Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: https://www.science-gate.com/IJAAS.html

Emerging risks in the smart city transition: Evidence from Ho Chi Minh City, Vietnam

Nguyen Quyet*

Institute of International Political Economy, University of Finance – Marketing, Ho Chi Minh City, Vietnam

ARTICLE INFO

Article history:
Received 9 March 2026
Received in revised form
3 September 2026
Accepted 3 October 2026

Keywords:
Smart city
Risk governance
DEMATEL
Urban resilience
Digital transformation

ABSTRACT

The development of smart cities offers significant opportunities to improve public service efficiency and overall quality of life. However, it also creates new risks arising from the interaction of technological, institutional, and environmental factors. This study develops a risk governance framework for the smart city transition of Ho Chi Minh City (HCMC), a rapidly digitalizing metropolis that continues to face structural vulnerabilities, including fragmented governance, uneven digital readiness, and high exposure to flooding, land subsidence, and urban heat. Drawing on ISO-based standards for risk governance and urban performance assessment, the study employs the DEMATEL method to map causal relationships among major risk categories, distinguish between "cause group" and "effect group" risks, and identify key leverage points across the system. The findings indicate that legal and governance risks, together with strategic risks, Internet of Things (IoT)-related risks, and climate-induced cross-infrastructure dependence, act as upstream drivers that increase Artificial Intelligence (AI)-related, blockchain-related, and socioeconomic vulnerabilities, resulting in cascading effects across the urban system. Based on the influence map, the study proposes four priority areas for intervention: (i) strengthening IoT security and device lifecycle governance; (ii) ensuring effective data protection and privacy compliance in AI-enabled systems; (iii) improving interoperability standards and cross-sector coordination; and (iv) integrating climate adaptation considerations into digital infrastructure planning. This framework provides an evidence-based foundation for guiding HCMC towards a sustainable, inclusive, and resilient smart city development pathway in the face of increasing uncertainty.

© 2026 The Authors. Published by IASE. This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

In December 2024, Ho Chi Minh City ran a five-day cybersecurity drill across its municipal departments not as a routine exercise, but as a frank institutional acknowledgement that the city's digital ambitions had outpaced its capacity to govern them. That gap, between what a rapidly digitalizing city deploys and what it can actually manage and protect, sits at the center of the problem this paper investigates. Smart city transitions generate not only new capabilities but a new configuration of risks in which institutional, technological, and socio-ecological dimensions interact in intricate and often unpredictable ways. Governing these risks requires analytical tools capable of mapping causal relationships among risk categories and identifying the leverage points where intervention is most efficient (Bakıcı et al., 2013).

Recent research shows that the risks associated with IoT, AI, and blockchain go beyond technical concerns like cybersecurity, privacy, interoperability, and cost-efficiency. Without effective coordination and standards, these risks can lead to governance and societal vulnerabilities, such as service disruptions, decreased public trust, and increased long-term costs. To shift from reactive to proactive prevention in smart city development, a systematic risk-management architecture that incorporates ISO guidelines and influence mapping methods is necessary (Lee, 2020; Ullah et al., 2021). The DEMATEL method effectively maps and quantifies influence pathways among risks in complex systems. It distinguishes between "cause-group" risks (upstream drivers) and "effect-group" risks (downstream outcomes). The application is

* Corresponding Author.
Email Address: nguyenquyet@ufm.edu.vn
https://doi.org/10.21833/ijaas.2026.09.021
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-8471-4304
2313-626X/© 2026 The Authors. Published by IASE.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0/)

particularly relevant in cities experiencing rapid digital infrastructure expansion, where technological risks (IoT, AI, blockchain) intersect with governance, legal, strategic, and climate-environmental risks. DEMATEL results can help identify high-leverage control points and design coordinated responses to reduce cascading effects across the system (Freire et al., 2023; Freitas et al., 2026; Kalinin et al., 2021).

HCMC presents a particularly salient context for this analysis. As Vietnam's primary economic and technological hub, the city has pursued ambitious digital transformation objectives under the National Smart City Strategy by the Prime Minister of Vietnam in 2018 and the special governance framework introduced by the National Assembly of Vietnam in 2023. Yet the city's smart city transition unfolds against a backdrop of well-documented structural vulnerabilities. On the cybersecurity front, Vietnam recorded 13,900 cyberattacks in 2023, a 9.5% year-on-year increase, with more than 550 government and educational websites reported compromised and injected with unauthorized content. HCMC alone hosts the largest concentration of exposed industrial IoT devices in the country, with 197 internet-detectable Modbus industrial control devices identified in the city, underscoring the immediacy of R1-type risks. On the governance front, HCMC operates across 101 fragmented databases totaling 155 TB that remain poorly interoperable across agencies, a structural condition that Resolution 98 explicitly sought to address but has not yet resolved (vietnamnet.vn). On the climate front, the city currently faces 159 flood-prone locations, 57 of which are classified as severe, and the municipal government has committed over USD 400 million to its first-phase tidal flood control project alone to mitigate worsening flood exposure. These conditions are not hypothetical risk scenarios but active, documented pressures that make HCMC a critical case for smart city risk governance research.

To address this complexity, the present study employs the Decision-Making Trial and Evaluation Laboratory (DEMATEL) method to map causal relationships among key risks associated with HCMC's smart city transition. By distinguishing between cause-driven and effect-driven risk categories, the analysis provides an evidence-based foundation for prioritizing interventions and strengthening urban resilience. Understanding these causal structures is essential not only for risk mitigation but also for guiding strategic alignment, regulatory reforms, and technology deployment as HCMC continues its trajectory toward a smarter and more sustainable urban future.

2. Related literature review

2.1. Definition

A smart city is understood as the coordinated integration of physical, digital, and human systems within the urban environment to deliver sustainable, prosperous, and inclusive outcomes for residents. Operationally, this integration relies on sensor-embedded infrastructure, IoT devices, and ICT platforms that generate and process real-time data across core urban domains: mobility, energy, water, waste, and public safety, enabling city administrators to coordinate services, strengthen resilience, and engage diverse stakeholders. Critically for the present study, contemporary scholarship converges on the view that smartness is not determined by technological sophistication alone but by the quality of the institutional arrangements, governance structures, regulatory frameworks, and cross-sector coordination mechanisms that govern how digital tools are deployed and maintained (Ullah et al., 2021). This institutional dimension directly shapes the risk landscape examined in this paper: weak governance, fragmented strategy, and climate-exposed infrastructure represent upstream vulnerabilities that no volume of technological investment can fully offset.

2.2. Cities' key performance metrics from ISO 37122:2019

The risk identification framework in this study draws on ISO (2019), the international standard for smart city performance metrics, which complements ISO (2018) (city services and quality of life) and ISO (2021) (urban resilience). ISO (2019) provides the conceptual boundary for what constitutes smart city functionality, covering ICT infrastructure, digital governance, IoT deployment, public safety, and environmental monitoring, and thereby anchors the selection of risk categories examined in Section 2.3. Specifically, the standard's emphasis on the interdependence between technological systems and governance performance (ISO, 2019) justifies treating regulatory quality and strategic coherence as upstream risk drivers, consistent with the causal structure uncovered by the DEMATEL analysis in Section 4.

2.3. Risk identification

Technical risks arise from the rollout and day-to-day operation of advanced digital systems, most notably IoT, AI, and blockchain, that form the backbone of smart city functions (Herath and Mittal, 2022). As emphasized by Al Sharif and Pokharel (2022), this class of risk typically manifests as cybersecurity exposures, interoperability frictions among heterogeneous systems, and elevated energy demand, all of which are intensified by the accelerated pace of technological uptake. Empirical work further underscores the urgency of mitigating IoT-specific vulnerabilities, given their capacity to disrupt essential municipal services and erode public trust. In parallel, recent contributions broaden the discussion of AI-related hazards, highlighting privacy infringements and regulatory non-conformance issues that collectively signal the need for stronger governance and oversight mechanisms (Al Sharif and Pokharel, 2022; Kim et al., 2023).

By contrast, non-technical risks originate in governance arrangements, legal frameworks, and organizational practices, all of which critically shape the feasibility and durability of smart city programs. Al Sharif and Pokharel (2022) stressed that governance inefficiencies, stakeholder misalignment, and legal ambiguity can stall or weaken implementation. Converging evidence supports this view, showing that governance-driven risks may amplify socioeconomic inequalities and dampen citizen participation (Kim et al., 2023). From a strategic standpoint, Singh et al. (2020) and Bibri and Krogstie (2017) argued for tighter alignment between ICT trajectories and sustainable urban development objectives to avoid directional drift and policy-technology disconnects.

Accordingly, this study differentiates the risk landscape into two overarching clusters: technical (e.g., IoT, AI, blockchain) and non-technical (socioeconomic, governance, legal, and strategic). This selection reflects the core challenge commonly faced by smart cities; importantly, these risks are mutually interacting rather than isolated. To capture and analyze these interdependencies, the study employs the DEMATEL method, which maps influence pathways among risks and pinpoints those that merit heightened managerial attention and prioritization in risk governance.

We use the following process to identify the risk set for HCMC: (i) a focused literature review to gather important smart city risks, and (ii) classification under a predetermined framework before causal analysis. To extract recurrent risk constructs, such as cybersecurity exposures, data privacy breaches, interoperability deficits, and energy efficiency concerns, as well as organizational and institutional constraints like governance bottlenecks, regulatory ambiguity, resource limitations, and stakeholder misalignment, we first screen peer-reviewed evidence on technology-intensive urban services that are common in HCMC (e.g., IoT-enabled mobility, digital public services, and data platforms). This is similar to the paper's Stage 1 emphasis on synthesizing risks that are frequently reported in the smart city literature as materially affecting public trust and service continuity. Second, to make the HCMC risk portfolio comparable and methodologically consistent with earlier work, we map the extracted risks onto the triad used in the article: technical (IoT, AI, blockchain and their operational vulnerabilities), organizational (capabilities, data governance, financing), and external environmental (public safety, policy and legal settings).

Third, we retain risks that both recur in the literature and plausibly cause cross-domain effects in the local setting because HCMC exhibits dense, interdependent infrastructures (transport, water, wastewater, health, and public safety) that are increasingly digitized. This satisfies the paper's requirement that items represent the main challenges and are appropriate inputs for subsequent DEMATEL analysis of influence pathways. Lastly, the HCMC-specific risk set becomes a traceable, evidence-based input vector for Stage 2 modeling (total influence matrix, thresholds, and cause and effect positioning) by codifying each risk with operational definitions and literature citations. This allows priority setting around high-leverage control points, such as IoT security, AI privacy compliance, and strategic alignment. Based on the identified risk factors, the seven categories are discussed below.

- Associated technical risks using IoT (R1): These are cybersecurity-related risks; as IoT device usage is increasing in services like transportation, energy, healthcare, etc., with the goal of intelligence, the susceptibility to data theft and hacker attacks rises. Smart city (SC) managers ought to think about incorporating IoT risk management into their planning (Ahad et al., 2020; Al Sharif and Pokharel, 2022; Ande et al., 2020; Kim et al., 2023; Lee, 2020).
- Risks associated with artificial intelligence technology (R2): These are privacy and security-related risks. Artificial intelligence-integrated systems that carry out tasks like data analysis in energy, education, healthcare, transportation, security, sustainable environment, and urban area management may give rise to legal problems, necessitating compliance checks with laws protecting fundamental rights, such as when AI systems violate privacy (Radu, 2020; Singh et al., 2020; Ullah et al., 2021).
- Blockchain-related technical risks (R3): The risks of blockchain are linked to the technology involved, including its relationship with security and privacy, low productivity, and efficiency in energy consumption, as well as risks related to the costs of implementing and operating the blockchain. Blockchain is a decentralized peer-to-peer network that records transactions and stores them in a ledger (Chentouf and Bouchkaren, 2023; Ullah et al., 2021).
- Risks to socioeconomic development (R4): These risks are associated with decision-makers' and stakeholders' mindsets. Involvement in multidisciplinary projects is necessary for the creation of SCs, which calls for skilled workers, expensive technology, and the use of technology by professionals, decision-makers, and citizens. Public participation in the proposed social factors is linked to innovations in SCs, and the capacity to propose is impacted by low population engagement. Such innovations thus represent socioeconomic risks (Al Sharif and Pokharel, 2022; Atitallah et al., 2020; Kim et al., 2023).
- Legal risks and governance (R5): These risks are associated with laws, regulations, political and social forces, and policies. Among the factors are concerns about resource management, stakeholder management, monitoring expertise, governance that takes projects into account, and SC approval. Data privacy-related legal concerns, including risks to data protection, are also

emphasized in SC projects (Ahad et al., 2020; Singh et al., 2020).

- Hazards in strategy (R6): These are dangers associated with the relationship between information and communication technologies (ICTs) and sustainable urban development agendas. Investments in ICTs are often wasted due to a lack of strategies that articulate this connection to socioeconomic and environmental issues (Bibri and Krogstie, 2017; Radu, 2020).
- Cross-infrastructure dependence under climate stress (R7): The combined effects of urban flooding, tidal surges, and land subsidence on power supply, telecom connectivity, and drainage can result in failures or deteriorated performance of smart city services, which can cause cascading disruptions of IoT networks, traffic signals, surveillance, data platforms, and control centers. This is especially noticeable in Ho Chi Minh City because of the city's frequent flooding, quick subsidence, delayed flood control projects, and rapidly rising electricity demand (Freitas et al., 2026).

2.4. Control of risks in smart cities

In urban governance and particularly in smart city contexts, risk is understood as the effect of uncertainty on objectives, where such effects may be positive or negative relative to expected scenarios. Consequently, risk management is conceived as a coordinated set of activities to steer and control risk in a systematic, transparent, and verifiable manner (ISO, 2018). A critical premise of the process is to establish scope, context, and criteria before assessment. At this stage, organizations define objectives, timelines, resources, tools, and interdependencies with related activities; they also articulate both external and internal context to clarify constraints, stakeholder expectations, and risk tolerance. The risk criteria component specifies acceptance thresholds, methods for quantifying likelihood and consequence, and comparison rules that support consistent decision-making over time (ISO, 2018).

The risk assessment phase is the core of the framework and comprises three interlinked sub-steps: identification, analysis, and evaluation. Identification develops an evidence-based risk inventory aligned with objectives and context; analysis examines the nature and characteristics of risk frequency, likelihood, consequence magnitude, uncertainty, and interdependencies using qualitative, quantitative, or hybrid techniques, depending on data availability; evaluation then compares analytical results against predefined criteria to prioritize interventions or to recalibrate objectives and resources (ISO, 2018). Following assessment, risk treatment involves selecting strategies (avoid, mitigate, transfer, accept with controls), executing actions, and measuring effectiveness and efficiency for learning and adaptation (ISO, 2018).

Risk management in smart cities (SCs) confronts a landscape that is both dynamic and interdependent, spanning digital technologies, urban infrastructure, and institutional arrangements. On the technical front, a substantial body of research identifies cybersecurity and privacy as critical vulnerabilities as large-scale data ecosystems, IoT networks, and AI systems are deployed across city services; traditional risk assessment methods (scenario, functional, and statistical analysis) often struggle to keep pace with the real-time and rapidly changing characteristics of SC infrastructures (Kalinin et al., 2021). Likewise, operational risks affecting critical technical systems such as urban gas pipeline networks demonstrate that failure probabilities are strongly conditioned by operating parameters and the robustness of safety barriers, underscoring the need for data-driven monitoring models to inform decision-making (Wang et al., 2021).

Beyond technical concerns, SCs are shaped by organizational–institutional risks and external environmental risks. The extended TOE-based framing by Ullah et al. (2021) groups SC risks into three major categories: technological (e.g., IoT, AI, blockchain; information security; system interoperability), organizational (IT capability, digital readiness, data governance, financial resources), and external (public security, intergovernmental governance, regulation, disasters, public health). This typology facilitates the detection of cascade effects: disruptions in digital infrastructure can exacerbate social risks (digital inequality, service discontinuity) and amplify environmental and safety risks (Khan et al., 2022).

Methodologically, recent studies recommend integrating formal risk management standards with multi-criteria decision-making (MCDM) tools to address the complexity and interdependence of SC risks. Among these, DEMATEL is frequently used to model cause–and–effect relationships among risks and to identify “control points” with system-wide influence; it can be combined with AHP, TOPSIS, and PROMETHEE to support ranking and strategy selection (Braga et al., 2021). This approach aligns with the shift toward proactive, evidence-based governance and enables resource prioritization for high-leverage risk nodes such as IoT security, platform data interoperability, and multi-stakeholder coordination (Freire et al., 2023).

In addition, methodological and applied contributions emphasize the need to align legal institutional governance with technological progress to reduce regulatory ambiguity and strengthen accountability in SC implementation (He et al., 2022). From an urban resilience perspective, the combined use of indicator frameworks and influence relationship analysis supports a transition toward adaptive governance, allowing cities to respond to rapid shifts in technology, society, and climate (Seker et al., 2024). Overall, risk management in SCs requires integrated architecture with standardized processes, quantitative measurement, relational

analytics, and institutional coordination to reduce systemic vulnerabilities while maximizing the public value of digital urban transformation.

3. Research methodology

3.1. DEMATEL

A technique known as the "Decision Making Trial and Evaluation Laboratory (DEMATEL)" was created in the early 1970s by Fontela and Gabus (1974). DEMATEL is a kind of structural modeling technique that is used to examine and demonstrate the causal relationship between the parts of a system. The DEMATEL method is used to examine factors affecting a particular system and leverage specialists' knowledge to enhance understanding of the relationships and interdependencies among factors. With the help of impact relation diagrams, the method not only transforms the interdependencies of factors into cause-and-effect relationships but also identifies the essential elements of a system (Bai et al., 2017).

The complex system must first be defined to apply the DEMATEL method, followed by the factors (variables in the DEMATEL method). It is important to identify the factors influencing the system. This is accomplished by using the opinions of experts or by reviewing the literature. To convey the connections and strengths of those connections, a measurement scale should also be created (Shen et al., 2011). For this purpose, a typical scale range is 0 to 4, which stands for “no influence,” “low influence,” “medium influence,” “high influence,” and “very high influence,” respectively. Respondents were asked to assess how each predictor affected the others for every social media addiction predictor. Researchers are advised to undertake a comprehensive sequence of preparatory and analytical procedures to effectively implement the DEMATEL technique (Chang and Chen, 2018).

Step 1: Using the linguistic scale of effect shown in the provided Table 1, the pairwise matrix is built by identifying the drivers and barriers and setting them in the matrix. Based on the expert's evaluation for the criterion, the average score can be determined using Equation 1. The notation of xij indicates the degree to which the respondent believes factor i affects factor j. For i = j, the diagonal elements are set to zero. To incorporate all opinions from H respondents, the average matrix A = [aij] can be constructed as follows:

$$a_{ij} = \frac{1}{H}\sum_{k=1}^{H} x_{ij}^{k} \quad (1)$$

Step 2: Calculate the normalized initial direct-relation matrix. The normalized initial direct-relation matrix D is obtained as $D = S \times A$, where S is the normalization factor defined in Eq. 2:

$$S = \min\left[\frac{1}{\max\limits_{1\le i\le n}\sum_{j=1}^{n} a_{ij}}, \frac{1}{\max\limits_{1\le j\le n}\sum_{i=1}^{n} a_{ij}}\right] \quad (2)$$

Step 3: The equation can be used to obtain the total relation matrix T.

$$T = D\,(I - D)^{-1} \quad (3)$$

where, I is the identity matrix.

Step 4: The sum of the rows and the sum of the columns are done and represented as r and c. Then the equation is used (r + c) and (r-c). Where r and c

$$r = \left[\sum_{j=1}^{n} t_{ij}\right]_{n\times 1} \quad (4)$$

$$c = \left[\sum_{i=1}^{n} t_{ij}\right]_{1\times n} \quad (5)$$

where, t_{ij} denotes the element in row i and column j of the total relation matrix $T = \left[t_{ij}\right]_{n\times n}$.

Step 5: To obtain the digraph, set up a threshold value. A decision maker must establish a threshold value to weed out some undesirable effects since matrix T shows how one element influences another. By doing this, only the impacts that are larger than the threshold value will be selected and displayed in the digraph. The average of the components in matrix T is used in this study to determine the threshold value. By mapping the dataset of (r+c, r-c), the digraph can be obtained. The threshold value α was set at the mean of all elements in the total influence matrix T (α = 0.530), following the convention established in the DEMATEL literature (Braga et al., 2021; Freitas et al., 2026). Only influence pathways whose weight exceeds α are retained in the network diagram, thereby filtering out negligible links and preserving the most consequential causal relationships for interpretation. Two methodological boundaries warrant acknowledgement at this stage. First, the causal structure produced by DEMATEL is not measured independently of the experts who generate it: the total influence matrix is an aggregation of subjective judgements, and its validity is therefore contingent on the quality, diversity, and contextual expertise of the panel. This is a structural feature of all expert-based MCDM methods rather than a failure specific to this application, and it is addressed in the study design through purposive sampling and pre-survey risk validation (Section 3.2); its full implications for result interpretation are discussed in Section 5.3.

Table 1: Scale and ranking system for linguistic terms

No	Linguistic terms	Normal value
1	No influence	0
2	Low influence	1
3	Medium influence	2
4	High influence	3
5	Very high influence	4

3.2. Sample and data collection

Expert selection followed purposive and convenience sampling criteria to maximize contextual relevance for HCMC's smart city governance environment. The panel comprised 10 validated respondents drawn from government agencies, academic institutions, private-sector technology firms, and civil-society organizations,

spanning a range of 7–18 years of professional experience in smart city, ICT, risk governance, and urban-infrastructure domains (see Table 2). This panel size is consistent with established DEMATEL practice: Fontela and Gabus (1974) originally applied DEMATEL with panels of 8–15 specialists; Braga et al. (2021) and Freitas et al. (2026) each employed panels of 8–12 experts in analogous smart city risk studies. Moreover, DEMATEL aggregates individual judgements into a group-level influence matrix, which reduces the sensitivity of results to individual respondent variation. Notwithstanding, we acknowledge that a larger and more diverse panel would strengthen generalizability, and we flag this as a priority for future replication studies (Section 5.3).

Table 2: Profile of expert panel

Expert	Sector	Role	Years of experience	Knowledge domain
E1	Government	Smart city project manager	12	Urban digital governance
E2	Government	IT infrastructure officer	9	IoT deployment & maintenance
E3	Government	Urban planning specialist	15	Land use & climate risk
E4	Academia	Associate professor	18	Smart city risk & governance
E5	Academia	Researcher	7	Cybersecurity & AI ethics
E6	Academia	Lecturer	10	Urban economics
E7	Private	ICT solutions director	14	IoT & blockchain systems
E8	Private	Data security consultant	11	Cybersecurity, data privacy
E9	Private	Environmental infrastructure engineer	8	Climate-resilient infrastructure
E10	NGO	Urban resilience advisor	16	Community governance & risk

Data were collected using a structured DEMATEL questionnaire, in which experts evaluated pairwise influence relationships among the seven risks on a 0-4 scale. Each expert completed a 7×7 direct influence matrix with zero values on the diagonal. Individual matrices were then averaged to construct the initial direct-relation matrix, following standard DEMATEL procedures. A second boundary concerns temporal scope. The data were collected at a single point in time, and the causal structure identified here, therefore, represents a cross-sectional snapshot of expert perceptions rather than a dynamic mapping of how smart city risks evolve. This constraint is consequential: the risk landscape in HCMC is shifting rapidly, shaped by Vietnam's new Personal Data Protection Law (No. 91/2025/QH15, effective January 2026), expanding AIoT deployment, and worsening monsoon exposure, all of which may alter the relative prominence and causal direction of risk factors. Readers should interpret the findings as a high-resolution picture of HCMC's risk governance environment at the time of the study, not as a permanent structural map. The implications for future research design are discussed in Section 5.3.

3.3. Construct validity check

To assess the construct validity of the DEMATEL findings, a post-hoc triangulation procedure was conducted following the approach recommended by Braga et al. (2021) and Freitas et al. (2026). This involved cross-referencing the five highest-weight causal pathways identified in the total influence matrix against independent documentary evidence pertaining to HCMC's smart city governance environment.

The dominant pathway R5 (governance) → R1 (IoT), with a weight of 0.767, highlights the important influence of governance on IoT-related risks. This relationship suggests that weaknesses in regulatory frameworks, inadequate enforcement, and insufficient cybersecurity requirements may increase the vulnerability of connected infrastructure, particularly industrial control systems and government digital services. These findings emphasize the need for stronger governance mechanisms, binding cybersecurity standards, and effective regulatory enforcement to support secure smart city development.

The pathway R7 (climate) → R1 (IoT), weight = 0.543, is corroborated by HCMC's documented flood exposure: with 159 inundation-prone locations and 57 classified as severe (vietnamnet.vn), street-level IoT nodes and data infrastructure in low-lying districts face recurrent physical disruption, a condition confirmed by peer-reviewed urban hydrology research on HCMC.

The prominence of R5 as the highest-prominence factor overall (r+c = 8.032) is further corroborated by legislative acknowledgement: Resolution 98/2023/QH15, which grants HCMC a special governance model precisely because existing institutional arrangements were deemed inadequate for the city's digital transformation scale, constitutes an independent, authoritative confirmation that governance quality is the binding constraint on HCMC's smart city system.

We note that this triangulation procedure does not constitute formal external validation in the experimental sense; rather, it follows the convergent validity logic applied in expert-based MCDM research, wherein consistency between quantitative causal structures and qualitative contextual evidence is treated as evidence of construct validity. Full external validation through longitudinal outcome data remains a direction for future research (see Section 5.3).

4. Results

4.1. Prominence and net effects of factors

The main conclusions from the DEMATEL analysis are divided into two sections in this section. The first section (Section 4.1), which corresponds to the fourth step of the DEMATEL approach, evaluates the overall influence and significance of each factor. In accordance with step 5 of the methodology, the

second section (Section 4.2) investigates the strongest causal relationships between the factors. The essential matrices utilized in steps 1 through 3 are in Table 3, which contains the average direct relation matrix, the normalized direct relation matrix, and the total relation matrix.

The results of DEMATEL, as reported in Table 4 and visualized in Fig. 1, show that the network displays a clear cause-and-effect structure. Four factors, R5 (legal risks and governance), R6 (hazards in strategy), R1 (IoT-related technical risks), and R7 (cross-infrastructure dependence under climate stress) exhibit positive net effects (r-c > 0), thus constituting the cause group. Among them, R5 shows the largest net effect, indicating that regulatory quality and governance are the most decisive upstream drivers of systemic risk. R6 and R1 further act as amplifiers, suggesting that weak strategic alignment and IoT vulnerabilities propagate disturbances across the system. R7 also operates as a causal driver; although its net effect is moderate, its prominence (r+c) is high, reflecting dense interactions with other risks under climate-induced interdependencies. By contrast, R2 (AI-related risks), R3 (blockchain-related risks), and R4 (risks to socioeconomic development) display negative r-c values, placing them in the effect group, i.e., they are predominantly shaped by upstream pressures rather than initiating them. The spatial configuration in Fig. 1 corroborates these patterns, with cause factors located in the positive r-c quadrant and effect factors in the negative region. Policy and managerial interventions should therefore prioritize governance reforms, strategic coherence, IoT security, and the coupling of climate-resilient infrastructure to reduce system-wide risk.

Table 3: DEMATEL matrix

	R1	R2	R3	R4	R5	R6	R7
Average direct relation matrix							
R1	0.000	3.750	2.500	2.667	2.333	2.333	3.500
R2	1.167	0.000	3.083	3.833	2.583	1.833	1.683
R3	2.917	3.417	0.000	2.500	1.833	1.500	2.783
R4	1.667	2.650	2.583	0.000	2.833	2.667	1.937
R5	3.500	3.500	2.750	3.083	0.000	3.583	3.417
R6	3.333	3.533	2.667	2.500	2.917	0.000	2.833
R7	2.883	3.833	2.750	2.250	3.583	2.127	0.000
Normalized direct relation matrix							
	R1	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
R1	0.000	0.180	0.120	0.128	0.112	0.112	0.168
R2	0.056	0.000	0.148	0.184	0.124	0.088	0.081
R3	0.140	0.164	0.000	0.120	0.088	0.072	0.134
R4	0.080	0.127	0.124	0.000	0.136	0.128	0.093
R5	0.168	0.168	0.132	0.148	0.000	0.172	0.164
R6	0.160	0.170	0.128	0.120	0.140	0.000	0.136
R7	0.138	0.184	0.132	0.108	0.172	0.102	0.000
Total relation matrix							
	R1	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
R1	0.409	**0.694**	**0.551**	**0.573**	**0.537**	0.483	**0.573**
R2	0.400	0.452	0.502	**0.544**	0.474	0.404	0.435
R3	0.482	**0.618**	0.392	0.513	0.465	0.405	0.496
R4	0.430	**0.578**	0.493	0.396	0.494	0.445	0.456
R5	**0.618**	**0.767**	**0.626**	**0.657**	0.501	**0.589**	**0.637**
R6	**0.567**	**0.710**	**0.576**	**0.587**	**0.576**	0.400	**0.569**
R7	**0.543**	**0.712**	**0.572**	**0.571**	**0.593**	0.487	0.442

0.530 is the threshold value. Values higher than this cutoff are shown in bold

Table 4: Prominence and net effects of factors

Factors	r	c	r+c	r-c	Effect
R_1: Associated technical risks using IoT	3.820	3.448	7.268	0.373	Cause
R_2: Risks associated with artificial intelligence technology	3.211	4.531	7.742	-1.320	Effect
R_3: Blockchain-related technical risks	3.371	3.712	7.083	-0.341	Effect
R_4: Risks to socioeconomic development	3.292	3.842	7.134	-0.550	Effect
R_5: Legal risks and governance	4.393	3.639	8.032	0.754	Cause
R_6: Hazards in strategy	3.984	3.212	7.196	0.772	Cause
R_7: Under climate stress, cross-infrastructure dependence	3.919	3.607	7.526	0.311	Cause

4.2. Causal relationships between the risk criteria

The relationship map presented in Fig. 2 illustrates the directional influence structure among the seven factors after applying the threshold of 0.530. The network clearly shows that R5, R6, R1, and R7, marked as cause factors, occupy central and initiating positions within the system. Among them, R5 (legal risks and governance) emerges as a dominant hub, exerting influence on almost all other nodes through multiple outgoing links, reflecting its foundational role in shaping technology-related and climate-induced risks. The strong pathway from R5 to R1 (weight = 0.767) indicates that governance weaknesses can directly intensify IoT-related vulnerabilities. Meanwhile, R6 (hazards in strategy) forms another influential driver, distributing effects across both technological and environmental domains.

Conversely, R2, R3, and R4 are positioned as effect factors, receiving more influence than they transmit. The prominent connection between R1 and R2 highlights the susceptibility of AI-related risks to upstream technical weaknesses. R4, associated with socioeconomic development, is also heavily affected by governance and strategy-related pressures, confirming its downstream position. The placement of R7 (cross-infrastructure dependence under climate stress) in the cause group shows that

climate-induced interdependencies propagate broadly through the system, reinforcing vulnerabilities in both technological and socioeconomic spheres. Overall, the map reveals a tightly interconnected network in which governance quality, strategic robustness, and climate-resilient infrastructure form the primary leverage points for risk mitigation.

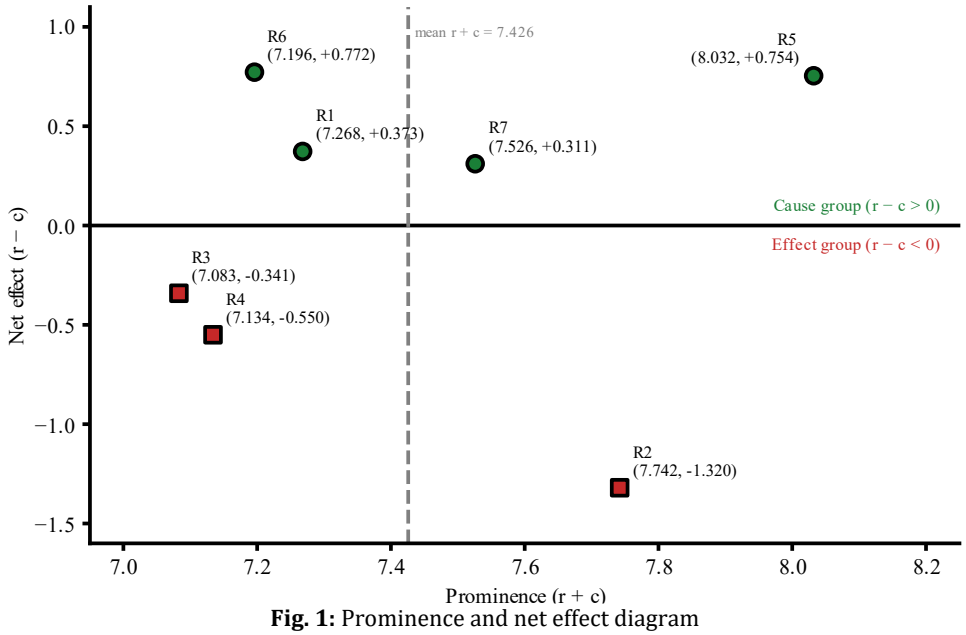


Fig. 1: Prominence and net effect diagram

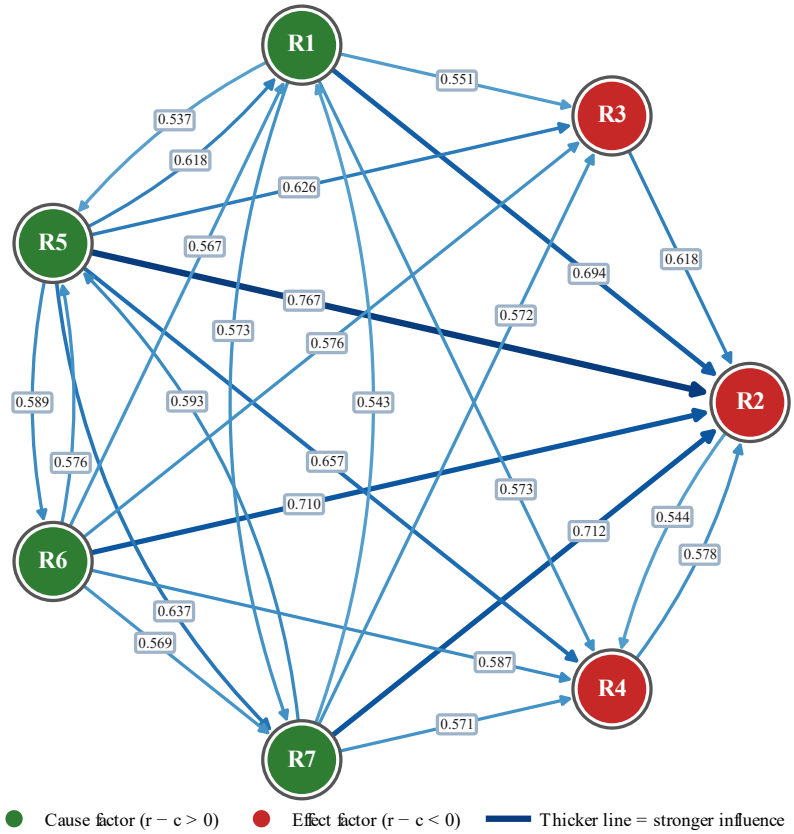


Fig. 2: Relationship map (threshold α = 0.530)

To assess the robustness of the network structure to the choice of threshold, a sensitivity analysis was conducted across four alternative values. The results are summarized in Table 5. Critically, the cause-group classification, the core analytical output of DEMATEL, is entirely determined by the sign of the net-effect index (r − c), which is derived directly from the total influence matrix T and is independent of the threshold parameter. Consequently, the four cause-group factors (R5, R6, R1, R7) and the three effect-group factors (R2, R3, R4) remain invariant across all tested thresholds. What varies is the number of influence pathways displayed in the network diagram: from 27 active links at α = 0.500 to 9 links at α = 0.600. Across all scenarios, the five highest-

weight pathways R5→R2 (0.767), R7→R2 (0.712), R6→R2 (0.710), R1→R2 (0.694), and R5→R4 (0.657) remain present without exception, confirming the structural primacy of governance and climate risks as upstream drivers of AI-related and socioeconomic vulnerabilities.

The threshold of α = 0.530 (mean of T) is therefore retained in the main analysis as it provides the most balanced representation of significant influence pathways, and the substantive conclusions of this study are robust to alternative threshold specifications.

Table 5: Threshold sensitivity of DEMATEL causal relationships

Threshold α	Active links	Cause group	Effect group	Top link preserved
0.500	27/42	R1, R5, R6, R7	R2, R3, R4	R5→R2 (0.767)
0.530 (baseline)	25/42	R1, R5, R6, R7	R2, R3, R4	R5→R2 (0.767)
0.550	22/42	R1, R5, R6, R7	R2, R3, R4	R5→R2 (0.767)
0.580	12/42	R1, R5, R6, R7	R2, R3, R4	R5→R2 (0.767)
0.600	9/42	R1, R5, R6, R7	R2, R3, R4	R5→R2 (0.767)

Cause-effect classification is determined by r-c values and is threshold invariant

5. Discussion and managerial implications

5.1. Discussion

The most striking result is the one that should, perhaps, be least surprising. Governance quality R5, legal risks, and governance is not merely a cause factor; it is the dominant upstream driver in the entire influence network, carrying the highest net-effect index (r−c = +0.755) and exerting the strongest single pathway in the system: R5→R1 at weight 0.767. Put plainly, weak regulatory frameworks do not just create legal risk in isolation; they actively manufacture IoT vulnerability, amplify AI privacy exposure, and propagate those weaknesses outward through every domain the city is trying to digitize. This is not a finding about technology. It is a finding about sequencing: HCMC has been building smart infrastructure faster than it has been building the governance capacity to govern it. Strategic misalignment (R6) tells a related but distinct story. With the second-highest net-effect index (r−c = +0.772) and strong outgoing links to both AI risks (0.710) and blockchain risks (0.576), R6 captures what happens when digital investments proceed without a coherent cross-sectoral framework. The 101 databases and 155 TB of city data that currently cannot talk to each other are the visible consequence of exactly this dynamic: each department built its own system, each system made local sense, and the aggregate result is a city that generates enormous amounts of data and can act on very little of it (vietnamnet.vn). AI systems trained on siloed inputs produce unreliable outputs; blockchain platforms that cannot interoperate with adjacent systems deliver no cross-domain value. The strategic hazard is not a future scenario; it is already the operating condition.

The placement of R7 climate-induced cross-infrastructure dependence in the cause group warrants scrutiny rather than simple acceptance. Its net-effect index is positive but modest (r−c = +0.312), yet its prominence score is high (r+c = 7.526), indicating dense interactions with every other risk category. One interpretation is straightforward: when 57 flood locations can knock IoT nodes offline for 18–72 hours, climate stress genuinely propagates risk across the digital system. A more cautious interpretation is also worth considering: the expert panel was drawn primarily from governance and ICT backgrounds and may have been better positioned to assess institutional risks than climate and digital interdependencies. We cannot fully disentangle these two explanations with the current data. What we can say is that R7's causal position is consistent with documented physical evidence and that treating it as an effect factor would be the more dangerous error.

The effect group R2 (AI), R3 (blockchain), and R4 (socioeconomic) is where most smart city risk discourse focuses its attention and, paradoxically, where DEMATEL suggests intervention is least efficient. These three factors receive more influence than they transmit. Addressing them directly, without first reducing upstream governance and strategic failures, is analogous to repeatedly draining a tank while the inlet valve remains open. R2, in particular, with incoming links from all four cause factors and the largest negative net-effect index (r−c = −1.320), is the clearest illustration: AI risk in HCMC is not primarily an AI problem. It is a governance problem wearing an AI face.

5.2. Managerial implications

The DEMATEL causal structure points to four concrete areas of intervention specific to HCMC's institutional and physical context.

IoT Device Lifecycle Governance: The strongest causal pathway in the model, governance quality driving IoT risk, has a direct local referent: HCMC's Urban Traffic Management and Operations Centre (UTMOC), operated by the Department of Transport since 2019, integrates approximately 1,000 surveillance cameras and over 200 AI-enabled signal controllers, yet OPSWAT's 2024 internet-wide scan identified 197 internet-detectable Modbus industrial control devices in the city (opswat.com). The Department of Transport, in coordination with the HCMC Digital Transformation Centre (DTC), should mandate NIST SP 800-213 compliance for all UTMOC-connected devices from Q3 2026 onward, enforce 90-day firmware update cycles, and commission annual third-party penetration testing through the Ministry of Information and Communications' certified vendor list. AI Privacy Compliance: AI-related risk (R2) is the effect factor receiving the two highest-weight incoming links in

the network (from R5 at 0.767 and R6 at 0.710), confirming that technical AI-safety measures cannot substitute for upstream governance action. HCMC's facial recognition cameras and Digital Citizen application now fall under Vietnam's Personal Data Protection Law (No. 91/2025/QH15, effective 1 January 2026). The HCMC People's Committee should require all city AI deployments to appoint a Data Protection Officer by Q1 2026 and complete an initial Data Protection Impact Assessment by Q2 2026, with biannual updates thereafter. All AI vendor contracts should include a data minimization clause and an automatic deletion protocol upon contract expiry.

Interoperability and Strategic Alignment: R6 carries the highest net-effect index among cause factors (r−c = +0.772) and distributes influence across both technological and socioeconomic domains. HCMC currently operates 101 fragmented databases totaling 155 TB, a condition the city's own Digital Transformation Centre describes as data territorialization. The Department of Information and Communications should mandate the FIWARE NGSI-LD open-API standard in all new smart city platform procurements from Q3 2026, establish a cross-departmental Data Governance Committee meeting quarterly, and set a target of connecting at least 30 of the 101 databases to a unified city data layer by the end of 2027.

Climate-Resilient Infrastructure: HCMC's 159 flood-prone locations, 57 classified as severe, directly threaten street-level IoT nodes and data relay stations in low-lying districts. The Department of Construction should enforce a minimum installation elevation of +0.5 m above the 1-in-10-year flood level for all new ground-level IoT nodes in severe inundation zones from 2026. The DTC should negotiate a Service-Level Agreement with EVN Southern Power Corporation, guaranteeing power restoration to critical digital nodes within 4 hours of an extreme weather event. An annual Digital Infrastructure Flood-Risk Audit, completed by 31 March each year before the monsoon season, should map all city IoT assets against the Smart Urban Operations Centre's updated inundation forecast layer. Collectively, these recommendations operationalize the DEMATEL output as a governance agenda: upstream interventions targeting R5 and R6 simultaneously reduce downstream risks to AI, blockchain, and socioeconomic development, while the climate-resilience measures harden digital infrastructure against a causal driver the city cannot eliminate but can systematically manage.

5.3. Limitations and future research directions

First, reliance on expert judgment: The expert panel comprised 10 respondents, which, while consistent with established DEMATEL norms, limits the statistical diversity of perspectives. Future studies should recruit larger panels (n≥20) encompassing a broader cross-section of district-level officials, GovTech startups, and resident-community representatives to capture heterogeneous risk perceptions across HCMC's administrative structure.

Second, sectoral and spatial scope: The analysis focuses on Ho Chi Minh City and several critical infrastructure subsystems (e.g., energy, data, mobility, and digital public services). Cities with different scales, governance arrangements, degrees of digitalization, or industrial ecosystems may display distinct risk pathways. Comparative designs across cities/regions and across functional domains (digital health, digital education, digital welfare) would help reveal domain-specific drivers and constraints, enabling more context-sensitive implementation strategies.

Third, a cross-sectional design amid rapid change: As flagged in Section 3.2, the findings represent a snapshot rather than a trajectory. The risk landscape is shifting: Vietnam's Personal Data Protection Law (No. 91/2025/QH15, effective January 2026) alters the regulatory context for R2; advancing AIoT and 5G deployments are expanding the attack surface of R1; and worsening monsoon seasons are intensifying R7. Future work should integrate DEMATEL with system dynamics or Bayesian network approaches to model how causal structures evolve under technological and climatic shocks, rather than capturing them at a single moment. Fourth, limited coverage of firm-level capabilities: The study prioritizes systemic and external conditions (institutions, infrastructure interdependencies, technological lock-ins) and does not probe deeply into the internal capacities of implementing entities (IT maturity, data governance, digital skills, information security culture, interoperability readiness). Subsequent studies could combine organization-level surveys, operational audits, readiness, maturity assessments, and granular cost decomposition (capex, opex, compliance, interoperability) to pinpoint micro-level bottlenecks and actionable levers.

Fifth, under-specified macro external shocks: Macroeconomic volatility, large-scale cybersecurity risks, cross-border data policy shifts, and supply chain disruptions for digital equipment may reconfigure the risk structure and alter intervention priorities. Future research should embed exogenous variables (e.g., climate indices, cyber risk indicators, business cycle metrics) and employ stress testing and Monte Carlo simulation to quantify uncertainty bounds and sensitivity of outcomes.

Taken together, these limitations outline a forward agenda that is multi-actor, multi-city, and multi-temporal, combining causal mapping with dynamic simulation and capability analysis to enhance the robustness and policy relevance of evidence for Ho Chi Minh City's smart city transition and for comparable urban contexts.

6. Conclusion

This study applied the DEMATEL method to map the causal structure of seven interrelated risks

confronting Ho Chi Minh City's smart city transition, distinguishing upstream "cause" factors from downstream "effect" factors and thereby identifying where governance intervention yields the greatest system-wide leverage. The results show that legal risks and governance (R5) and strategic misalignment (R6), together with IoT-related risk (R1) and climate-induced cross-infrastructure dependence (R7), function as the principal drivers of the network, while AI-related risk (R2), blockchain-related risk (R3), and socioeconomic risk (R4) are predominantly effect factors that absorb, rather than generate, systemic risk.

This finding reframes the conventional focus of smart city risk discourse, which concentrates heavily on technology-specific threats, by showing that durable risk mitigation in HCMC depends first on strengthening governance quality and strategic coordination. Building on this evidence, the study proposes four priority interventions, IoT device lifecycle governance, AI privacy compliance, interoperability and strategic alignment, and climate-resilient infrastructure that operationalize the DEMATEL findings into an actionable governance agenda.

Beyond its empirical contribution to HCMC, the study offers a replicable risk governance framework that other rapidly digitalizing, climate-exposed cities in the Global South can adapt to their own institutional contexts. Future research extending this cross-sectional analysis with longitudinal and multi-city data, as outlined in Section 5.3, would further strengthen the generalizability and policy relevance of these findings.

List of abbreviations

AHP	Analytic hierarchy process
AI	Artificial intelligence
AIoT	Artificial intelligence of things
API	Application programming interface
capex	Capital expenditure
DEMATEL	Decision-making trial and evaluation laboratory
DTC	Digital Transformation Centre
EVN	Vietnam Electricity
FIWARE	Open-source platform for smart solutions
HCMC	Ho Chi Minh City
ICT	Information and communication technology
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information technology
NGSI-LD	Next generation service interfaces for linked data
NIST	National Institute of Standards and Technology
NGO	Non-governmental organization
opex	Operational expenditure
OPSWAT	Cybersecurity technology company
PROMETHEE	Preference ranking organization method for enrichment evaluation
SC	Smart city
TOE	Technology–organization–environment
TOPSIS	Technique for order of preference by similarity to ideal solution
UTMOC	Urban Traffic Management and Operations Centre

Acknowledgment

This research was funded by the University of Finance - Marketing (UFM), Ho Chi Minh City, Vietnam.

Compliance with ethical standards

Ethical considerations

All participating experts were informed in advance of the study's purpose, procedures, and use of data, and provided informed consent before completing the DEMATEL questionnaire. Participation was entirely voluntary; experts could withdraw at any time without consequence, and all individual responses were anonymized and aggregated before analysis; no personally identifiable information is reported in this manuscript.

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Ahad MA, Paiva S, Tripathi G, and Feroz N (2020). Enabling technologies and sustainable smart cities. Sustainable Cities and Society, 61: 102301. https://doi.org/10.1016/j.scs.2020.102301

Al Sharif R and Pokharel S (2022). Smart city dimensions and associated risks: Review of literature. Sustainable Cities and Society, 77: 103542. https://doi.org/10.1016/j.scs.2021.103542

Ande R, Adebisi B, Hammoudeh M, and Saleem J (2020). Internet of Things: Evolution and technologies from a security perspective. Sustainable Cities and Society, 54: 101728. https://doi.org/10.1016/j.scs.2019.101728

Atitallah SB, Driss M, Boulila W, and Ghézala HB (2020). Leveraging deep learning and IoT big data analytics to support the smart cities development: Review and future directions. Computer Science Review, 38: 100303. https://doi.org/10.1016/j.cosrev.2020.100303

Bai C, Sarkis J, and Dou Y (2017). Constructing a process model for low-carbon supply chain cooperation practices based on the DEMATEL and the NK model. Supply Chain Management: An International Journal, 22(3): 237-257. https://doi.org/10.1108/SCM-09-2015-0361

Bakıcı T, Almirall E, and Wareham J (2013). A smart city initiative: The case of Barcelona. Journal of the Knowledge Economy, 4: 135-148. https://doi.org/10.1007/s13132-012-0084-9

Bibri SE and Krogstie J (2017). Smart sustainable cities of the future: An extensive interdisciplinary literature review. Sustainable Cities and Society, 31: 183-212. https://doi.org/10.1016/j.scs.2017.02.016 **PMCid:PMC7177348**

Braga IF, Ferreira FA, Ferreira JJ, Correia RJ, Pereira LF, and Falcão PF (2021). A DEMATEL analysis of smart city determinants.

Technology in Society, 66: 101687. https://doi.org/10.1016/j.techsoc.2021.101687

Chang CC and Chen PY (2018). Analysis of critical factors for social games based on extended technology acceptance model: A DEMATEL approach. Behaviour & Information Technology, 37(8): 774-785. https://doi.org/10.1080/0144929X.2018.1480654

Chentouf FZ and Bouchkaren S (2023). Security and privacy in smart city: A secure e-voting system based on blockchain. International Journal of Electrical and Computer Engineering, 13(2): 1848-1857. https://doi.org/10.11591/ijece.v13i2.pp1848-1857

Fontela E and Gabus A (1974). DEMATEL: Progress achieved. Futures, 6(4): 361-363. https://doi.org/10.1016/0016-3287(74)90086-X

Freire CA, Ferreira FA, Carayannis EG, and Ferreira JJ (2023). Artificial intelligence and smart cities: A DEMATEL approach to adaptation challenges and initiatives. IEEE Transactions on Engineering Management, 70(5): 1881-1899. https://doi.org/10.1109/TEM.2021.3098665

Freitas AC, Oliveira CRSD, Gomes PFDO, Chiroli DMDG, Gerônimo BM, Zola FC, and Aragão FV (2026). Risk management in smart cities: Influence analysis using DEMATEL. Environmental Hazards, 25(3): 247-273. https://doi.org/10.1080/17477891.2025.2467637

He W, Li W, and Deng P (2022). Legal governance in the smart cities of China: Functions, problems, and solutions. Sustainability, 14(15): 9738. https://doi.org/10.3390/su14159738

Herath HMKKMB and Mittal M (2022). Adoption of artificial intelligence in smart cities: A comprehensive review. International Journal of Information Management Data Insights, 2(1): 100076. https://doi.org/10.1016/j.jjimei.2022.100076

ISO (2018). BS ISO 37120:2018: Sustainable cities and communities. Indicators for city services and quality of life. International Organization for Standardization. Geneva, Switzerland.

ISO (2019). BS ISO 37122:2019: Sustainable cities and communities. Indicators for smart cities. International Organization for Standardization. Geneva, Switzerland.

ISO (2021). ISO 37123:2021 Sustainable cities and communities-Indicators for smart cities. International Organization for Standardization. Geneva, Switzerland.

Kalinin M, Krundyshev V, and Zegzhda P (2021). Cybersecurity risk assessment in smart city infrastructures. Machines, 9(4): 78. https://doi.org/10.3390/machines9040078

Khan MA, Siddiqui MS, Rahmani MKI, and Husain S (2022). Investigation of big data analytics for sustainable smart city development: An emerging country. IEEE Access, 10: 16028-16036. https://doi.org/10.1109/ACCESS.2021.3115987

Kim K, Alshenaifi IM, Ramachandran S, Kim J, Zia T, and Almorjan A (2023). Cybersecurity and cyber forensics for smart cities: A comprehensive literature review and survey. Sensors, 23(7): 3681. https://doi.org/10.3390/s23073681 **PMid:37050740 PMCid:PMC10099346**

Lee I (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. Future Internet, 12(9): 157. https://doi.org/10.3390/fi12090157

Radu LD (2020). Disruptive technologies in smart cities: A survey on current trends and challenges. Smart Cities, 3(3): 1022-1038. https://doi.org/10.3390/smartcities3030051

Seker S, Aydin N, and Tuzkaya UR (2024). What is needed to design sustainable and resilient cities: Neutrosophic fuzzy based DEMATEL for designing cities. International Journal of Disaster Risk Reduction, 108: 104569. https://doi.org/10.1016/j.ijdrr.2024.104569

Shen YC, Lin GT, and Tzeng GH (2011). Combined DEMATEL techniques with novel MCDM for the organic light emitting diode technology selection. Expert Systems with Applications, 38(3): 1468-1481. https://doi.org/10.1016/j.eswa.2010.07.056

Singh S, Sharma PK, Yoon B, Shojafar M, Cho GH, and Ra IH (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. Sustainable Cities and Society, 63: 102364. https://doi.org/10.1016/j.scs.2020.102364

Ullah F, Qayyum S, Thaheem MJ, Al-Turjman F, and Sepasgozar SM (2021). Risk management in sustainable smart cities governance: A TOE framework. Technological Forecasting and Social Change, 167: 120743. https://doi.org/10.1016/j.techfore.2021.120743

Wang W, Mou D, Li F, Dong C, and Khan F (2021). Dynamic failure probability analysis of urban gas pipeline network. Journal of Loss Prevention in the Process Industries, 72: 104552. https://doi.org/10.1016/j.jlp.2021.104552