.22054/ims.2021.59476.1925