

A Legal and Security Study on Data Privacy in Smart Cities with a Focus on IoT and Blockchain

Ghazaleh Shahinzadeh^{1*}  | Khodadad Khodadadi Dashtaki²  | Zahra Moradi³  | S. Mohammadali Zanjani⁴⁻⁵ 

¹ Faculty of Law and Social Sciences, Payame Noor University, Isfahan, Iran, ghazaleh.shahinzadeh@isfahan.pnu.ac.ir

² Department of Law, Faculty of Law and Social Sciences, Payam Noor University, Tehran, Iran, khodadadi.kh@pnu.ac.ir

³ Faculty member of Department of Law, Faculty of Law and Social Sciences, Payam Noor University, Tehran, Iran. zahramoradi_80@pnu.ac.ir

⁴ Department of Electrical Engineering, Na.C., Islamic Azad University, Najafabad, Iran. smazanjani@iau.ac.ir

⁵ Smart Microgrid Research Center, Na.C., Islamic Azad University, Najafabad, Iran.

Correspondence

Ghazaleh Shahinzadeh, M.Sc., Faculty of Law and Social Sciences, Payame Noor University, Isfahan, Iran.

Email:

ghazaleh.shahinzadeh@isfahan.pnu.ac.ir

Main Subjects:

Smart City

Paper History:

Received: 10 August 2024

Revised: 5 September 2024

Accepted: 15 September 2024

Abstract

The advancement of smart cities and the expansion of the Internet of Things (IoT), along with the need to reduce energy consumption in green smart cities, signify a revolution in urban planning and management. Despite social improvements and increased efficiency, these advancements bring new challenges, particularly in the realm of security and privacy protection. The widespread use of sensors and smart devices leads to the collection and processing of vast amounts of data, which, if mismanaged, can pose significant threats to data security and individual privacy. Blockchain, as an emerging technology, offers new capabilities for enhancing security and privacy. This study conducts a detailed examination of the impact of existing policies and laws on security and privacy in smart cities and analyzes the role of IoT and blockchain technologies in improving these areas. It also explores the security and privacy challenges and the integration of these technologies into urban management. This research aims to optimize the use of modern technologies while ensuring the security and privacy of citizens in smart cities, thereby enhancing overall efficiency and public welfare while safeguarding citizens' privacy rights.

Keywords: Blockchain, Data security, Internet of Things, Privacy, Smart cities.

Highlights

- Analysis of data privacy and security challenges in the context of IoT and blockchain technologies in smart cities.
- In-depth examination of legal frameworks governing data protection and privacy in urban environments.
- Proposal of blockchain as a solution for addressing privacy concerns in IoT ecosystems within smart city infrastructure.
- Case study focusing on smart city legal and regulatory environments, with a spotlight on Iranian data protection laws.

Citation: Gh. Shahinzadeh, K. K. Dashtaki, Z. Moradi, S.M. Zanjani, "A Legal and Security Study on Data Privacy in Smart Cities with a Focus on IoT and Blockchain," *Journal of Southern Communication Engineering*, vol. 15, no. 57, pp. 90-115, 2025, doi:10.30495/jce.2025.1993480.1342 [in Persian].

COPYRIGHTS

©2025 by the authors. Published by the Islamic Azad University Bushehr Branch. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY 4.0) <https://creativecommons.org/licenses/by/4.0>



1. Introduction

With the rapid acceleration of urbanization, smart cities have emerged as pivotal factors in transforming urban spaces. These cities, leveraging advanced technologies such as the Internet of Things (IoT) and big data analytics, bring significant improvements to the quality of life for citizens. Urban experts and planners are integrating cutting-edge technologies, including cloud computing and sensors, to redesign urban infrastructures for comprehensive and multidimensional interaction with smart networks [1].

Recent research highlights that cities such as London, New York, and Paris are increasingly embracing smart transformations. These developments involve building new infrastructure and enhancing existing assets and networks [2]. Moreover, the Indian government has launched a plan to develop 100 smart cities aimed at driving economic growth through technological solutions for citizen engagement. Similarly, China is adopting a government-driven approach to implementing smart cities, resulting in enhanced economic structures and increased labor competitiveness [3].

Global spending on smart city projects is estimated to be approximately \$81 billion, with projections to rise to \$1.91 trillion by 2030. Key technologies deployed in these cities include cloud computing, IoT, and networks of sensors. However, the transformation of existing infrastructures and the management of new citizen interactions present significant challenges for governments and local authorities, particularly in political, regulatory, and technical domains [4]. As smart cities evolve and IoT expands, security and privacy issues have become increasingly prominent. The use of advanced technologies, such as IoT and big data analytics, necessitates a strong focus on information security and privacy protection [5].

While existing research emphasizes the development of smart cities, comprehensive analyses of data security threats and privacy complexities appear to be lacking. The primary objective of this study is to address this gap by providing an in-depth analysis of the issues and challenges related to privacy and security in smart cities [6]. Data security in the face of cyber threats and unauthorized access is considered one of the most critical and sensitive challenges [7-9]. This paper aims to cover the existing gap by conducting a thorough examination of the threats and complexities associated with data security and privacy and addressing essential questions regarding how these issues should be managed in the digital age [10]. In this context, the present study evaluates the existing legal and regulatory frameworks and analyzes their effectiveness in coping with emerging technologies and innovative approaches, aiming to strike a balance between technological advancement and individual rights.

2. Innovation and contributions

The novelty of this research lies in its interdisciplinary approach, bridging the gap between computer science and legal studies to tackle privacy and security issues in smart cities. First, it provides a critical assessment of how blockchain technology, when integrated with IoT infrastructures, can mitigate privacy concerns through decentralized transparent data management. Unlike existing centralized systems, blockchain enhances trust among stakeholders by enabling secure, immutable data exchanges without a need for third-party intermediaries. Second, this study introduces a legal-technical framework that evaluates current privacy regulations—such as GDPR, CCPA, and sector-specific data protection laws—within the context of smart city ecosystems. It assesses whether these regulations are sufficient to address the complex privacy and security challenges posed by IoT networks and proposes enhancements that could better align with the rapidly evolving digital environment. Finally, this paper's contribution extends to a case study on the Iranian legal landscape, offering a unique perspective on how developing nations are navigating the balance between urban innovation and citizen data protection. By examining the legal efficacy of Iranian data protection policies, the study highlights the global relevance of these challenges and offers tailored solutions for emerging smart cities around the world.

3. Materials and Methods

This research employs a combination of legal analysis, case studies, and technical assessments to evaluate the data privacy implications of IoT and blockchain integration in smart cities. From a legal perspective, the study conducts a doctrinal analysis of key international and national privacy frameworks, including GDPR, CCPA, and Iran's data protection laws. It examines how these regulations govern data collection, storage, and dissemination in smart city contexts and explores potential gaps in their application, particularly concerning IoT and blockchain technologies. Furthermore, the study reviews court cases, regulatory enforcement actions, and policy documents to assess the real-world application of these legal frameworks. Technologically, the paper uses system security evaluation methodologies to assess blockchain's ability to enhance data protection in IoT networks. This involves the examination of cryptographic techniques, data hashing, consensus protocols, and smart contracts that form the core of blockchain security model. The effectiveness of blockchain in mitigating threats such as unauthorized access, data breaches, and privacy violations within smart city networks is critically analyzed. The research also includes a comparative case study on Iran's smart city initiatives, focusing on legal frameworks and their interaction with technological innovation. This case study highlights the regional differences in regulatory approaches and the potential for international harmonization of privacy standards in the context of global urban development.

4. Results and Discussion

The results of the legal analysis indicate that existing privacy laws, such as GDPR and CCPA, are insufficient to fully address the privacy risks posed by IoT devices in smart cities. These frameworks often focus on centralized systems, which fail to account for the decentralized, distributed nature of IoT networks. For instance, while GDPR emphasizes data minimization and purpose limitation, IoT systems continuously collect and process vast amounts of data, making compliance with these principles challenging. From a technological standpoint, blockchain shows promise in mitigating some of the security challenges associated with IoT data management. The use of cryptographic protocols ensures that data transmitted within a smart city environment is encrypted and verified, reducing the risk of data breaches. Moreover, the blockchain decentralized nature aligns with the distributed architecture of IoT systems, enhancing data integrity and security. However, the study also identifies scalability and latency as potential limitations of blockchain technology in large-scale urban environments. The Iranian case study reveals that the country's current data protection frameworks are underdeveloped in comparison to international standards. Although recent legislative initiatives, such as the Data Protection and Privacy in Cyberspace Bill, show progress, significant gaps remain in the enforcement and regulatory oversight of data privacy in smart cities. The integration of blockchain technologies into Iranian smart city projects offers a pathway to enhancing citizen trust, but it will require substantial legal reforms to ensure compliance with global privacy norms.

5. Conclusion

The examination of security and privacy issues in smart cities and the proposal of improvement strategies reveal that, with the advancement of technology and the expansion of smart cities, data security and the protection of individual privacy have become critical challenges in these environments. These issues encompass unauthorized access to data, cyber threats, and privacy violations, which require innovative and effective solutions for resolution. To enhance security and privacy in smart cities, several measures are essential, including the reform and improvement of relevant laws and regulations, the development of appropriate technological infrastructure, education and awareness for citizens, and collaboration between institutions and industries. Moreover, leveraging modern technologies such as the IoT and blockchain can significantly improve data security and privacy protection in smart cities. The effective implementation of these solutions, alongside the coordination of various institutions and industries, can pave the way for building smart cities with a high level of security and privacy. Therefore, a thorough analysis of these issues and the presentation of improvement solutions will contribute to the progress and development of smart urban environments, enhancing citizen satisfaction within these cities.

6. Acknowledgement

We want to extend our sincere gratitude to the editorial board of "The Journal of Southern Communication Engineering" for providing the opportunity to publish this article.

References

- [1] F. Moqaddari, "Redefining the concept of smart cities and the process of urban smartification based on the conceptual and functional evolution of smart cities," *Urban Design Discourse; Review of Contemporary Literature and Theories*, vol. 1, no. 2, 2020 (in Persian).
- [2] H. M. Kim, S. Sabri, and A. Kent, "Smart cities as a platform for technological and social innovation in productivity, sustainability, and livability: A conceptual framework," in *Smart Cities for Technological and Social Innovation*, Academic Press, 2021, pp. 9–28, doi: [10.1016/b978-0-12-818886-6.00002-2](https://doi.org/10.1016/b978-0-12-818886-6.00002-2).
- [3] A. Randhawa and A. Kumar, "Exploring sustainability of smart development initiatives in India," *International Journal of Sustainable Built Environment*, vol. 6, no. 2, pp. 701–710, 2017, doi: [10.1016/j.ijbsbe.2017.08.002](https://doi.org/10.1016/j.ijbsbe.2017.08.002).
- [4] M. Whaiduzzaman, A. Barros, M. Chanda, S. Barman, T. Sultana, M. S. Rahman, and C. Fidge, "A review of emerging technologies for IoT-based smart cities," *Sensors*, vol. 22, no. 23, p. 9271, 2022, doi: [10.3390/s22239271](https://doi.org/10.3390/s22239271).
- [5] A. Venkatesh and M. S. Eastaff, "A study of data storage security issues in cloud computing," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 3, no. 1, pp. 1741–1745, 2018, doi: [10.9756/bijsec.9012](https://doi.org/10.9756/bijsec.9012).
- [6] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and privacy of smart cities: a survey, research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1718–1743, 2018, doi: [10.1109/COMST.2018.2655555](https://doi.org/10.1109/COMST.2018.2655555).

[10.1109/comst.2018.2867288](https://doi.org/10.1109/comst.2018.2867288).

- [7] B. Hammi, R. Khatoun, S. Zeadally, A. Fayad, and L. Khoukhi, "IoT technologies for smart cities," *IET Networks*, vol. 7, no. 1, pp. 1–13, 2018, doi: [10.1049/iet-net.2017.0163](https://doi.org/10.1049/iet-net.2017.0163).
- [8] M. H. P. Rizi and S. A. H. Seno, "A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city," *Internet of Things*, vol. 20, p. 100584, 2022, doi: [10.1016/j.iot.2022.100584](https://doi.org/10.1016/j.iot.2022.100584).
- [9] L. D. Radu, "Disruptive technologies in smart cities: a survey on current trends and challenges," *Smart Cities*, vol. 3, no. 3, pp. 1022–1038, 2020, doi: [10.3390/smartcities3030051](https://doi.org/10.3390/smartcities3030051).
- [10] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," *Information Systems Frontiers*, pp. 1–22, 2022, doi: [10.1007/s10796-020-10044-1](https://doi.org/10.1007/s10796-020-10044-1).

Declaration of Competing Interest: Authors do not have conflict of interest. The content of the paper is approved by the authors.

Author Contributions: Ghazaleh Shahinzadeh: literature review, data analysis, and manuscript writing; Khodadad Khodadadi Dashtaki: Supervision; Zahra Moradi: Supervision; S. Mohammadali Zanjani: manuscript editing.

Open Access: Journal of Southern Communication Engineering is an open access journal. All papers are immediately available to read and reuse upon publication.

مطالعه حقوقی و امنیتی حریم خصوصی داده‌ها در شهرهای هوشمند با تمرکز بر اینترنت اشیا و بلاک چین

غزاله شاهین زاده^{۱*} | خداداد خدادادی دشتکی^۲ | زهرا مرادی^۳ | سیدمحمدعلی زنجانی^{۴-۵}

چکیده:

پیشرفت شهرهای هوشمند و گسترش اینترنت اشیا، به همراه نیاز به کاهش مصرف انرژی در شهرهای هوشمند سبز، نمایانگر یک انقلاب در شهرسازی و مدیریت شهری است. با وجود بهبودهای اجتماعی و افزایش کارایی، این پیشرفت‌ها چالش‌های جدیدی به خصوص در زمینه امنیت و حفظ حریم خصوصی به همراه دارند. استفاده بیش‌ازپیش از حسگرها و دستگاه‌های هوشمند، منجر به جمع‌آوری و پردازش حجم زیادی از اطلاعات شده است که در صورت مدیریت نامناسب، می‌تواند به تهدیدی برای امنیت داده‌ها و حریم خصوصی افراد تبدیل شود. بلاک‌چین به‌عنوان یک فناوری نوین، قابلیت‌های جدیدی برای افزایش امنیت و حفظ حریم خصوصی ارائه می‌دهد. این تحقیق به بررسی دقیق تأثیر سیاست‌ها و قوانین موجود بر امنیت و حریم خصوصی در شهرهای هوشمند پرداخته و نقش فناوری‌های اینترنت اشیا و بلاک‌چین را در بهبود این زمینه‌ها تحلیل می‌کند. همچنین چالش‌های امنیتی و حریم خصوصی و نحوه ادغام این فناوری‌ها در مدیریت شهری موردبررسی قرار گرفته است. هدف این تحقیق، استفاده بهینه از فناوری‌های نوین و حفظ امنیت و حریم خصوصی شهروندان در شهرهای هوشمند است، تا به این وسیله کارایی و رفاه عمومی ارتقا یابد و حقوق حریم خصوصی شهروندان محافظت شود.

کلیدواژه‌ها: امنیت داده، اینترنت اشیا، بلاک‌چین، حفظ حریم خصوصی، شهرهای هوشمند.

^۱ دانشکده حقوق و علوم اجتماعی، دانشگاه پیام نور، اصفهان، ایران.

ghazaleh.shahinzadeh@isfahan.pnu.ac.ir

^۲ گروه حقوق، دانشکده حقوق و علوم اجتماعی، دانشگاه پیام نور، تهران، ایران.

khodadadi.kh@pnu.ac.ir

^۳ گروه حقوق، دانشکده حقوق و علوم اجتماعی، دانشگاه پیام نور، تهران، ایران.

zahramoradi_80@pnu.ac.ir

^۴ دانشکده مهندسی برق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

smazanjani@iau.ac.ir

^۵ مرکز تحقیقات ریزشبکه های هوشمند، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

نویسنده مسئول:

* غزاله شاهین زاده، دانش آموخته کارشناسی ارشد، دانشکده حقوق و علوم اجتماعی، دانشگاه پیام نور، اصفهان، ایران.
ghazaleh.shahinzadeh@isfahan.pnu.ac.ir

موضوع اصلی:

شهرهای هوشمند

تاریخچه مقاله:

تاریخ دریافت: ۲۰ مردادماه ۱۴۰۳

تاریخ بازنگری: ۱۵ شهریور ۱۴۰۳

تاریخ پذیرش: ۲۵ شهریور ۱۴۰۳

تازه‌های تحقیق:

- تحلیل چالش‌های حفظ حریم خصوصی و امنیت داده‌ها در بستر اینترنت اشیا و فناوری بلاک‌چین در شهرهای هوشمند.
- بررسی عمیق چارچوب‌های حقوقی حاکم بر حفاظت از داده‌ها و حریم خصوصی در محیط‌های شهری.
- پیشنهاد به‌کارگیری بلاک‌چین به‌عنوان راه‌حلی برای رفع نگرانی‌های مربوط به حریم خصوصی در اکوسیستم‌های اینترنت اشیا در زیرساخت‌های شهرهای هوشمند.
- مطالعه موردی با تمرکز بر وضعیت حقوقی و مقرراتی شهرهای هوشمند، با تأکید ویژه بر قوانین حفاظت از داده‌ها در ایران.

COPYRIGHTS

©2025 by the authors. Published by the Islamic Azad University Bushehr Branch. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY 4.0) <https://creativecommons.org/licenses/by/4.0>



۱- مقدمه

با پیشرفت سریع فرآیند شهرنشینی، شهرهای هوشمند به عنوان عوامل اساسی در تغییر و تحول فضاهای شهری مطرح هستند. این شهرها با بهره‌گیری از فناوری‌های پیشرفته مانند اینترنت اشیا و تجزیه و تحلیل داده‌های بزرگ، بهبود قابل توجهی را در کیفیت زندگی شهروندان به ارمغان می‌آورند. کارشناسان شهری و برنامه‌ریزان با تلفیق فناوری‌های نوین از جمله محاسبات ابری و حسگرها، زیرساخت‌های شهری را به منظور ایجاد تعامل جامع و چندبعدی با شبکه‌های هوشمند بازطراحی می‌کنند [۱]. تحقیقات اخیر نشان می‌دهد که در سطح جهان، شهرهایی از جمله لندن، نیویورک و پاریس، به‌سوی تحولات هوشمند گرایش پیدا کرده‌اند. این تحولات شامل توسعه زیرساخت‌های جدید و بهبود دارایی‌ها و شبکه‌های موجود می‌شود [۲]. همچنین، دولت هند به منظور ایجاد رشد اقتصادی از طریق راه‌حل‌های فناورانه برای تعامل با شهروندان برنامه‌ای را برای توسعه ۱۰۰ شهر هوشمند تدوین کرده است. همچنین، چین از یک رویکرد دولت‌محور برای راه‌اندازی شهرهای هوشمند بهره‌می‌برد که منجر به بهبود ساختارهای اقتصادی و افزایش رقابت‌پذیری نیروی کار می‌شود [۳].

هزینه‌های جهانی مرتبط با پروژه‌های شهرهای هوشمند حدود ۸۱ میلیارد دلار برآورد شده است و انتظار می‌رود که تا سال ۲۰۲۲ به ۱۵۸ میلیارد دلار افزایش یابد. از جمله فناوری‌های استفاده شده در این شهرها می‌توان به محاسبات ابری، اینترنت اشیا، شبکه و حسگرها اشاره کرد. با این حال، تبدیل زیرساخت‌های موجود و مدیریت تعاملات جدید شهروندان، چالش‌های قابل توجهی را برای دولت‌ها و مقامات محلی، به‌ویژه در زمینه‌های سیاسی، نظارتی و فنی ایجاد می‌کند [۴].

در جریان پیشرفت شهرهای هوشمند و گسترش اینترنت اشیا، مسائل امنیتی و حریم خصوصی به‌ویژه اهمیت زیادی پیدا کرده‌اند. استفاده از فناوری‌های پیشرفته مانند اینترنت اشیا و تجزیه و تحلیل داده‌های بزرگ، نیازمند توجه ویژه به امنیت اطلاعات و حفظ حریم خصوصی است [۵].

تحقیقات موجود بر موضوع شهرهای هوشمند تأکید دارند، اما به نظر می‌رسد که تحلیل‌های جامعی از تهدیدات امنیت داده‌ها و پیچیدگی‌های حریم خصوصی انجام نشده‌اند. هدف اصلی این تحقیق پر کردن این شکاف با انجام یک تحلیل جامع از مسائل و پیچیدگی‌های مرتبط با حریم خصوصی و امنیت در شهرهای هوشمند است [۶]. امنیت اطلاعات در مقابل تهدیدات سایبری و دسترسی‌های غیرمجاز، یکی از چالش‌های بزرگ و حساس محسوب می‌شود [۷-۹]. این مقاله قصد دارد با بررسی جامع تهدیدات و پیچیدگی‌های مرتبط با امنیت داده‌ها و حریم خصوصی، شکاف موجود را پوشش دهد و به سؤالات اساسی در مورد نحوه مدیریت این مسائل در عصر دیجیتال پاسخ دهد [۱۰].

در این راستا، مقاله حاضر به ارزیابی موجودیت چارچوب‌های قانونی و نظارتی پرداخته و به تحلیل کارایی آن‌ها در برابر فناوری‌های نوظهور و رویکردهای نوآورانه می‌پردازد تا بتوان به تعادلی میان پیشرفت و حقوق فردی دست یافت. در ادامه و در بخش دوم، چارچوب قانونی جمع‌آوری و استفاده از داده‌ها در شهرهای هوشمند مورد بررسی قرار می‌گیرد که شامل انواع داده‌های جمع‌آوری شده، چالش‌های حقوقی مرتبط با حفاظت از حریم خصوصی، و تأثیر مقررات قانونی بر حریم خصوصی است. سپس، در بخش سوم، پیشرفت‌های فناوری و چالش‌های امنیتی مرتبط با حفظ حریم خصوصی در شهرهای هوشمند (از جمله روش‌های جلوگیری از نفوذ، مدیریت داده‌های حساس، و استفاده از روش‌های رمزنگاری) بررسی می‌شوند. در بخش چهارم، اثربخشی قوانین و مقررات حفاظت از داده در شهرهای هوشمند ایران مورد بررسی و تحلیل قرار می‌گیرد. در بخش پایانی، نتایج کلی از تحقیق و بررسی‌های انجام شده ارائه می‌شود و اهمیت این مطالعه برای درک بهتر چالش‌های حقوقی و امنیتی حریم خصوصی در شهرهای هوشمند بیان شده، پیشنهاداتی برای اقدامات آینده و توسعه مطالعات بیشتر در این زمینه ارائه می‌شود.

۲- چشم‌انداز حقوقی جمع‌آوری و استفاده از داده‌ها در شهرهای هوشمند

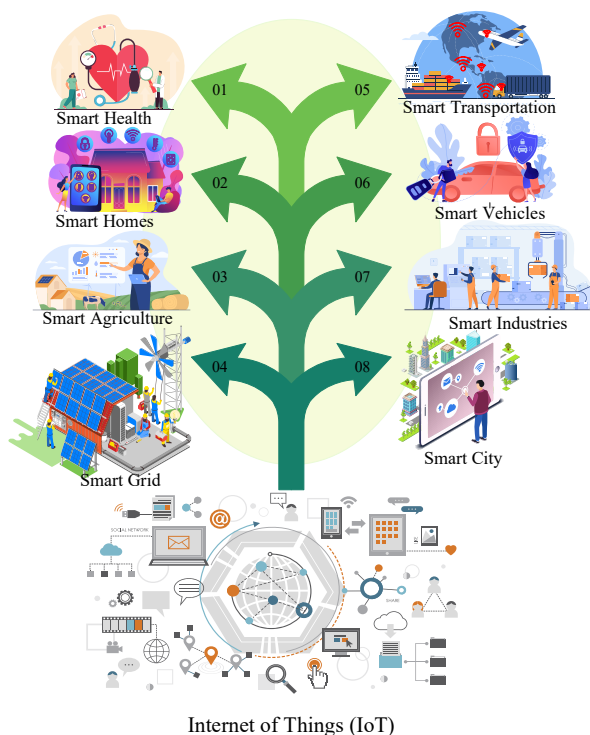
این بخش به بررسی چارچوب قانونی جمع‌آوری و استفاده از داده‌ها در شهرهای هوشمند می‌پردازد و به جوانب مختلفی که برای اطمینان از حفظ حقوق حریم خصوصی و امنیت داده‌ها اساسی است، می‌پردازد. ابتدا، انواع مختلف داده‌هایی که در شهرهای هوشمند جمع‌آوری می‌شود، از داده‌های حسگری تا داده‌های تولیدشده توسط شهروندان بررسی می‌شوند تا اهمیت گستردگی و عمق اطلاعات جمع‌آوری شده را برای امکان اجرای عملیات و خدمات شهری نشان دهد. سپس چالش‌های حقوقی مرتبط با حفاظت از حریم خصوصی و داده‌ها در شهرهای هوشمند و مسائلی مانند مالکیت داده‌ها، رضایت و شفافیت، و همچنین

پیچیدگی‌های اطمینان از رضایت در میان پیشرفته‌های فناوری سریع و مداوم بررسی می‌شوند. با شناسایی این موانع قانونی، سیاست‌گذاران و ذی‌نفعان می‌توانند استراتژی‌های قوی را برای کاهش خطرات و حفظ استانداردهای حریم خصوصی در حالی توسعه دهند که از مزایای فناوری‌های شهر هوشمند بهره می‌برند.

در ادامه، تأثیر مقررات قانونی بر حفظ حریم خصوصی در شهرهای هوشمند بررسی می‌شود تا دلایل نیاز به چارچوب‌های قانونی واکنش‌گر، برای به‌روزرسانی پاسخ به تغییرات فناوری مورد تأکید واقع شود. با ارزیابی کارایی مفاد قانونی فعلی، بخش‌هایی شناسایی می‌شوند که نیاز به بهبود نوآوری‌های قانونی دارند تا حقوق و حریم خصوصی شهروندان در شهرهای هوشمند حفظ شود.

۲-۱- انواع داده‌های جمع‌آوری شده در شهر هوشمند

در شهرهای هوشمند، انواع گوناگونی از داده‌ها از طریق حسگرها، دستگاه‌ها و سامانه‌های متصل به یکدیگر جمع‌آوری می‌شوند. این داده‌ها شامل اطلاعات شخصی مانند هویت افراد، موضوعات موردعلاقه و رفتارها یا سبک زندگی است، همچنین داده‌های غیرشخصی مرتبط با زیرساخت‌های شهری، الگوهای ترافیکی، شرایط محیطی، کیفیت هوا، مدیریت پسماند و مصرف انرژی را نیز شامل می‌شوند [۱۱]. جمع‌آوری این داده‌های متنوع، سامانه‌های شهر هوشمند را قادر می‌سازد تا خدمات شهری را بهینه‌سازی کند، کارایی را افزایش دهد و کیفیت زندگی کلان شهروندان را بهبود بخشد. اطلاعات شخصی شامل داده‌هایی مانند هویت و رفتار افراد است که با آن‌ها مرتبط می‌شوند. این موارد شامل نام، آدرس، اطلاعات تماس، فعالیت‌های رسانه‌ای اجتماعی و حتی داده‌های بیومتریک می‌شود. اطلاعات شخصی اغلب از طریق منابع مختلفی مانند دستگاه‌های هوشمند، برنامه‌های تلفن همراه، دوربین‌های نظارتی و شبکه‌های وای-فای عمومی جمع‌آوری می‌شوند. جمع‌آوری و پردازش اطلاعات شخصی در شهرهای هوشمند برای اهداف مختلفی مانند ارائه خدمات شخصی‌سازی شده، تبلیغات هدفمند و نیز برنامه‌ریزی شهری بر اساس الگوهای رفتاری شهروندان انجام می‌شود. این فرآیند نیازمند توجه ویژه به مسائل امنیتی و حفاظت از حریم خصوصی شهروندان است تا در کنار توسعه شهرهای هوشمند، امنیت اطلاعات فراهم شود و حقوق شهروندان محفوظ بماند [۱۲]. در شکل ۱ تصویری از انتقال داده‌ها در یک شهر هوشمند نمایش داده شده است.



شکل ۱: تصویری از انتقال داده‌ها در یک شهر هوشمند.

Figure 1. An Illustration of Data Transmission in a Smart City.

بالین حال، جمع‌آوری و پردازش داده‌های شخصی، موجب نگرانی‌های قابل توجهی درباره حفظ حریم خصوصی و استفاده ناصحیح یا دسترسی غیرمجاز به اطلاعات حساس می‌شود. از سوی دیگر، داده‌های غیرشخصی از طریق حسگرهای متعددی که در زیرساخت‌های شهری مانند روشنایی هوشمند معابر و خیابان‌ها، دوربین‌های ترافیک، ایستگاه‌های هواشناسی و سامانه‌های مدیریت پسماند نصب شده‌اند، جمع‌آوری می‌شوند. جمع‌آوری و تجزیه و تحلیل داده‌های غیرشخصی نقش مهمی در بهینه‌سازی خدمات شهری، بهبود تخصیص منابع و تصمیم‌گیری مبتنی بر داده‌ها برای برنامه‌ریزی و مدیریت شهری ایفا می‌کند [۱۳].

۲-۲- چالش‌های حقوقی در حفاظت از حریم خصوصی و داده‌ها

جمع‌آوری، ذخیره‌سازی و استفاده از داده‌ها در شهرهای هوشمند با مسائل قانونی و حریم خصوصی مهمی همراه است که باید به‌طور جدی مدنظر قرار گیرد. این مسائل شامل مواردی همچون مالکیت داده، رضایت، شفافیت، مسئولیت و امنیت می‌شوند. با وجود طبیعت یکپارچه و به‌هم‌پیوسته سامانه‌های شهر هوشمند و پیچیدگی اجرای قوانین و مقررات موجود، به‌ویژه در زمینه حمایت از حقوق حفاظت داده و حریم خصوصی، این چالش‌ها بیش‌ازپیش اهمیت پیدا می‌کنند [۱۴]. در جمهوری اسلامی ایران نیز، ملاحظات قانونی مرتبط با جمع‌آوری داده در شهرهای هوشمند باید با اصولی که در قانون اساسی و قوانین و مقررات مختلف حاکم بر حریم خصوصی و حفاظت داده تعریف شده‌اند، سازگاری داشته باشند. به‌عنوان مثال، مجموعه قوانین مدنی و قانون تجارت الکترونیکی، مقرراتی را در خصوص حریم خصوصی و حفاظت داده در معاملات الکترونیکی ارائه می‌دهند. همچنین، قانون حفاظت اطلاعات شخصی^۱ اصولی را برای جمع‌آوری، پردازش و ذخیره‌سازی داده‌های شخصی تعیین می‌کند و اهمیت اخذ رضایت افراد و تضمین امنیت داده‌ها را مورد تأکید قرار می‌دهد [۱۵]. در کشورهای دیگر نیز، مانند اتحادیه اروپا، قوانین حفاظت داده و حریم خصوصی نقش اساسی در جمع‌آوری و استفاده از داده‌ها در شهرهای هوشمند ایفا می‌کنند. به‌عنوان مثال، قانون عمومی حفاظت داده^۲ یکی از تنظیمات مهم در اتحادیه اروپا است که چارچوب جامعی برای حفاظت از داده‌های شخصی فراهم می‌کند. در قوانین عمومی حفاظت داده، افراد بر روی داده‌های شخصی خود کنترل دارند و سازمان‌ها باید رضایت برای جمع‌آوری داده‌ها را به‌طور صریح کسب کنند و به افراد درباره هدف و مدت زمان پردازش داده‌ها اطلاع دهند [۱۶].

در ایالات متحده، قوانین متفاوتی مربوط به حفاظت از داده و حریم خصوصی در سطح فدرال و ایالتی وجود دارند که بر ارگان‌ها و سازمان‌ها اعمال می‌شوند. به‌عنوان مثال، قانون حفاظت از حریم خصوصی سال ۱۹۷۴ یکی از قوانین اصلی در سطح فدرال است که محدودیت‌هایی بر جمع‌آوری، استفاده و افشای اطلاعات شخصی افراد را برای سازمان‌های فدرال تعیین می‌کند. همچنین، ایالت‌های مختلف نیز قوانین حفاظت از حریم خصوصی خود را دارند، از جمله قانون مصرف‌کننده کالیفرنیا^۳ و قانون حفاظت از داده مصرف‌کننده ویرجینیا^۴ که به افراد حقوقی خاص درباره داده‌های شخصی خود اعطا می‌کند و تعهداتی را برای کسب‌وکارها تحمیل می‌کند [۱۷]. در چین، قوانین حفاظت داده و حریم خصوصی عمدتاً تحت قوانین امنیت سایبری و دستورالعمل امنیت اطلاعات شخصی^۵ تنظیم می‌شوند. این قوانین از سازمان‌ها می‌خواهند که رضایت افراد را برای جمع‌آوری داده‌ها کسب کنند، تدابیر امنیتی برای حفاظت از اطلاعات شخصی اجرا کنند و انتقال داده‌ها به‌صورت چند سویه را محدود کنند. همچنین، دولت چین نقش مهمی در نظارت بر جمع‌آوری و استفاده از داده‌ها، به‌ویژه در زمینه امنیت ملی و منافع عمومی ایفا می‌کند [۱۸].

بالین وجود، در حوزه شهرهای هوشمند، با وجود چارچوب‌های قانونی برای نظارت بر جمع‌آوری داده‌ها و حفاظت از حریم خصوصی، چالش‌ها و بحث‌های فعالی وجود دارد. برقراری تعادل مناسب بین مزایای خدمات مبتنی بر داده و حقوق حریم خصوصی افراد نیازمند بحث و تبادل نظر مداوم بین سیاست‌گذاران، ارائه‌دهندگان فناوری و شهروندان است تا اطمینان حاصل شود که موازین قانونی و حریم خصوصی به‌طور کامل رعایت شده است.

^۱ Personal Data Protection Law (PDPL)

^۲ European Union (EU)

^۳ General Data Protection Regulation (GDPR)

^۴ California Consumer Privacy Act (CCPA)

^۵ Consumer Data Protection Act (CDPA)

^۶ Personal Information Security Structure (PISS)

۳-۲- تأثیر مقررات حقوقی بر حفظ حریم خصوصی

تأثیر قوانین مربوط به جمع‌آوری داده‌ها بر حفظ حریم خصوصی، رضایت عمومی شهروندان و شفافیت در شهرهای هوشمند بسیار حائز اهمیت است. این قوانین نقش بسزایی در تعیین نگرش و پذیرش طرح‌های شهر هوشمند ایفا می‌کنند. با اجرای قوانین و سازوکارهای مسئولیت، اعتماد به حفظ حقوق حریم خصوصی تقویت می‌شود و این موضوع، باعث افزایش اعتماد به پروژه‌های شهر هوشمند می‌شود. همچنین، افزایش شفافیت در مورد جمع‌آوری، پردازش و استفاده از داده‌ها به طریق معناداری به افزایش رضایت عمومی و پذیرش گسترده‌تر راه‌حل‌های شهر هوشمند کمک می‌کند [۱۹].

قوانین قوی مرتبط با جمع‌آوری داده‌ها می‌توانند به طرز چشمگیری بر اعتماد عمومی و مشارکت فعال در پروژه‌های شهر هوشمند اثرگذار باشند. این قوانین باعث می‌شوند شفافیت و مسئولیت در استفاده از داده‌ها در مرکز توجه قرار گیرند تا فناوری‌های شهر هوشمند به صورت مسئولانه و اخلاقی اجرا شوند. این تدابیر در نهایت منجر به بهبود خدمات شهری و افزایش آسایش شهروندان نیز می‌شوند. اگرچه جزئیات این قوانین ممکن است در کشورهای مختلف متفاوت باشند، اما هدف اساسی آن‌ها همواره ثابت است: حفاظت از حریم خصوصی، ترویج شفافیت و تضمین رضایت عمومی در استفاده از داده‌های شهر هوشمند [۲۰]. در جدول ۱، انواع داده‌های جمع‌آوری‌شده در شهر هوشمند، اهمیت، نقاط قوت و ضعف نفوذ اطلاعات، قوانین و پروتکل‌های استفاده‌شده در آن بخش و راهکارهای حفظ حریم خصوصی و امنیت داده‌ها مقایسه و بررسی شده‌اند.

۳- پیشرفت فناوری و چالش‌های امنیت حریم خصوصی در شهرهای هوشمند

۳-۱- نقش پروتکل‌های رمزنگاری در امنیت و حریم خصوصی داده‌های شهر هوشمند

در شهرهای هوشمند، استفاده از رمزنگاری و پروتکل‌های امنیتی برای داده‌ها امری حیاتی در جهت حفظ حریم خصوصی و محافظت از اطلاعات حساس است. رمزنگاری به معنای تبدیل داده‌ها به شکلی است که تنها با استفاده از یک کلید رمزگشایی، قابل دسترسی است. با بهره‌گیری از الگوریتم‌های قوی رمزنگاری، شهرهای هوشمند می‌توانند اطمینان حاصل کنند که داده‌های ارسالی و ذخیره شده در سامانه‌ها به طور محرمانه باقی می‌مانند و از دسترسی غیرمجاز محافظت می‌شوند. در این شهرها، از انواع مختلفی از پروتکل‌های رمزنگاری برای بهبود امنیت داده‌ها استفاده می‌شود [۲۱]. به عنوان مثال، از پروتکل امنیت لایه انتقال استفاده می‌شود که یک پروتکل پرکاربرد است و ارتباط امن را در شبکه‌ها فراهم می‌کند. این پروتکل، داده‌های ارسالی بین دستگاه‌ها یا برنامه‌ها را رمزنگاری می‌کند و از انشعاب و تغییر داده‌ها جلوگیری می‌کند. پروتکل لایه امنیتی سوکت‌های امن^۱ نیز پروتکل دیگری است که به طور گسترده برای ایجاد اتصال امن بین یک مشتری و یک سرور استفاده می‌شود و اطمینان از صحت و محرمانگی داده‌ها را فراهم می‌کند [۲۲]. استفاده از پروتکل‌های رمزنگاری در شهرهای هوشمند به طرز قابل توجهی امنیت داده‌ها را تضمین می‌کند، اما لازم است به قواعد و ضعف‌های مرتبط با این پروتکل‌ها توجه کنیم. الگوریتم‌ها و پروتکل‌های رمزنگاری قوی می‌توانند اطلاعات را از دسترسی غیرمجاز محافظت کرده و حریم خصوصی را بهبود بخشند. با این حال، پیچیدگی روش‌های رمزنگاری ممکن است به سرعت پردازش داده‌ها آسیب بزند. همچنین، اجرای دقیق و مدیریت صحیح پروتکل‌های رمزنگاری برای جلوگیری از آسیب و تأمین مدیریت امنیتی کلیدها امری حیاتی است [۲۳]. در کشورهای مختلف، جزئیات قوانین و مقررات مربوط به رمزنگاری ممکن است متفاوت باشد. برخی کشورها ممکن است نیازمندی‌های سخت‌گیرانه‌تری درباره رمزنگاری برای امنیت داده‌ها داشته باشند، در حالی که دیگران ممکن است به رویکردهای منعطف‌تری متوجه شوند. این فهم از تفاوت‌ها بسیار حیاتی است تا اجرای مؤثر پروتکل‌های رمزنگاری در شهرهای هوشمند، برای ایجاد تعادل بین امنیت داده‌ها و کارایی عملیاتی را فراهم کند.

¹ Secure Sockets Layer (SSL)

جدول ۱: انواع داده‌ها و اهمیت حفاظت از حریم خصوصی و امنیت داده‌ها در شهر هوشمند

Table 1. Types of Data and the Importance of Privacy and Data Security Protection in a Smart City

نوع داده	اهمیت	نقاط قوت	نقاط ضعف نفوذ اطلاعات	قوانین و پروتکل‌ها	راهکارهای حفظ حریم خصوصی و امنیت
داده‌های حمل‌ونقل (نظیر داده‌های ترافیکی، موقعیت و وسایل نقلیه عمومی)	بهبود مدیریت ترافیک و کاهش ازدحام، افزایش کارایی سیستم حمل‌ونقل عمومی	تحلیل داده‌ها برای بهبود جریان ترافیک و کاهش زمان سفر	احتمال سرقت داده‌های موقعیت مکانی، حمله سایبری به سامانه‌های حمل‌ونقل	قانون عمومی حفاظت داده، قوانین محلی حمل‌ونقل	رمزنگاری داده‌ها، استفاده از پروتکل‌های امنیتی نظیر HTTPS، ایجاد سامانه‌های تشخیص نفوذ
داده‌های محیط‌زیست (نظیر کیفیت هوا، سطح نویز، دما)	پایش و بهبود کیفیت محیط‌زیست، ایجاد سیاست‌های زیست‌محیطی	داده‌های دقیق و لحظه‌ای برای اتخاذ تصمیمات سریع	دسترسی غیرمجاز به داده‌ها، تغییر داده‌ها توسط مهاجمان	قوانین محیط‌زیستی محلی و بین‌المللی	استفاده از سامانه‌های امنیتی مبتنی بر اینترنت اشیا، اعمال محدودیت‌های دسترسی، استفاده از بلاک‌چین برای ثبت تغییرات
داده‌های انرژی (نظیر مصرف برق و گاز، تولید انرژی تجدیدپذیر)	بهینه‌سازی مصرف انرژی، کاهش هزینه‌ها، افزایش استفاده از انرژی‌های تجدیدپذیر	بهبود مدیریت مصرف و تولید انرژی، کاهش هزینه‌ها	احتمال دسترسی غیرمجاز به داده‌های مصرف انرژی، حملات به سامانه‌های شبکه برق	استانداردهای امنیت انرژی نظیر ISO 27001	رمزنگاری داده‌ها، ایجاد شبکه‌های مجزا برای داده‌های حساس، پایش مستمر سامانه‌ها
داده‌های سلامت (نظیر داده‌های مربوط به بیماری‌ها، وضعیت اورژانس)	بهبود خدمات سلامت، کاهش زمان واکنش در شرایط اضطراری	بهبود پاسخگویی به شرایط اضطراری و مدیریت بهداشت عمومی	سرقت داده‌های حساس سلامت، تهدید به حریم خصوصی بیماران	قانون قابلیت حمل و پاسخ‌گویی بیمه سلامت ^۱ ، قانون عمومی حفاظت داده، قوانین محلی بهداشت و سلامت	استفاده از رمزنگاری پیشرفته، اعمال محدودیت‌های دسترسی، آموزش کارکنان بهداشتی در زمینه امنیت اطلاعات
داده‌های ایمنی (نظیر داده‌های امنیتی عمومی، نظارت تصویری)	افزایش امنیت عمومی، کاهش جرائم	ارتقاء سطح امنیت و پیشگیری از جرائم	سوءاستفاده از داده‌های نظارت تصویری، نقض حریم خصوصی افراد	قوانین محلی امنیت عمومی، استانداردهای بین‌المللی نظارت	ذخیره‌سازی داده‌های نظارتی در محیط‌های امن، استفاده از فناوری‌های تشخیص نفوذ، کنترل دسترسی به داده‌های حساس
داده‌های شهروندی (نظیر نظرات و پیشنهادات شهروندان، درخواست‌های خدمات شهری)	بهبود خدمات شهری، افزایش مشارکت شهروندان	ارتقاء کیفیت خدمات و افزایش رضایتمندی شهروندان	نقض حریم خصوصی شهروندان، سوءاستفاده از داده‌های شهروندی	قانون عمومی حفاظت داده، قوانین محلی حمایت از داده‌های شخصی	استفاده از پروتکل‌های امنیتی نظیر پروتکل امنیت لایه انتقال ^۲ ، اعمال سیاست‌های محرمانگی داده، استفاده از سامانه مدیریت دسترسی

^۱Health Insurance Portability and Accountability Act (HIPAA)^۲ Transport Layer Security (TLS)

۳-۲- تأثیر تهدیدات سایبری بر امنیت اطلاعات در شهرهای هوشمند

افزایش اتصالات و وابستگی به زیرساخت دیجیتال در شهرهای هوشمند، منجر به گسترش قابل توجه حملات سایبری شده است. این چالش‌ها بیشتر از مسائل معمولی نفوذ داده‌ها بوده و شامل حملات سایبری پیشرفته به زیرساخت‌های اساسی، داده‌های حساس و خدمات ضروری می‌شوند. با پیشرفت شهرهای هوشمند، پیچیدگی سامانه‌های متصل به آن‌ها منجر به تشدید این تأثیرات مخاطره‌آمیز شده و نیاز به استراتژی‌های جامع مدیریت ریسک و اقدامات امنیتی پیشگیرانه را افزایش داده است [۲۴]. شهرهای هوشمند با توسعه فناوری و اتصالات دیجیتال، به‌صورت قابل توجهی با تهدیدات امنیت سایبری مواجه هستند که خطرات قابل توجهی برای سلامت عملکرد و حریم شخصی ساکنان آن‌ها ایجاد می‌کنند. این تهدیدات شامل موارد زیر است:

* نفوذ داده: دسترسی غیرمجاز به مخازن داده حساس مانند پروفایل‌های شهروندی، سوابق مالی و پایگاه‌های داده زیرساختی می‌تواند باعث نفوذ داده شده و پیامدهای جدی برای حریم خصوصی و اعتماد شهروندان شود.

* دسترسی غیرمجاز: سازوکارهای احراز هویت ضعیف و کنترل دسترسی نامناسب ممکن است دسترسی غیرمجاز به سامانه‌ها و شبکه‌های حیاتی را فراهم کند که به مهاجمان شرور، امکان بهره‌برداری از آسیب‌پذیری‌ها و تخریب اصالت داده را می‌دهد.

* اختلال در خدمات: حملات سایبری به خدمات ضروری مانند سامانه‌های حمل‌ونقل، شبکه‌های انرژی و شبکه‌های اورژانس می‌تواند عملیات را مختل کرده، خطاهای خدماتی ایجاد کرده و زندگی روزمره شهروندان را مختل کند.

* حملات بدخواهانه به زیرساخت‌های اساسی: حملات سایبری پیشرفته از جمله حملات باج‌افزارها، حملات تخریب خدمات توزیع شده^۱ و تهدیدات پیشرفته و مداوم^۲ ممکن است خطرات قابل توجهی برای اصالت و دسترسی به زیرساخت‌های اساسی مانند سامانه‌های تأمین آب، شبکه‌های برق و شبکه‌های ارتباطی ایجاد کنند. این تهدیدات نشان می‌دهند که شهرهای هوشمند نیازمند استراتژی‌های جامع مدیریت ریسک و اقدامات امنیتی پیشگیرانه هستند تا بتوانند به‌طور مؤثری با چالش‌های امنیت سایبری روبرو شده، امنیت شهروندان را حفظ کنند.

مثال‌های جهانی از وقایع امنیت سایبری در شهرهای هوشمند نشان‌دهنده میزان خطرناک بودن تهدیدات واقعی است. به‌عنوان نمونه، حمله رنسوم‌وئر به شهر آتلانتا در سال ۲۰۱۸ باعث اختلالات گسترده در خدمات، ضررهای مالی و چالش‌های عملیاتی بلندمدت شد. همچنین، نفوذ داده به سیستم اندازه‌گیری هوشمند در کره جنوبی، حریم خصوصی هزاران ساکن را به خطر انداخت و آسیب‌پذیری‌های موجود در زیرساخت‌های شهری را نشان داد [۲۵]. برای کاهش این خطرات و مقابله با تهدیدات امنیت سایبری، باید اولویت شهرهای هوشمند در اجرای اقدامات قوی امنیت سایبری و استراتژی‌های دفاعی پیشگیرانه باشد. یکی از موارد مهم در امنیت سایبری، ارزیابی‌های منظم آسیب‌پذیری است. این ارزیابی‌ها به‌منظور شناسایی نقاط ضعف سیستم و اولویت‌بندی تلاش‌های اصلاحی در برابر تهدیدات سایبری انجام می‌شود. همچنین، آزمایش‌های نفوذ نیز برای شبیه‌سازی حملات سایبری واقعی و ارزیابی اثربخشی کنترل‌های امنیتی موجود، شناسایی آسیب‌پذیری‌ها و اعتبارسنجی رویه‌های پاسخ به حوادث انجام می‌شود. علاوه بر این، بررسی‌های امنیتی نیز به‌صورت دوره‌ای از سیاست‌ها، رویه‌ها و پیکربندی‌های امنیتی انجام می‌شود تا از رعایت استانداردها و بهترین روش‌های صنعت اطمینان حاصل شود. همچنین، پروتکل‌های امنیتی قوی مانند شبکه‌های انتقال امن^۳، رمزنگاری و احراز هویت چندگانه نیز به‌منظور حفاظت از داده‌های در حال انتقال و جلوگیری از دسترسی غیرمجاز، پیاده‌سازی می‌شوند. از جمله دیگر تلاش‌های امنیتی، استقرار دیواره‌های آتشین و سامانه‌های تشخیص نفوذ^۴ است. این ابزارها به‌منظور نظارت بر ترافیک شبکه، شناسایی فعالیت‌های مشکوک و مسدود کردن ترافیک مخرب در زمان واقعی استفاده می‌شوند. همچنین، آموزش شهروندان در مورد خطرات امنیت سایبری، بهترین روش‌ها و روش‌های گزارش حوادث نیز برای تقویت آن‌ها به‌عنوان شرکت‌کنندگان فعال در دفاع مشترک در برابر تهدیدات سایبری انجام می‌شود. همچنین، ترویج همکاری و به اشتراک‌گذاری اطلاعات بین نهادهای دولتی، شرکای بخش خصوصی و متخصصان امنیت سایبری نیز از دیگر تلاش‌های مهم در این زمینه است. در نهایت، ایجاد یک چارچوب قانونی و حقوقی قوی و کامل نیز به‌منظور تعیین تدابیر و ضوابطی برای حفاظت از داده‌ها، تأمین امنیت شبکه‌ها و سامانه‌های اطلاعاتی، و تعیین مسئولیت‌ها و وظایف مراجع مختلف از

^۱ Distributed Denial of Service (DDoS)

^۲ Advanced Persistent Threats (APTs)

^۳ Virtual Private Networks (VPNs)

^۴ Intrusion Detection Systems (IDS)

جمله مراجع سیاست‌گذاری، مراجع نظارتی و مراجع قضایی قابل‌استفاده است. این چارچوب باید شامل قوانین محافظت از داده‌ها، امنیت اطلاعات، حفظ حریم خصوصی شهروندان و تعیین فناوری‌های امنیتی مناسب برای استفاده در شهرها باشد تا امنیت سایبری به بهترین شکل ممکن تضمین شود. علاوه بر این، وظیفه مراجع قضایی رصد قوانین و در صورت نقض آن‌ها انجام تحقیقات و پیگیری است. به‌علاوه، مراجع نظارتی، مسئول ارزیابی تمامیت و امنیت سامانه‌های اطلاعاتی هستند و مسئولیت نظارت بر اجرای قوانین را دارند. همچنین، مراجع سیاست‌گذاری باید سیاست‌ها و دستورالعمل‌های لازم برای افزایش امنیت سایبری در شهرها را تدوین و اجرا کنند و اقدامات آموزشی و آگاهی‌زا برای شهروندان راه‌اندازی کنند. این تدابیر در کنار همکاری و تعامل فعال بین این مراجع، می‌توانند بهبود قابل‌توجهی در امنیت سایبری شهرهای هوشمند به ارمغان بیاورند و از تهدید داده‌ها و حریم خصوصی شهروندان جلوگیری کنند [۲۶]. با انتخاب رویکردی پیشگیرانه نسبت به امنیت سایبری و اجرای سازوکارهای دفاعی قوی، شهرهای هوشمند می‌توانند قابلیت انعطاف خود را در برابر تهدیدات سایبری افزایش داده و زیرساخت‌های اساسی خود را محافظت کنند، همچنین حریم شخصی و رفاه ساکنان خود را در یک محیط شهری دیجیتال و افزایشی تضمین کنند.

۳-۳- استانداردها و پروتکل‌های اینترنت اشیا^۱ در شهر هوشمند

سازوکارهای امنیتی سنتی مانند رمزنگاری و زیرساخت، به دلیل پیچیدگی و مصرف منابع بالا، ممکن است برای پلتفرم‌های اینترنت اشیا عملی نباشند. به همین دلیل، استانداردهای جدید با طراحی‌های امنیتی سبک‌وزن برای پاسخگویی به نیازهای خاص امنیتی اکوسیستم اینترنت اشیا توسعه یافته‌اند. یکی از چالش‌های کلیدی در این زمینه، نیاز به استفاده از استانداردهای متعدد توسط دستگاه‌ها است، چراکه اینترنت اشیا بر پایه فناوری‌های موجود و پروتکل‌های ارتباطی مختلف بنا شده است. در این راستا، پروتکل‌هایی مانند پروتکل کاربرد محدود^۲ و پروتکل انتقال تله‌متری پیام^۳ طراحی شده‌اند. پروتکل کاربرد محدود پروتکلی سبک برای شبکه‌های محدود منابع است که شامل سازوکارهای امنیتی مانند امنیت لایه انتقال دیتاگرام^۴ و احراز هویت کلید پیش‌اشتراکی^۵ است. پروتکل انتقال تله‌متری نیز پروتکلی مناسب برای شبکه‌های کم‌عَرَض و نامعتبر است که از سازوکارهای امنیتی مانند امنیت لایه انتقال و امنیت ماشین به ماشین سبک^۶ بهره می‌برد. تهدیدات امنیتی در اینترنت اشیا به دلیل حضور آن‌ها در تمامی لایه‌های معماری اینترنت اشیا، از لایه‌های داده لینک و شبکه تا لایه‌های جلسه و کاربرد، نگرانی عمده‌ای به حساب می‌آیند. برای مقابله با این تهدیدات، پروتکل‌های مختلف اینترنت اشیا با ویژگی‌های امنیتی در لایه‌های مختلف معماری طراحی شده‌اند. به‌عنوان مثال، پروتکل‌هایی مانند e802.15.4 و WirelessHART ویژگی‌های امنیتی خاصی ارائه می‌دهند؛ WirelessHART با استفاده از رمزنگاری AES-128 و تکنیک‌های دیگری مانند حفظ یکپارچگی داده‌ها و احراز هویت، امنیت بالایی را تأمین می‌کند. همچنین، پروتکل مسیریابی برای شبکه‌های کم‌قدرت و با تلفات بالا^۷ با استفاده از "حوزه امنیت" در سرآیند خود، سطوح مختلفی از امنیت را ارائه می‌دهد و از ویژگی‌هایی مانند اعتبارسنجی داده‌ها، امنیت معنایی، و مدیریت کلید برخوردار است. باین‌حال، پروتکل مسیریابی برای شبکه‌های کم‌قدرت و با تلفات بالا با تهدیدات امنیتی مختلفی مانند حملات انتخابی، حملات Sinkhole و حملات Sybil مواجه است که RFC 7416 به بررسی این حملات پرداخته و راهکارهایی برای مقابله با آن‌ها پیشنهاد داده است.

در ادامه پروتکل‌ها و استانداردهای اینترنت اشیا در شهر هوشمند را مورد بررسی قرار می‌دهیم [۲۷].

*** پروتکل کاربرد محدود:** پروتکل کاربرد محدود برای استفاده در شبکه‌های محدود منابع مانند اینترنت اشیا طراحی شده و امکان ارتباط ساده و کارآمد بین دستگاه‌ها را فراهم می‌کند. پروتکل کاربرد محدود مشابه پروتکل انتقال ابرمتن^۸ است اما بهینه‌تر و سبک‌تر است. این پروتکل از مدل درخواست/پاسخ استفاده می‌کند و می‌تواند به‌صورت هم‌زمان در شبکه‌های بی‌سیم و سیمی

^۱ Internet of Things (IoT)

^۲ Constrained Application Protocol (CoAP)

^۳ Message Queuing Telemetry Transport (MQTT)

^۴ Datagram Transport Layer Security (DTLS)

^۵ Pre-Shared Key (PSK)

^۶ Lightweight Machine-to-Machine (LwM2M)

^۷ Routing Protocol for Low-Power and Lossy Networks (RPL)

^۸ Hypertext Transfer Protocol (HTTP)

کار کند. پروتکل کاربرد محدود شامل سازوکارهای امنیتی مانند امنیت لایه انتقال دیتاگرام و احراز هویت کلید پیش‌اشتراکی است که اطمینان حاصل می‌کند داده‌های منتقل شده بین دستگاه‌ها محافظت شده‌اند و از دسترسی غیرمجاز جلوگیری می‌شود.

*** پروتکل انتقال تله‌متری پیام:** پروتکل انتقال تله‌متری پیام برای استفاده در شبکه‌های کم‌عرضه و نامعتبر طراحی شده است و شامل سازوکارهای امنیتی مانند امنیت لایه انتقال و امنیت ماشین به ماشین سبک است. این پروتکل از مدل انتشار/اشتراک استفاده می‌کند که اجازه می‌دهد دستگاه‌ها به‌طور کارآمد داده‌ها را به یک سرور مرکزی ارسال کرده و دیگر دستگاه‌ها بتوانند به این داده‌ها دسترسی پیدا کنند. از ویژگی‌های مهم امنیتی این پروتکل، استفاده از پروتکل امنیت لایه انتقال برای رمزنگاری داده‌ها و حفظ یکپارچگی و محرمانگی اطلاعات و نیز سازوکارهای امنیتی ماشین به ماشین سبک برای احراز هویت و کنترل دسترسی به داده‌ها است.

*** توصیه ITU-T Y.2060:** توصیه ITU-T Y.2060 مروری جامع بر مفهوم و محدوده اینترنت اشیا ارائه می‌دهد و شامل مدل مرجع چهار لایه‌ای با قابلیت‌های مدیریت و امنیت است. این مدل لایه‌های ادراک، شبکه، خدمات و اپلیکیشن را پوشش می‌دهد و راهکارهای امنیتی و مدیریت داده‌ها را در هر لایه پیشنهاد می‌کند. مدیریت داده‌ها شامل روش‌هایی برای مدیریت امن داده‌ها و حفاظت از حریم خصوصی کاربران، و احراز هویت است و در کنترل دسترسی، راهکارهایی برای احراز هویت کاربران و دستگاه‌ها و کنترل دسترسی به داده‌ها ارائه می‌دهد.

*** توصیه ITU-T Y.2061:** توصیه ITU-T Y.2061 برای توسعه و ارتقاء شبکه‌های نسل بعدی^۱ و کاربردهای ارتباطات ماشین محور^۲ امنیتی در نظر گرفته شده است. این توصیه شامل راهنماها و روش‌هایی برای ایجاد و مدیریت سامانه‌های ارتباطی امن و کارآمد است که بتوانند نیازهای ارتباطات ماشین به ماشین را پاسخگو باشند. این استاندارد شامل راهکارهایی برای ایجاد و مدیریت شبکه‌های امن ماشین به ماشین و روش‌هایی برای کنترل دسترسی و احراز هویت کاربران و دستگاه‌ها است.

*** استانداردهای IETF-RFC 4919 & 4944:** این استانداردها راهکارهایی برای پیاده‌سازی شبکه‌های مبتنی بر IPv6 در سامانه‌های محدود مانند شبکه‌های سنسوری ارائه می‌دهند. استاندارد LoWPAN6 با کاهش اندازه سرآیندهای IPv6، امکان استفاده از این پروتکل‌ها در سامانه‌های محدود را فراهم می‌کند. LoWPAN6 برای بهبود امنیت و کارایی در شبکه‌های محدود منابع طراحی شده است و از تکنیک‌های رمزنگاری برای حفاظت از داده‌ها و جلوگیری از دسترسی غیرمجاز استفاده می‌کند.

*** استاندارد IETF-RFC 6550:** این استاندارد، پروتکل مسیریابی برای شبکه‌های کم‌مصرف و مستهلک^۳ را معرفی می‌کند و شامل سه حالت امنیتی است: غیرامن، پیش‌نصب شده، و احراز هویت شده. راهکارهایی برای مسیریابی امن در شبکه‌های کم‌مصرف و مستهلک و روش‌هایی برای احراز هویت و کنترل دسترسی به داده‌ها در این استاندارد گنجانده شده است.

*** استاندارد نام‌گذاری اشیاء^۴:** مشابه سیستم نام دامنه^۵، این استاندارد چارچوبی برای نام‌گذاری اشیاء در سامانه‌های توزیع شده فراهم می‌کند و درخواست‌ها را به محل صحیح هدایت می‌کند. تضمین نام‌گذاری یکتا برای دستگاه‌ها و سرویس‌ها و روش‌هایی برای کنترل دسترسی و احراز هویت در نام‌گذاری اشیاء از ویژگی‌های امنیتی این استاندارد هستند.

*** استاندارد پروتکل انتقال تله‌متری پیام^۶:** این پروتکل، پیام‌رسانی سبک است که برای صف‌بندی پیام‌ها در مسافت‌های طولانی طراحی شده است و با استفاده از رمزنگاری و سیاست‌های دسترسی، اطمینان از حفظ حریم خصوصی حتی در صورت به‌خطر افتادن سرور را فراهم می‌کند. استفاده از تکنیک‌های رمزنگاری برای حفاظت از داده‌ها و روش‌هایی برای کنترل دسترسی و احراز هویت کاربران و دستگاه‌ها از ویژگی‌های امنیتی این استاندارد هستند.

*** استانداردهای امنیت لایه انتقال / امنیت لایه انتقال دیتاگرام:** امنیت لایه انتقال و امنیت لایه انتقال دیتاگرام استانداردهایی برای تأمین امنیت در لایه حمل‌ونقل هستند و از سازوکارهایی مانند RSA، HMAC، و AES بهره می‌برند. این

¹ Next Generation Networks (NGN)

² Machine-Oriented Communications (MOC)

³ Low-Power and Lossy Networks (LLNs)

⁴ Object Naming Service (ONS)

⁵ Domain Name System (DNS)

⁶ MQTT: OASIS (Organization for the Advancement of Structured Information Standards)

استانداردها از تکنیک‌های رمزنگاری برای حفاظت از داده‌ها و تضمین یکپارچگی و محرمانگی اطلاعات بین دستگاه‌ها استفاده می‌کنند.

*** استانداردهای IEEE 1888.3:** این استانداردها برای تضمین امنیت پروتکل‌های شبکه سبز فراگیر^۱ طراحی شده‌اند و شامل راهکارهایی برای حفاظت اطلاعات، حفظ یکپارچگی، محرمانگی، احراز هویت و کنترل دسترسی هستند. استفاده از تکنیک‌های رمزنگاری برای حفاظت از داده‌ها و روش‌هایی برای کنترل دسترسی و احراز هویت کاربران و دستگاه‌ها از ویژگی‌های امنیتی این استاندارد هستند.

*** پروتکل کنترل انتقال جریان^۲:** پروتکل کنترل انتقال جریان یک پروتکل لایه حمل‌ونقل است که قابلیت انتقال داده‌ها به‌صورت پیام‌محور را دارد و از ویژگی‌هایی مانند چند مسیریابی و مقاومت در برابر حملات امنیتی بهره می‌برد. راهکارهایی برای مسیریابی امن و مقاوم در برابر حملات و روش‌هایی برای کنترل دسترسی و احراز هویت کاربران و دستگاه‌ها از ویژگی‌های امنیتی این پروتکل هستند.

*** گروه محاسبات مطمئن^۳:** این گروه، سازوکارهای امنیتی متنوعی مانند ماژول پلتفرم مطمئن^۴ و به‌روزرسانی اعتماد از راه دور^۵ برای اطمینان از امنیت دستگاه‌های اینترنت اشیا ارائه می‌دهد. استفاده از ماژول پلتفرم مطمئن و به‌روزرسانی اعتماد از راه دور برای تضمین امنیت دستگاه‌ها و روش‌هایی برای حفاظت از داده‌ها و کنترل دسترسی به اطلاعات از ویژگی‌های امنیتی این گروه هستند.

*** استاندارد ISO/IEC 27001:** یک استاندارد بین‌المللی برای مدیریت امنیت اطلاعات است که به سازمان‌ها کمک می‌کند تا یک سیستم مدیریت امنیت اطلاعات^۶ موثر را پیاده‌سازی کنند. این استاندارد شامل سیاست‌ها، فرآیندها، رویه‌ها، و کنترل‌های لازم برای مدیریت و حفاظت از اطلاعات است. تضمین مدیریت موثر امنیت اطلاعات در سازمان‌ها و استفاده از کنترل‌های امنیتی مختلف برای حفاظت از داده‌ها و اطلاعات حساس از ویژگی‌های این استاندارد هستند.

*** استاندارد ISO/IEC 29100:** این استاندارد، یک چارچوب بین‌المللی برای حفظ حریم خصوصی اطلاعات است که شامل راهنمایی‌ها و اصولی برای مدیریت حریم خصوصی داده‌ها است. تضمین حفظ حریم خصوصی داده‌ها و اطلاعات شخصی و راهنمایی‌هایی برای مدیریت ریسک‌های مرتبط با حریم خصوصی اطلاعات از ویژگی‌های این استاندارد هستند.

در لایه‌های مختلف شهر هوشمند، انتخاب پروتکل‌ها و استانداردهای مناسب برای تأمین امنیت و حریم خصوصی اطلاعات اهمیت زیادی دارد. براساس توضیحات استانداردها و پروتکل‌های فوق، برای داده‌های حمل‌ونقل مانند داده‌های ترافیکی و موقعیت وسایل نقلیه عمومی، پروتکل‌هایی نظیر پروتکل کاربرد محدود و پروتکل انتقال تله‌متری پیام به دلیل قابلیت‌های امنیتی آن‌ها شامل امنیت لایه انتقال دیتاگرام و امنیت لایه انتقال، می‌توانند به‌خوبی عمل کنند. این پروتکل‌ها امنیت انتقال داده‌ها را با استفاده از رمزنگاری و احراز هویت فراهم می‌کنند، که در حفاظت از اطلاعات حساس و جلوگیری از دسترسی غیرمجاز به داده‌های ترافیکی و موقعیت کمک می‌کند.

همچنین، توصیه ITU-T Y.2060 با ارائه راهکارهای مدیریت و امنیت داده‌ها در لایه‌های مختلف شبکه، به تقویت امنیت در این زمینه کمک می‌کند. برای داده‌های محیط‌زیست نظیر کیفیت هوا، سطح نویز و دما، استانداردهایی مانند LoWPAN6 و RFC 6550 می‌توانند مفید واقع شوند. LoWPAN6 به دلیل طراحی بهینه برای شبکه‌های محدود و استفاده از تکنیک‌های رمزنگاری، امنیت داده‌های محیط‌زیست را تأمین می‌کند. همچنین، RFC 6550 با ارائه روش‌های مسیریابی امن در شبکه‌های کم‌مصرف و مستهلک، از امنیت داده‌های محیط‌زیست در برابر تهدیدات محافظت می‌کند. این استانداردها به همراه توصیه ITU-T Y.2061 که راهکارهایی برای شبکه‌های نسل بعدی ارائه می‌دهد، می‌توانند به مدیریت و حفظ حریم خصوصی داده‌های محیط‌زیست کمک کنند.

¹ Proactive Green Communication Networks (PGCN)

² Stream Control Transmission Protocol (SCTP)

³ Trusted Computing Group (TCG)

⁴ Trusted Platform Module (TPM)

⁵ Remote Trust Update (RTU)

⁶ Information Security Management System (ISMS)

در خصوص داده‌های انرژی، سلامت، ایمنی و شهروندی، استفاده از استانداردهای SCTP، ISO/IEC 27001 و ISO/IEC 29100 برای تأمین امنیت و حریم خصوصی اطلاعات بسیار مناسب است. SCTP به دلیل ویژگی‌های امنیتی مانند چند مسیریابی و مقاومت در برابر حملات، می‌تواند به امنیت داده‌های انرژی، سلامت و ایمنی کمک کند. استانداردهای ISO/IEC 27001 و ISO/IEC 29100 نیز با فراهم کردن چارچوب‌های مدیریت امنیت اطلاعات و حفظ حریم خصوصی، از محافظت مؤثر داده‌های حساس و شخصی شهروندان اطمینان حاصل می‌کنند. این استانداردها به همراه گروه محاسبات مطمئن با ارائه سازوکارهایی مانند مازول پلتفرم مطمئن، به حفظ امنیت و حریم خصوصی در تمام لایه‌های اطلاعات شهری کمک می‌کنند.

در جدول ۲، نقش پروتکل‌های رمزنگاری در امنیت و حریم خصوصی داده‌های شهر هوشمند، کاربردها، نقاط قوت و نقاط ضعف استانداردها و پروتکل‌های امنیتی در امنیت اینترنت اشیا در شهر هوشمند مورد بررسی قرار گرفته است [۲۸].

۳-۴- ارتباط بین اینترنت اشیا و بلاک‌چین در افزایش امنیت و اعتماد

استفاده از اینترنت اشیا و فناوری بلاک‌چین به‌عنوان دو مولفه اساسی در تقویت امنیت و افزایش اعتماد در شهرهای هوشمند بسیار اهمیت دارد. اینترنت اشیا به‌عنوان یک زیرساخت برای اتصال و ارتباط دستگاه‌ها و سنسورها عمل می‌کند که این کار، جمع‌آوری و بهره‌برداری از داده‌ها برای کاربردهای مختلف در شهرهای هوشمند را آسان‌تر می‌کند. با این وجود، حجم بزرگ داده‌های تولیدشده توسط دستگاه‌های اینترنت اشیا منجر به چالش‌های امنیتی مختلفی می‌شود که نیازمند راه‌حل‌های مؤثر هستند. فناوری بلاک‌چین به‌عنوان یک راه‌حل جذاب برای مقابله با این چالش‌های امنیتی در شهرهای هوشمند مطرح شده است [۲۹].

بلاک‌چین به‌عنوان یک دفترچه ردیابی غیرمتمرکز و غیرقابل تغییر عمل می‌کند که امکان ارائه شفافیت، صحت داده‌ها و جلوگیری از تغییرات غیرمجاز را فراهم می‌کند. این فناوری، اعتماد بین افراد و نهادها را تقویت می‌کند. با استفاده از بلاک‌چین، شهرهای هوشمند می‌توانند امنیت تراکنش‌های داده، اعتبارسنجی منابع داده و پیشگیری از فعالیت‌های غیرمجاز را بهبود بخشند [۳۰]. به‌عنوان مثال، در بخش داده‌های حمل‌ونقل، بلاک‌چین می‌تواند از دست‌کاری داده‌ها جلوگیری کرده و شفافیت در تأیید و مدیریت داده‌ها را بهبود بخشد. برای داده‌های محیط‌زیست، بلاک‌چین با ثبت امن و شفاف داده‌های کیفیت هوا، نویز و دما، به محافظت از صحت و امنیت این داده‌ها کمک می‌کند. در حوزه انرژی، سلامت و ایمنی، بلاک‌چین می‌تواند نظارت بر داده‌های انرژی و حفاظت از اطلاعات حساس سلامت و ایمنی را تضمین کند و با ارائه لایه‌های اضافی امنیت و شفافیت، اعتماد را در مدیریت این داده‌ها افزایش دهد.

از نظر حقوقی، ادغام فناوری بلاک‌چین در شهرهای هوشمند نیازمند ایجاد یک چارچوب قانونی جامع است که بتواند استفاده از این فناوری، مسئولیت‌ها، رعایت مقررات را به‌خوبی اداره کند. جنبه‌های حقوقی ارتباطی با مالکیت داده، حفاظت از حریم خصوصی و مسئولیت در صورت نقض داده‌ها باید به‌دقت در این چارچوب مشخص شوند تا حقوق و منافع همه طرفین را تضمین کند. همچنین، نظارت قضایی نقش حیاتی در حل اختلافات ناشی از تراکنش‌های بر پایه بلاک‌چین و اجرای توافقات حقوقی دارد. دادگاه‌ها و نهادهای قضایی باید دانش لازم را درک کرده و به‌طور مؤثر در راستای اصول حقوقی عمل کنند.

همچنین، تصویب قوانین مرتبط، با امکان ارائه شواهد بر پایه بلاک‌چین و اجرای قراردادهای هوشمند، نیازمند بررسی دقیق و روشن‌سازی در چارچوب حقوقی است. به‌عنوان مثال، سامانه بهداشت استونی یک نمونه موفق از ادغام فناوری بلاک‌چین است که امنیت و صحت پرونده‌های پزشکی بیماران را تضمین می‌کند و به افراد، کنترل بر روی اطلاعات شخصی سلامت خود را می‌دهد؛ درحالی‌که استانداردهای حریم خصوصی را حفظ می‌کند.

به‌عنوان مثال دیگر، در دب، فناوری بلاک‌چین برای امنیت تراکنش‌های ثبت املاک استفاده می‌شود که خطر فعالیت‌های تقلبی را کاهش داده و اعتماد در بخش ملکی را افزایش می‌دهد. بنابراین، ادغام هماهنگ اینترنت اشیا و فناوری بلاک‌چین یک الگوی تحولی برای افزایش امنیت و اعتماد در شهرهای هوشمند فراهم می‌کند. در جدول ۳، ارتباط بین اینترنت اشیا و بلاک‌چین در افزایش امنیت و اعتماد در بخش‌های مختلف داده‌های شهر هوشمند بررسی شده است.

جدول ۲: کاربردها، نقاط قوت و ضعف پروتکل‌ها و استانداردهای امنیتی در حفاظت از داده‌های شهر هوشمند

Table 2. Applications, Strengths, and Weaknesses of Security Protocols and Standards for Protecting Smart City Data

پروتکل/استاندارد	کاربرد	نقاط قوت امنیتی	نقاط ضعف امنیتی
CoAP	پروتکل کاربردی	- استفاده از DTLS برای رمزنگاری داده‌ها. - احراز هویت کلید پیش‌اشتراکی برای جلوگیری از دسترسی غیرمجاز. - بهینه‌شده برای شبکه‌های محدود منابع.	- DTLS ممکن است در شبکه‌های با تأخیر بالا یا از دست رفتن بسته‌ها به درستی عمل نکند. - ضعف در حفاظت در برابر حملات DoS.
MQTT	پروتکل پیام‌رسانی	- استفاده از TLS برای رمزنگاری داده‌ها. - LwM2M برای احراز هویت و کنترل دسترسی. - مدل انتشار اشتراک کارآمد در شبکه‌های کم‌عرضه.	- TLS ممکن است بر روی عملکرد شبکه تأثیر بگذارد. - امنیت LwM2M به میزان پیاده‌سازی بستگی دارد و ممکن است به‌طور کامل پیاده‌سازی نشود.
ITU-T Y.2060	مدل مرجع و مدیریت داده‌ها	- شامل راهکارهای امنیتی در تمام لایه‌ها. - ارائه روش‌های احراز هویت و کنترل دسترسی. - جامع و کامل در مدیریت امنیت داده‌ها.	- نیاز به پیاده‌سازی پیچیده در مقایسه با استانداردهای ساده‌تر. - ممکن است به‌صورت کامل در همه پیاده‌سازی‌ها مورد استفاده قرار نگیرد.
ITU-T Y.2061	شبکه‌های نسل بعدی	- شامل راهنماهای امنیتی برای M2M. - روش‌های احراز هویت و کنترل دسترسی. - تمرکز بر روی امنیت و کارایی شبکه‌های نسل بعدی.	- ممکن است نیاز به منابع زیاد برای پیاده‌سازی داشته باشد. - پیچیدگی در پیاده‌سازی شبکه‌های M2M امن.
IETF-RFC 4919 & 4944	پروتکل‌های IPv6 و شبکه‌های محدود	- کاهش اندازه سرآیندها برای بهبود کارایی. - تکنیک‌های رمزنگاری برای حفاظت از داده‌ها. - مناسب برای شبکه‌های محدود منابع.	- محدودیت در عملکرد امنیتی به دلیل اندازه محدود بسته‌ها. - ممکن است در شبکه‌های بسیار محدود به اندازه کافی امن نباشد.
IETF-RFC 6550	پروتکل مسیریابی LLNs	- سه حالت امنیتی: غیرامن، پیش‌نصب شده، و احراز هویت شده. - روش‌های امن برای مسیریابی و کنترل دسترسی. - طراحی شده برای شبکه‌های کم‌مصرف.	- ممکن است پیاده‌سازی حالت‌های امنیتی به‌طور کامل در همه موارد عملیاتی نباشد. - پیچیدگی در تنظیم و مدیریت وضعیت‌های امنیتی مختلف.
ONS	نام‌گذاری و DNS	- تضمین نام‌گذاری یکتا برای دستگاه‌ها و سرویس‌ها. - روش‌های کنترل دسترسی و احراز هویت. - مشابه DNS برای نام‌گذاری اشیاء توزیع شده.	- ممکن است در برابر حملات DNS به اندازه کافی مقاوم نباشد. - نیاز به پیاده‌سازی‌های صحیح برای حفاظت از اطلاعات.
OASIS: MQTT	پروتکل پیام‌رسانی	- رمزنگاری و سیاست‌های دسترسی. - مناسب برای مسافت‌های طولانی. - حمایت از حفاظت از حریم خصوصی حتی در صورت به‌خطر افتادن سرور.	- امنیت به پیاده‌سازی صحیح رمزنگاری و سیاست‌های دسترسی بستگی دارد. - ممکن است در شرایط خاص آسیب‌پذیر باشد.
TLS/DTLS	امنیت لایه حمل و نقل	- استفاده از تکنیک‌های رمزنگاری قوی مانند RSA، AES و HMAC. - حفاظت از یکپارچگی و محرمانگی اطلاعات. - قابل استفاده در انواع پروتکل‌ها.	- ممکن است به دلیل نیاز به منابع پردازشی، بر عملکرد شبکه تأثیر بگذارد. - پیاده‌سازی نادرست می‌تواند به مشکلات امنیتی منجر شود.
IEEE 1888.3	شبکه‌های سبز فراگیر	- استفاده از تکنیک‌های رمزنگاری برای حفاظت از داده‌ها. - شامل روش‌های کنترل دسترسی و احراز هویت. - طراحی شده برای بهبود امنیت در شبکه‌های سبز.	- ممکن است نیاز به منابع و پیچیدگی در پیاده‌سازی داشته باشد. - ممکن است در برابر حملات جدید به‌روز نباشد.
SCTP	پروتکل حمل و نقل	- قابلیت انتقال داده‌ها به‌صورت پیام‌محور. - ویژگی‌های امنیتی مانند چند مسیریابی و مقاومت در برابر حملات. - کنترل دسترسی و احراز هویت.	- ممکن است در مقایسه با TCP و UDP پیچیدگی بیشتری داشته باشد. - نیاز به پیکربندی دقیق برای استفاده از ویژگی‌های امنیتی.
TCG	امنیت دستگاه‌ها	- استفاده از ماژول پلتفرم مطمئن و به‌روزرسانی اعتماد از راه دور. - تضمین امنیت دستگاه‌ها و حفاظت از داده‌ها. - روش‌های کنترل دسترسی و احراز هویت.	- ممکن است به منابع اضافی و پیچیدگی در پیاده‌سازی نیاز داشته باشد. - پیاده‌سازی نادرست می‌تواند به مشکلات امنیتی منجر شود.

ISO/IEC 27001	مدیریت امنیت اطلاعات	- ایجاد یک سیستم مدیریت امنیت اطلاعات موثر. - شامل سیاست‌ها، فرآیندها، و کنترل‌های امنیتی. - مناسب برای مدیریت و حفاظت از اطلاعات حساس.	- پیچیده و زمان‌بر باشد. - نیاز به به‌روزرسانی دارد و ممکن است به نظارت مداوم برای حفظ امنیت نیازمند باشد.
ISO/IEC 29100	حفظ حریم خصوصی اطلاعات	- شامل راهنمایی‌ها برای مدیریت حریم خصوصی داده‌ها. - تضمین حریم خصوصی و حفاظت از اطلاعات شخصی. - مناسب برای مدیریت ریسک‌های حریم خصوصی.	- ممکن است در همه موارد، پیاده‌سازی به‌صورت کامل عملیاتی نباشد. - نیاز به پیاده‌سازی‌های دقیق برای حفاظت از حریم خصوصی.

جدول ۳: بررسی نقش اینترنت اشیا و بلاک‌چین در امنیت و اعتماد در بخش‌های مختلف داده‌های شهر هوشمند

Table 3. Analysis of the Role of IoT and Blockchain in Security and Trust Across Different Data Segments in Smart Cities

بخش داده‌های شهر هوشمند	کاربرد اینترنت اشیا	نقش بلاک‌چین	نقاط قوت	نقاط ضعف
حمل و نقل	جمع‌آوری و ارسال داده‌های ترافیکی و موقعیت وسایل نقلیه	ذخیره‌سازی امن داده‌های ترافیکی و موقعیت وسایل نقلیه، تأیید صحت داده‌ها	افزایش شفافیت، کاهش تقلب، بهبود ترافیک	نیاز به منابع پردازشی بالا، پیچیدگی پیاده‌سازی
محیط زیست	پایش کیفیت هوا، سطح نویز، دما و سایر شاخص‌های محیطی	ثبت تغییرات و داده‌های محیطی در بلاک‌چین به‌صورت غیرقابل تغییر	افزایش دقت و صحت داده، قابلیت ردیابی تغییر	نیاز به ذخیره‌سازی بزرگ، پیچیدگی یکپارچه‌سازی
انرژی	مدیریت مصرف و تولید انرژی، پایش مصرف انرژی	ثبت و تأیید تراکنش‌های انرژی و قراردادهای هوشمند برای مدیریت مصرف	بهبود کارایی و شفافیت، کاهش اتلاف انرژی	هزینه‌های پیاده‌سازی بالا، نیاز به فناوری‌های پیشرفته
سلامت	جمع‌آوری داده‌های پزشکی و سلامت، مانیتورینگ وضعیت بیماران	ذخیره‌سازی امن داده‌های پزشکی، کنترل دسترسی با قراردادهای هوشمند	افزایش امنیت و حریم خصوصی، بهبود دسترسی به داده‌ها	پیچیدگی پیاده‌سازی، نیاز به زیرساخت‌های مناسب
ایمنی	نظارت تصویری، جمع‌آوری داده‌های امنیت عمومی	ذخیره‌سازی امن داده‌های نظارتی، تضمین صحت داده‌ها	بهبود امنیت عمومی، جلوگیری از دست‌کاری داده‌ها	نیاز به ظرفیت ذخیره‌سازی بزرگ، پیچیدگی مدیریت داده‌ها
خدمات شهری	جمع‌آوری نظرات و پیشنهادات شهروندان و نیز درخواست‌های خدمات شهری	ثبت و پیگیری درخواست‌ها و نظرات شهروندان به‌صورت شفاف و قابل ردیابی	افزایش نرخ مشارکت شهروندان، بهبود خدمات شهری	پیچیدگی پیاده‌سازی، نیاز به آموزش شهروندان

۳-۵- نقش دولت و نهادهای مرتبط در اجرای قوانین حفاظت از داده‌ها

یکی از موارد مهم در حفاظت از داده‌ها در شهرهای هوشمند، همکاری و هماهنگی میان دولت، صنعت و نهادهای قضایی است. دولت‌ها مسئول تصویب قوانین و مقررات مربوط به حفاظت از داده‌ها و حریم خصوصی هستند و باید به‌طور شفاف و مسئولانه، حقوق افراد را در مورد جمع‌آوری، پردازش و استفاده از داده‌ها تضمین کنند. بازیگران صنعتی، از جمله توسعه‌دهندگان راه‌حل‌های شهر هوشمند، نیز در طراحی و پیاده‌سازی سامانه‌ای امن و رعایت بهترین شیوه‌های حریم خصوصی مسئولیت دارند. همچنین، نهادهای قضایی نقش حیاتی در اجرای قوانین و حل اختلافات مربوط به حریم خصوصی ایفا می‌کنند. علاوه بر این، شراکت‌های عمومی و خصوصی در افزایش امنیت و حریم خصوصی در شهرهای هوشمند حائز اهمیت است [۳۱].

همکاری بین نهادهای دولتی، شرکت‌های خصوصی و سازمان‌های جامعه مدنی می‌تواند منجر به راه‌حل‌های جامع و مؤثرتری شود و در به اشتراک‌گذاری تخصص، منابع و بهترین شیوه‌ها برای حل چالش‌های امنیت سایبری کمک کند. همچنین، می‌توانند همکاری در زمینه تحقیق و توسعه را ترویج کنند تا امکان اجرای فناوری‌های نوآورانه و پروتکل‌های امنیتی فراهم شود. اقدامات

مشترک می‌تواند برنامه‌های آموزشی، کارگاه‌ها و کمپین‌های آگاهی را فراهم کند تا افراد، سازمان‌ها و جوامع را در مورد خطرات امنیتی و بهترین شیوه‌های حفاظت از داده آموزش دهد.

۴- مطالعه موردی اثربخشی قوانین و مقررات حفاظت از داده‌های شهرهای هوشمند در ایران

۴-۱- بررسی وضعیت فعلی قانونی حفاظت از داده‌های شهرهای هوشمند در ایران

وضعیت فعلی قوانین و مقررات مربوط به داده‌ها در شهرهای هوشمند در ایران به دلیل عدم وجود یک متن قانونی یکپارچه و منسجم در این زمینه، با مشکلاتی روبه‌رو است. این خلأ قانونی باعث ایجاد یک وضعیت جدی در ارتباط با حفاظت از داده‌ها در شهرهای هوشمند شده است. بنابراین، لازم است هر یک از نهادهای مسئول در این زمینه، با توجه به صلاحیت‌ها و وظایف محدود خود، اقداماتی را برای پر کردن این خلأ اساسی و ایجاد یک چارچوب قانونی واحد و کارآمد برای حفاظت از داده‌ها در شهرهای هوشمند ایران انجام دهند [۳۲]. جدول ۴ بررسی نقش دولت و نهادهای مرتبط در حفاظت از داده‌های شهر هوشمند و جدول ۵ قوانین و مقررات داده و بخش‌های مختلف متولی آن را نمایش می‌دهد.

این وضعیت از سال ۱۳۸۴ به وجود آمده است، هنگامی که "لایحه حفظ حریم خصوصی" به مجلس شورای اسلامی ارائه شد. متأسفانه، قبل از رسیدگی و تصویب، در فروردین سال ۱۳۸۵ دولت جدید این لایحه را پس گرفت و از آن زمان تاکنون هیچ اقدامی در این زمینه انجام نشده است. این لایحه شامل ۷ سرفصل بود که به موضوعاتی مانند حریم خصوصی جسمانی، حریم خصوصی اماکن و منازل، حریم خصوصی در محل کار، حریم خصوصی اطلاعات، اطلاعات شخصی در فعالیت‌های رسانه‌ای، حریم خصوصی ارتباطات و مسئولیت‌های ناشی از نقض حریم خصوصی پرداخته بود. بنابراین، از آنجایی که قانون‌گذاری، وظیفه اصلی و اولیه مجلس شورای اسلامی است، انتظار ورود کمیسیون تنظیم مقررات ارتباطات به حوزه حریم خصوصی، به‌طور عمومی، امکان‌پذیر نیست. اما اگر ضرورتی احساس شود، این کمیسیون می‌تواند الزام‌های فنی حفاظت از حریم خصوصی کاربران را برای افراد و شرکت‌های فعال در این حوزه با وضع مصوبات مناسب، به اجرا بگذارد. از آنجایی که هیچ‌یک از نهادهای موجود در کشور مسئولیت اجرای قوانین حریم خصوصی را به عهده نگرفته‌اند، احتمال ایجاد یک نهاد جدید با ساختار و تشکیلات منحصر به فرد، ضروری به نظر می‌رسد [۳۳]. اما پاسخ به این سؤال که کدام یک از نهادهای موجود در کشور مسئولیت اجرای چنین قوانینی را بر عهده بگیرد و یا آیا نهاد جدیدی باید ایجاد شود، سؤالی پیچیده است که پاسخ آن به شرایط و موقعیت‌های خاص کشور وابسته است.

به‌طور کلی، تا زمانی که متن قانونی منسجم در این زمینه وجود نداشته باشد، نمی‌توان به‌طور قطعی، نقش و مسئولیت نهادهای نظارتی و اجرایی را در این زمینه مشخص کرد. با اهمیت بالایی که این موضوع دارد، توجه به ایجاد یک نهاد مسئول در این زمینه ضروری است تا حریم خصوصی در کشور به‌خوبی حفظ شود.

۴-۲- نواقص قوانین و مقررات مربوط به شهر هوشمند و فضای مجازی

به‌منظور تأکید بر اهمیت بی‌پایان داده‌ها در جهان امروز، "لایحه حمایت از داده و حریم خصوصی در فضای مجازی" توسط سازمان فناوری اطلاعات ایران، پژوهشگاه قوه قضاییه و دانشگاه علم و فرهنگ تدوین شده است. این لایحه به‌عنوان یکی از مهم‌ترین قوانین در زمینه حفظ حریم خصوصی و اطلاعات کاربران در فضای سایبر به‌شمار می‌آید. در بخش چهارم این لایحه با عنوان "تنظیم و نظارت بر پردازش داده‌های شخصی"، چهار نهاد اصلی، مسئولیت نظارت بر پردازش داده‌های شخصی را بر عهده دارند. این چهار نهاد شامل کمیسیون صیانت و حفاظت از داده‌های شخصی، هیئت نظارت، کارگروه‌های تخصصی و دبیرخانه اجرایی کمیسیون هستند که در سایر کشورها به‌عنوان نهادهایی که از داده‌ها محافظت می‌کنند، شناخته می‌شوند. در ماده ۴۰ این لایحه، اعضای کمیسیون صیانت و حفاظت از داده‌های شخصی به شرح زیر تعریف شده‌اند: وزیر ارتباطات و فناوری اطلاعات به‌عنوان رئیس کمیسیون، وزیر اطلاعات، وزیر کشور، وزیر دادگستری، وزیر فرهنگ و ارشاد اسلامی، وزیر اقتصاد و امور دارایی، دبیر شورای عالی انقلاب فرهنگی، رئیس مرکز ملی فضای مجازی، معاون پیشگیری از وقوع جرم قوه قضاییه، رئیس کمیسیون اصل نودم مجلس شورای اسلامی، دادستان کل کشور، و دبیر شورای اجرایی فناوری اطلاعات به‌عنوان دبیر کمیسیون [۴۱-۴۲].

جدول ۴: بررسی نقش دولت و نهادهای مرتبط در حفاظت از داده‌های شهر هوشمند

Table 4. Analysis of the Role of Government and Related Institutions in Protecting Smart City Data

نهاد/سازمان	نقش	وظایف و مسئولیت‌ها	چالش‌ها	اقدامات کلیدی پیشنهادی
هیات دولت	تعیین سیاست‌ها و قوانین کلی حفاظت از داده‌ها	تدوین و تصویب قوانین، ایجاد زیرساخت‌های قانونی، نظارت بر اجرای قوانین	هماهنگی بین نهادهای مختلف، تأمین بودجه و منابع لازم	ایجاد واحدهای تخصصی، برگزاری جلسات هماهنگی بین نهادهای تخصصی بودجه مناسب، تصویب قوانین ملی نظیر قانون عمومی حفاظت داده
وزارت ارتباطات و فناوری اطلاعات	نظارت بر اجرای قوانین و مقررات در حوزه فناوری اطلاعات	تدوین استانداردها و پروتکل‌های امنیتی، نظارت بر عملکرد شرکت‌های فناوری	پیچیدگی فناوری، تغییرات سریع در حوزه فناوری	به‌روزرسانی استانداردها، همکاری با نهادهای بین‌المللی، ارتقاء دانش فنی، اجرای استانداردهای امنیتی نظیر ISO 27001
سازمان ملی استاندارد	تدوین و تصویب استانداردهای ملی در حوزه امنیت داده‌ها	ایجاد و انتشار استانداردهای امنیتی، نظارت بر اجرای استانداردها توسط شرکت‌ها و نهادهای	هماهنگی با سایر نهادهای پذیرش و انطباق با استانداردهای بین‌المللی	مشارکت فعال در نهادهای بین‌المللی استانداردسازی، برگزاری کارگاه‌ها و دوره‌های آموزشی
شهرداری‌ها	اجرای قوانین و مقررات در سطح محلی	مدیریت داده‌های شهری، نظارت بر پروژه‌های شهر هوشمند، همکاری با شرکت‌های خصوصی	محدودیت‌های مالی، پیچیدگی مدیریت داده‌ها	جذب سرمایه‌گذار خصوصی، استفاده از پلتفرم‌های مدیریت داده هوشمند، آموزش و توانمندسازی پرسنل
سازمان حفاظت از داده‌ها	حفاظت از حقوق شهروندان در زمینه داده‌ها	نظارت بر جمع‌آوری، پردازش و ذخیره‌سازی داده‌ها، رسیدگی به شکایات و تخلفات	حفظ تعادل بین حفاظت از داده‌ها و استفاده از داده‌ها برای بهبود خدمات	استفاده از فناوری‌های پیشرفته نظارتی، برگزاری کمپین‌های آگاهی‌رسانی، توسعه سامانه‌هایی برای گزارش‌دهی شفاف
نیروی انتظامی	تأمین امنیت فیزیکی و سایبری شهر هوشمند	پیشگیری و مقابله با جرائم سایبری، نظارت بر امنیت شبکه‌ها و سامانه‌ها	مقابله با تهدیدات پیچیده سایبری، تأمین تجهیزات و نیروی انسانی متخصص	ارتقاء سطح آموزش و توانمندسازی نیروی انسانی، همکاری با نهادهای بین‌المللی، استفاده از فناوری‌های نوین امنیتی
شرکت‌های فناوری	پیاده‌سازی و نگهداری سامانه‌های امن	توسعه و اجرای راهکارهای امنیتی، حفاظت از داده‌های کاربران	رقابت در بازار، تأمین منابع مالی برای امنیت داده‌ها	همکاری با نهادهای دولتی، ارتقاء سطح امنیت داخلی، توسعه راهکارهای نوآورانه
مراکز تحقیقاتی و دانشگاه‌ها	پژوهش و توسعه فناوری‌های امنیتی	انجام تحقیقات در زمینه امنیت سایبری، آموزش نیروی انسانی متخصص	تأمین مالی تحقیقات، نیاز به همکاری با صنعت	ارائه دوره‌های آموزشی تخصصی، انتشار مقالات و نتایج تحقیقاتی
نهادهای بین‌المللی	تدوین استانداردها و پروتکل‌های بین‌المللی	ایجاد و انتشار استانداردها و راهنماهای بین‌المللی، نظارت بر اجرای استانداردها	هماهنگی بین کشورها، پذیرش و انطباق با شرایط محلی	تقویت همکاری‌ها در حوزه بین‌المللی، به‌روزرسانی مداوم استانداردها، تبادل دانش و تجربیات، ایجاد استانداردهای بین‌المللی نظیر ISO

جدول ۵: ماده‌های قانونی مرتبط با حوزه حریم خصوصی و امنیت داده و بخش‌های مختلف متولی
Table 5. Legal Provisions Related to Privacy and Data Security and the Responsible Sectors

مراجع	نام نهاد یا سازمان	ماده قانونی مرتبط
مراجع سیاست‌گذاری و تقنینی	مجمع تشخیص مصلحت نظام	بند ۱ اصل ۱۱۰ قانون اساسی: «تعیین سیاست‌های کلی نظام جمهوری اسلامی ایران» [۳۴]
	مجلس شورای اسلامی	اصل ۷۱ قانون اساسی: «مجلس شورای اسلامی در عموم مسائل در حدود مقرر در قانون اساسی می‌تواند قانون وضع کند.» [۳۵]
	شورای عالی فضای مجازی	«تدوین سیاست‌ها و تصویب مقررات کلان موردنیاز فضای مجازی مانند توافقنامه‌های درجه و سطح خدمات، حمایت از حقوق کاربران فضای مجازی و تنظیم روابط فعالان فضای مجازی در چارچوب مصوبات شورای عالی.» [۳۶]
مراجع نظارتی و اجرا	کمیسیون تنظیم مقررات ارتباطات	سیاست‌گذاری، تدوین و تصویب مقررات در حوزه ارتباطات و فناوری اطلاعات [۳۷]
	وزارت ارتباطات و فناوری اطلاعات	قانون اهداف و وظایف وزارت ارتباطات و فناوری اطلاعات: بند ک. «تدوین و پیشنهاد استانداردهای ملی مربوط به ارتباطات و فناوری اطلاعات در کشور به مراجع ذی‌ربط.» بند ف. «حفاظت و حراست و عدم ضبط و افشای انواع مراسلات و امانات پستی و همچنین مکالمات تلفنی و مبادلات شبکه اطلاع‌رسانی و اطلاعات مربوط به اشخاص حقیقی و حقوقی طبق قانون.» [۳۸]
	سازمان تنظیم مقررات و ارتباطات رادیویی	بند ۹، ماده ۶ اساسنامه با موضوع وظایف و اختیارات سازمان: «حمایت از حقوق استفاده‌کنندگان خدمات پستی، مخابراتی و فناوری اطلاعات و نظارت مستمر بر اعمال صحیح آن‌ها، تدوین و پیشنهاد دستورالعمل‌های لازم به‌منظور تنظیم روابط ارائه‌کنندگان خدمات پستی، مخابراتی و فناوری اطلاعات و پیشنهاد اصلاح قوانین پستی، مخابراتی و ارتباطی به مراجع ذی‌صلاح قانونی.» [۳۹]
	کارگروه تعیین مصادیق محتوای مجرمانه	ماده ۲۲ قانون جرائم رایانه‌ای: «مسئولیت نظارت بر فضای مجازی و پالایش تارنماهای حاوی محتوای مجرمانه.»
	سازمان فناوری اطلاعات	ماده ۲ اساسنامه: «مدیریت، حمایت و ساماندهی امور مربوط به امنیت فضای تبادل اطلاعات، نرم‌افزار و سخت‌افزار، بالابردن آمادگی الکترونیکی، توسعه اینترنت، توسعه فناوری اطلاعات و کاربردهای آن در کشور.» بند ۱۱ ماده ۷ اساسنامه: «ایجاد، توسعه، نگهداری و بهره‌برداری از مراکز داده ملی اینترنتی به‌منظور میزبانی و حفظ داده‌های حساس دولتی.» [۴۰]
مراجع قضایی	قوه قضاییه	اصل ۱۵۶ قانون اساسی: «رسیدگی و صدور حکم در مورد تظلمات، تعدیات، شکایات، حل‌وفصل دعاوی و رفع خصومات و اخذ تصمیم و اقدام لازم.»
	کارگروه تعیین مصادیق محتوای مجرمانه	ماده ۲۲ قانون جرائم رایانه‌ای: «رسیدگی به شکایات مردمی.»

با توجه به ماده ۴۰، با تشکیل جلسات کمیسیون، احکام عضویت اعضا توسط رئیس کمیسیون صادر می‌گردد. همچنین، کارگروه‌های تخصصی که از نمایندگان نهادهای مسئول امور حاکمیتی مرتبط با صیانت و حفاظت از داده‌های شخصی تشکیل شده‌اند، وظایف مشخص شده در این لایحه را بر عهده دارند و در جلسات اولیه کمیسیون، آیین‌نامه تشکیل کارگروه‌ها تصویب خواهد شد.

مطابق ماده ۴۷ و ۴۸، توجه به نکات زیر ضروری است:

- ۱- نظارت نه تنها بر پردازش داده‌های شخصی، بلکه باید بر کنترل‌کننده و پردازشگر نیز صورت پذیرد.
 - ۲- در نظر گرفتن چهار رکن، یعنی کمیسیون، هیئت نظارت، کارگروه تخصصی و دبیرخانه اجرایی، باعث پیچیده شدن فرایند تنظیم و نظارت و افزایش سازوکار اداری خواهد شد.
 - ۳- اعطای صلاحیت برای حل و فصل اختلافات بین کارگروه‌های تخصصی و هیئت نظارت و سایر نهادهای حاکمیتی، در تناقض با صلاحیت‌های دیوان عدالت اداری است.
 - ۴- عضویت نمایندگان نهادهای مسئول امور حاکمیتی در کارگروه‌های تخصصی باید واضح‌تر معرفی شود.
- با توجه به این موضوعات، پیشنهاد می‌شود یک کمیسیون برای نظارت بر اجرای صحیح این لایحه و همچنین کنترل‌کنندگان و پردازشگران تشکیل شود و وظایف، صلاحیت‌ها و اختیارات نهادهای مذکور بدون ارجاع به مصوبات بعدی در متن خود لایحه پیش‌بینی شود تا سازوکارهای اداری پیچیده در مسیر حمایت و صیانت از داده‌های شخصی کاهش یابد.

۳-۴- راهکارهای پیشنهادی برای ارتقای قوانین در حوزه زیرساخت‌های فناوری در شهر هوشمند

با توجه به کاستی‌های موجود در قوانین و مقررات مرتبط با داده و حریم خصوصی در شهر هوشمند و با توجه به اهمیت فزاینده استفاده از فناوری‌های مدرن از جمله اینترنت اشیا و بلاک‌چین در توسعه شهر هوشمند، باید راهکارهایی ارائه شود که بتوانند این نواقص را برطرف سازند و همچنین تضمین رعایت الزامات حقوقی مرتبط را فراهم کنند.

در جدول ۶، راهکارهای پیشنهادی برای ارتقای قوانین در حوزه زیرساخت‌های فناوری برای شهر هوشمند در ایران با محوریت اینترنت اشیا و زیرساخت‌های محاسبات ابری بررسی شده است. به علاوه، لازم است تا این راهکارها با اصول اصلاحی و جلب اعتماد مردم در توسعه شهر هوشمند هماهنگ شوند تا پایداری و پذیرش عمومی آن‌ها تضمین شود.

در این راستا، گزینه‌هایی برای بهبود قوانین و مقررات مربوط به داده و حریم خصوصی در شهر هوشمند پیشنهاد می‌شود. این گزینه‌ها شامل اصلاح و بهبود قوانین موجود، ایجاد قوانین جدید، تشکیل کمیسیون‌ها و هیات‌های تخصصی، آموزش و اطلاع‌رسانی، ارتقای زیرساخت‌های فناوری، همکاری بین نهادها، استفاده از فناوری بلاک‌چین، تشویق به استفاده مسئولانه از داده‌ها، تضمین حقوق حریم خصوصی، راه‌اندازی سازوکارهای نظارت و بازرسی، و ارتقای آگاهی عمومی هستند. این گزینه‌ها می‌توانند بهبود قابل توجهی در امنیت و حفاظت داده‌ها در شهر هوشمند به دنبال داشته باشند. این اقدامات به منظور ساماندهی و کنترل مناسب داده‌ها، حفاظت از حریم خصوصی شهروندان، ایجاد زیرساخت‌های مناسب و ایجاد محیطی امن و پایدار برای توسعه شهر هوشمند ضروری است. برای اطمینان از اجرای موثر این راهکارها، نیاز به هماهنگی بین نهادها، ارائه آموزش‌های تخصصی برای کارکنان مربوطه، و ایجاد سازوکارهای قوی برای نظارت و ارزیابی پیشرفت این اقدامات وجود دارد [۴۳].

در بخش داده‌های حمل و نقل، بلاک‌چین می‌تواند با ایجاد یک دفتر کل غیرقابل تغییر و شفاف، امنیت و اعتماد را افزایش دهد. پروتکل‌هایی مانند پروتکل کاربرد محدود و پروتکل انتقال تله‌متری پیام برای انتقال داده‌های ترافیکی و موقعیت وسایل نقلیه عمومی، می‌توانند به خوبی از ویژگی‌های بلاک‌چین بهره‌برداری کنند. با استفاده از بلاک‌چین، داده‌های ترافیکی ثبت و تأیید شده و به صورت غیرقابل تغییر در دفتر کل توزیع شده ذخیره می‌شوند. این کار از تغییرات غیرمجاز و دست‌کاری داده‌ها جلوگیری کرده و به تقویت امنیت و اعتبار اطلاعات کمک می‌کند. بلاک‌چین همچنین می‌تواند با ارائه شفافیت در فرآیندهای تأیید و مدیریت داده‌ها، به اعتمادسازی بیشتر بین ذینفعان مختلف از جمله اپراتورها و کاربران نهایی کمک کند.

برای داده‌های محیط‌زیست، بلاک‌چین می‌تواند به بهبود امنیت داده‌های کیفیت هوا، سطح نویز و دما کمک کند. استفاده از بلاک‌چین در این بخش به همراه اس‌تنداردهایی مانند LoWPAN6 و RFC 6550 می‌تولند به ثبت و ذخیره‌سازی داده‌ها به صورت امن و شفاف کمک کند. بلاک‌چین با ایجاد یک سیستم ثبت داده غیرقابل تغییر و توزیع شده، اطمینان می‌دهد که داده‌های محیط‌زیست به صورت معتبر و بدون تغییرات غیرمجاز در دسترس قرار گیرند. این ویژگی به همراه تکنیک‌های رمزنگاری و روش‌های مسیریابی امن، از صحت و امنیت داده‌های محیط‌زیست محافظت می‌کند و شفافیت و اعتماد را در میان سازمان‌ها و شهروندان افزایش می‌دهد.

جدول ۶: راهکارهای پیشنهادی برای ارتقای قوانین در حوزه زیرساخت‌های فناوری در شهر هوشمند

Table 6. Proposed Solutions for Enhancing Laws in the Domain of Technology Infrastructure in Smart Cities

حوزه	چالش‌ها	راهکارهای پیشنهادی	اهداف
اینترنت اشیا	امنیت داده‌ها، تعامل بین دستگاه‌ها، حجم بالای داده‌ها	۱. استانداردسازی و پروتکل‌های امنیتی: تدوین و اجرای استانداردهای امنیتی برای دستگاه‌های اینترنت اشیا، استفاده از پروتکل‌های رمزنگاری برای داده‌های در حال انتقال. ۲. شبکه‌های ارتباطی پیشرفته: بهبود زیرساخت‌های مخابراتی برای پشتیبانی از دستگاه‌های اینترنت اشیا، سرمایه‌گذاری در فناوری‌های 5G برای افزایش سرعت و کاهش تأخیر. ۳. مدیریت و تجزیه و تحلیل داده‌ها: پیاده‌سازی انواع سامانه‌های تحلیل داده‌های بزرگ برای پردازش و مدیریت حجم بالای داده‌های اینترنت اشیا. ۴. ایجاد چارچوب‌های قانونی: تدوین قوانین برای حفاظت از حریم خصوصی و امنیت داده‌های اینترنت اشیا و تنظیم مقررات برای مسئولیت‌پذیری تولیدکنندگان و ارائه‌دهندگان خدمات.	۱. افزایش امنیت: حفاظت از داده‌های کاربران و دستگاه‌های متصل ۲. بهبود عملکرد شبکه: کاهش تأخیر و افزایش سرعت انتقال داده‌ها. ۳. مدیریت کارآمد داده‌ها: پردازش و تحلیل داده‌های با حجم بالا به‌صورت مؤثر. ۴. پایداری و اطمینان: افزایش اعتماد عمومی به فناوری‌های اینترنت اشیا از طریق مقررات شفاف و مؤثر.
زیرساخت‌های محاسبات ابری	امنیت و حریم خصوصی داده‌ها، تضمین دسترسی پیوسته، هزینه‌ها	۱. حفاظت از داده‌ها: تدوین مقررات برای حفاظت از داده‌های ذخیره شده در فضای ابری، استفاده از فناوری‌های رمزنگاری قوی برای داده‌های استراحت و در حال انتقال. ۲. پشتیبانی از زیرساخت‌های ابری: ارتقاء زیرساخت‌های شبکه برای پشتیبانی از سرویس‌های ابری، افزایش پهنای باند و بهبود سرعت انتقال. ۳. تضمین دسترسی و عملکرد: توسعه سامانه‌های پشتیبانی و بازیابی برای تضمین دسترسی پیوسته و کاهش زمان‌های خرابی. ۴. مدیریت هزینه‌ها: ایجاد مقررات برای مدیریت هزینه‌های استفاده از خدمات ابری، نظارت بر قراردادهای پرداخت‌ها، تشویق به استفاده بهینه از منابع ابری.	۱. افزایش امنیت داده‌ها: حفاظت از داده‌های حساس و حفظ حریم خصوصی کاربران. ۲. بهبود دسترسی و عملکرد: تضمین دسترسی پیوسته و کارایی بالا برای خدمات ابری. ۳. مدیریت بهینه هزینه‌ها: کاهش هزینه‌های مربوط به استفاده از خدمات ابری و افزایش بهره‌وری. ۴. پایداری و مقیاس‌پذیری: ارائه زیرساخت‌های مقیاس‌پذیر و پایدار برای پشتیبانی از رشد سریع نیازهای ابری.
بلاک‌چین	مقیاس‌پذیری، هزینه‌ها، تنظیمات قانونی	۱. توسعه زیرساخت‌های بلاک‌چین: سرمایه‌گذاری در توسعه و بهینه‌سازی زیرساخت‌های بلاک‌چین برای مقیاس‌پذیری و کارایی. ۲. تدوین قوانین و مقررات: تنظیم قوانین و مقررات مربوط به استفاده از فناوری بلاک‌چین، از جمله قوانین مربوط به قراردادهای هوشمند و حفظ حریم خصوصی. ۳. یکپارچگی با سامانه‌های موجود: ایجاد راهکارهای یکپارچه برای ادغام بلاک‌چین با سامانه‌های اطلاعاتی و زیرساخت‌های فناوری موجود. ۴. آموزش و توسعه مهارت‌ها: آموزش نیروی انسانی و توسعه مهارت‌های مربوط به بلاک‌چین در سطح ملی.	۱. افزایش مقیاس‌پذیری: بهبود مقیاس‌پذیری و عملکرد شبکه‌های بلاک‌چین. ۲. کاهش هزینه‌ها: کاهش هزینه‌های مربوط به پیاده‌سازی و نگهداری بلاک‌چین. ۳. شفافیت و امنیت: افزایش شفافیت و امنیت داده‌ها از طریق فناوری بلاک‌چین. ۴. پذیرش و توسعه: تسهیل پذیرش فناوری بلاک‌چین و ایجاد زیرساخت‌های مناسب برای توسعه بیشتر.

در داده‌های انرژی، سلامت، و ایمنی، بلاک‌چین می‌تواند به ارائه لایه‌های اضافی امنیت و شفافیت کمک کند. به‌عنوان مثال، در داده‌های انرژی مانند مصرف برق و گاز، بلاک‌چین می‌تواند به نظارت و تأیید صحت داده‌ها در شبکه‌های انرژی کمک کند. داده‌های سلامت و ایمنی که شامل اطلاعات حساس و شخصی است، می‌تواند با استفاده از بلاک‌چین به‌صورت غیرقابل تغییر و امن، ذخیره شده و به اشتراک گذاشته شوند. استانداردهای SCTP، ISO/IEC 27001، و ISO/IEC 29100 می‌توانند با بهره‌برداری از ویژگی‌های بلاک‌چین، از جمله قابلیت‌های ثبت غیرقابل تغییر و تأیید هویت، به بهبود امنیت و حریم خصوصی داده‌های حساس کمک کنند. این امر به بهبود اعتماد در مدیریت و دسترسی به اطلاعات مهم سلامت و ایمنی می‌انجامد.

در نهایت، بلاک چین می‌تواند در داده‌های شهروندی نیز به افزایش امنیت و اعتماد کمک کند. با استفاده از بلاک چین، نظرات و پیشنهادات شهروندان و درخواست‌های خدمات شهری می‌تواند به صورت امن و شفاف ثبت و مدیریت شود. بلاک چین با ارائه یک سامانه ثبت غیرقابل تغییر و تأیید هویت کاربران، به جلوگیری از تقلب و دست‌کاری در اطلاعات شهروندان کمک می‌کند. این ویژگی به همراه پروتکل‌ها و استانداردهای موجود، از جمله ONS و OASIS، به افزایش اعتماد عمومی و بهبود تعاملات میان شهروندان و نهادهای شهری کمک می‌کند. بلاک چین با ارائه امنیت و شفافیت اضافی، می‌تواند به بهبود کیفیت خدمات شهری و ارتقاء رضایت شهروندان منجر شود. با اعمال این راهکارها به طرز موثر، می‌توان بهبود قوانین و مقررات مربوط به داده و حریم خصوصی در شهر هوشمند را تضمین کرد و محدودیت‌های قانونی برای استفاده از اینترنت اشیا و فناوری بلاک چین را بهبود بخشید. همچنین، امکان ایجاد یک محیط امن و پایدار برای افراد و نهادها در این حوزه فراهم می‌شود.

۵- نتیجه‌گیری

بررسی وضعیت امنیتی و حریم خصوصی در شهرهای هوشمند و ارائه راهکارهای بهبود آن‌ها نشان می‌دهد که با پیشرفت فناوری و گسترش شهرهای هوشمند، مسائل امنیت داده‌ها و حریم خصوصی افراد به یکی از چالش‌های اساسی این محیط‌ها تبدیل شده است. این مسائل شامل مواردی نظیر دسترسی غیرمجاز به داده‌ها، تهدیدات سایبری و نقض حریم خصوصی افراد هستند که نیازمند راهکارهای نوین و موثر برای حل آن‌ها هستند. برای بهبود وضعیت امنیتی و حریم خصوصی در شهرهای هوشمند، اقداماتی از جمله اصلاح و بهبود قوانین و مقررات مربوطه، ایجاد زیرساخت‌های فناوری مناسب، آموزش و آگاهی‌بخشی به افراد و همکاری بین نهادها و صنایع، ضروری است. همچنین، بهره‌گیری از فناوری‌های نوین از قبیل اینترنت اشیا و بلاک چین می‌تواند بهبود قابل توجهی در امنیت و حفاظت از داده‌ها و حریم خصوصی در شهرهای هوشمند ایجاد کند. با اعمال موثر این راهکارها و هماهنگی نهادها و صنایع مختلف، امکان ساخت شهرهای هوشمند با سطح بالایی از امنیت و حریم خصوصی ممکن می‌شود. به همین دلیل، تجزیه و تحلیل دقیق این مسائل و ارائه راهکارهای بهبود، به پیشرفت و توسعه محیط‌های شهری هوشمند و افزایش رضایت شهروندان از آن‌ها کمک می‌کند.

مراجع

- [1] F. Moqaddari, "Redefining the concept of smart cities and the process of urban smartification based on the conceptual and functional evolution of smart cities," *Urban Design Discourse; Review of Contemporary Literature and Theories*, vol. 1, no. 2, 2020 [in Persian].
- [2] H. M. Kim, S. Sabri, and A. Kent, "Smart cities as a platform for technological and social innovation in productivity, sustainability, and livability: A conceptual framework," in *Smart Cities for Technological and Social Innovation*, Academic Press, 2021, pp. 9–28, doi: [10.1016/b978-0-12-818886-6.00002-2](https://doi.org/10.1016/b978-0-12-818886-6.00002-2).
- [3] A. Randhawa and A. Kumar, "Exploring sustainability of smart development initiatives in India," *International Journal of Sustainable Built Environment*, vol. 6, no. 2, pp. 701–710, 2017, doi: [10.1016/j.ijsbe.2017.08.002](https://doi.org/10.1016/j.ijsbe.2017.08.002).
- [4] M. Whaiduzzaman, A. Barros, M. Chanda, S. Barman, T. Sultana, M. S. Rahman, and C. Fidge, "A review of emerging technologies for IoT-based smart cities," *Sensors*, vol. 22, no. 23, p. 9271, 2022, doi: [10.3390/s22239271](https://doi.org/10.3390/s22239271).
- [5] A. Venkatesh and M. S. Eastaff, "A study of data storage security issues in cloud computing," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 3, no. 1, pp. 1741–1745, 2018, doi: [10.9756/bijssesc.9012](https://doi.org/10.9756/bijssesc.9012).
- [6] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and privacy of smart cities: a survey, research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1718–1743, 2018, doi: [10.1109/comst.2018.2867288](https://doi.org/10.1109/comst.2018.2867288).
- [7] B. Hammi, R. Khatoun, S. Zeadally, A. Fayad, and L. Khoukhi, "IoT technologies for smart cities," *IET Networks*, vol. 7, no. 1, pp. 1–13, 2018, doi: [10.1049/iet-net.2017.0163](https://doi.org/10.1049/iet-net.2017.0163).

- [8] M. H. P. Rizi and S. A. H. Seno, "A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city," *Internet of Things*, vol. 20, p. 100584, 2022, doi: [10.1016/j.iot.2022.100584](https://doi.org/10.1016/j.iot.2022.100584).
- [9] L. D. Radu, "Disruptive technologies in smart cities: a survey on current trends and challenges," *Smart Cities*, vol. 3, no. 3, pp. 1022–1038, 2020, doi: [10.3390/smartcities3030051](https://doi.org/10.3390/smartcities3030051).
- [10] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," *Information Systems Frontiers*, pp. 1–22, 2022, doi: [10.1007/s10796-020-10044-1](https://doi.org/10.1007/s10796-020-10044-1).
- [11] S. M. Zanjani, S. M. Zanjani, H. Shahinzadeh, M. Moazzami, F. Ebrahimi and N. Nourmahnad, "Leveraging Big Data Intelligence for Electronic Health Data Collection and Mining in Smart Innovative Cities: Approaches and Applications," *7th Iranian Conference on Advances in Enterprise Architecture (ICAEA)*, Tehran, Iran, Islamic Republic of, 2023, pp. 45–52, doi: [10.1109/ICAEA60387.2023.10414446](https://doi.org/10.1109/ICAEA60387.2023.10414446).
- [12] H. K. Channi and R. Kumar, "The role of smart sensors in smart city," in *Smart Sensor Networks: Analytics, Sharing and Control*, Cham: Springer International Publishing, 2021, pp. 27–48, doi: [10.1007/978-3-030-77214-7_2](https://doi.org/10.1007/978-3-030-77214-7_2).
- [13] A. Jantarani, M. Barati, M. Ghobakhloo, A. Shahin, and M. Talari, "Identifying the requirements of using the Industrial Internet of Things in the automotive supply chain," *Journal of Operations Management*, vol. 2, no. 7, pp. 27–54, 2022.
- [14] L. Xia, D. T. Semirumi, and R. Rezaei, "A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy," *Sustainable Cities and Society*, vol. 98, p. 104771, 2023, doi: [10.1016/j.scs.2023.104771](https://doi.org/10.1016/j.scs.2023.104771).
- [15] Faghihi and Jamshidi, "A review of user data protection laws in selected countries," *Expert Reports (Islamic Consultative Assembly Research Center)*, vol. 94, no. 26, pp. 506–543, 2018 [in Persian].
- [16] F. Farahmand, "A comparative study of the data protection regulation with the General Data Protection Regulation (GDPR)," *Technology Law*, 2023, doi: [10.22133/mtlj.2023.383528.1164](https://doi.org/10.22133/mtlj.2023.383528.1164) [in Persian].
- [17] S. G. Jamison, "Creating a National Data Privacy Law for the United States," *Cybaris Intell. Prop. L. Rev.*, vol. 10, p. 1, 2019.
- [18] G. Pyo and C. Ji, "Cybersecurity and Data Protection: A Study on China's New Cybersecurity Legal Regime and How It Affects Inbound Investment in China," *International Lawyer*, vol. 51, p. 537, 2018.
- [19] J. Eslami and K. Pishgadam, "A comparative study of the concept of freedom in the Citizen Rights Charter and the Universal Declaration of Human Rights," *Legal Research*, vol. 20, no. 45, pp. 95–123, 2021, doi: [10.48300/jlr.2021.129106](https://doi.org/10.48300/jlr.2021.129106) [in Persian].
- [20] H. Mazarei, M. Dadvar, and M. Atabakzadeh, "Distributed Denial of Service Attacks Detection in Internet of Things Using the Majority Voting Approach," *Journal of Southern Communication Engineering*, vol. 13, no. 49, pp. 23–48, 2023, doi: [10.30495/jce.2023.1984927.1201](https://doi.org/10.30495/jce.2023.1984927.1201).
- [21] F. Fazli, M. Mansubassiri, and F. Babazadeh, "A-RPL: Routing Algorithm with the Ability to Support Mobility in Internet of Things Networks," *Journal of Southern Communication Engineering*, vol. 13, no. 50, pp. 11–32, 2023, doi: [10.30495/jce.2023.1975641.1183](https://doi.org/10.30495/jce.2023.1975641.1183).
- [22] S. Tahmasebi Limooni, S. Ghasemi, and R. Ghorbanloo, "Identifying the common threats and vulnerabilities in the Internet of Things (IoT) and offering security policies for confronting them," *Journal of Knowledge Studies*, vol. 12, no. 44, pp. 32–54, 2019.
- [23] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks," *Multimedia Tools and Applications*, vol. 77, pp. 18295–18325, 2018, doi: [10.1007/s11042-017-5376-4](https://doi.org/10.1007/s11042-017-5376-4).

- [24] A. H. Salehi Shayegan, A. Zakeri, and A. Salehi Shayegan, "Optimizing resources allocation for fog computing-based internet of things networks to reduce latency cost," *Computational Economics*, vol. 1, no. 3, pp. 99-112, 2022.
- [25] P. Lis and J. Mendel, "Cyberattacks on critical infrastructure: An economic perspective," *Economics and Business Review*, vol. 5, no. 2, pp. 24-47, 2019, doi: [10.18559/ebr.2019.2.2](https://doi.org/10.18559/ebr.2019.2.2).
- [26] A. R. Berkel, P. M. Singh, and M. J. van Sinderen, "An information security architecture for smart cities," in *Business Modeling and Software Design: 8th International Symposium, BMSD 2018, Vienna, Austria, July 2-4, 2018, Proceedings 8*, Springer International Publishing, 2018, pp. 167-184, doi: [10.1007/978-3-319-94214-8_11](https://doi.org/10.1007/978-3-319-94214-8_11).
- [27] R. Gupta, N. K. Jadav, A. Nair, S. Tanwar, and H. Shahinzadeh, "Blockchain and AI-based secure onion routing framework for data dissemination in IoT environment underlying 6g networks," in *2022 Sixth International Conference on Smart Cities, Internet of Things and Applications (SCIoT)*, 2022, pp. 1-6, doi: [10.1109/sciot56583.2022.9953671](https://doi.org/10.1109/sciot56583.2022.9953671).
- [28] G. Shahinzadeh, H. Shahinzadeh, and S. Tanwar, "Security and Privacy Issues in the Internet of Things: A Comprehensive Survey of Protocols, Standards, and the Revolutionary Role of Blockchain," in *2024 8th International Conference on Smart Cities, Internet of Things and Applications (SCIoT)*, 2024, pp. 59-67, doi: [10.1109/sciot62588.2024.10570131](https://doi.org/10.1109/sciot62588.2024.10570131).
- [29] A. Asilian, H. Shahinzadeh, S. M. Zanjani, G. B. Gharehpetian, A. Y. Abdelaziz, and S. Tanwar, "The Role of Microelectronics for Smart Cities, Smart Grids and Industry 5.0: Challenges, Solutions, and Opportunities," in *13th Smart Grid Conference (SGC)*, 2023, pp. 1-12, doi: [10.1109/sgc61621.2023.10459310](https://doi.org/10.1109/sgc61621.2023.10459310).
- [30] S. M. Zanjani, H. Shahinzadeh, S. M. Kargar, M. Moazzami, F. Ebrahimi, and M. Hemmati, "Internet of Things Security: A Review on Challenges, Solutions and Research Directions," in *2023 7th International Conference on Internet of Things and Applications (IoT)*, 2023, pp. 1-8, doi: [10.1109/iot60973.2023.10365381](https://doi.org/10.1109/iot60973.2023.10365381).
- [31] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134-46145, 2018, doi: [10.1109/ACCESS.2018.2853985](https://doi.org/10.1109/ACCESS.2018.2853985).
- [32] M. Taghavayi and M. Shafie, "Analysis of indicators and strategies for achieving urban smartification (Case study: Isfahan City)," *Spatial Planning*, vol. 12, no. 1, pp. 51-80, 2022, doi: [10.22108/sppl.2022.131222.1621](https://doi.org/10.22108/sppl.2022.131222.1621) [in Persian].
- [33] A. Tavakoli and D. Dehghani, "The conflict between security-oriented approaches and fair trial principles," *Criminal Law Research Quarterly*, vol. 1, no. 3, pp. 7-34, 2013 [in Persian].
- [34] Esmaeili and T. Tahan-Nazif, "An analysis of the nature of the Supreme Council of the Cultural Revolution in the Constitutional Law of the Islamic Republic of Iran," *Islamic Law Research Journal*, vol. 28, no. 9, pp. 87-120, 2008 [in Persian].
- [35] S. E. Hosseini, "The limitations of the Islamic Consultative Assembly in legislation (Article 71 of the Constitution)," *Islamic Government*, vol. 66, no. 17, pp. 163-194, 2012 [in Persian].
- [36] B. Ansari and Alvandenjad, "The nature and position of regulatory bodies in cyberspace governance in Iran," *Legal Lessons*, vol. 6, no. 1, pp. 281-314, 2020 (in Persian).
- [37] A. Asgharnia, Rostami, and Vali, "Critique and pathology of the legal system regulating economic competition in Iran from a competition law perspective," *Industrial Economics Research Quarterly*, vol. 4, no. 11, pp. 61-76, 2020, doi: [10.30473/indeco.2020.7549](https://doi.org/10.30473/indeco.2020.7549) [in Persian].
- [38] K. Khorramdel, Estavarsangari, K. Alaei, and Zarabi, "Challenges related to regulatory authorities overseeing audio and video production in cyberspace," *Administrative Law Research Quarterly*, vol. 9, no. 30, pp. 31-56, 2022, doi: [10.52547/qjal.9.30.31](https://doi.org/10.52547/qjal.9.30.31) [in Persian].

- [39] Salami, Mazhari, and Mohammadi, "Urban management responsibilities in realizing citizens' environmental rights (with a focus on the resolutions of Tehran City Council)," *Comparative Law Research and Development Quarterly*, vol. 4, no. 11, pp. 84-111, 2021, doi: [10.22034/law.2021.533814.1092](https://doi.org/10.22034/law.2021.533814.1092) [in Persian].
- [40] F. Elashti and J. Javan Jafari Bojnordi, "Violation of the freedom of information flow in situational crime prevention in cyberspace," *Criminal Law Research Quarterly*, vol. 5, no. 18, pp. 69-100, 2017, doi: [10.22054/jclr.2017.7400](https://doi.org/10.22054/jclr.2017.7400) [in Persian].
- [41] N. A. Nemati, Nabiollah, and S. Sadeghi-Neshat, "Civil liability for breaches of data security in cyber threats," *Security and Protective Research*, vol. 23, no. 6, pp. 157-186, 2017 [in Persian].
- [42] Ghanad, Aligholi, and Amireh, "The concept and importance of personal data and privacy protection in cyberspace," *Technology Law*, vol. 1, no. 1, pp. 297-322, 2020, doi: [10.22133/clj.2020.243290.1016](https://doi.org/10.22133/clj.2020.243290.1016) [in Persian].
- [43] W. Kozłowski and K. Suwar, "Smart city: definitions, dimensions, and initiatives," 2021, doi: [10.35808/ersj/2442](https://doi.org/10.35808/ersj/2442).