Open Access

Urban Ecoligy Researches

Vol. -(-), (Series -): -

Doi: 10.30473/grup.2026.79531.3012

E-ISSN: 2538-3949 P-ISSN: 2538-3930

ORIGINAL ARTICLE

Designing a Government Governance Model for Implementing a Safe Smart City: An Indigenous Framework for the Tehran Metropolis

Hasan Alvedari[*1], **Moslem Soleymanpor**[2]

1. Associate Professor. Department of Public Administration, Payame Noor University, Tehran, Iran.
2. Assistant Professor., Department of Business Management, Payame Noor university, Tehran, Iran.

***Correspondence**
Hasan Alvedari
E-mail: alvedari@pnu.ac.ir

Receive Date: 17/Aug/2026
Revise Date: 09/Oct/2026
2026Accept Date: 09/Nov 2026

How to cite
Alvedari, H., & Soleymanpor. M. (2025) Designing a Government Governance Model for Implementing a Safe Smart City: An Indigenous Framework for the Tehran Metropolis. *Urban Ecoligy Researches*, -(-), -.

EXTENDED A B S T R A C T

Introduction

Rapid urbanization and the increasing complexity of contemporary cities have challenged traditional approaches to urban management, particularly in public service delivery, infrastructure development, and administrative efficiency. In response, smart cities have emerged as an innovative model that uses information and communication technologies (ICT), digital infrastructure, and data-driven systems to improve urban quality of life and optimize public resources. However, smart city development is not merely a technological process; it also requires effective governance, institutional coordination, regulatory oversight, and stakeholder participation. Government governance is particularly important in implementing secure smart cities because it provides the institutional and regulatory foundations for coordinating different actors and protecting public interests. The growing use of interconnected technologies and extensive urban data creates challenges related to cybersecurity, privacy, transparency, equal access, and responsible data management. Addressing these challenges requires clear policies, defined institutional responsibilities, effective coordination mechanisms, and appropriate technical and organizational capacities. These requirements are especially significant in Iran, where responsibilities for urban management, digital infrastructure, security, and standardization are distributed across multiple governmental and municipal institutions. Such institutional fragmentation may complicate coordinated decision-making and the integration of security requirements into smart city initiatives. Despite increasing international attention to smart city governance and security, the specific governance requirements of secure smart city implementation in Iran remain insufficiently understood. Existing approaches do not adequately explain how the country's institutional, legal, and organizational conditions shape the government's role in this process. Therefore, this study aims to design a public governance model for implementing a secure smart city in the metropolis of Tehran. It addresses two research questions: What are the main dimensions and factors of government governance in secure smart city implementation, and how can these dimensions be conceptually organized to explain the government's role in this process?

Mothodology

This study is applied-developmental in purpose and qualitative in method, employing thematic analysis based on Brown and Clarke's (2006) model. The statistical population consisted of experts, managers, and specialists from executive agencies involved in smart city initiatives in Tehran province. Participants included 13 experts selected through purposive sampling until theoretical saturation. Inclusion criteria comprised holding a

doctoral degree or specialized knowledge in public administration, having work experience and research activity in the relevant field, and willingness to participate. The participant composition included six municipal employees, four governorship staff, and three police security personnel. Data were collected through semi-structured interviews. Participants were asked to express their views, experiences, and opinions regarding the concept of smart cities and the role of government governance in their implementation. Interviews continued until theoretical saturation, meaning that when no new data emerged and responses became repetitive, the interview process was terminated. For data analysis, MAXQDA software was used, utilizing thematic network analysis developed by Attride-Stirling (2001). In this method, themes are systematically organized into three levels: basic themes, organizing themes, and global themes. The thematic analysis process followed six phases: (1) familiarization with data; (2) generating initial codes, where interview texts were carefully studied and independent ideas were identified as basic themes; (3) searching for themes, where organizing and global themes were abstracted; (4) reviewing themes; (5) defining and naming themes; and (6) producing the report. To ensure reliability, inter-coder agreement was used. In addition to the primary researcher, another researcher independently coded the findings. Cohen's kappa coefficient yielded 0.78, indicating acceptable reliability. For validity, the final findings were presented to three university experts and approved. In the open coding stage, 56 initial codes were extracted.

Findings

The findings revealed that the role of government governance in secure smart city implementation can be explained through one global theme, six organizing themes, and 20 basic themes. The global theme is "The Role of Government Governance in Secure Smart City Implementation." The six organizing themes include: (1) Policy, Strategic, and Legal-Regulatory Framework; (2) Institutional Architecture and Inter-organizational Coordination; (3) Data Governance, Privacy, and Transparency; (4) Risk Management, Security, and Resilience; (5) Stakeholder Participation and Social Legitimacy; and (6) Standards, Technical-Organizational Capabilities, and Capacity Building. The first theme emphasizes the lack of a cohesive national strategy for secure smart cities, ambiguity in responsible agencies' roles, integrating security requirements into data and critical infrastructure laws, and mandatory incident reporting. The second theme highlights establishing provincial and municipal special groups headed by governors/mayors, creating joint working groups for coordinated risk assessment, and formalizing public-private partnership contracts with security and data ownership clauses. The third theme underscores classifying sensitive urban data, defining access rules, conducting mandatory privacy and security impact assessments, and launching public dashboards for transparency. The fourth theme emphasizes periodic cyber and privacy risk assessments, developing business continuity and crisis management plans, establishing security operations at the city level, and integrating physical security with cybersecurity. The fifth theme includes forming city advisory councils, using public consultation channels, implementing awareness campaigns, and ensuring human oversight of automated systems. The sixth theme necessitates adopting national cybersecurity standards, promoting interoperability and open data standards, investing in training and certification, and aligning urban initiatives with national programs.

Discussion and Conclusion

The findings indicate that a secure smart city is not merely a technological project but an institutional, political, managerial, and social process requiring restructuring relationships among government, municipalities, the private sector, security institutions, universities, and citizens. The first theme aligns with Li et al. (2023) and Linenicka et al. (2025) regarding coherent cybersecurity frameworks. It corresponds with Afshari et al. (2024) concerning public policy in Tehran, though the present study emphasizes the security dimension more. The second theme is consistent with Chatterji and Mukkai (2024) and Akgün et al. (2024) regarding institutional fragmentation barriers. The role of municipalities is particularly important; based on expert statements, municipalities are at

the forefront but lack adequate authority, resources, and data access. The third theme aligns with OECD (2023) and Fabrègue and Bogoni (2023) concerning data governance and privacy. The fourth theme corresponds with Nucci et al. (2023) and Li et al. (2023). The fifth theme directly align with Afshari et al. (2024). The sixth theme is consistent with Shafiei and Ayat (1404) and Fouladi and Kamali (1404). The study concludes that secure smart city implementation in tehran requires a transition from a project-oriented and technology-centric approach to a governance-oriented approach. The government must formulate a national secure smart city strategy, define institutional roles, incorporate security and privacy requirements into laws and contracts, establish inter-agency coordination mechanisms, and facilitate participation of municipalities, the private sector, universities, and civil society. The proposed model demonstrates that the six dimensions interact to shape smart city governance capacity. Policy-making without effective institutional architecture is not implementable; institutional architecture without data governance may lead to fragmentation; data governance without social participation will lack legitimacy; and all components without technical capacity and specialized human resources will not yield results. Practically, it is recommended that the government establish a national coordinating body for secure smart cities, but this should not lead to excessive centralization. At provincial and municipal levels, permanent working groups should be formed with participation of governorships, municipalities, police, service agencies, IT departments, universities, the private sector, and civil society. Every smart project should be assessed for security, privacy, access equity, and interoperability impacts before deployment.

K E Y W O R D S
Government Governance, Smart City, Urban Security, Data Governance, Cybersecurity.

Copyright © 2026, by the author(s). Published by Payame Noor University, Tehran, Iran.
This is an open access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

فصلنامه علمی

پژوهش‌های بوم‌شناسی شهری

سال –، شماره –، پیاپی، فصل سال (–)

Doi: 10.30473/grup.2026.79531.3012

E-ISSN: 2538-3949 P-ISSN: 2538-3930

«مقاله پژوهشی»

طراحی الگوی حکمرانی دولتی برای پیاده‌سازی شهر هوشمند امن: یک چارچوب بومی برای کلان‌شهر تهران

حسن الوداری[1*]، مسلم سلیمان‌پور[2]

۱. دانشیار، گروه مدیریت دولتی، دانشگاه پیام نور، تهران، ایران.
۲. استادیار، گروه مدیریت بازرگانی، دانشگاه پیام نور، تهران، ایران.

***نویسنده مسئول:** حسن الوداری
رایانامه:
E-mail: alvedari@pnu.ac.ir

تاریخ دریافت: ۱۴۰۵/۰۵/۲۶
تاریخ بازنگری: ۱۴۰۵/۰۷/۱۷
تاریخ پذیرش: ۱۴۰۵/۰۸/۱۸

استناد به این مقاله:
الوداری، حسن و سلیمان‌پور، مسلم (۱۴۰۵). طراحی الگوی حکمرانی دولتی برای پیاده‌سازی شهر هوشمند امن: یک چارچوب بومی برای کلان‌شهر تهران. *فصلنامه علمی پژوهش‌های بوم‌شناسی شهری*، سال (شماره)، صفحه.

چکیده

پیاده‌سازی شهر هوشمند امن، فرایندی چندبعدی است که علاوه‌بر زیرساخت‌های فناورانه، به حکمرانی مؤثر، هماهنگی نهادی، حفاظت از داده‌ها، مدیریت ریسک و مشارکت ذی‌نفعان نیاز دارد. پژوهش حاضر با هدف طراحی الگوی حکمرانی دولتی برای پیاده‌سازی شهر هوشمند امن در کلان‌شهر تهران انجام شد. این پژوهش از نظر هدف، کاربردی ـ توسعه‌ای و از نظر روش، کیفی است. داده‌ها از طریق مصاحبه‌های نیمه ساختاریافته با خبرگان، مدیران و کارشناسان دستگاه‌های اجرایی مرتبط گردآوری و با استفاده از تحلیل مضمون و شبکه مضامین تحلیل شدند. نمونه‌گیری به‌صورت هدفمند و تا دستیابی به اشباع نظری ادامه یافت. یافته‌ها، پس از تأیید نهایی شمارش مضامین، شامل یک مضمون فراگیر، شش مضمون سازمان‌دهنده و ۲۱ مضمون پایه است. شش مضمون سازمان‌دهنده عبارت‌اند از: چارچوب سیاست‌گذاری، راهبردی و قانونی ـ نظارتی، معماری نهادی و هماهنگی بین‌سازمانی، حکمرانی داده‌ها، حریم خصوصی و شفافیت، مدیریت ریسک، امنیت و تاب‌آوری، مشارکت ذی‌نفعان و مشروعیت اجتماعی، و استانداردها، قابلیت‌های فنی ـ سازمانی و ظرفیت‌سازی. سهم علمی پژوهش، ارائه چارچوبی بومی و یکپارچه است که ابعاد سیاست‌گذاری، ساختار نهادی، حکمرانی داده، امنیت و تاب‌آوری، مشارکت اجتماعی و ظرفیت‌های فنی و سازمانی را در قالب الگویی منسجم برای تبیین نقش حکمرانی دولتی در پیاده‌سازی شهر هوشمند امن در تهران به هم پیوند می‌دهد. این چارچوب نشان می‌دهد که تحقق شهر هوشمند امن صرفاً به توسعه فناوری وابسته نیست، بلکه مستلزم هماهنگی میان نهادهای مسئول، حفاظت از داده‌ها، مدیریت ریسک، مشارکت ذی‌نفعان و تقویت ظرفیت‌های اجرایی است. نتایج پژوهش می‌تواند مبنایی برای تدوین سیاست‌ها و سازوکارهای هماهنگ‌کننده در حکمرانی شهر هوشمند امن در زمینه نهادی و اجرایی ایران فراهم آورد.

واژه‌های کلیدی

حکمرانی دولتی، شهر هوشمند، امنیت شهری، حکمرانی داده، امنیت سایبری.

حق انتشار این مستند، متعلق به نویسندگان آن است. © ۱۴۰۵ ناشر این مقاله، دانشگاه پیام نور است.
این مقاله تحت گواهی زیر منتشرشده و هر نوع استفاده غیرتجاری از آن مشروط بر استناد صحیح به مقاله و با رعایت شرایط مندرج در آدرس زیر مجاز است.
This is an open access article under the CC BY (http://creativecommons.org/licenses/by/4.0/).

مقدمه

گسترش فناوری‌های اطلاعات و ارتباطات در مدیریت شهری، زمینه شکل‌گیری شهرهای هوشمند را فراهم کرده است. شهر هوشمند با بهره‌گیری از داده‌ها، زیرساخت‌های دیجیتال و سامانه‌های هوشمند می‌تواند به بهبود ارائه خدمات عمومی، افزایش هماهنگی در مدیریت شهری و ارتقای کیفیت زندگی شهروندان کمک کند (Afshari et al., 2024). حکمرانی دولتی ستون فقرات اجرای یک شهر هوشمند امن است چون اولاً دولت می‌تواند یک سیاست منسجم و چارچوب قانونی ایجاد کند که امنیت سایبری، حفاظت از داده‌ها و ایمنی شهری را در یک جهت استراتژیک واحد ادغام کند و از ابتکارات پراکنده و متناقض در وزارتخانه‌ها و شهرداری‌ها جلوگیری کند (Lnenicka et al., 2025). بدون یک تکیه‌گاه سیاستی مرکزی، پروژه‌های شهر هوشمند در معرض خطر تبدیل شدن به طرح‌های آزمایشی هستند که فاقد استانداردهای امنیتی، قابلیت همکاری و مکانیسم‌های پاسخگویی هستند (OECD, 2023). در پیاده‌سازی شهر هوشمند امن، رهبری دولت و هماهنگی میان سطوح ملی و محلی برای تدوین راهبردهای منسجم امنیت سایبری، حفاظت از داده‌ها و تعیین روشن مسئولیت‌های سازمانی ضروری است. سازمان همکاری و توسعه اقتصادی تأکید می‌کند که امنیت سایبری شهرها صرفاً مسئولیت دولت‌های محلی نیست و دولت ملی می‌تواند با ایفای نقش راهبر و هم‌راستا کردن راهبردهای سطوح مختلف حکومتی، به انسجام اقدامات امنیتی کمک کند (OECD, 2023). همچنین، بهره‌گیری از فناوری‌های دیجیتال در شهر هوشمند، در کنار بهبود کارایی خدمات و تصمیم‌گیری عمومی، مستلزم حفاظت از حریم خصوصی، رعایت حقوق بنیادین و آزادی‌های مدنی و پیشگیری از تبعیض در استفاده از داده‌ها و سامانه‌های الگوریتمی است. بر این اساس، ایجاد چارچوب‌های اخلاقی، شفافیت در استفاده از داده‌ها و تعیین مسئولیت‌های نظارتی می‌تواند به حفاظت از حقوق شهروندان و تقویت اعتماد عمومی کمک کند (OECD, 2023). توسعه شهر هوشمند صرفاً یک تلاش تکنولوژیکی نیست، بلکه یک چالش اساساً سیاسی و اداری است که نیاز به بازنگری در فرآیندهای حکمرانی، تخصیص منابع و مشارکت ذی‌نفعان دارد. چارچوب‌های سیاستی نه‌تنها باید اهداف و سازوکارهای اجرایی روشنی را بیان کنند، بلکه باید همکاری بین سازمان‌های دولتی، بازیگران بخش خصوصی و جامعه مدنی را نیز تقویت کنند (Afshari et al., 2024). بدون حاکمیت دولتی کارآمد و هماهنگ، پیاده‌سازی یک شهر هوشمند امن ناگزیر با شکست مواجه خواهد شد، زیرا موانع نهادی، فنی، امنیتی و اجتماعی به‌طور سیستماتیک ریشه می‌دوانند و پیامدهای نامطلوبی برای شهروندان، زیرساخت‌های حیاتی و اعتماد عمومی ایجاد می‌کنند (Misra et al., 2025, Akgün et al., 2024).

فقدان جهت‌گیری بلندمدت و اهداف مشخص در سطوح ملی و محلی منجر به پروژه‌های پراکنده و ناهماهنگ که اساساً امنیت یکپارچه شهری را تضعیف می‌کنند (Chatterji & Mukkai, 2024). طراحی الگوی بومی حکمرانی دولتی برای شهر هوشمند امن در تهران اهمیت فراوان دارد چون‌که هماهنگی نهادهای دولتی، بخش خصوصی و جامعه مدنی، تعیین مسئولیت‌ها و کاهش پراکندگی مدیریت شهری را تسهیل می‌کند (کرمی، ۱۴۰۳). همچنین شناسایی و مدیریت چالش‌های امنیت سایبری و حریم خصوصی، پیش‌شرط هوشمندسازی شهر تهران است (صدیقی و همکاران، ۱۴۰۰). علیرغم توجه روزافزون علمی به حکمرانی هوشمند شهری در سطح جهانی، شکاف‌های قابل‌توجهی در همچنان وجود دارد. مطالعات موجود عمدتاً از مدل‌های غربی بدون در نظر گرفتن واقعیت‌های نهادی، فرهنگی و سیاسی منحصربه‌فرد ایران استفاده می‌کنند که منجر به راهنمایی ناکافی برای اجرای ایمن شهر هوشمند می‌شود. با وجود راهبردها و پروژه‌های متعدد، توصیه‌های امنیت سایبری و حفاظت از داده پراکنده‌اند و چارچوبی جامع و اعتبارسنجی شده برای دسته‌بندی و اجرای آن‌ها وجود ندارد.

پژوهش حاضر با هدف پر کردن این شکاف نظری، به تدوین مدلی برای درک نقش حکمرانی دولتی در پیاده‌سازی شهر هوشمند در تهران می‌پردازد. بر همین اساس، سؤالات اصلی پژوهش عبارت‌اند از

۱. الگوی حکمرانی دولتی برای پیاده‌سازی شهر هوشمند امن از چه ابعاد و مؤلفه‌هایی تشکیل می‌شود؟

۲. این ابعاد چگونه در قالب چارچوبی منسجم با یکدیگر ارتباط می‌یابند؟

پاسخ به این سؤال‌ها می‌تواند مبنایی برای تبیین علمی نقش دولت در هم‌راستا کردن الزامات حکمرانی، مدیریت و امنیت در فرایند هوشمندسازی شهری فراهم آورد.

مبانی نظری

شهر هوشمند مفهومی چندبعدی است که از ترکیب فناوری‌های اطلاعات و ارتباطات، زیرساخت‌های شهری، سرمایه انسانی، حکمرانی، مشارکت شهروندی و توسعه پایدار

شکل می‌گیرد. فناوری زمانی به بهبود عملکرد شهری منجر می‌شود که درون ساختارهای مناسب نهادی، حقوقی، مدیریتی و اجتماعی به کار گرفته شود (Mora et al., 2023: 5). از این منظر، شهر هوشمند یک نظام اجتماعی ـ فنی است. در این نظام، تجهیزات و سامانه‌های فناورانه با سازمان‌ها، قوانین، فرایندهای تصمیم‌گیری، کارکنان، شهروندان و شبکه‌های ذی‌نفعان در تعامل هستند (Shi & Cao, 2022). بنابراین، موفقیت شهر هوشمند به قابلیت اتصال سامانه‌ها، توانمندی سازمانی، اعتماد عمومی، شفافیت، امنیت داده و هماهنگی نهادی وابسته است (Hardi et al., 2025).

مفهوم حکمرانی شهر هوشمند

حکمرانی شهر هوشمند به مجموعه ساختارها، فرایندها، قواعد و روابطی اطلاق می‌شود که از طریق آن‌ها تصمیم‌گیری، ارائه خدمات، مدیریت داده، هماهنگی سازمان‌ها و مشارکت شهروندان در محیط شهری انجام می‌گیرد. در این رویکرد، شهر هوشمند صرفاً پروژه شهرداری یا یک طرح فناوری اطلاعات نیست، بلکه شبکه‌ای از کنشگران شامل دولت مرکزی، وزارتخانه‌ها، استانداری، فرمانداری، شهرداری، شوراهای اسلامی شهر، دستگاه‌های خدمات‌رسان، پلیس، بخش خصوصی، دانشگاه و جامعه مدنی در آن نقش دارند (Raghava Rao & Kumar, 2022).

نظریه حکمرانی شبکه‌ای

نظریه حکمرانی شبکه‌ای، مبنای اصلی نظری پژوهش حاضر است. بر اساس این نظریه، مسائل عمومی پیچیده را نمی‌توان تنها از طریق سلسله‌مراتب اداری و فرماندهی متمرکز حل کرد. حل این مسائل نیازمند همکاری شبکه‌ای میان دولت، نهادهای عمومی، بخش خصوصی، دانشگاه، سازمان‌های مدنی و شهروندان است (Kim & Kim, 2021). پیاده‌سازی شهر هوشمند نمونه‌ای از یک مسئله پیچیده عمومی است، زیرا هیچ سازمانی به‌تنهایی مالک همه منابع، داده‌ها، تخصص‌ها و اختیارات لازم برای اجرای آن نیست. دولت از قدرت قانونی، منابع و ظرفیت هماهنگی برخوردار است، شهرداری به نیازها و خدمات محلی نزدیک‌تر است، بخش خصوصی فناوری و سرمایه را فراهم می‌کند، دانشگاه دانش و ظرفیت تحلیلی دارد، و شهروندان هم استفاده‌کننده و هم تولیدکننده داده‌های شهری هستند (Mora et al., 2023). مقایسه مفاهیم شهر هوشمند، حکمرانی هوشمند و حکمرانی شبکه‌ای نشان می‌دهد که این مفاهیم، با وجود ارتباط نزدیک، از نظر کارکرد نظری یکسان نیستند شهر هوشمند بر بهره‌گیری از فناوری‌های اطلاعاتی و ارتباطی، سرمایه انسانی و اجتماعی و حکمرانی مشارکتی برای ارتقای کیفیت زندگی و دستیابی به توسعه اقتصادی پایدار شهری تأکید دارد (Caragliu et al., 2011). حکمرانی هوشمند نیز به چگونگی سازمان‌دهی تصمیم‌گیری، مدیریت اطلاعات و تعامل میان بازیگران شهری در راستای بهبود عملکرد حکومت و تحقق ارزش عمومی مربوط می‌شود (Meijer & Bolívar, 2016). بنابراین، این مفاهیم به ترتیب بستر تحول شهری، شیوه اداره و هماهنگی امور و الگوی تعامل میان بازیگران را تبیین می‌کنند.

نظریه نهادی

نظریه نهادی نیز برای تبیین پژوهش حاضر اهمیت دارد. این نظریه بیان می‌کند که عملکرد سازمان‌ها تنها تحت تأثیر منابع فنی و اقتصادی نیست، بلکه قوانین، هنجارها، ساختارهای رسمی، فرهنگ‌سازمانی و انتظارات اجتماعی نیز بر رفتار آن‌ها اثر می‌گذارند (Akgün et al., 2024). بر اساس این نظریه، پیاده‌سازی شهر هوشمند در تهران زمانی موفق خواهد بود که با ساختارهای رسمی و غیررسمی موجود سازگار شود. وجود نهادهای متعدد، پراکندگی مسئولیت‌ها، تفاوت سطح اختیارات شهرداری‌ها، محدودیت‌های قانونی، فرهنگ‌سازمانی و مقاومت کارکنان می‌تواند بر اجرای طرح‌های هوشمندسازی اثر بگذارد.

نظریه حکمرانی داده

شهر هوشمند بر داده استوار است. داده‌های مکانی، ترافیکی، جمعیتی، زیست‌محیطی، خدماتی و رفتاری، مبنای تصمیم‌گیری و ارائه خدمات هوشمند قرار می‌گیرند (Subrahmanyam, 2025). به همین دلیل، حکمرانی داده یکی از ارکان نظری پژوهش حاضر است. حکمرانی داده شامل قواعد و سازوکارهایی برای تعیین مالکیت داده، کیفیت داده، طبقه‌بندی داده، سطح دسترسی، اشتراک‌گذاری، حفظ امنیت، رعایت حریم خصوصی و پاسخگویی در برابر سوءاستفاده از داده است نبود حکمرانی داده می‌تواند پیامدهایی مانند پراکندگی اطلاعات، موازی‌کاری، نقض حریم خصوصی، کاهش اعتماد عمومی و آسیب‌پذیری سایبری ایجاد کند (Lnenicka et al., 2025).

نظریه مدیریت ریسک و تاب‌آوری

نظریه مدیریت ریسک و تاب‌آوری بر شناسایی، ارزیابی و کاهش تهدیدات سیستمی در محیط‌های پیچیده تأکید دارد. در شهر هوشمند، ریسک‌ها شامل تهدیدات سایبری، نقض حریم خصوصی، خرابی زیرساخت‌های حیاتی و بحران‌های طبیعی هستند(Li et al., 2023) . تاب‌آوری شهری به توانایی سیستم شهری برای جذب شوک‌ها، حفظ عملکردهای اساسی و بازیابی سریع پس از اختلالات اشاره دارد (Lnenicka et al.,

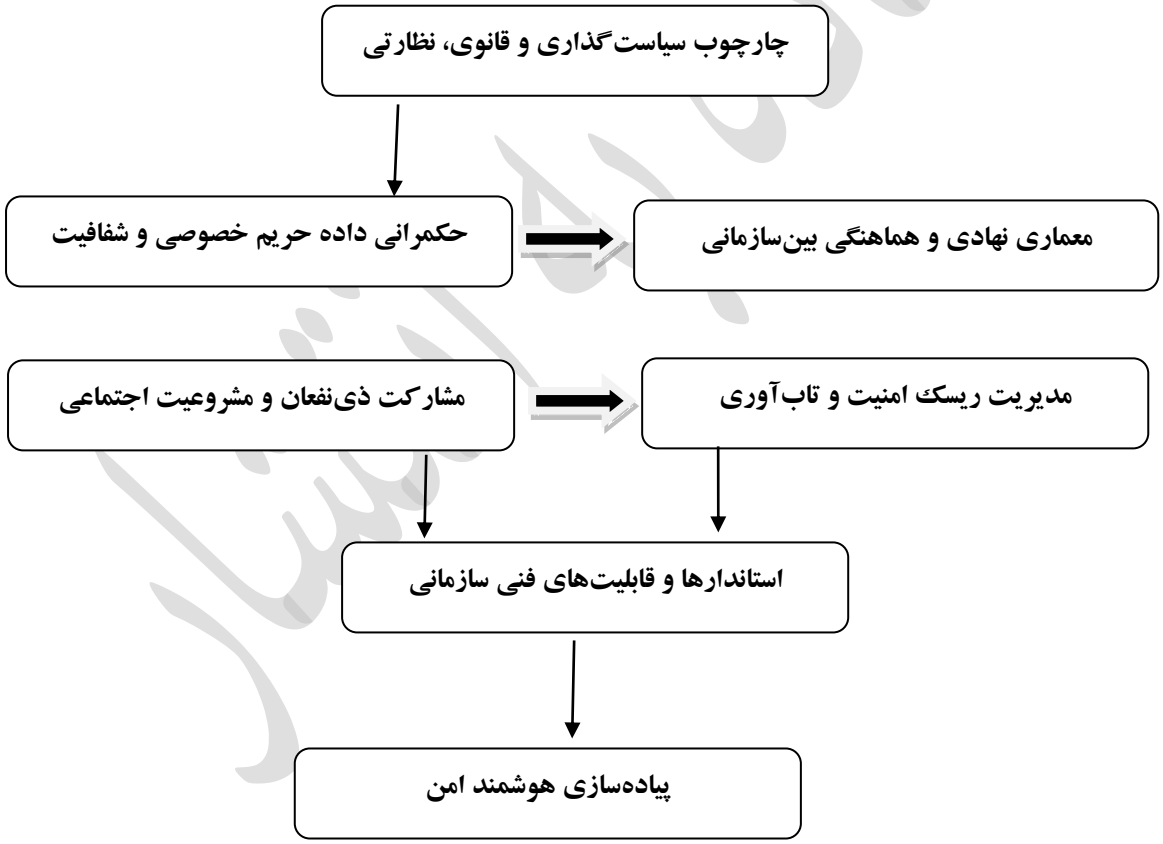
2025). در این پژوهش، مدیریت ریسک با مؤلفه‌هایی مانند ارزیابی دوره‌ای ریسک، برنامه تداوم خدمات، مدیریت بحران و ادغام ایمنی فیزیکی با امنیت سایبری عملیاتی می‌شود.

با توجه به ماهیت مسئله پژوهش، نظریه حکمرانی شبکه‌ای به‌عنوان نظریه مبنای اصلی انتخاب می‌شود. دلیل این انتخاب آن است که اجرای شهر هوشمند امن در تهران چندبازیگری است و به همکاری نهادهای مختلف نیاز دارد، چندسطحی است و دولت، استان، فرمانداری و شهرداری را در برمی‌گیرد و هم‌زمان مسائل فناوری، حقوقی، امنیتی، اجتماعی و مدیریتی را شامل می‌شود، بدون اعتماد، مشارکت و هماهنگی میان بازیگران قابل تحقق نیست. در این چارچوب، نظریه نهادی، نظریه حکمرانی داده و نظریه مدیریت ریسک و تاب‌آوری به‌عنوان نظریه‌های مکمل استفاده می‌شوند. نظریه حکمرانی شبکه‌ای، روابط میان بازیگران را تبیین می‌کند، نظریه نهادی، اثر قوانین و ساختارهای سازمانی را توضیح می‌دهد، نظریه حکمرانی داده، چگونگی تنظیم جریان اطلاعات را نشان می‌دهد و نظریه مدیریت ریسک، چارچوبی برای شناسایی و کاهش تهدیدات ارائه می‌دهد.

مدل مفهومی پژوهش

در پژوهش حاضر، «نقش حکمرانی دولتی در پیاده‌سازی شهر هوشمند امن» به‌عنوان مقوله محوری در نظر گرفته می‌شود. این مقوله از شش سازه اصلی تشکیل شده است: چارچوب سیاست‌گذاری، راهبردی و قانونی ـ نظارتی، معماری نهادی و هماهنگی بین‌سازمانی، حکمرانی داده، حریم خصوصی و شفافیت، مدیریت ریسک، امنیت و تاب‌آوری، مشارکت ذی‌نفعان و مشروعیت اجتماعی و استانداردها، قابلیت‌های فنی ـ سازمانی و ظرفیت‌سازی.

مدل مفهومی این مؤلفه‌ها به صورت شکل زیر است:



شکل ۱. مدل مفهومی پژوهش برگرفته از لنیکا و همکاران (۲۰۲۵)

پیشینه پژوهش

پژوهش‌های انجام شده درباره شهر هوشمند را می‌توان در سه دسته کلی طبقه‌بندی کرد: دسته نخست، بر شناسایی ابعاد و شاخص‌های شهر هوشمند تمرکز دارند، دسته دوم چالش‌های تحقق و پیاده‌سازی شهر هوشمند را بررسی کرده‌اند و دسته سوم به حکمرانی، مشارکت ذی‌نفعان، حکمرانی داده و امنیت شهر هوشمند پرداخته‌اند. بررسی انتقادی این مطالعات نشان می‌دهد که اگرچه ادبیات پژوهش به‌تدریج از رویکرد صرفاً فناورانه فاصله

گرفته است، همچنان خلأهایی در تبیین نقش دولت و سازوکارهای نهادی لازم برای پیاده‌سازی شهر هوشمند امن در ایران وجود دارد.

توانایی مروی و ضخیمی (۱۴۰۵)، در مقاله‌ای با عنوان «تحقق‌پذیری شهر هوشمند به‌مثابه برساخت اجتماعی در ایران: تدوین مدل مفهومی با رویکرد نظریه داده بنیاد» شهر هوشمند را به‌مثابه یک برساخت اجتماعی بررسی کرده‌اند. یافته‌های این پژوهش بر هم‌آفرینی، شفافیت، اعتماد عمومی، محله‌محوری، مدیریت یکپارچه، مشارکت شهروندان، عدالت اجتماعی و توسعه ظرفیت‌های آموزشی تأکید دارد. نقطه قوت این مطالعه، عبور از نگاه فناوری‌محور و توجه به زمینه اجتماعی و فرهنگی تحقق شهر هوشمند در ایران است. با وجود این، پژوهش مذکور عمدتاً بر بعد اجتماعی و مشارکتی تمرکز دارد و مؤلفه‌هایی مانند امنیت سایبری، حفاظت از داده‌های حساس، مدیریت ریسک، قابلیت همکاری سامانه‌ها و نقش دولت به‌عنوان تنظیم‌گر و هماهنگ‌کننده را به‌صورت جامع وارد مدل نکرده است.

افشاری[1] و همکاران (۲۰۲۴)، در مقاله‌ای با عنوان «سیاست‌گذاری عمومی در تهران به سوی توسعه دولت الکترونیک و پیاده‌سازی شهر هوشمند» بر نقش اعتماد عمومی، مشارکت شهروندان، سواد دیجیتال، شفافیت و هم‌آفرینی در توسعه دولت الکترونیک و شهر هوشمند تأکید کرده‌اند. این پژوهش نشان می‌دهد که حتی پیشرفته‌ترین فناوری‌ها بدون پذیرش اجتماعی و مشارکت شهروندان نمی‌توانند به تحول پایدار شهری منجر شوند. بااین‌حال، تمرکز آن بیشتر بر مشارکت عمومی و سیاست‌گذاری دولت الکترونیک است و موضوع امنیت شهر هوشمند، حفاظت از زیرساخت‌های حیاتی، مدیریت ریسک سایبری و تعیین مسئولیت سازمان‌ها را به‌طور کامل پوشش نمی‌دهد.

شفیعی و آیت (۱۴۰۴)، در مقاله‌شان با موضوع «شناسایی و تحلیل ابعاد و شاخص‌های توسعه شهر هوشمند» هشت بعد اقتصاد هوشمند، محیط‌زیست هوشمند، حکمرانی هوشمند، پویایی هوشمند، انرژی هوشمند، زندگی هوشمند، فناوری هوشمند و مردم هوشمند را شناسایی کرده‌اند. اهمیت این پژوهش در ارائه تصویری جامع از ابعاد شهر هوشمند است، با این حال، تمرکز اصلی آن بر طبقه‌بندی شاخص‌ها بوده و چگونگی تعامل میان نهادهای مسئول، نحوه هماهنگی دستگاه‌ها و الزامات امنیتی اجرای این شاخص‌ها به‌طور مستقل بررسی نشده است و درباره پرسش چه سازوکار حکمرانی برای تحقق آن لازم است؟ تبیین ارائه نمی‌کند.

فولادی و کمالی (۱۴۰۴)، در مقاله‌شان با عنوان «شاخص‌های بومی سنجش شهر هوشمند در کلان‌شهرهای ایران: یک مطالعه مرور نظام‌مند و تحلیل کیفی» نشان دادند که شاخص‌های شهر هوشمند در ایران تنها ماهیت فناورانه ندارند، بلکه تحت تأثیر عوامل اجتماعی، فرهنگی، نهادی، محیطی و حکمرانی قرار می‌گیرند. نقطه قوت این پژوهش، توجه به زمینه بومی و اهمیت مؤلفه‌هایی مانند شفافیت داده، مشارکت دیجیتال، تاب‌آوری، عدالت دسترسی و سواد دیجیتال است. بااین‌حال، مطالعه مذکور بیشتر بر سنجش و ارزیابی شهر هوشمند تمرکز دارد و فرایند سیاست‌گذاری، تقسیم مسئولیت میان دولت و شهرداری و الزامات امنیتی اجرای پروژه‌های هوشمندسازی را به‌صورت عملیاتی تبیین نمی‌کند.

توانایی و همکاران (۱۴۰۱)، در پژوهشی با عنوان «واکاوی چالش‌های پیش روی تحقق‌پذیری شهر هوشمند مطالعه موردی: شهر مشهد» چالش‌های تحقق شهر هوشمند را بررسی کرده‌اند. نتایج آنان بر ضرورت برنامه‌ریزی در حوزه‌های محیط‌زیست هوشمند، اقتصاد هوشمند، حکمرانی هوشمند و مردم هوشمند تأکید دارد. اهمیت این پژوهش در نشان دادن این نکته است که تحقق شهر هوشمند در ایران با موانع مدیریتی، سازمانی و نهادی مواجه است و صرفاً با تأمین تجهیزات فناورانه امکان‌پذیر نیست. بااین‌حال، این پژوهش بیشتر ماهیت آسیب‌شناسانه دارد و یک الگوی جامع برای نقش دولت در سیاست‌گذاری، تنظیم‌گری، حکمرانی داده، هماهنگی بین‌سازمانی و مدیریت امنیت شهر هوشمند ارائه نمی‌کند.

در پژوهشی صابری‌فر (۱۳۹۹)، «تعیین و تشخیص عوامل مؤثر در طراحی سازمان هوشمند برای مدیریت شهری، مطالعه موردی شهرداری مشهد»، بر ضرورت بازآرایی سازمان شهری، توسعه قابلیت‌های سازمانی، استفاده از فناوری اطلاعات و ایجاد هماهنگی میان اجزای سازمانی تأکید کرده است. اهمیت این مطالعه برای پژوهش حاضر از آن جهت است که نشان می‌دهد حکمرانی هوشمند، پویایی هوشمند، زندگی هوشمند، مردم هوشمند، اقتصاد هوشمند و سرانجام محیط هوشمند، به ترتیب بیشترین اثر را بر ایجاد سازمان هوشمند برای اداره و مدیریت شهر دارند. در حالی که مسئله پژوهش حاضر در سطحی گسترده‌تر، رابطه میان دولت، شهرداری، نهادهای امنیتی، دستگاه‌های خدمات‌رسان، بخش خصوصی، دانشگاه و جامعه مدنی را بررسی می‌کند. همچنین، موضوعاتی مانند حاکمیت داده، حفاظت از حریم خصوصی، گزارش‌دهی حوادث سایبری و تاب‌آوری زیرساخت‌های حیاتی در آن مطالعه به‌صورت محورهای مستقل بررسی نشده‌اند.

1. Afshari

در مطالعات خارجی نیز هاردی و همکاران[1] (۲۰۲۵)، در مقاله‌شان با عنوان «حکومت‌داری هوشمند شهری و قابلیت همکاری: افزایش امنیت انسانی در یوگیاکارتا و ماکاسار، اندونزی» نشان داده‌اند که یکپارچگی زیرساخت‌های فناورانه، مشارکت کاربران، مدیریت تغییر و همکاری بین سازمان‌ها، نقش مهمی در ارتقای امنیت انسانی و کیفیت خدمات شهری دارد. این مطالعه اهمیت قابلیت همکاری و ارتباط میان دولت و شهروندان را برجسته می‌کند، اما زمینه نهادی آن با ایران متفاوت است و نمی‌توان نتایج آن را بدون بومی‌سازی در تهران به کار گرفت.

غفاری و همکاران(۱۴۰۴)، در مقاله‌شان با عنوان « تصویرپردازی ازحکمرانی هوشمند برای تهران آینده در افق ۲۰۵۰» بیان کردند تصویر سیاسی حکمرانی هوشمند از ۸ مضمون ملاحظات قانونی، برنامه‌ریزی هوشمند، ادغام حکمرانی سیاسی، حکمرانی شبکه‌ای هوشمند، دستیابی به آمار و اطلاعات هوشمند، کاهش فساد اداری، امنیت هوشمند، شفافیت و تصویر اقتصادی حکمرانی هوشمند از ۸ مضمون ظرفیت‌سازی بهینه اقتصاد شهری، یکپارچه‌سازی درآمدهای شهری، عملکرد هوشمند سازمان، ثبات و شکوفایی اقتصادی، مدیریت هوشمند هزینه‌ها، مدیریت نظام پاداش، کارایی و اثربخشی، ساماندهی کسب و کارهای الکترونیک و تصویر اجتماعی- فرهنگی حکمرانی هوشمند از۷ مضمون که شامل مشارکت‌پذیری فعالانه اجتماعی، فرهنگ‌سازی اجتماعی، آموزش الکترونیک، مشارکت الکترونیک، مسئولیت‌پذیری اجتماعی، ارتقای کیفیت زندگی و پاسخگویی است، شکل گرفته است

نوچی و همکاران[2] (۲۰۲۳)، در پژوهشی با عنوان «روندهای تاریخی در حکمرانی هوشمند شهری برای مدیریت مراکز شهری باستانی در ایران: مطالعه موردی شهرداری سقز» تهدیدهای فناورانه، سازمانی و امنیتی را شناسایی کرده و بر جمع‌آوری متمرکز داده، ارزیابی مستمر ریسک، یکپارچگی سازمان‌های مدیریت بحران و جذب نیروی متخصص تأکید کرده‌اند. تفاوت پژوهش حاضر با مطالعه مذکور در این است که علاوه‌بر مدیریت ریسک، ابعاد سیاست‌گذاری، حاکمیت داده، مشارکت اجتماعی، قابلیت همکاری و معماری نهادی را نیز در یک چارچوب واحد بررسی می‌کند.

مورا و همکاران[3] (۲۰۲۳)، در تحقیقی با عنوان «حکمرانی شهر هوشمند از دیدگاه مدیریت نوآوری: چارچوب نظری، بررسی شیوه‌های فعلی و دستور کار تحقیقاتی آینده» شهر هوشمند را نه یک محصول یا وضعیت نهایی، بلکه فرایندی مستمر از نوآوری، سیاست‌گذاری، یادگیری نهادی و توسعه فناوری می‌دانند. این دیدگاه برای پژوهش حاضر اهمیت دارد، زیرا نشان می‌دهد هوشمندسازی شهری باید به‌عنوان یک فرایند نهادی و مدیریتی در نظر گرفته شود. بااین‌حال، چارچوب ارائه‌شده در این پژوهش، اگرچه بر حکمرانی یکپارچه و مشارکتی تأکید دارد، الزامات خاص امنیتی و حقوقی شهرهای ایران را بررسی نمی‌کند.

مطالعات بین‌المللی درباره حکمرانی داده نیز بر ضرورت وجود قواعد روشن برای جمع‌آوری، مالکیت، دسترسی، اشتراک‌گذاری و حفاظت از داده‌های شهری تأکید کرده‌اند. گزارش سازمان توسعه و همکاری اقتصادی[4] (۲۰۲۳) نشان می‌دهد که حکمرانی داده یکی از ارکان اصلی شهر هوشمند است و نبود قواعد روشن می‌تواند به نقض حریم خصوصی، کاهش اعتماد عمومی و استفاده ناهماهنگ از داده‌ها منجر شود.

فابریگ و بوگونی[5] (۲۰۲۳)، نیز بر پیوند میان حکمرانی داده، حریم خصوصی و اعتماد عمومی تأکید کرده‌اند. بااین‌حال، این مطالعات بیشتر در سطح سیاست‌گذاری عمومی و چارچوب‌های کلی انجام شده‌اند و چگونگی ترجمه این الزامات به ساختار نهادی و اجرایی تهران را بررسی نکرده‌اند. بررسی مطالعات پیشین حاکی از این است که بیشتر پژوهش‌ها تنها یکی از ابعاد شهر هوشمند، مانند فناوری، مشارکت، شاخص‌ها، سازمان یا امنیت را بررسی کرده‌اند و ارتباط میان این ابعاد را در قالب یک مدل منسجم نشان نداده‌اند و در بخش مهمی از مطالعات، دولت یا به‌عنوان نهاد اجرایی مستقیم یا به‌عنوان سیاست‌گذار کلی در نظر گرفته شده است، درحالی‌که نقش‌های چندگانه دولت شامل سیاست‌گذاری، تنظیم‌گری، هماهنگی بین‌سازمانی، تضمین حقوق عمومی، مدیریت ریسک و توانمندسازی بازیگران کمتر به‌صورت یکپارچه بررسی شده است.

بر همین اساس، پژوهش حاضر با هدف پر کردن این خلأها، نقش حکمرانی دولتی در پیاده‌سازی شهر هوشمند امن در تهران را بررسی می‌کند. نوآوری این پژوهش در آن است که امنیت را به یک مؤلفه مستقل و جدا از حکمرانی محدود نمی‌کند، بلکه آن را در سراسر چرخه سیاست‌گذاری، طراحی، اجرا، ارزیابی و بهره‌برداری از شهر هوشمند جاری می‌سازد. در

1. Hardi et al
2. Nucci et al
3. Mora et al
4. OECD (Organisation for Economic Co-operation and Development)
5. Fabrègue & Bogoni

مدل پیشنهادی، شش بعد «چارچوب سیاست‌گذاری و قانونی ـ نظارتی»، «معماری نهادی و هماهنگی بین‌سازمانی»، «حکمرانی داده، حریم خصوصی و شفافیت»، «مدیریت ریسک، امنیت و تاب‌آوری»، «مشارکت ذی‌نفعان و مشروعیت اجتماعی» و «استانداردها، قابلیت‌های فنی ـ سازمانی و ظرفیت‌سازی» به‌عنوان مؤلفه‌های اصلی نقش حکمرانی دولتی در نظر گرفته شده‌اند.

روش انجام پژوهش

این پژوهش از نظر هدف، کاربردی و توسعه‌ای محسوب می‌شود و با رویکردی کیفی انجام شده است. روش مورد استفاده در این مطالعه، تحلیل مضمون[1] است که با عناوینی همچون تحلیل موضوعی و تحلیل تماتیک نیز شناخته می‌شود. تحلیل مضمون یکی از روش‌های متداول برای تحلیل داده‌های کیفی حاصل از مصاحبه است که مهارت‌های اساسی موردنیاز برای بسیاری از تحلیل‌های کیفی دیگر را نیز فراهم می‌آورد (براون و کلارک، ۲۰۰۶).

جامعه آماری این پژوهش را خبرگان و مدیران و کارشناسان دستگاه‌های اجرایی مؤثر در شهر تهران تشکیل می‌دهند. مشارکت‌کنندگان در پژوهش شامل ۱۳ نفر از خبرگان بودند که با استفاده از روش نمونه‌گیری هدفمند تا رسیدن به سطح اشباع نظری انتخاب شدند. معیار ورود به پژوهش شامل داشتن تحصیلات دکتری یا دانش تخصصی در حوزه مدیریت دولتی، داشتن سابقه کار و فعالیت پژوهشی در حوزه مورد مطالعه و تمایل به مشارکت در پژوهش بود. ترکیب مشارکت‌کنندگان شامل ۶ نفر از کارکنان فرمانداری، ۴ نفر از کارکنان شهرداری و سه نفر از پلیس امنیت بود. داده‌های این پژوهش از طریق مصاحبه‌های نیمه ساختاریافته با خبرگان گردآوری شد. در این مصاحبه‌ها، از مشارکت‌کنندگان خواسته شد تا دیدگاه‌ها، تجربیات و نظرات خود را درباره مفهوم شهر هوشمند و نقش حکمرانی دولتی در پیاده‌سازی آن بیان کنند. مصاحبه‌ها تا رسیدن به اشباع نظری ادامه یافت، به این معنا که هنگامی که داده‌های جدیدی از مصاحبه‌های بعدی به دست نیامد و پاسخ‌ها تکراری شدند، فرآیند مصاحبه متوقف گردید. برای تحلیل اطلاعات، از نرم‌افزار MAXQDA استفاده شد. روش تحلیل مضمون به کار رفته در این پژوهش، بر اساس الگوی براون و کلارک[2] (۲۰۰۶) و با استفاده از روش تحلیل شبکه مضامین[3] که توسط آرتاید استرلینگ[4] (۲۰۰۱) توسعه یافته است، انجام شد. در این پژوهش، این دو رویکرد به‌عنوان دو روش مستقل و موازی به کار نرفتند، بلکه تحلیل مضمون براون و کلارک مبنای شناسایی و توسعه مضامین قرار گرفت و شبکه مضامین آتریـد–استرلینگ برای طبقه‌بندی، سازمان‌دهی و نمایش ساختار روابط میان مضامین استخراج شده استفاده شد.

مراحل تحلیل مضمون بر اساس الگوی براون و کلارک (۲۰۰۶) به شرح زیر است:

۱. آشنایی با داده‌ها: شامل انتخاب موضوع، بیان مسئله، بیان اهداف و سؤالات پژوهش، انتخاب طرح پژوهش و تعیین قلمرو، جامعه و نمونه.

۲. ایجاد کدهای اولیه: در این مرحله، متون مصاحبه‌ها به دقت و به‌طور مکرر مطالعه شدند و ایده‌های مستقل در قالب مضامین پایه شناسایی و به هر یک کد اختصاص داده شد. در صورت وجود بخش‌هایی با مضامین مشابه در متن مصاحبه‌های قبلی، از همان کدهای قبلی به‌عنوان نشانگر استفاده شد.

۳. جستجوی مضامین: پس از دستیابی به مضامین پایه، مضامین سازمان‌دهنده و مضامین فراگیر با توجه به مضامین پایه انتزاع شدند.

۴. بازبینی مضامین: در این مرحله، مضامین شناسایی‌شده مورد بازبینی و اصلاح قرار گرفتند.

۵. تعریف و نام‌گذاری مضامین: مضامین نهایی تعریف و نام‌گذاری شدند.

۶. تحلیل پایانی و گزارش: در نهایت، مدل کیفی پژوهش ارائه شد.

مشارکت‌کنندگان حاضر شامل ۱۱ مدرک کارشناسی ارشد و ۲ دکتری از استانداری، فرمانداری و شهرداری و پلیس امنیت بودند.

ویژگی‌های جمعیت‌شناختی خبرگان در جدول (۱) آمده است.

1. Thematic Analysis
2. Braun and Clarke
3. Thematic Network Analysis
4. Artaid Sterling

جدول ۱. ویژگی های جمعیت‌شناختی خبرگان پژوهش

کد مصاحبه‌شونده	سن	جنسیت	تحصیلات	سمت سازمانی	میزان سابقه کار
P01	۵۲	مرد	کارشناسی ارشد	مدیر	۲۲
P02	۴۲	مرد	کارشناسی ارشد	سرپرست	۱۸
P03	۴۴	مرد	دکتری	مدیر	۱۶
P04	۳۹	مرد	کارشناسی ارشد	مدیر	۱۷
P05	۳۵	مرد	کارشناسی ارشد	مدیر	۱۵
P06	۴۲	مرد	کارشناسی ارشد	کارشناس ارشد	۱۶
P07	۴۷	زن	دکتری	مدیر	۲۰
P08	۴۶	مرد	کارشناسی ارشد	کارشناس	۱۹
P09	۴۷	مرد	کارشناسی ارشد	سرپرست	۲۱
P10	۳۹	مرد	کارشناسی ارشد	مدیر	۱۷
P11	۴۰	مرد	کارشناسی ارشد	کارشناس	۱۳
P12	۳۷	زن	کارشناسی ارشد	مدیر	۱۶
P13	۵۴	مرد	کارشناسی ارشد	سرپرست	۲۳

یافته‌های پژوهش

در این پژوهش، داده‌ها از طریق مصاحبه‌های نیمه ساختاریافته با ۱۳ نفر از خبرگان گردآوری شد. فرآیند مصاحبه تا رسیدن به «اشباع نظری» ادامه یافت، به این معنا که نمونه‌گیری تا جایی تداوم داشت که پاسخ‌های دریافت شده به تکرار رسیده و داده جدیدی حاصل نشود. پس از پیاده‌سازی مصاحبه‌ها و تکمیل آن‌ها با یادداشت‌های میدانی برداشت‌شده در طول جلسات، پژوهشگر به مطالعه دقیق و مکرر متون مصاحبه پرداخت. در این مرحله، ایده‌های مستقل در قالب مضامین پایه شناسایی شدند و سپس با انتزاع از این مضامین، مضامین سازمان‌دهنده و مضامین فراگیر استخراج گردید. در نهایت، شبکه مضامین ترسیم شد.

شبکه مضامین، روابط میان مضامین را به‌صورت غیرخطی نمایش می‌دهد، در این شبکه هیچ سلسله‌مراتبی میان مضامین وجود ندارد و تأکید اصلی بر وابستگی و ارتباط میان اجزای شبکه است. پس از ترسیم شبکه، این ساختار مورد بررسی و تحلیل قرار می‌گیرد. برای اطمینان از پایایی پژوهش، از روش «توافق بین دو کدگذار» استفاده شد. بدین ترتیب که علاوه‌بر پژوهشگر اصلی که کدگذاری اولیه را انجام داد، پژوهشگر دیگری نیز به‌صورت مستقل به کدگذاری یافته‌ها پرداخت. نزدیکی نتایج این دو کدگذاری، نشان‌دهنده توافق و در نتیجه پایایی مناسب است. برای محاسبه کمی میزان توافق، از ضریب کاپا استفاده شد که مقدار آن ۰,۷۸ به دست آمد، این مقدار نشان‌دهنده پایایی قابل‌قبول پژوهش است. همچنین، برای تأمین روایی پژوهش، علاوه‌بر به‌کارگیری راهبرد «حساسیت پژوهشگر» در طول فرآیند، یافته‌های نهایی در اختیار سه تن از خبرگان دانشگاهی قرار گرفت و مورد تأیید ایشان واقع شد. کدگذاری، فرآیندی تحلیلی است که از طریق آن مفاهیم، ویژگی‌ها و ابعاد آن‌ها در داده‌ها شناسایی و کشف می‌شوند. در مرحله کدگذاری باز، در مجموع ۵۶ کد اولیه از پاسخ‌های خبرگان استخراج گردید. به‌عنوان نمونه، گزیده‌ای از کدهای اولیه استخراج‌شده از متون مصاحبه‌شوندگان در جدول (۲) ارائه شده است.

جدول ۲. گزیده‌ای از کدگذاری اولیه روی متن مصاحبه‌ها

مصاحبه‌شونده	متون مصاحبه	کد اولیه
مصاحبه‌شونده ۱	به نظر من، بزرگ‌ترین خلأ ما در حال حاضر نبود یک استراتژی ملی منسجم برای شهر هوشمند امن است. ما نیاز داریم که یک چارچوب ملی تعریف شود که در آن الزامات امنیتی، پروتکل‌های تبادل داده و مکانیزم‌های نظارتی به صورت یکپارچه مشخص شده باشد. بدون این استراتژی، سرمایه‌گذاری‌های کلان در حوزه شهر هوشمند با ریسک‌های امنیتی جدی مواجه خواهد شد	استراتژی ملی شهر هوشمند امن
مصاحبه‌شونده ۲	شهرداری‌ها در خط مقدم پیاده‌سازی شهر هوشمند قرار دارند، اما متأسفانه اختیارات و منابع کافی برای این مأموریت بزرگ را ندارند. نقش شهرداری باید از یک مجری صرف به یک بازیگر استراتژیک در حکمرانی شهر هوشمند ارتقا یابد. این یعنی مشارکت در تصمیم‌گیری‌های کلان و دسترسی به داده‌های ملی	نقش شهرداری‌ها
مصاحبه‌شونده ۳	یکی از نگرانی‌های اصلی در پیاده‌سازی شهر هوشمند، مسئله حفاظت از داده‌های شهروندان است. ما با حجم عظیمی از داده‌های حساس مانند موقعیت مکانی، الگوهای رفتاری، اطلاعات مالی. اگر زیرساخت‌های امنیتی مناسبی برای حفاظت از این داده‌ها ایجاد نکنیم، با فاجعه‌ای در حوزه حریم خصوصی مواجه خواهیم شد. پیشنهاد من تصویب قانون خاصی برای حفاظت از داده‌های شهر هوشمند است	حفاظت از داده‌ها

سپس با مطالعه دقیق و پی‌درپی برای هر مصاحبه ایده‌ای مستقل در قالب مضامین پایه شناسایی و به هرکدام یک کد اختصاص داده شد و در صورت وجود بخش‌هایی با مضامین مشابه در متن مصاحبه‌های قبلی از همان کد استفاده شد. در ادامه کدهای اولیه استخراج و پس از دستیابی به مضامین پایه، مضامین سازمان دهنده و فراگیر با توجه به مضمون پایه انتخاب گردیدند. در این مرحله مصاحبه‌ها شامل ۱ مضمون فراگیر، ۶ مضمون سازمان‌یافته، ۲۰ مضمون پایه و ۵۶ کد اولیه برای طراحی مدل شناسایی شدند.

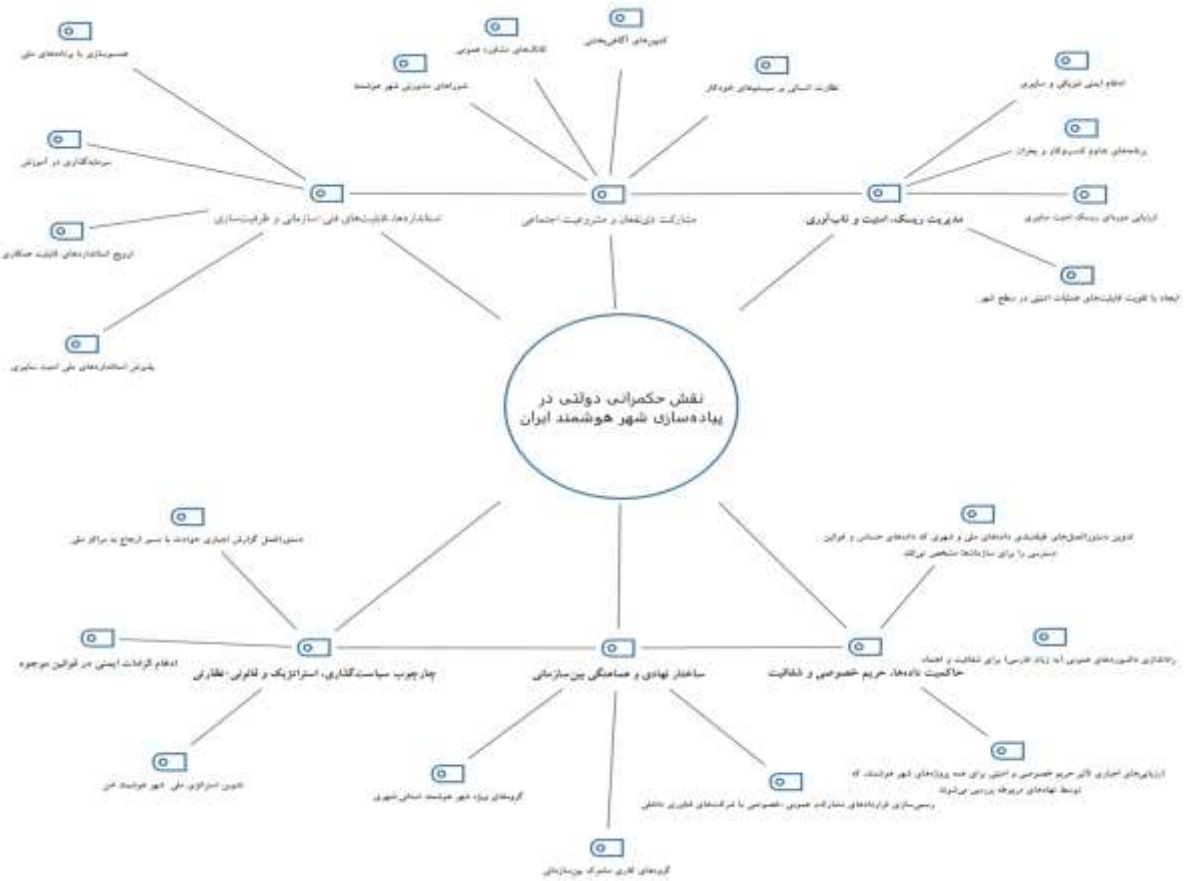
جدول ۳- الف. نتایج تحلیل مضمون

مضمون فراگیر	مضمون سازمان‌دهنده	مضامین پایه	کدهای اولیه
نقش حکمرانی دولتی در پیاده‌سازی شهر هوشمند امن	۱. چارچوب سیاست‌گذاری، استراتژیک و قانونی-نظارتی	تدوین استراتژی ملی شهر هوشمند امن با نقش‌های مشخص نهادی ادغام الزامات ایمنی در قوانین داده، زیرساخت حیاتی و تجارت الکترونیک دستورالعمل گزارش اجباری حوادث با مسیر ارجاع به مراکز ملی	استراتژی ملی شهر هوشمند امن نقش شورای عالی فضای مجازی نقش وزارت ارتباطات نقش شهرداری‌ها نقش سازمان‌های امنیتی حفاظت از داده‌ها زیرساخت حیاتی تجارت الکترونیک مقررات اینترنت اشیا سیستم‌های نظارتی شهری گزارش اجباری حوادث مراکز ملی امنیت سایبری

جدول ۳-ب. نتایج تحلیل مضمون

مضمون فراگیر	مضمون سازمان‌دهنده	مضامین پایه	کدهای اولیه
نقش حکمرانی دولتی در پیاده‌سازی شهر هوشمند امن	۲. معماری نهادی و هماهنگی بین‌سازمانی	تعیین گروه‌های ویژه استانی و شهری به ریاست فرماندار/شهردار ایجاد گروه‌های کاری مشترک برای ارزیابی و واکنش هماهنگ به ریسک رسمی‌سازی قراردادهای مشارکت عمومی-خصوصی با بندهای امنیتی و مالکیت داده	گروه ویژه استانی/شهری فرماندار و شهردار پلیس و اورژانس خدمات رفاهی اداره فناوری اطلاعات استان گروه کاری مشترک ارزیابی و واکنش هماهنگ به ریسک مشارکت عمومی-خصوصی مالکیت داده‌ها تعهدات امنیتی پیمانکار
	۳. حاکمیت داده‌ها، حریم خصوصی و شفافیت	تدوین دستورالعمل طبقه‌بندی داده‌های حساس شهری و قوانین دسترسی ارزیابی اجباری تأثیر حریم خصوصی و امنیتی پیش از استقرار پروژه‌ها راه‌اندازی داشبورد عمومی ایمنی و عملکرد خدمات برای شفافیت	طبقه‌بندی داده‌های حساس داده‌های مکانی قوانین دسترسی به داده ارزیابی اثر حریم خصوصی ارزیابی اثر امنیتی بررسی پیش از استقرار داشبورد عمومی شاخص‌های ایمنی آمار تجمیع‌شده حوادث شفافیت اطلاعاتی
	۴. مدیریت ریسک، امنیت و تاب‌آوری	ارزیابی دوره‌ای ریسک سایبری و حریم خصوصی برای سیستم‌های شهر هوشمند توسعه برنامه‌های تداوم کسب‌وکار و مدیریت بحران خدمات حیاتی ایجاد/تقویت عملیات امنیتی شهری - ادغام ایمنی فیزیکی با امنیت سایبری در سیستم‌ها	ارزیابی دوره‌ای ریسک ریسک امنیت سایبری ریسک حریم خصوصی تداوم کسب‌وکار مدیریت بحران خدمات حیاتی شهری عملیات امنیتی شهری ایمنی فیزیکی امنیت سایبری
	۵. مشارکت ذی‌نفعان و مشروعیت اجتماعی	تشکیل شورای مشورتی شهر با حضور دانشگاه، بخش خصوصی و جامعه مدنی استفاده از کانال‌های موجود برای دریافت بازخورد ایمنی شهروندان اجرای کمپین‌های آگاهی‌بخشی درباره خطرات سایبری و گزارش‌دهی حوادث تضمین نظارت انسانی بر سیستم‌های خودکار با پروتکل‌های شفاف	شورای مشورتی شهر بازخورد شهروندی کمپین آگاهی‌بخشی سایبری نظارت انسانی بر سیستم‌های خودکار پروتکل‌های عملیاتی شفاف مشارکت دانشگاه مشارکت بخش خصوصی مشارکت جامعه مدنی
	۶. استانداردها، قابلیت‌های فنی–سازمانی و ظرفیت‌سازی	پذیرش استانداردهای ملی امنیت سایبری به‌عنوان مبنای پروژه‌ها ترویج استانداردهای قابلیت همکاری و داده‌های باز سرمایه‌گذاری در آموزش و گواهی‌نامه کارکنان فناوری و امنیت همسوسازی ابتکارات شهری با برنامه‌های ملی شهر هوشمند و امنیت سایبری	استانداردهای ملی امنیت سایبری قابلیت همکاری سامانه‌ها داده‌های باز آموزش کارکنان فناوری گواهی‌نامه تخصصی همسویی با برنامه ملی پشتیبانی فنی زیرساخت‌های مشترک

به‌منظور تبیین بهتر مقوله‌بندی‌های صورت گرفته مدل کیفی پژوهش به صورت زیر ارائه می‌شود.



شکل ۲. نقش حکمرانی دولتی در پیاده‌سازی شهر هوشمند

مضامین شامل موارد زیر هستند: **مضمون فراگیر: نقش حکمرانی دولتی در پیاده‌سازی شهر هوشمند امن** این مضمون، تمام شش محور و ۲۱ مؤلفه عملیاتی است.

۲. مضامین سازمان‌یافته: ۶ مورد

هر یک از شش عنوان شماره‌گذاری‌شده، یک مضمون سازمان‌یافته است:

۱. چارچوب سیاست‌گذاری، استراتژیک و قانونی-نظارتی
۲. معماری نهادی و هماهنگی بین‌سازمانی
۳. حاکمیت داده‌ها، حریم خصوصی و شفافیت
۴. مدیریت ریسک، امنیت و تاب‌آوری
۵. مشارکت ذی‌نفعان و مشروعیت اجتماعی
۶. استانداردها، قابلیت‌های فنی-سازمانی و ظرفیت‌سازی.

۳. مضامین پایه:

هر بند عملیاتی یک مضمون پایه است:

محور ۱: چارچوب سیاست‌گذاری، استراتژیک و قانونی نظارتی (۳ مضمون پایه)

۱. تدوین استراتژی ملی شهر هوشمند امن با نقش‌های مشخص نهادی
۲. ادغام الزامات ایمنی در قوانین داده، زیرساخت حیاتی و تجارت الکترونیک
۳. دستورالعمل گزارش اجباری حوادث با مسیر ارجاع به مراکز ملی
۴. محور ۲: ساختار نهادی و هماهنگی بین سازمانی (۳ مضمون پایه)
۵. تعیین گروه‌های ویژه استانی و شهری به ریاست فرماندار/شهردار
۶. ایجاد گروه‌های کاری مشترک برای ارزیابی و واکنش هماهنگ به ریسک
۷. رسمی‌سازی قراردادهای مشارکت عمومی و خصوصی با بندهای امنیتی و مالکیت داده.

محور ۳: حاکمیت داده، حریم خصوصی و شفافیت (۳ مضمون پایه)

۸. تدوین دستورالعمل طبقه‌بندی داده‌های حساس شهری و قوانین دسترسی
۹. ارزیابی اجباری تأثیر حریم خصوصی و امنیتی پیش از استقرار پروژه‌ها
۱۰. راه‌اندازی داشبورد عمومی ایمنی و عملکرد خدمات برای شفافیت.

محور ۴: مدیریت ریسک، امنیت و تاب‌آوری (۴ مضمون پایه)

۱۱. ارزیابی دوره‌ای ریسک سایبری و حریم خصوصی برای سیستم‌های شهر هوشمند
۱۲. توسعه برنامه‌های تداوم کسب‌وکار و مدیریت بحران خدمات حیاتی
۱۳. ایجاد/تقویت قابلیت عملیات امنیتی در سطح شهر
۱۴. ادغام ایمنی فیزیکی با امنیت سایبری
۱۵. محور ۵: مشارکت ذینفعان و مشروعیت اجتماعی (۴ مضمون پایه)
۱۶. تشکیل شورای مشورتی شهر با حضور دانشگاه، بخش خصوصی و جامعه مدنی
۱۷. استفاده از کانال‌های مشاوره عمومی برای دریافت بازخورد ایمنی
۱۸. اجرای کمپین‌های آگاهی‌بخشی درباره خطرات سایبری و گزارش‌دهی حوادث
۱۹. تضمین نظارت انسانی بر سیستم‌های خودکار با پروتکل‌های شفاف
۲۰. محور ۶: استانداردها و ظرفیت‌سازی (۴ مضمون پایه)
۲۱. پذیرش استانداردهای ملی امنیت سایبری به‌عنوان مبنای پروژه‌ها
۲۲. ترویج استانداردهای قابلیت همکاری و داده‌های باز
۲۳. سرمایه‌گذاری در آموزش و گواهی‌نامه کارکنان فناوری و امنیت
۲۴. همسوسازی ابتکارات شهری با برنامه‌های ملی شهر هوشمند و امنیت سایبری

بحث و نتیجه‌گیری

پژوهش حاضر با هدف تبیین نقش حکمرانی دولتی در پیاده‌سازی شهر هوشمند امن در ایران انجام شد. تحلیل مضمون مصاحبه‌های نیمه ساختاریافته با خبرگان و مدیران دستگاه‌های اجرایی، به شناسایی یک مضمون فراگیر، شش مضمون سازمان‌دهنده و ۲۰ مضمون پایه منجر شد. مضمون فراگیر پژوهش، «نقش حکمرانی دولتی در پیاده‌سازی شهر هوشمند امن» است و شش بعد اصلی آن عبارت‌اند از: چارچوب سیاست‌گذاری، استراتژیک و قانونی ـ نظارتی، معماری نهادی و هماهنگی بین‌سازمانی، حاکمیت داده‌ها، حریم خصوصی و شفافیت، مدیریت ریسک، امنیت و تاب‌آوری، مشارکت ذی‌نفعان و مشروعیت اجتماعی، و استانداردها، قابلیت‌های فنی ـ سازمانی و ظرفیت‌سازی. یافته‌ها بیانگر آن است که شهر هوشمند صرفاً یک پروژه فناورانه یا مجموعه‌ای از سامانه‌های دیجیتال نیست، بلکه فرایندی نهادی، سیاسی، مدیریتی و اجتماعی است که تحقق آن به بازآرایی روابط میان دولت، شهرداری، بخش خصوصی، نهادهای امنیتی، دانشگاه و شهروندان نیاز دارد.

اولین مضمون سازمان دهنده پژوهش بر اهمیت وجود چارچوب سیاست‌گذاری، استراتژیک و قانونی ـ نظارتی تأکید دارد. خبرگان، فقدان راهبرد ملی منسجم برای شهر هوشمند امن، ابهام در نقش دستگاه‌های مسئول، ضرورت ادغام الزامات امنیتی در قوانین داده، زیرساخت‌های حیاتی و تجارت الکترونیک و همچنین لزوم گزارش اجباری حوادث را از الزامات اساسی دانستند. بر این اساس، پیاده‌سازی شهر هوشمند بدون تعیین اهداف ملی، تقسیم کار نهادی، استانداردهای الزام‌آور و سازوکارهای نظارت و پاسخگویی، به مجموعه‌ای از طرح‌های پراکنده و ناهماهنگ تبدیل خواهد شد. نتایج این پژوهش با دیدگاه لی و همکاران[1] (۲۰۲۳) هم‌راستا است که حکمرانی دولتی را فراهم‌کننده اقتدار، مشروعیت و ظرفیت هماهنگی برای همسوسازی فناوری، زیرساخت و ایمنی عمومی می‌دانند. همچنین با یافته‌های لنیکا و همکاران[2] (۲۰۲۵) درباره ضرورت ایجاد چارچوب‌های منسجم امنیت سایبری و حفاظت از داده در شهرهای هوشمند مطابقت دارد. از دیدگاه این مطالعات، نبود سیاست مرکزی و چارچوب قانونی مشترک، خطر ناسازگاری سامانه‌ها، ضعف امنیتی و فقدان پاسخگویی را افزایش می‌دهد.

یافته حاضر با پژوهش افشاری و همکاران درباره سیاست‌گذاری عمومی در تهران نیز هم‌راستایی دارد. آنان بر ضرورت ایجاد اکوسیستمی تأکید کردند که فناوری را با حکمرانی، قانون‌گذاری و شمول اجتماعی هماهنگ سازد. بااین‌حال، پژوهش حاضر نسبت به مطالعه مذکور بر بعد امنیتی و انتظامی حکمرانی تأکید بیشتری دارد. در حالی که

1. Lee et al
2. Lnenicka

افشاری و همکاران (۲۰۲۴) بیشتر بر اعتماد عمومی، مشارکت شهروندان و سواد دیجیتال تمرکز کرده‌اند، یافته‌های این پژوهش نشان می‌دهد که این مؤلفه‌ها زمانی می‌توانند به تحقق شهر هوشمند منجر شوند که در چارچوبی رسمی از الزامات امنیتی، گزارش‌دهی حوادث، حفاظت از زیرساخت‌های حیاتی و تقسیم مسئولیت‌های نهادی قرار گیرند.

دومین مضمون سازمان‌دهنده، معماری نهادی و هماهنگی بین‌سازمانی است. یافته‌ها نشان داد که برای پیاده‌سازی شهر هوشمند امن، ایجاد گروه‌های ویژه استانی و شهری، تشکیل گروه‌های کاری مشترک برای ارزیابی و واکنش هماهنگ به ریسک و رسمی‌سازی قراردادهای مشارکت عمومی ـ خصوصی با درج بندهای امنیتی و مالکیت داده ضروری است. این یافته بیانگر آن است که مسئله اصلی شهر هوشمند در ایران تنها کمبود فناوری نیست، بلکه پراکندگی مسئولیت‌ها، ضعف هماهنگی و نبود سازوکار مشخص برای همکاری دستگاه‌هاست. نتیجه‌گیری حاضر با یافته‌های چاترجی و موکای (۲۰۲۴) درباره آثار منفی پراکندگی زیرساخت‌های دیجیتال و ضعف ظرفیت نهادی هم‌راستا است، که نشان دادند نبود هماهنگی میان سازمان‌ها و ضعف ظرفیت نهادی می‌تواند اجرای برنامه‌های شهر هوشمند را با مشکل مواجه کند. همچنین، یافته حاضر با پژوهش آکجون و همکاران[1] (۲۰۲۴) درباره موانع بخش عمومی در اجرای پروژه‌های شهر هوشمند همخوانی دارد که محدودیت‌های سازمانی، نهادی و مدیریتی به‌عنوان موانع اساسی اجرای موفق شناخته شده‌اند. از سوی دیگر، پژوهش هاردی و همکاران (۲۰۲۵) نشان داد که قابلیت همکاری سامانه‌ها و مشارکت کاربران، نقش مهمی در تقویت ارتباط دولت و شهروندان دارد. یافته پژوهش حاضر نیز همین ضرورت را تأیید می‌کند و اما آن را به سطح ساختارهای رسمی حکمرانی ارتقا داده و بر لزوم ایجاد کارگروه‌های مشترک و تعیین مسئولیت‌های مشخص تأکید می‌کند.

در این زمینه، نقش شهرداری‌ها اهمیت ویژه‌ای دارد. بر اساس اظهارات خبرگان، شهرداری‌ها در خط مقدم ارائه خدمات هوشمند قرار دارند، اما در بسیاری از موارد از اختیارات، منابع مالی، دسترسی به داده‌ها و ظرفیت تخصصی کافی برخوردار نیستند. بنابراین، یکی از پیش‌شرط‌های حکمرانی مؤثر، ارتقای جایگاه شهرداری از مجری طرح‌های ملی به بازیگر راهبردی و شریک تصمیم‌گیری است. این یافته با پژوهش توانایی مروی و همکاران (۱۴۰۱) درباره تحقق‌پذیری شهر هوشمند به‌مثابه برساخت اجتماعی در ایران هم‌راستا است که بر مدیریت یکپارچه، بهبود ارتباطات میان نقش‌آفرینان و انسجام برنامه‌ای تأکید داشت. با وجود این، پژوهش حاضر علاوه‌بر مدیریت یکپارچه، بر نقش فرمانداری، پلیس، مراکز امنیت سایبری و نهادهای مسئول زیرساخت‌های حیاتی تأکید می‌کند و از این طریق، مدل جامع‌تری از معماری نهادی شهر هوشمند امن ارائه می‌دهد.

سومین مضمون، حاکمیت داده‌ها، حریم خصوصی و شفافیت است. یافته‌ها نشان داد که طبقه‌بندی داده‌های حساس شهری، تعیین قوانین دسترسی، انجام ارزیابی اجباری تأثیر حریم خصوصی و امنیتی پیش از اجرای پروژه‌ها و ایجاد داشبورد عمومی برای ارائه شاخص‌های ایمنی و عملکرد خدمات، از مؤلفه‌های مهم حکمرانی شهر هوشمند هستند. این یافته اهمیت داده را در ساختار شهر هوشمند دوگانه نشان می‌دهد که از یک‌سو منبع اصلی تصمیم‌گیری، افزایش کارایی و بهبود خدمات است و از سوی دیگر، در صورت نبود سازوکارهای قانونی و فنی مناسب، می‌تواند به منبع تهدید علیه حریم خصوصی، امنیت فردی و اعتماد عمومی تبدیل شود.

یافته‌های این بخش با گزارش OECD درباره حکمرانی داده در شهرهای هوشمند هم‌راستا است که بر ضرورت تعیین قواعد روشن برای دسترسی، اشتراک‌گذاری، حفاظت و استفاده مجدد از داده‌های شهری تأکید داشته است و با نتایج فابریگ و بوگونی[2] (۲۰۲۳) درباره پیوند میان حکمرانی داده و حفاظت از حریم خصوصی در شهرهای هوشمند نوظهور مطابقت دارد. پژوهش میسرا و همکاران (۲۰۲۵) بر چالش تعادل میان نظارت، امنیت، حریم خصوصی و حاکمیت دیجیتال تأکید کرده است. یافته‌های پژوهش حاضر این تعارض را در بستر ایران به‌صورت عملیاتی‌تر صورت‌بندی کرده و ابزارهایی همچون طبقه‌بندی داده‌ها، ارزیابی اثر حریم خصوصی و داشبوردهای عمومی را به‌عنوان سازوکارهای قابل اجرا پیشنهاد می‌کند.

در عین حال، در این محور نوعی تفاوت با رویکردهای صرفاً فناوری‌محور مشاهده می‌شود. برخی مطالعات، از جمله مطالعات مربوط به اینترنت اشیا، هوش مصنوعی و رایانش ابری، بیشتر بر قابلیت‌های فنی این فناوری‌ها برای بهبود خدمات شهری تمرکز دارند، اما یافته‌های پژوهش حاضر نشان می‌دهد که ارزش فناوری به‌تنهایی تعیین‌کننده موفقیت شهر هوشمند نیست، بلکه چگونگی جمع‌آوری، ذخیره‌سازی، پردازش و استفاده از داده‌ها، میزان شفافیت نهادهای عمومی و امکان نظارت شهروندان نیز اهمیت دارد. از این منظر، پژوهش حاضر با دیدگاه مورا و همکاران هم‌راستا است که گذار به شهر هوشمند را یک فرایند

1. Akgün et al

2. Fabrègue & Bogoni

نوآوری شهری و مدیریتی می‌دانند، نه دستیابی به یک محصول یا وضعیت نهایی.

چهارمین مضمون سازمان‌دهنده، مدیریت ریسک، امنیت و تاب‌آوری است. نتایج تحقیق انجام ارزیابی‌های دوره‌ای ریسک سایبری و حریم خصوصی، تدوین برنامه‌های تداوم کسب‌وکار و مدیریت بحران، ایجاد یا تقویت عملیات امنیتی در سطح شهر و ادغام ایمنی فیزیکی با امنیت سایبری تأکید دارد. این یافته نشان می‌دهد که امنیت شهر هوشمند نباید به حفاظت از شبکه‌ها و سامانه‌های نرم‌افزاری محدود شود، بلکه باید خدمات حیاتی، زیرساخت‌های فیزیکی، مراکز داده، حمل‌ونقل، انرژی، آب، بهداشت و ارتباطات را نیز در برگیرد.

نتیجه فوق با پژوهش نوچی و همکاران (۲۰۲۳) درباره حکمرانی شهر هوشمند در شهرداری سقز هم‌راستا است. آنان تهدیدهای فناورانه، سازمانی و امنیتی را شناسایی کرده و بر ایجاد نظام متمرکز جمع‌آوری داده، ارزیابی مستمر ریسک و تقویت ظرفیت‌های تخصصی تأکید کردند. همچنین، یافته حاضر با مدل حکمرانی امنیت عمومی شهری لی و همکاران (۲۰۲۳) همخوانی دارد که هر دو بر مدیریت یکپارچه بحران، هماهنگی بین سازمان‌ها و استفاده از فناوری برای پیشگیری، تشخیص و پاسخ به تهدیدها تأکید می‌کنند. تفاوت مهم این پژوهش با برخی مطالعات پیشین آن است که امنیت را به‌عنوان یکی از ابعاد مستقل شهر هوشمند بررسی نمی‌کند، بلکه آن را در سراسر چرخه سیاست‌گذاری، طراحی، اجرا و ارزیابی پروژه‌ها جاری می‌سازد. امنیت از نظر یافته‌های پژوهش حاضر باید از آغاز در معماری شهر هوشمند نهادینه شود.

پنجمین مضمون، مشارکت ذی‌نفعان و مشروعیت اجتماعی است. تشکیل شورای مشورتی شهر با حضور دانشگاه، بخش خصوصی و جامعه مدنی، استفاده از کانال‌های مشاوره عمومی، اجرای کمپین‌های آگاهی‌بخشی درباره تهدیدهای سایبری و گزارش‌دهی حوادث و تضمین نظارت انسانی بر سیستم‌های خودکار، از مهم‌ترین مؤلفه‌های این محور هستند. یافته‌ها نشان داد که حکمرانی دولتی مؤثر به معنای تمرکز کامل قدرت در دولت نیست، بلکه دولت باید زمینه مشارکت، گفت‌وگو و نظارت اجتماعی را فراهم کند.

این نتیجه به‌طور مستقیم با پژوهش افشاری و همکاران (۲۰۲۴) هم‌راستا است. آنان اعتماد عمومی، مشارکت شهروندان و سواد دیجیتال را از عوامل حیاتی موفقیت شهر هوشمند تهران دانستند. همچنین با مطالعه توانایی مروی و همکاران درباره شهر هوشمند به‌مثابه برساخت اجتماعی همخوانی دارد، زیرا در آن پژوهش نیز هم‌آفرینی، شفافیت، اعتماد عمومی، تنوع اجتماعی و همه‌شمولی به‌عنوان شرایط تحقق شهر هوشمند شناسایی شدند. پژوهش حاضر نشان می‌دهد که مشارکت اجتماعی فقط برای بهبود کیفیت خدمات یا افزایش رضایت شهروندان ضروری نیست، بلکه برای شناسایی تهدیدها، گزارش حوادث، تقویت اعتماد و مشروعیت‌بخشی به تصمیم‌های فناورانه نیز اهمیت دارد. با این حال، یافته‌های پژوهش حاضر با رویکردهای اقتدارگرایانه یا فناوری‌محور که شهروندان را صرفاً مصرف‌کننده خدمات دیجیتال تلقی می‌کنند، هم‌راستا نیست. در چنین رویکردهایی، نظارت، تصمیم‌گیری الگوریتمی و جمع‌آوری داده بدون مشارکت مؤثر شهروندان انجام می‌شود. در مقابل، نتایج این پژوهش بر نظارت انسانی، پروتکل‌های شفاف و امکان دریافت بازخورد عمومی تأکید دارد. بنابراین، مشروعیت اجتماعی باید هم‌زمان با کارایی فنی و امنیتی مورد توجه قرار گیرد، زیرا اجرای سامانه‌هایی که از نظر فنی پیشرفته‌اند اما فاقد اعتماد عمومی هستند، در بلندمدت با مقاومت اجتماعی و کاهش استفاده شهروندان مواجه خواهد شد.

ششمین مضمون، استانداردها، قابلیت‌های فنی ـ سازمانی و ظرفیت‌سازی است. یافته‌ها پذیرش استانداردهای ملی امنیت سایبری، ترویج قابلیت همکاری سامانه‌ها و داده‌های باز، سرمایه‌گذاری در آموزش و صدور گواهی‌نامه برای کارکنان فناوری و امنیت و همسوسازی ابتکارات شهری با برنامه‌های ملی را ضروری دانستند. این مضمون نشان می‌دهد که حتی در صورت وجود قوانین و ساختارهای نهادی، نبود ظرفیت اجرایی می‌تواند مانع تحقق شهر هوشمند شود.

یافته‌های این بخش با پژوهش شفیعی و آیت (۱۴۰۴) همخوانی دارد که بر ضرورت توجه هم‌زمان به ابعاد مختلف توسعه تأکید داشتند. همچنین، با نتایج فولادی و کمالی (۱۴۰۴) درباره اهمیت شاخص‌های بومی، زیرساخت، حکمرانی داده‌محور، تاب‌آوری، عدالت دسترسی و سواد دیجیتال هم‌راستا است. پژوهش حاضر نیز نشان می‌دهد که استانداردهای جهانی باید با شرایط نهادی، اقتصادی، فنی و اجتماعی ایران سازگار شوند. در نتیجه نمی‌توان مدل‌های شهر هوشمند کشورهای توسعه‌یافته را بدون اصلاح و بومی‌سازی در ایران اجرا کرد.

در عین حال، یافته‌های پژوهش حاضر نشان می‌دهد که میان تأکید بر استانداردهای ملی و ضرورت قابلیت همکاری بین‌المللی یا بین‌سازمانی باید توازن ایجاد شود. استانداردهای کاملاً بسته و انحصاری ممکن است به جزیره‌ای‌شدن سامانه‌ها و افزایش وابستگی به تأمین‌کنندگان خاص منجر شود. از سوی دیگر، استفاده بدون ملاحظه از استانداردهای خارجی می‌تواند با الزامات امنیتی، حقوقی و نهادی کشور سازگار نباشد. بنابراین، رویکرد مطلوب، تدوین استانداردهای بومی و باز، مبتنی بر قابلیت همکاری، امنیت، انعطاف‌پذیری و امکان ارزیابی مستقل است.

در مجموع، مقایسه یافته‌های پژوهش با پیشینه نشان می‌دهد که نتایج در بیشتر موارد با مطالعات داخلی و خارجی هم‌راستا است، پژوهش حاضر ابعاد پراکنده حکمرانی شهر هوشمند را در یک چارچوب منسجم و بومی برای ایران ترکیب می‌کند و امنیت سایبری، حفاظت از داده، تاب‌آوری و ایمنی فیزیکی را در کنار مشارکت اجتماعی، شفافیت و ظرفیت‌سازی قرار می‌دهد و نقش دولت را نه به‌عنوان مجری مستقیم همه امور، بلکه به‌عنوان سیاست‌گذار، تنظیم‌گر، هماهنگ‌کننده، تضمین‌کننده حقوق عمومی و توانمندساز شبکه‌ای از بازیگران تبیین می‌کند.

بر اساس یافته‌های پژوهش، پیاده‌سازی شهر هوشمند امن در ایران صرفاً به تأمین زیرساخت‌های فناورانه یا اجرای پروژه‌های هوشمندسازی محدود نمی‌شود، بلکه مستلزم توجه به الزامات نهادی، سیاستی، امنیتی و اجتماعی در قالب رویکردی حکمرانی‌محور است. در پاسخ به پرسش اصلی پژوهش درباره ابعاد حکمرانی دولتی مؤثر بر پیاده‌سازی شهر هوشمند امن، شش بعد شامل سیاست‌گذاری و راهبردهای قانونی ـ نظارتی، معماری نهادی و هماهنگی بین‌سازمانی، حکمرانی داده‌ها و حریم خصوصی، مدیریت ریسک و تاب‌آوری، مشارکت ذی‌نفعان و مشروعیت اجتماعی و استانداردها و ظرفیت‌های فنی ـ سازمانی شناسایی شد. این ابعاد بیانگر آن‌اند که مسئولیت دولت در این حوزه تنها به تأمین منابع و اجرای برنامه‌ها محدود نیست، بلکه سیاست‌گذاری، تنظیم‌گری، ایجاد هماهنگی میان نهادها و صیانت از حقوق شهروندان را نیز دربرمی‌گیرد. در این چارچوب، شهرداری‌ها نیز می‌توانند در کنار دولت، به‌عنوان بازیگران مؤثر در تصمیم‌گیری و اجرای راهبردهای شهر هوشمند امن ایفای نقش کنند.

یافته‌های مربوط به ابعاد شش‌گانه، نشان می‌دهد که این ابعاد در چارچوب مفهومی پژوهش، حوزه‌های مرتبط و مکمل حکمرانی شهر هوشمند امن را نشان می‌دهند، یافته‌های مربوط به سیاست‌گذاری بر اهمیت وجود جهت‌گیری‌های روشن و الزامات قانونی تأکید دارند، درحالی‌که بعد معماری نهادی، ضرورت تعیین مسئولیت‌ها و هماهنگی میان سازمان‌ها را برجسته می‌سازد. همچنین، توجه به حکمرانی داده‌ها، امنیت و حریم خصوصی، مشارکت ذی‌نفعان و ظرفیت‌های فنی و انسانی نشان می‌دهد که پیاده‌سازی شهر هوشمند امن، موضوعی چندبعدی است و نمی‌توان آن را صرفاً از منظر فناوری یا امنیت فنی تحلیل کرد. بنابراین سهم نظری پژوهش در ارائه چارچوبی زمینه‌مند برای تبیین نقش حکمرانی دولتی در شهر هوشمند امن است. از منظر کاربردی، یافته‌های پژوهش بر ضرورت توجه سیاست‌گذاران به ایجاد سازوکارهای هماهنگی ملی و محلی، شفاف‌سازی مسئولیت نهادهای ذی‌ربط، تدوین الزامات مرتبط با امنیت و حریم خصوصی و تقویت مشارکت ذی‌نفعان دلالت دارد.

راهکارها

شایسته است اهمیت نسبی شش مضمون سازمان‌دهنده در شهرهای بزرگ، از جمله تهران، مشهد، اصفهان، شیراز و تبریز بررسی شود و مطالعات آینده نقش شهروندان، گروه‌های کم‌برخوردار، سالمندان، افراد دارای معلولیت و ساکنان مناطق پیرامونی را در حکمرانی شهر هوشمند بررسی کنند تا ابعاد عدالت دیجیتال و همه‌شمولی در مدل تقویت شود و رابطه میان اعتماد عمومی، سواد دیجیتال، مشارکت شهروندی و پذیرش خدمات هوشمند با استفاده از مطالعات پیمایشی تحلیل شود.

در نهایت، شهر هوشمند امن در ایران زمانی تحقق خواهد یافت که فناوری در خدمت حکمرانی پاسخگو، شفاف، مشارکتی و تاب‌آور قرار گیرد. دولت باید به‌جای تمرکز صرف بر خرید و استقرار تجهیزات، بر ایجاد نهادهای هماهنگ، قوانین روشن، زیرساخت‌های قابل اعتماد، نیروی انسانی متخصص و مشارکت معنادار شهروندان تمرکز کند. چنین رویکردی می‌تواند زمینه‌ساز شکل‌گیری شهری باشد که نه‌تنها هوشمند و کارآمد، بلکه امن، عادلانه، پاسخگو و متناسب با ویژگی‌های نهادی و اجتماعی ایران است.

مشارکت نویسندگان

جمع‌آوری داده‌ها: نویسنده اول و نویسنده دوم تهیه گزارش پژوهش: نویسنده دوم تحلیل داده‌ها نویسنده اول و دوم

تعارض منافع

بنابر اظهار نویسندگان این مقاله تعارض منافع ندارد.

تأمین مالی

پژوهش حاضر از هیچ مؤسسه و نهادی حمایت مالی دریافت نکرده و کلیه هزینه‌ها در طول فرآیند اجرای پژوهش بر عهده پژوهشگر بوده است.

سپاسگزاری

نویسنده برخود وظیفه می‌داند از کلیه استادان و پژوهشگرانی که در تدوین این مقاله ما را یاری رساندند، تقدیر و تشکر نماید.

References

Afshari, H., Zolghadr, M., & Partovi, A. (2024). Public Policy in Tehran toward E-Government Development and Smart City Implementation. *Digital Transformation and Administration Innovatio*n, 2(3), 114–130. (in Persian). https://doi.org/10.61838/dtai.2.3.12

Akgün, E. Z., Gerli, P., Mora, L., & McTigue, C. (2024). Breaking barriers for breaking ground: A categorisation of public sector challenges to smart city project implementation. *Public Policy and Administration*, 39(3), 1–18. https://doi.org/10.1177/09520767241263233

Attride-Stirling, J. (2001). Thematic networks: an analytic tool for qualitative research. Qualitative research, 1(3), 385-405.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101.

Caragliu, A., Del Bo, C., & Nijkamp, P. (2011). Smart Cities in Europe. *Journal of Urban Technology*, 18(2), 65–82. https://doi.org/10.1080/10630732.2011.601117

Chatterji, S., & Mukkai, S. (2024). Digital infrastructure fragmentation and institutional capacity in India's Smart Cities Mission. *Journal of Urban Technology*, 32(4), 512–530. https://doi.org/10.1080/10630732.2025.2549672

Fabrègue, N., & Bogoni, L. (2023). Data governance and privacy in emerging smart cities. *South African Journal of Information Management*, 25(1), 1–16. https://doi.org/10.4102/sajim.v25i1.1847

Fooladi, P., Kamali, M. (2025). Indigenous indicators for smart city assessment in Iranian metropolises: A systematic review and qualitative analysis. *Governance and Smart City*, 1(1), 1-11. (In Persian).

Hardi, R., Nurmandi, A., Purwaningsih, T., & Manaf, H. A. (2025). Smart city governance and interoperability: enhancing human security in Yogyakarta and Makassar, Indonesia. *Frontiers in Political Science*, *7*, 1553177. https://doi.org/10.3389/fpos.2025.1553177

Karami, H., Faghihi, A & Memarzadeh Tehran, G. (2024). Designing an Operational Governance Model for Smart City. Iranian Public Administration Studies, 7(2), 175–206. (In Persian). https://doi.org/10.22034/jipas.2024.368996.1504

Kim, C., & Kim, K. A. (2021). The institutional change from E-Government toward Smarter City; comparative analysis between royal borough of Greenwich, UK, and Seongdong-gu, South Korea. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(1), 1-33. https://doi.org/10.3390/joitmc7010042

Li, G., Wang, J., & Wang, X. (2023). Construction and path of urban public safety governance and crisis management optimization model integrating artificial intelligence technology. *Sustainability*, *15*(9), 1-19. https://doi.org/10.3390/su15097487

Lnenicka, M., Kysela, T., & Horák, O. (2025). Building security and resilience: A guide to implementing effective cybersecurity and data protection measures in smart cities. *Smart and Sustainable Built Environment*. *15*(2), 908-937. https://doi.org/10.1108/SASBE-09-2024-0363

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.https://doi.org/10.1177/0020852314564308

Misra, S., Kumar, R., & Singh, A. (2025). Smart city surveillance: Governance challenges in balancing privacy, security, and digital sovereignty. *Sustainable Development*, 34(1), 10–25. https://doi.org/10.1002/sd.70620

Mora, L., Gerli, P., Ardito, L., & Messeni Petruzzelli, A. (2023). Smart city governance from an innovation management perspective: Theoretical framing, review of current practices, and future research agenda. *Technovation*, 123, 1–14. 10.1016/j.technovation.2023.102717

Nucci, L., Heydari, A., Gilani, N., Aminpoor, S., Liu, Y., & Gheisari, M. (2023). Historical trends in smart city governance for the management of ancient urban centers in Iran: A case study of Saqqez Municipality. *International Journal of Innovative Management*, *3*(3), 203-211. https://doi.org/10.61838/kman.ijimob.3.3.25

OECD. (2023). *Smart city data governance* (pp. 15–42). OECD Publishing. https://www.oecd.org/en/publications/smart-city-data-governance_e57ce301-en/full-report.html

OECD. (2025). *Implementation challenges that hinder the strategic use of AI in government*. OECD Publishing. 20–35.

Raghava Rao, K., and Kumar, D. S. (2022). *Smart City governance using big data technologies in advanced analytics and deep learning models*. (Hoboken, New Jersey, United States: Wiley), 311–324.

Saberifar, R. (2019). Determining and identifying effective factors in designing a smart organization for urban management (case study: Mashhad Municipality). Research in Urban Planning Geography, 8(2), 445–467. (in Persian). https://doi.org/10.22059/jurbangeo.2020.299143.1245

Sedighi, N, Sanae, M R., & Ehtesham Rathi, R. (2021). Identifying and assessing cybersecurity and privacy challenges in the transition of Tehran metropolis to a smart city under conditions of uncertainty. Smart Business Management Studies, 10(38), 109–136. (In Persian).

Shafiei, S., & Ayat, M. (2025). Identifying and Analyzing Dimensions and Indicators of Smart City Development. *Strategic Management Studies Quarterly*, 16(61), 167-196. (In Persian) Doi: 10.22034/smsj.2023.391055.1822

Shi, D., & Cao, X. (2022). Research on the effectiveness of government governance in the context of smart cities. International Conference on Intelligent Traffic Systems and Smart City (ITSSC 2021), 5. https://doi.org/10.1117/12.2627766

Subrahmanyam, S. (2025). Data Governance and Privacy in Smart Cities. *Citizen-Centric Artificial Intelligence for Smart Cities*, 433–456. https://doi.org/10.4018/979-8-3693-7832-8.ch017

Tavanaei Marvi, L., & Zakhimi, N. (2026). Towards a Socially Constructed Smart City in Iran: Developing a Grounded Theory-Informed Conceptual Framework. *Human Geography Research*, 58(2), 163-179. (In Persian) https://doi.org/10.22059/jhgr.2026.396514.1008815

Tavanaei Marvi, L., Behzadfar, M., & Mofidi Shemirani, S. M. (2022). Analysis Smart City Implementation Challenges Case Study: Mashhad. *Sustainable city*, *5*(1), 45-58. (In Persian) Doi: 10.22034/jsc.2022.311642.1578