Abar, M. (2025). AI-Driven IoT Scenario Building and Policy Analysis: A Comparative Societal Impact Study in New York, Berlin, Tehran, and Zurich. *Social informatics journal, Vol. 4, No. 2*, 11_44

UDC: 004.78:004.8

https://doi.org/10.58898/sij.v4i2.11-44

AI-Driven IoT Scenario Building and Policy Analysis: A Comparative Societal Impact Study in New York, Berlin, Tehran, and Zurich

Mehdi Abar[1*]

[1] Allameh Tabataba'i University, Iran, abar.edu.science@gmail.com

Abstract: The rapid expansion of the Internet of Things (IoT) and its integration with Artificial Intelligence (AI) are transforming urban and rural landscapes, creating both opportunities and governance challenges. This study applies AI-driven foresight methodologies to analyze the societal impact of IoT through a structured five-phase framework: technology description, forecasting, foresight, impact assessment, and policy analysis. The STEEP framework (Social, Technological, Economic, Environmental, and Political) is used to identify key drivers, evaluate their uncertainty and impact, and develop scenario-based policy recommendations. To forecast IoT development, this research references the Gartner IoT Hype Cycle (2020) and integrates insights from more recent reports, such as the Emerging Technologies Hype Cycle 2024, AI Hype Cycle 2024, and Smart City Hype Cycle 2022. Findings highlight the need for adaptive governance strategies to address cybersecurity risks, interoperability challenges, and digital divides. Policy options were identified using classical Technology Assessment (TA) approaches and can be further explored through Participatory TA and Constructive TA to enhance stakeholder engagement. Future research should focus on quantifying societal impacts using methods such as Scanning and Tracking Analysis and expanding discussions on policy frameworks beyond Parliamentary TA. This study contributes to the field of Technology Assessment (TA) by combining quantitative forecasting and qualitative scenario-building, offering a structured approach for IoT governance and policy development.

Keywords: IoT, Internet of Things, AI, Technology Assessment, Foresight, Digital Transformation.

[*]Corresponding author: Mehdi Abar, abar.edu.science@gmail.com

1. Introduction, Problem Statement, Logic, Implication, Methodology

1.1 Introduction

1.1.1 Context & Importance

The fusion of Artificial Intelligence (AI) and the Internet of Things (IoT) is transforming urban and rural landscapes, driving advancements in smart infrastructure, public services, and security. AI enhances IoT applications ranging from smart grids and intelligent traffic systems to healthcare monitoring and environmental sensing (Kitchin, 2020). However, the governance and deployment of AI-driven IoT solutions vary significantly across cities, shaped by local policies, economic structures, and regulatory landscapes (Weber, 2019).

This study compares the societal impact of AI-IoT integration across cities by employing scenario-building techniques and policy analysis to evaluate cybersecurity risks, digital divides, and interoperability challenges (Brous, Janssen, & Herder, 2020). By examining these intersections between IoT, AI, and governance, the research identifies both opportunities and risks associated with these technologies.

Furthermore, understanding the socio-technical implications of IoT is critical for policymakers, technology developers, and urban planners (Castells, 1996). This study contributes to discussions on responsible and equitable IoT deployment, ensuring that digital transformation benefits reach all layers of society.

Research Objective

This research, based on Technology Assessment (TA) principles, aims to support the sustainable and responsible development of IoT technologies. It evaluates societal impacts and governance policies in urban and rural contexts. By applying TA methodologies, the study ensures IoT deployment aligns with ethical, economic, and social sustainability.

Problem Statement

The rapid development of the Internet of Things (IoT) and its integration with Artificial Intelligence (AI) are transforming urban and rural environments. However, these Technological Developments (TD) introduce challenges related to cybersecurity threats, digital divides, and interoperability issues. The governance of IoT technologies varies across regions, leading to societal fragmentation and policy discrepancies.

The uneven adoption of IoT across different governance systems can exacerbate societal inequalities, leading to Cultural Lag, a concept introduced by Ogburn (1922), which suggests that when technological advancements outpace social adaptation, a misalignment occurs, causing societal disruptions (Ogburn, 1922). Similarly, Beck's (1992) Risk Society theory argues that technological progress intensifies human-made risks, shifting threats from natural disasters to cyber vulnerabilities (Beck, 1992). In the IoT era, risks such as data breaches, surveillance concerns, and AI-driven biases exemplify this shift.

Furthermore, Giddens' (1994) Reflexive Modernization theory emphasizes that, unlike traditional risks, modern technology-driven threats are unpredictable, necessitating scenario-building methodologies to manage uncertainties (Giddens, 1994). Additionally, Castells (1996) highlights how digital transfor-

mation polarizes societies, exacerbating technological divides (Castells, 1996). Heidegger (2005) differentiates between older, nature-preserving technologies and modern, irreversible technological interventions, emphasizing the long-term societal consequences of uncontrolled technological expansion (Heidegger, 2005).

By integrating these theoretical perspectives, this study adopts a Technology Assessment (TA) framework to analyze IoT's societal impacts and propose equitable policy solutions to mitigate these challenges.

1.2.1 Existing Gap

Despite advancements in IoT scenario modeling and policy evaluation, key gaps persist:

a) Societal Fragmentation – Research focuses on technology and economics but often neglects digital divides and sociopolitical barriers in urban-rural IoT adoption (James, 2022).

b) Comparative Urban Analysis – Most IoT policy studies lack city-specific insights. The diverse governance models of New York, Tokyo, Tehran, and Zurich require tailored policies (Raj & Sundararajan, 2020; Wenge et al., 2021).

c) AI-Driven Policymaking – Traditional policies rely on historical data, overlooking AI-enhanced foresight. Integrating Hype Cycle Analysis and Scenario Storytelling enables future-oriented policy strategies (Huang & Zhang, 2021).

1.2.3 Research questions

1. What are the key directions of IoT development in societal technology, and how do they shape urban and rural dynamics?
2. How can these technological directions be described through scenario analysis, and what policy options can be prescribed to address their societal impacts?

1.3 Logic and Rationale of the Research

This research is based on Technology Assessment (TA), a framework for evaluating the societal, economic, and political impacts of emerging technologies. Key assumptions include:

a) IoT adoption is a societal transformation, not just a technological shift (Feenberg, 1999).

b) Existing policies are reactive, lacking future-oriented strategies (Bijker et al., 2012).

c) AI-driven scenario analysis improves IoT governance and policy adaptation (Grunwald, 2018).

To establish a historical and theoretical foundation for Technology Assessment (TA), we considered the four phases of TA evolution (Grunwald, 2009):

1) Philosophy of Technology
2) Sociology of Technology
3) Technology Policy (TP)
4) Technology Assessment (TA)

1.3.1 Philosophy of Technology

The Philosophy of Technology examines AI-IoT development through five principles:

i. Technology is value-laden, reflecting cultural, political, and economic forces (Feenberg, 1999).
ii. Technology has agency, shaping human behavior and institutions (Winner, 1980).
iii. Technology is systemic, embedded within complex socio-technical networks (Vermaas et al., 2011).
iv. Technology evolves through social struggles, not linear progress (Bijker et al., 2012).
v. Technology is dynamic, continuously reshaping society (Grunwald, 2018).

1.3.2 Sociology of Technology

Three key perspectives explain technology-society interactions:

i. Social Construction of Technology (SCOT) – Innovation is shaped by social, political, and economic contexts (Bijker & Pinch, 1987).
ii. Technological Determinism – Technology autonomously drives societal change (Smith & Marx, 1994)
iii. Co-Evolution (Soft Determinism) – Technology and society mutually influence each other (Rip & Kemp, 1998).

By integrating these perspectives, this research highlights how AI-driven IoT adoption in different cities is neither purely determined by technology nor entirely shaped by social forces, but rather co-evolves with economic, political, and cultural factors.

1.3.3 Technology Policy (TP)

Technology policy has evolved through three generations:

i. Growth-Oriented Innovation (1950s-1970s) – R&D investments for economic growth (Schumpeter, 1942).
ii. National Innovation Systems (1980s-1990s) – Collaboration between firms, universities, and governments (Freeman, 1987; Lundvall, 1992).
iii. Socio-Technical Systems (2000s-present) – Emphasizing sustainability and policy integration (Geels, 2004).

This study applies the third-generation approach, integrating AI-driven foresight and scenario analysis for IoT governance.

1.3.4 Technology Assessment (TA)

TA has evolved into two models:

i. First-Generation TA ("Speaking Truth to Power") – Expert-driven analysis guiding policymakers (Collingridge, 1980).
ii. Second-Generation TA ("Dialoguing with Society") – Participatory assessment involving stakeholders (Grunwald, 2019).

This research aligns with the second-generation TA, incorporating AI-driven foresight and scenario-building to develop inclusive IoT policies. But of course, this research methodology foundation is *Classic TA*.

1.4 General Framework of the Research (Methodology)

1.4.1 Theoretical and Conceptual Foundations

- Research Perspective: Prospective, using scenario-building to anticipate future IoT developments.
- Study Timeframe: Trend analysis, mapping AI-IoT adoption patterns over time.
- Research Type: Descriptive and prescriptive, analysing trends while recommending policy strategies.

1.4.2 Sources and Types of Data

- Primary data – Expert interviews, stakeholder workshops, scenario-building.
- Secondary data – Policy documents, academic literature, industry reports, smart city initiatives.

1.4.3 Data Collection Methods

- Qualitative: Policy Analysis – Review of regulatory frameworks and AI-IoT governance models. Scenario Development – Using the STEEP framework for foresight-driven IoT projections. Comparative Policy Evaluation – Assessing policies based on effectiveness, efficiency, implement feasibility, and adoption.
- Quantitative: Trend Analysis – Measuring IoT adoption via investment, market penetration, and regulations. Technology Maturity Assessment – Applying Hype Cycle & Time-to-Plateau indicators to track IoT evolution

1.5 Structure of the Study

1.5.1 Level of Analysis

The research will be conducted at multiple levels, including city governance structures, national regulatory frameworks, and international IoT development trends.

1.5.2 Unit of Analysis

The primary unit of analysis is the city-level implementation of AI-driven IoT policies. Comparative case studies of New York, Berlin, Tehran, and Zurich will be used to assess the societal impact of different governance models.

1.5.3 Data Analysis Techniques and Methods

The study employs:

- PESTEL analysis for evaluating external environmental impacts on IoT policies.
- Scenario-based analysis to explore potential future outcomes.
- Multi-criteria decision analysis (MCDA) to assess policy effectiveness, efficiency, implement feasibility, and adoption.
- Comparative analysis of the selected cities to identify best practices and policy gaps

1.5.4 Workflow and Organizational Setup

Table 1. Workflow and Organizational Setup

	Phase 1	**Phase 2**	**Phase 3**	**Phase 4**	**Phase 5**
Stage	Description of Tech	Forecasting Tech	Foresight Societal Tech	Impacts Analysis	Policies Analysis
Data		Quan	Qual	Quan-Qual	Quan-Qual
Identification		Hype Cycle (Vars-Times)	Scenario Building (TDS-STEEP)	Matrix of Scenarios-(Vars-Times) Combination of Phase 2&3 Matrix of Phase 4-PESTEL	Matrix of Phase 4-Policy Options
Analysis (Case Studies)					1. Effectiveness 2. Efficiency 3. Implement Feasibility 4. Adoption
Evaluation (Case Studies)					Means of 4 Criteria

This study applies a *Technology Assessment (TA) framework* incorporating scenario construction, forecasting, impact analysis, and policy evaluation (Grunwald, 2018; Bijker et al., 2012; Godet, 2006).

- Phase 1: Description of Technology – Defines IoT and its complementary technologies, explaining their functions and interactions.
- Phase 2: Forecasting Technology – Uses Hype Cycle Analysis to predict IoT evolution, assessing technological maturity and adoption trends (Gartner, 2020; Wu et al., 2022).
- Phase 3: Foresight Technology – Applies STEEP analysis to explore external social, economic, environmental, and political influences on IoT (Godet, 2006; Ralston, 2011).
- Phase 4: Impact Analysis – Uses PESTEL to evaluate societal, technological, and legal consequences of AI-IoT adoption (Grunwald, 2018; Wenge et al., 2021).

- Phase 5: Policy Analysis – Assesses IoT governance models based on effectiveness, efficiency, implement feasibility, and adoption, guiding urban-rural policy decisions (Huang & Zhang, 2021; Wenge et al., 2021)

2. Results

2.1 phase 1. Description of IoT

2.1.1 Definition

The Internet of Things (IoT) refers to a network of interconnected devices that collect, transmit, and process data without human intervention. These devices, embedded with sensors, software, and connectivity, enable real-time monitoring, automation, and decision-making across various sectors (Atzori et al., 2010).

2.1.2 applications

Smart Homes, Smart Cities, Healthcare IoT, Smart Factories, IoT in Logistics, Agricultural IoT, Connected Vehicles, Things as Customer, IoT Security Systems, IoT Integration

2.1.3 Complementary or Enablers of IoT

Table 2. Complementary or Enablers of IoT

Technology	Role in IoT
Artificial Intelligence (AI)	Enhances IoT with data analytics, automation, and predictive decision-making (Atzori et al., 2010).
Cloud Computing	Provides scalable storage and processing power for IoT-generated big data (Botta et al., 2016).
Edge Computing	Reduces latency by processing data closer to IoT devices, improving real-time decision-making (Shi et al., 2016).
5G Networks	Enables high-speed, low-latency connectivity essential for IoT applications (Shafi et al., 2017).
Blockchain	Secures IoT transactions and data exchange through decentralized ledgers (Dai et al., 2019).
Big Data Analytics	Extracts insights from massive IoT datasets to optimize system performance (Sun et al., 2016).
Cybersecurity Protocols	Protects IoT networks from cyber threats and unauthorized access (Roman et al., 2013).
RFID & NFC	Facilitates IoT-enabled tracking, identification, and authentication (Want, 2006).
Digital Twins	Creates virtual replicas of IoT systems for simulation and optimization (Tao et al., 2018).
Low-Power Wide-Area Networks (LPWANs)	Supports long-range, low-energy IoT communication (Raza et al., 2017).

2.1.4 Workflow for IoT Data Processing

2.1.4.1 Simple Workflow:

1. Data Collection: Sensors and devices capture real-world data (e.g., temperature, motion, health metrics).
2. Data Transmission: Collected data is transmitted via networks (Wi-Fi, 5G, LPWAN) to processing units that is now Data Centers.
3. Data Processing & Analysis: AI and cloud computing analyze the data for insights and decision-making.
4. Action & Automation: Processed data triggers automated responses or provides insights for human intervention.

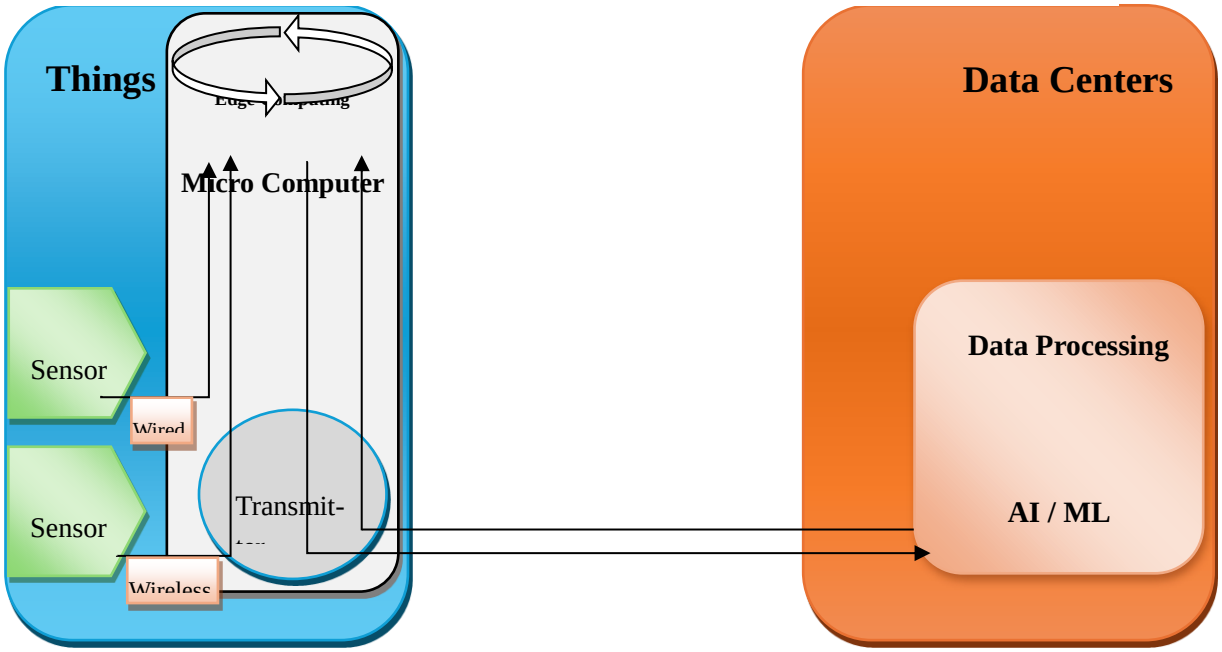

Figure 1. Workflow for IoT Data Processing

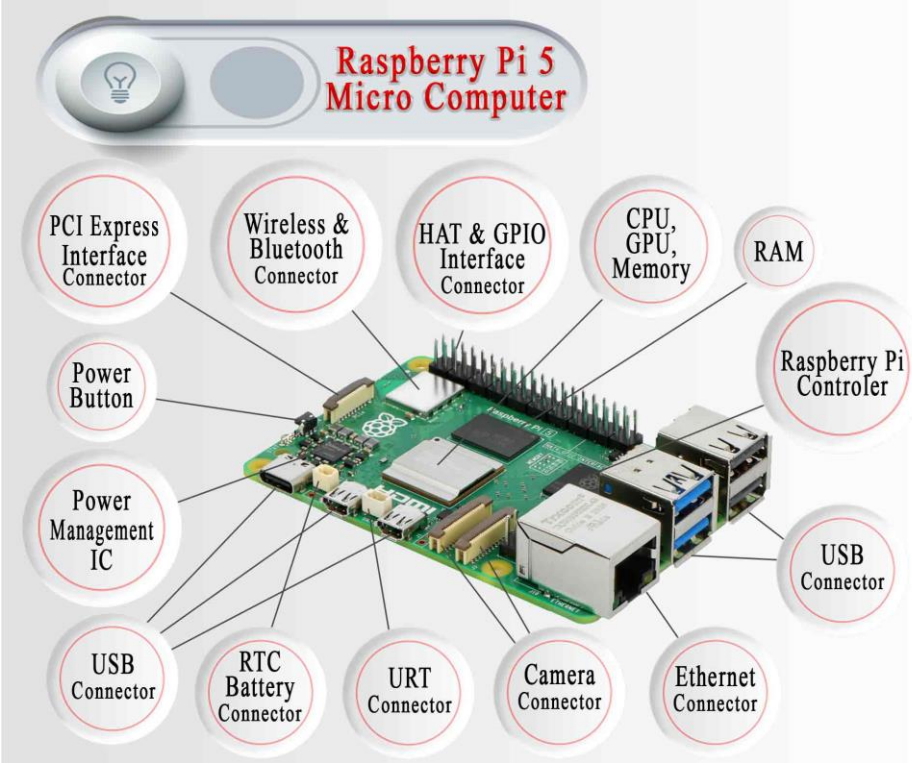

Figure 1. Raspberry Pi 5

2.1.5 Context and Actors of IoT

The Internet of Things (IoT) operates within a complex socio-technical ecosystem, influenced by economic, regulatory, and technological factors (Atzori et al., 2010). Key actors driving IoT adoption and governance include:

Table 3. Context and Actors of IoT

Actor	Role in IoT Ecosystem
Governments & Regulators	Establish policies, cybersecurity frameworks, and data protection laws.
Technology Companies	Develop IoT hardware, software, cloud platforms, and AI integration.
Industries & Enterprises	Implement IoT for automation, efficiency, and predictive analytics.
Consumers & Users	Drive demand for smart home devices, healthcare applications, and personal IoT products.
Academia & Research Institutions	Advance IoT standards, security protocols, and data governance practices.

2.2 Phase 2. Forecasting IoT

The latest comprehensive update of the IoT Hype Cycle was in 2020. Since then, the IoT landscape has evolved significantly. As we are now in 2025, it is essential to recognize that many IoT technologies have likely advanced through different phases.

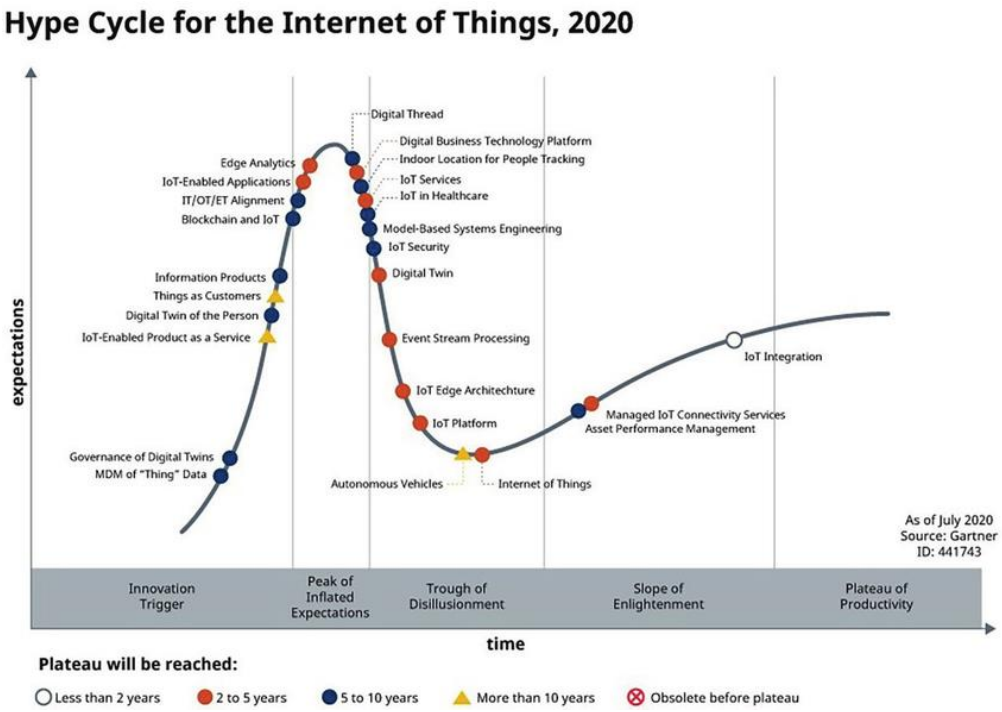

Figure 2. IoT Hype Cycle

The applications of IoT technologies have been recognized, and their *time to plateau* has been mapped based on insights from the most recent Hype Cycle reports. These reports, including the Emerging Technologies Hype Cycle 2024, AI Hype Cycle 2024, and Smart City Hype Cycle 2022, provide valuable perspectives on the evolving landscape and the shifting phases of IoT technologies.

Table 4. IoT Applications or Variables

IoT Variable	Description	Time to Plateau (Years)	Current Status
Smart Homes	For home automation and monitoring	1-5	Increasing adoption; interoperability.
Smart Cities	IoT for urban infrastructure management	11-15	Pilot projects in progress; scaling remains a challenge.
Healthcare IoT	Connected medical devices and telemedicine	6-10	Adoption accelerating with wearable tech and remote care.
Smart Factories	End-to-end automation and IoT integration	6-10	Steady progress with Industry 4.0 initiatives.
IoT in Logistics	Fleet tracking, cold chain monitoring	1-5	Widely adopted in global supply chains.
Agricultural IoT	Precision farming and livestock monitoring	6-10	Growing adoption in developed countries.
Connected Vehicles	Autonomous and connected vehicle systems	6-10	Advancing but far from full mainstream deployment.
Things as Customer	Devices autonomously ordering based on usage patterns	6-10	Early adoption; still evolving with some use cases.

IoT Security Systems	Advanced home and enterprise security systems	1-5	Growing adoption as security risks increase.
IoT Integration	Connecting and managing IoT devices across platforms	6-10	Ongoing improvements in standardization and interoperability.

2.3 Phase 3. Foresight of Societal IoT

2.3.1 IoT Technology Development System (TDS)

The IoT Technology Development System (TDS) consists of three key components:

1. *External Forces*: Factors such as economic conditions, technological advancements, and global trends influence the development and deployment of IoT technologies (Grunwald, 2018).
2. *System*: The core IoT ecosystem, which includes hardware, software, AI, cloud computing, and 5G connectivity, enabling the interconnectivity and data processing critical for IoT (Gubbi et al., 2013).
3. *Arena*: The governance policies, societal values, norms, and ethical considerations that affect how IoT technologies are adopted and regulated (Bijker et al., 2012).

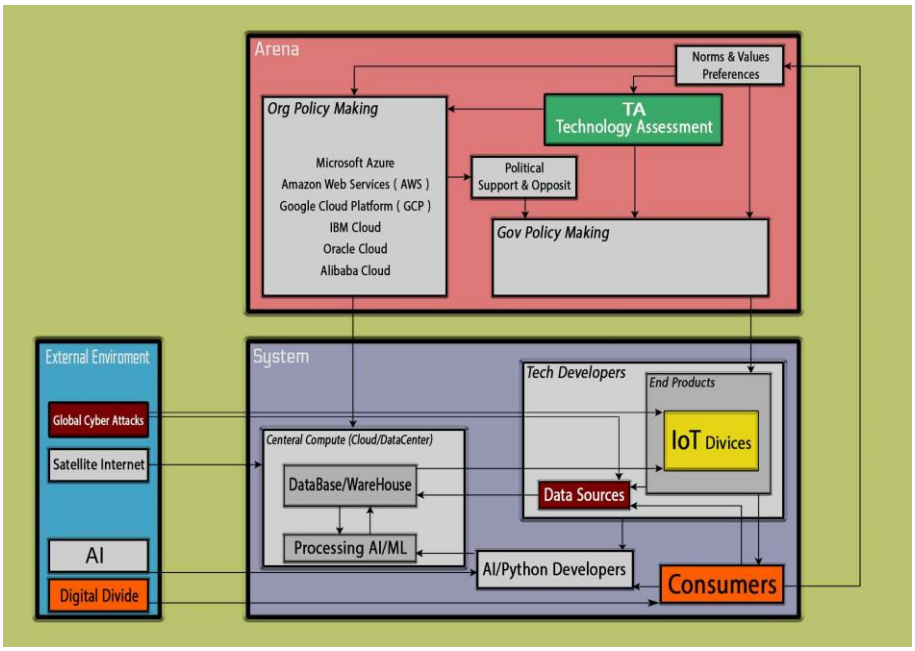

Figure 3. IoT, Technology Development Delivery (TDS)

2.3.2 Societal IoT Scenario Building Using STEEP Analysis

In this phase, STEEP analysis (Social, Technological, Economic, Environmental, and Political) is employed to construct societal IoT scenarios. The analysis evaluates the uncertainty and impact of each driver within the STEEP framework. AI-driven foresight methodologies are utilized to enhance the scenario-building process, enabling more accurate predictions of the future trajectories of IoT technologies in

diverse societal contexts.

Table 5. Societal IoT Scenario Budling Using STEEP

STEEP			Drivers	Uncertainty	Impact	Total
	Social 	1	IoT in Healthcare	6	8	14
		2	Digital Divide	9	8	17
		3	Privacy Concerns	7	8	15
		4	Workplace Collaboration	4	6	10
		5	Public Safety	6	9	15
	Technological 	1	Low-Power IoT Sensors	3	7	10
		2	AI-Driven Predictive Maintenance	5	9	14
		3	5G Networks	4	9	13
		4	Interoperability Challenges	8	7	15
		5	Global Cyberattack on IoT Systems	8	9	17
	Environmental 	1	Precision Agriculture	6	7	13
		2	Smart Grids	5	8	13
		3	E-Waste Management	7	6	13
		4	Environmental Monitoring	5	7	12
		5	Carbon Footprint Reduction	4	7	11
	Economic 	1	Cost Reduction in Manufacturing	3	8	11
		2	Subscription Services	5	6	11
		3	Barriers for Small Businesses	6	7	13
		4	Job Displacement	7	8	15
		5	Wearable IoT Market Growth	4	7	11
	Political 	1	Data Privacy Regulations	6	8	14
		2	Trade Policies	6	7	13
		3	Public Investment	5	8	13
		4	Surveillance Risks	7	9	16
		5	International Standards	5	8	13

Drivers in STEEP	Explanation
IoT in Healthcare	Use of connected medical devices and telemedicine for improved healthcare services.
Digital Divide	The gap between urban and rural areas in access to IoT and digital technologies.
Privacy Concerns	Risks associated with data collection, storage, and misuse in IoT systems.
Workplace Collaboration	IoT-enabled tools enhancing remote work, productivity, and efficiency.
Public Safety	Use of IoT in emergency response, surveillance, and disaster management.
Low-Power IoT Sensors	Energy-efficient sensors improving IoT device longevity and adoption.
AI-Driven Predictive Maintenance	AI-powered analytics predicting equipment failures before they occur.
5G Networks	Faster, more reliable connectivity enabling advanced IoT applications.
Interoperability Challenges	Difficulty in integrating different IoT systems and platforms.
Global Cyberattack on IoT Systems	Large-scale cybersecurity threats targeting interconnected IoT devices.
Precision Agriculture	Use of IoT to optimize farming, irrigation, and crop monitoring.
Smart Grids	IoT-powered energy management for efficient and sustainable power distribution.
E-Waste Management	Challenges and solutions for handling discarded IoT devices and components.
Environmental Monitoring	IoT-driven tracking of air, water, and soil quality for sustainability.
Carbon Footprint Reduction	IoT applications for energy efficiency and lowering environmental impact.
Cost Reduction in Manufacturing	IoT-driven automation improving production efficiency and cutting expenses.
Subscription Services	IoT business models shifting toward service-based, recurring revenue structures.
Barriers for Small Businesses	Challenges faced by small firms in adopting and integrating IoT solutions.
Job Displacement	Potential workforce disruption due to automation and AI-driven IoT.
Wearable IoT Market Growth	Expansion of IoT-based wearables for health, fitness, and productivity.
Data Privacy Regulations	Legal frameworks governing IoT data security and consumer rights.
Trade Policies	International regulations affecting IoT supply chains and adoption.
Public Investment	Government funding and incentives for IoT research and infrastructure.
Surveillance Risks	Ethical and security concerns over mass IoT-based monitoring.
International Standards	Global efforts to establish IoT interoperability and security guidelines.

2.3.3 Four Scenarios of Societal IoT (Trajectories)

Table 6. Four Scenarios of Societal IoT (Trajectories)

		Digital Divides	
		Low	High
Global Cyber Attacks on IoT Systems	Low	Scenario 1: ***"Equitable Tech Haven"***	Scenario 2: ***"Disconnected Prosperity"***
	High	Scenario 3: ***"Resilient United Front"***	Scenario 4: ***"Fragmented Societies"***

2.3.3.1 Scenario 1: *"Equitable Tech Haven"*

With minimal cyber threats, urban and rural societies equally benefit from IoT technologies. This fosters harmony through improved healthcare, education, and smart infrastructure, reducing societal tensions and promoting shared prosperity.

Figure 4. Equitable Tech Haven (Generated by DALL-E, 2025)

2.3.3.2 Scenario 2: *"Disconnected Prosperity"*

Urban societies thrive with smart IoT solutions, while rural areas lack access due to economic and infrastructure gaps. The digital divide widens societal inequality, fueling rural-to-urban migration and straining urban systems.

Figure 5. Disconnected Prosperity (Generated by DALL-E, 2025)

2.3.3.3 Scenario 3: *"Resilient United Front"*

Frequent cyberattacks push urban and rural societies to collaborate, leading to unified cybersecurity measures and equitable IoT adoption. Shared challenges foster stronger social bonds, bridging the gap between communities.

Figure 6. Resilient United Front (Generated by DALL-E, 2025)

Figure 8. Resilient United Front (Generated by DALL-E, 2025)

2.3.3.4 Scenario 4: *"Fragmented Societies"*

Rural areas are left behind in IoT adoption, while urban systems are plagued by frequent cyberattacks. The combination of technological exclusion and insecurity creates distrust, protests, and societal fragmentation.

Figure 9. Fragmented Societies (Generated by DALL-E, 2025)

2.4 Phase 4. Impacts Analysis

2.4.1 Matrix of Scenarios-(Vars-Times) Combination of Phase 2&3

2.4.1.1 Scenarios Related to Cities

Table 7. Scenarios Related to Cities

Scenario	Cities Likely to Fit This Scenario	Characteristics in Relation to Digital Divide
Equitable Tech Haven	***Zurich***, Tokyo, San Francisco	Cities with universal broadband, inclusive IoT, and equal digital access.
Disconnected Prosperity	***New York***, Dubai, London, Hong Kong, Shanghai, Los Angeles, Paris, Sydney, Beijing, Chicago, Moscow, Istanbul	Advanced urban IoT, but widening digital divides between rich and poor areas.
Resilient United Front	***Berlin***, Toronto, Stockholm, Helsinki, Amsterdam, Barcelona, Madrid, Brussels, Seoul, Melbourne, Montreal	Cities bridging the digital divide through public-private partnerships and smart policies for equitable IoT adoption.
Fragmented Societies	***Tehran***, São Paulo, Mumbai, Lagos, Jakarta, Mexico City, Cairo, Manila, Nairobi, Bangkok, Buenos Aires,	Cities with uneven IoT access, where tech hubs thrive but rural and low-income areas lag due to weak policies and infrastructure.

2.4.1.2 Equitable Tech Haven

Table 8. Equitable Tech Haven - (Vars-Times)

Scenario	Variable	0-5 Years	5-10 Years	10-15 Years
Equitable Tech Haven	Smart Homes	Widespread adoption due to improved affordability and interoperability.		
	Smart Cities			Scaled urban projects improve infrastructure and quality of life.
	Healthcare IoT		Expanded adoption of connected healthcare tools, enabling remote monitoring and patient care.	
	Smart Factories		Industry 4.0 advancements lead to greater IoT integration and productivity.	
	IoT in Logistics	IoT solutions optimize global supply chains, enhancing efficiency and tracking capabilities.		
	Agricultural IoT		Precision farming becomes widespread, improving yield and resource management.	
	Connected Vehicles		Autonomous and connected vehicles grow in adoption, reducing accidents and increasing convenience.	
	Things as Customer		Devices gain autonomy in reordering supplies, enhancing customer experiences.	
	IoT Security Systems	Advanced systems address rising security threats in homes and enterprises.		
	IoT Integration		Enhanced standardization simplifies device integration across platforms.	

Figure 10. Zurich, Equitable Tech Haven (Generated by DALL-E, 2025)

2.4.1.3 Disconnected Prosperity

Table 9. Disconnected Prosperity- (Vars-Times)

Scenario	Variable	0-5 Years	5-10 Years	10-15 Years
Disconnected Prosperity	Smart Homes	Growth focused in urban areas, with rural areas lagging behind.		
	Smart Cities			Projects are implemented unevenly, favoring affluent regions.
	Healthcare IoT		Healthcare IoT adoption primarily benefits wealthier communities, increasing the tech gap.	
	Smart Factories		Factories in developed regions lead automation trends, leaving smaller players struggling to compete.	
	IoT in Logistics	Adoption benefits global companies, while smaller businesses face barriers to entry.		
	Agricultural IoT		Adoption skewed toward large, well-funded farms; small-scale farmers see limited benefits.	
	Connected Vehicles		Connected vehicles remain exclusive to wealthier regions.	
	Things as Customer		Autonomous ordering technology is available only to select groups with compatible devices.	

	IoT Security Systems	Security systems primarily benefit urban and wealthier users.		
	IoT Integration		Fragmented standards hinder seamless IoT integration in less developed regions.	

Figure 11. New York, Disconnected Prosperity (Generated by DALL-E, 2025)

2.4.1.4 Resilient United Front

Table 10. Resilient United Front - (Vars-Times)

Scenario	Variable	0-5 Years	5-10 Years	10-15 Years
Resilient United Front	Smart Homes	Accelerated adoption as a result of unified efforts to reduce barriers and costs.		
	Smart Cities			Collaborative global initiatives bring smart city projects to diverse regions.
	Healthcare IoT		Healthcare IoT spreads evenly, addressing the needs of both rural and urban communities.	
	Smart Factories		Unified standards make IoT-based automation accessible across industries and regions.	
	IoT in Logistics	Widespread adoption improves supply chain efficiency worldwide.		
	Agricultural IoT		Global adoption reduces food in-	

			security through precision agriculture.	
	Connected Vehicles		Safety and convenience improvements benefit both developed and developing countries.	
	Things as Customer		Unified efforts improve access to IoT-based autonomous ordering systems.	
	IoT Security Systems	IoT security systems ensure equitable protection across regions and demographics.		
	IoT Integration		Standardized frameworks ensure seamless integration of IoT devices globally.	

Figure 12. Berlin, Resilient United Front (Generated by DALL-E, 2025)

2.4.1.5 Fragmented Societies

Table 11. Fragmented Societies - (Vars-Tines)

Scenario	Variable	0-5 Years	5-10 Years	10-15 Years
Fragmented Societies	Smart Homes	Urban areas adopt IoT solutions rapidly, while rural areas are left behind.		
	Smart Cities			Implementation benefits select regions, exacerbating social disparities.
	Healthcare IoT		Limited adoption creates unequal access to advanced healthcare solutions.	
	Smart Factories		High-tech factories emerge in select areas, widening the industrial technology gap.	
	IoT in Logistics	Large logistics companies dominate with IoT solutions, excluding smaller players.		
	Agricultural IoT		Unequal access limits precision farming to affluent regions.	
	Connected Vehicles		Connected vehicle technologies fail to reach rural and less developed areas.	
	Things as Customer		Use cases remain underdeveloped in less technologically advanced regions.	
	IoT Security Systems	Adoption focused on high-income areas, leaving other regions vulnerable to cyber threats.		
	IoT Integration		Lack of standardized frameworks hinders global adoption and interoperability.	

Figure 13. Tehran, Fragmented Societies (Generated by DALL-E, 2025)

2.4.2 Matrix of Phase 4-PESTEL

2.4.2.1 Equitable Tech Haven

Table 12. Equitable Tech Haven Impacts Identification

Scenario	IoT Variable	Political (P)	Economic (E)	Social (S)	Technological (T)	Environmental (E)	Legal (L)
Equitable Tech Haven	Smart Homes	Government incentives for smart living	Affordable smart home solutions	High public adoption	AI & 5G improve automation	Energy-efficient devices	Strong data protection laws
	Smart Cities	Global smart city initiatives	Public-private partnerships	Inclusive urban development	AI and IoT-driven infrastructure	Eco-friendly urban planning	Smart city cybersecurity laws
	Healthcare IoT	Government healthcare IoT policies	IoT reduces medical costs	Universal access to remote healthcare	AI-enhanced patient monitoring	Sustainable medical IoT devices	GDPR/HIPAA-compliant IoT health data
	Smart Factories	Industry 4.0-friendly policies	IoT-driven cost reduction	Workforce reskilling programs	IoT-robotics synergy	Waste reduction & sustainability	AI & automation labor laws
	IoT in Logistics	IoT-enabled trade regulations	Cost-efficient global supply chains	Improved logistics accessibility	Blockchain-integrated tracking	Carbon footprint monitoring	IoT-enabled trade compliance
	Agricultural IoT	Smart farming policies	Increased crop yield with IoT	Widespread rural IoT adoption	AI-driven precision farming	Climate-smart agriculture	Data ownership in agri-tech
	Connected Vehicles	Autonomous vehicle regulations	IoT-based transportation cost reduction	Public trust in smart mobility	AI-powered road safety & navigation	Emission reduction via IoT	Legal liability for self-driving cars

	Things as Customer	Consumer protection regulations	AI-driven automated purchases	Changing shopping behaviors	AI-powered demand prediction	Sustainable automated purchases	IoT commerce security laws
	IoT Security Systems	Cybersecurity funding & policies	IoT security market growth	Growing demand for secure homes & businesses	AI-driven threat detection	Green security tech	IoT security compliance laws
	IoT Integration	Global IoT standardization	Increased business IoT investment	Interoperability benefits for consumers	Seamless cross-platform IoT connectivity	Sustainability via IoT integration	Universal IoT regulations

2.4.2.2 Disconnected Prosperity

Table 13. Disconnected Prosperity Impacts Identification

Scenario	IoT Variable	Political (P)	Economic (E)	Social (S)	Technological (T)	Environmental (E)	Legal (L)
Disconnected Prosperity	Smart Homes	Urban-focused regulations	Affordable in cities, expensive in rural areas	Digital divide increases	AI-driven smart homes in urban zones	Rising electronic waste	Weak IoT privacy enforcement
	Smart Cities	Unequal government investments	Wealthy cities progress, rural areas lag	Urban-rural gap widens	AI-powered city services in select regions	Limited eco-friendly urban projects	Localized cybersecurity laws
	Healthcare IoT	Private sector dominates IoT health	Costly remote healthcare solutions	Limited access in rural areas	AI diagnostics available to select patients	High energy demand for health IoT	Fragmented healthcare data protection
	Smart Factories	Automation incentives for large firms	IoT increases productivity, but favors big corporations	Job displacement	AI-powered robotic assembly lines	Pollution from manufacturing waste	Labor laws struggle with automation
	IoT in Logistics	IoT-driven trade laws for large firms	Logistics optimization benefits major players	Unequal efficiency in supply chains	AI-driven logistics for top-tier companies	Environmental impact remains unaddressed	Trade laws prioritize corporate IoT interests
	Agricultural IoT	IoT farming benefits big agribusiness	Small farmers struggle to afford IoT	Rural farmers left behind	Precision farming tech only for major farms	Limited water management tech adoption	Agricultural IoT data rights unclear
	Connected Vehicles	Regulations favor urban IoT mobility	Smart cars are expensive	Rural areas lack IoT transport networks	AI driving technology develops unevenly	Urban areas benefit from green transport	Autonomous driving legal gaps remain
	Things as Customer	AI-driven markets expand	Personalized e-commerce grows in urban zones	IoT-based consumer habits increase	AI-predictive purchasing advances	Limited sustainability in urban commerce	E-commerce data privacy gaps widen

	IoT Security Systems	Cybersecurity policy gaps persist	IoT security costs high for individuals	Urban security IoT thrives, rural areas ignored	AI-driven security advances in premium markets	IoT devices increase electronic waste	Weak enforcement of IoT safety laws
	IoT Integration	No universal IoT regulation	Interoperability gaps increase costs	Consumer access to IoT depends on geography	IoT ecosystems fragmented across markets	Environmental gains limited to select regions	IoT regulatory frameworks remain incomplete

2.4.2.3 Resilient United Front

Table 14. Resilient United Front Impacts Identification

Scenario	IoT Variable	Political (P)	Economic (E)	Social (S)	Technological (T)	Environmental (E)	Legal (L)
Resilient United Front	Smart Homes	Strong pro-tech policies	IoT tax incentives for accessibility	High smart home adoption across society	AI & IoT-driven smart utilities	IoT-enabled energy-efficient homes	Comprehensive data security laws
	Smart Cities	Standardized global smart city frameworks	Sustainable IoT investment	Inclusive urban development	AI-powered municipal services	Climate-friendly infrastructure	Global IoT smart city regulations
	Healthcare IoT	Universal IoT healthcare policies	Cost-efficient IoT health services	Digital healthcare accessible to all	AI-powered telemedicine in all regions	Sustainable energy use in IoT health	Standardized health IoT data protection
	Smart Factories	Balanced regulations for automation & labor	IoT streamlines production costs fairly	Workforce reskilled for AI-driven roles	Smart robotics & IoT optimize production	Zero-waste IoT manufacturing	Fair labor laws for automation
	IoT in Logistics	IoT-driven trade harmonization	Efficient supply chains reduce costs	IoT logistics benefits all businesses	Blockchain-enabled logistics innovation	Green packaging & IoT tracking	IoT-integrated global trade laws
	Agricultural IoT	Pro-farming IoT policies	Fair access to precision farming	IoT adoption widespread among farmers	AI-driven agricultural innovation	Smart irrigation reduces water waste	Strong agricultural IoT regulations
	Connected Vehicles	Balanced IoT transport policies	Cost-effective IoT-enabled transport	Public trust in self-driving vehicles	AI-enhanced V2X connectivity	IoT-driven sustainable transport	Legal liability for autonomous accidents
	Things as Customer	Consumer rights protected in AI commerce	IoT enhances shopping efficiency	Widespread trust in AI-driven buying	AI demand forecasting is precise	Sustainability-focused smart commerce	Consumer IoT commerce laws strengthened
	IoT Security Systems	Global IoT security cooperation	IoT security affordability increases	Trust in IoT security solutions	AI-powered real-time cyber defense	Sustainable energy-efficient security tech	Universal IoT security compliance laws

	IoT Integration	Global IoT standardization	Widespread business & consumer adoption	Cross-platform IoT benefits all	Seamless IoT network interoperability	Circular economy enabled by IoT	Universal IoT regulatory frameworks

2.4.2.4 Fragmented Societies

Table 15. Fragmented Societies Impacts Identification

Scenario	IoT Variable	Political (P)	Economic (E)	Social (S)	Technological (T)	Environmental (E)	Legal (L)
Fragmented Societies	Smart Homes	Uneven smart home policies	High-cost limits adoption	Tech access limited to elite groups	AI-powered luxury automation	Waste from disposable IoT devices	Weak data privacy laws
	Smart Cities	Unequal investment in urban tech	Smart infrastructure only in select regions	Widening gap between smart and non-smart cities	IoT-enabled cities exist in isolation	Limited sustainability efforts	Patchwork of conflicting IoT city regulations
	Healthcare IoT	No universal IoT health policies	Expensive IoT healthcare	Limited remote care access for rural populations	AI-driven healthcare available only in wealthy areas	High energy demand for IoT health tech	Fragmented IoT medical data laws
	Smart Factories	No policies to address workforce impact	Automation benefits big corporations	Job losses create economic disparity	IoT robotics advance but are restricted to top firms	Increased industrial pollution	Outdated labor laws don't regulate IoT workforce
	IoT in Logistics	Trade policies favor large corporations	Small businesses struggle with IoT adoption	Unbalanced logistics networks	AI-driven logistics only benefits major firms	No sustainability measures in supply chains	Loopholes in IoT tracking regulations
	Agricultural IoT	Lack of rural IoT support policies	Cost of smart farming is prohibitive for small farmers	Rural tech gap grows	Precision agriculture is available only to agribusiness	Overuse of resources due to poor regulation	No clear ownership of agricultural IoT data
	Connected Vehicles	Self-driving laws favor corporations	Smart transport is expensive	Public transit lacks IoT integration	AI-driven mobility is exclusive to high-income areas	Urban green transport exists, but rural areas lack it	Liability gaps in autonomous vehicle laws
	Things as Customer	AI-driven markets benefit large corporations	Economic power shifts to AI commerce platforms	Consumer manipulation via IoT algorithms	AI-predicted purchasing creates digital monopolies	No regulation on eco-friendly consumer IoT	Gaps in AI-based consumer rights laws
	IoT Security Systems	IoT security is a luxury service	Costly cybersecurity solutions	Rising cybercrime due to weak protection	AI-driven security tech is inaccessible to most	Cybersecurity waste increases	No universal IoT cybersecurity laws

	IoT Integration	No global IoT standards	Poor interoperability raises business costs	IoT ecosystems create market silos	Tech fragmentation stifles innovation	Sustainability limited to corporate initiatives	Unregulated data-sharing across platforms

2.5 Phase 5. Policies Analysis

In this phase, AI-driven policy options related to the dimensions of the impact matrix from Phase 4 were identified, analyzed, and evaluated based on four criteria. This evaluation is specific to *the selected city* for comparison. We have chosen three-time scopes: short-term, mid-term, and long-term. The long-term scope focuses on *participatory policie*s that are constructive in nature.

Policy Option	1. Effectiveness
	2. Efficiency
	3. Implement Feasibility
	4. Adoption
	Means of 4 criteria

L	Low
M	Medium
H	High

2.5.1 Equitable Tech Haven policies, Zurich Evaluated

Policy Focus: foster a sustainable, inclusive, and secure IoT ecosystem by promoting environmental responsibility, bridging the digital divide, enhancing cybersecurity and data privacy, ensuring interoperability through open standards, and driving economic growth through innovation and fair access.

Table 16. Equitable Tech Haven policies, Zurich Evaluated

Scenario	Variable	0-5 years (Short-Term)		5-10 years (Mid-Term)		10-15 years (Long-Term)
Equitable Tech Haven	Smart Homes	Develop incentives for affordable smart home technology for low-income households	H H M H H	Standardize IoT protocols to ensure cross-compatibility of devices for all income groups	H H H H H	Implement national programs to upgrade rural homes with smart technologies and energy-efficient solutions
	Smart Cities	Pilot smart city projects focused on sustainability and low-cost technology for urban areas	M M M M M	Scale-up smart city infrastructure with a focus on inclusivity and low environmental impact	H H M H H	Ensure nationwide smart city policies that integrate environmental sustainability and equitable access for all socioeconomic groups
	Healthcare IoT	Provide subsidies for IoT-based remote healthcare in underserved areas	H H M H H	Create a universal health data framework that supports IoT-driven healthcare solutions for all demographics	H H H H H	Expand universal access to IoT-based healthcare systems, focusing on affordability and environmental impact
	Smart Factories	Introduce tax incentives for SMEs to adopt smart factory	M M	Encourage collaboration between large corporations and	H H	Implement global best practices for smart factory sustainability,

		technologies with a focus on energy efficiency	M M M	small businesses for IoT integration	H H H	ensuring lower waste and optimized resource use
	IoT in Logistics	Encourage IoT adoption for efficient supply chain management with a focus on minimizing carbon footprints	H H M H H	Support the development of IoT-enabled circular supply chains, reducing waste and emissions	H H H H H	Establish national and global IoT logistics policies to optimize shipping efficiency while minimizing environmental impacts
	Agricultural IoT	Offer subsidies for IoT technologies in small-scale farming to increase food security and reduce resource waste	M M M M M	Scale-up IoT-driven precision farming techniques to maximize crop yield while minimizing water and pesticide use	H H H H H	Mandate sustainable agricultural practices supported by IoT technology, ensuring equitable access for all farmers
	Connected Vehicles	Introduce policies to promote electric and IoT-enabled vehicles in urban areas to reduce pollution	M M M M M	Expand the adoption of autonomous, electric, and connected vehicles in public transport systems, reducing emissions	H H H H H	Ensure a global shift towards fully IoT-enabled, sustainable transport systems that are affordable for all urban and rural populations
	Things as Customer	Implement consumer protection policies for IoT-based purchasing, ensuring transparency and fair pricing	M M M M M	Develop standards for IoT-based consumer purchases that promote sustainable practices (e.g., promoting eco-friendly products)	H H H H H	Promote circular economy principles in IoT, encouraging devices to be reused and recycled, reducing e-waste
	IoT Security Systems	Strengthen public awareness and education on IoT security risks, making them accessible to all demographics	H H M H H	Mandate robust IoT security standards to protect consumer data while promoting environmental responsibility	H H H H H	Ensure global cooperation on IoT security, creating policies that also prioritize energy-efficient, low-carbon solutions in cybersecurity
	IoT Integration	Promote open-source IoT platforms and encourage collaboration between tech companies to ensure interoperability	M M M M M	Establish regulatory frameworks for seamless IoT integration across industries, with an emphasis on sustainability and inclusivity	H H H H H	international IoT integration standards that ensure devices from all sectors work together efficiently, minimizing environmental impact

2.5.2 Disconnected Prosperity policies, New York Evaluated

Policy Focus: Bridging urban-rural technology gaps, ensuring affordability, and expanding IoT services beyond privileged communities. guiding the scenario toward "Equitable Tech Haven."

Table 17. Disconnected Prosperity policies, New York Evaluated

Scenario	Variable	0-5 years		5-10 years		10-15 years
Disconnected Prosperity	Smart Homes	Expanding affordable smart home technology in rural areas	M M M M M	Standardizing smart home ecosystems to reduce entry barriers	H H H H H	Nationwide smart housing policies for universal adoption
	Smart Cities	Incentives for expanding smart city initiatives to underserved areas	L L L L L	Infrastructure funding for smart city projects beyond major urban hubs	M M L M M	National smart city integration for equitable growth
	Healthcare IoT	Extending IoT-driven healthcare subsidies to rural clinics	M M L M M	Mandating interoperability of healthcare IoT systems	H H M H H	Universal IoT-enabled healthcare access policies
	Smart Factories	Tax relief for SMEs adopting IoT-driven manufacturing	L L M L L	Upskilling initiatives for workers in IoT-enabled factories	M M M M M	Smart factory adoption policies to ensure industrial balance
	IoT in Logistics	Expanding IoT logistics networks to remote and rural areas	M M M M M	Incentives for small businesses to integrate IoT logistics	H H H H H	Full-scale IoT logistics adoption nationwide
	Agricultural IoT	Government grants for IoT-based farming innovations	L L L L L	Expanding connectivity in remote agricultural zones	M M M M M	Universal IoT-enabled agricultural policies for sustainability
	Connected Vehicles	Ensuring IoT-driven vehicle technology is accessible beyond urban centers	L L L L L	Developing equitable IoT transportation policies	M M M M M	Integrating smart mobility solutions for all communities
	Things as Customer	Regulating fair access to IoT-based commerce for all	L L	Expanding consumer pro-	M M	Enabling widespread and

		demographics	L L L	tection in IoT-driven transactions	M M M	equitable IoT-driven consumer services
	IoT Security Systems	Strengthening legal frameworks for IoT cybersecurity	M M M M M	Expanding IoT security requirements for businesses	H H H H H	Coordinated international cybersecurity governance
	IoT Integration	Encouraging open-source IoT solutions for broader adoption	L L L L L	Establishing legal mandates for IoT interoperability	M M M M M	Achieving full-scale IoT integration across economic sectors

2.5.3 Resilient United Front policies, Berline Evaluated

Policy Focus: Strengthening global cooperation, promoting standardization, and ensuring equitable IoT adoption across borders. guiding the scenario toward "Equitable Tech Haven."

Table 18. Resilient United Front policies, Berline Evaluated

Scenario	Variable	0-5 Years		5-10 Years		10-15 Years
Resilient United Front	Smart Homes	Strengthening local smart home initiatives with subsidies	L L L L L	Global collaboration on smart home technology standards	M M M M M	Equitable IoT housing policies with long-term sustainability focus
	Smart Cities	Establishing multi-stakeholder collaborations for smart city deployment	L L L L L	Incentivizing cross-sector smart city partnerships	M M L M M	Global frameworks for equitable smart city expansion
	Healthcare IoT	Public investments in IoT-driven health solutions	M M M M L	Standardized global protocols for IoT health data	H M M M M	Universal adoption of IoT-driven healthcare infrastructure
	Smart Factories	Investing in local workforce training for IoT industries	L L L L	Encouraging international IoT manufacturing collaboration	M M M M	Standardizing IoT-based industrial automation worldwide

			L		M	
	IoT in Logistics	Expanding IoT-based supply chain resilience strategies	M M M M L	Harmonizing IoT logistics standards across countries	M M M M M	Full integration of IoT logistics into global supply chains
	Agricultural IoT	Promoting cooperative smart farming initiatives	L L L L L	Standardizing IoT agricultural best practices globally	M M M M M	Establishing IoT-driven sustainable agriculture mandates
	Connected Vehicles	Incentives for cross-border IoT transportation projects	L L L L L	Coordinated international smart mobility policies	M M M M M	Seamless IoT-driven transportation frameworks globally
	Things as Customer	Establishing fair digital commerce regulations for IoT-driven transactions	L L L L L	Strengthening global consumer rights in IoT-driven markets	M M M M M	Standardized worldwide policies for IoT commerce accessibility
	IoT Security Systems	International agreements on IoT security frameworks	M M M M L	Cross-border cybersecurity cooperation in IoT governance	M M M M M	Establishing a global IoT security alliance
	IoT Integration	Developing open-source IoT frameworks for universal access	L L L L L	Expanding multi-national IoT standardization efforts	M M M M M	Ensuring seamless cross-industry IoT integration worldwide

2.5.4 Fragmented Societies, Tehran Evaluated

Policy Focus: bridging gaps in fragmented societies by ensuring accessibility, security, standardization, and widespread adoption. guiding the scenario toward "Equitable Tech Haven."

Table 19. Fragmented Societies, Tehran Evaluated

Scenario	Variable	0-5 years		0-10 years		0-15 years
F r	Smart Homes	Government incentives for	M	Standardizing smart home	H	Ensuring nationwide smart

		IoT adoption in low-income areas	M M M M	interoperability	H H H H	home infrastructure accessibility
	Smart Cities	Public-private partnerships for smart city pilots	L L L L L	Expanding smart infrastructure to rural areas	M M M M M	Mandating smart city policies for equitable urban planning
	Healthcare IoT	Subsidizing IoT-based remote healthcare for underserved populations	M M M M M	Expanding IoT health infrastructure in public hospitals	H H H H H	Creating universal IoT-driven healthcare frameworks
	Smart Factories	Supporting IoT training programs for workforce upskilling	M M L L L	Tax incentives for SMEs to adopt smart factory solutions	H H H H H	Full integration of smart manufacturing in all industries
	IoT in Logistics	Encouraging IoT-enabled supply chain transparency	M H H H H	IoT-driven optimization for public transportation	H H H H H	Nationwide integration of IoT logistics in infrastructure planning
	Agricultural IoT	Government subsidies for IoT-based precision farming	L L L L L	Expanding rural connectivity to support smart farming	M M M M M	Nationwide smart agriculture policies for sustainability
	Connected Vehicles	Regulation and investment in IoT-based traffic management	M M L L L	Expanding IoT-based vehicle safety standards	M M M M M	Full-scale smart mobility integration across cities
	Things as Customer	Encouraging development of autonomous commerce platforms	L L L L L	Establishing consumer protection laws for IoT-based purchasing	M M M M M	Ensuring universal accessibility and affordability

	IoT Security Systems	Strengthening cybersecurity policies for IoT protection	H H H H H	Mandating IoT security compliance in businesses	H H H H H	Global cooperation on IoT cybersecurity governance
	IoT Integration	Developing open standards for IoT interoperability	M M M M M	Enforcing global IoT integration policies	H H H H H	Full-scale seamless IoT adoption across sectors

3. Conclusion and Future Implications

3.1 Summary of Key Findings

This study applied AI-driven foresight methodologies across five phases, transitioning from IoT description to IoT governance recommendations through a structured framework TA. This study evaluated policy options or TP (Technology policy) in 4 directions of societal technology of IoT, related to the impacts matrix and selected city. Challenges and opportunities to IoT policies for selected cities, addressed to ***Table 16-19*** with Scoring of Low-High.

3.2 Primary Research Questions

1) What are the key directions of IoT development in societal technology, and how do they shape urban and rural dynamics?

As shown in ***Table 6*** the four scenarios of societal IoT foresight highlight different trajectories for technological adoption and policy responses. These scenarios are influenced by *the digital divide*, shaping urban and rural dynamics by determining access to infrastructure, connectivity, and innovation adoption rates.

2) How can these technological directions be described through scenario analysis, and what policy options can be prescribed to address their societal impacts?

As shown in ***Table 8-11***, we first enriched the scenarios with quantitative IoT data extracted from the Hype Cycle (Vars-Times) in ***Table 4***, which represents the novelty of this research. Then, as shown in ***Table 12–15***, we identified the societal impacts of IoT development using the PESTEL framework for each scenario. Finally, based on the selected cities from ***Table 7,*** for each matrix of identified impacts we developed a matrix of policy options (***Table 16–19***), aligning them with the dimensions of Vars-Times and evaluating them within the context of the selected cities.

3.3 Future Research Directions

This study identified societal impacts (Tables 12–15) but did not conduct an in-depth evaluation. Future research could apply *Scanning Method* or *Tracking Method* to analyze these impacts systematically, using specific metrics for quantification and assessment.

The policy options derived (Tables 16–19) were based on a classical TA approach, primarily suited for *Parliamentary TA*. Future studies could expand this discussion by integrating *Participatory TA* and *Constructive TA*, incorporating stakeholder engagement and technology co-creation for more inclusive and adaptive IoT governance.

Conflict of interests

The authors declare no conflict of interest.

References

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

Bijker, W. E., & Pinch, T. (1987). The social construction of facts and artifacts. *Technology and Culture*, *9*(3), 404-424.

Bijker, W. E., Hughes, T. P., & Pinch, T. (2012). *The social construction of technological systems: New directions in the sociology and history of technology*. MIT Press.

Botta, A., Donato, W. D., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and Internet of Things: A survey. *Future Generation Computer Systems*, *56*, 684-700.

Collingridge, D. (1980). *The social control of technology*. St. Martin's Press.

Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal*, *6*(5), 8076-8094.

Feenberg, A. (1999). *Questioning technology*. Routledge.

Freeman, C. (1987). *Technology policy and economic performance: Lessons from Japan*. Pinter Publishers.

Gartner. (2020). *Hype cycle for emerging technologies*. Gartner Research.

Geels, F. W. (2004). From sectoral systems of innovation to socio-technical systems. *Research Policy*, *33*(6-7), 897-920.

Grunwald, A. (2018). *Technology assessment in practice and theory*. Routledge.

Grunwald, A. (2019). The hermeneutic side of responsible research and innovation. *Journal of Responsible Innovation*, 6(1), 20-38.

Godet, M. (2006). Scenario building: Uses and abuses. *Long Range Planning*, *29*(2), 164-171. https://doi.org/10.1016/0024-6301(95)00032-1

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

Huang, J., & Zhang, T. (2021). Multi-criteria evaluation framework for IoT policies. *Policy & Internet*, *13*(2), 1-18.

James, A. (2022). Digital divides and the future of IoT governance. *Telecommunications Policy*, *46*(5), 102134.

Lundvall, B. Å. (1992). *National systems of innovation: Towards a theory of innovation and interactive learning*. Pinter Publishers.

Ralston, S. (2011). *Foresight: The art and science of anticipating the future*. Wiley.

Raza, U., Kulkarni, P., & Sooriyabandara, M. (2017). Low-power wide-area networks: An overview. *IEEE Communications Surveys & Tutorials*, *19*(2), 855-873.

Raj, R., & Sundararajan, A. (2020). Governance challenges in smart city IoT policy. *Information Systems Journal*, *30*(1), 15-32.

Rip, A., & Kemp, R. (1998). Technological change. *Human Choice and Climate Change*, *2*, 327-399.

Roman, R., Najera, P., & Lopez, J. (2013). Securing the Internet of Things. *Computer*, *44*(9), 51-58.

Schumpeter, J. A. (1942). *Capitalism, socialism, and democracy*. Harper & Row.

Smith, M. R., & Marx, L. (1994). *Does technology drive history? The dilemma of technological determinism*. MIT Press.

Shafi, M., Molisch, A. F., Smith, P. J., Haustein, T., Zhu, P., Tufvesson, F., … & Wunder, G. (2017). 5G: A tutorial overview. *IEEE Communications Surveys & Tutorials*, *19*(3), 1617-1655.

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, *3*(5), 637-646.

Sun, X., Yan, H., Zhang, W., & Vasilakos, A. V. (2016). Internet of Things and big data analytics for smart and connected communities. *IEEE Access*, *4*, 766-773.

Tao, F., Zhang, H., Liu, A., & Nee, A. Y. C. (2018). Digital twin in industry: State-of-the-art. *IEEE Transactions on Industrial Informatics*, 15(4), 2405-2415.

Vermaas, P. E., Kroes, P., van de Poel, I., Franssen, M., & Houkes, W. (2011). *A philosophy of technology: From technical artefacts to sociotechnical systems*. Morgan & Claypool Publishers.

Want, R. (2006). An introduction to RFID technology. *IEEE Pervasive Computing*, *5*(1), 25-33.

Wenge, H., Zhao, Q., & Liu, Y. (2021). PESTEL analysis for IoT policymaking in global cities. *Urban Studies*, *58*(4), 765-783.

Wenge, H., Ziegler, P., & Kwon, H. (2021). PESTEL-driven IoT policy formulation in metropolitan regions. *International Journal of Technology Policy*, *22*(5), 451-473.

Winner, L. (1980). Do artifacts have politics? *Daedalus*, *109*(1), 121-136.

Wu, B., Chen, X., & Li, Z. (2022). AI-based cybersecurity strategies for IoT protection: A review. *Journal of Cybersecurity & AI*, *9*(3), 211-229.