

Computational Discovery and Intelligent Systems CDIS

ISSN: 3070-5037/© 2026, The Authors. CDIS (CC BY 4.0) License.

Journal Homepage

<https://pub.scientificirg.com/index.php/CDIS>



IoT-Enabled Smart Cities Architectures Connectivity Edge Computing Digital Twins and Security

Asmaa A. Attwa^{a,1} , and Amer Ibrahim^b 

^a Faculty of Applied Health Sciences Technology, Beni-Suef University, Beni-Suef City, 62511, Egypt; E-mail: asmaa.abdelhamed@fahst.bsu.edu.eg

^b Department of Computer Science and Software Engineering, United Arab Emirates University, UAE; E-mail: Amer.ibrahim@uaeu.ac.ae

ABSTRACT

The Internet of Things (IoT) supports urban monitoring and service management by connecting sensors, actuators, communication networks, and computing platforms. This survey examines IoT-enabled smart cities across five themes: layered reference architectures; connectivity, including low-power wide-area networks (LPWAN), fifth-generation (5G) cellular networks, satellite links, and prospective sixth-generation (6G) technologies; edge and fog computing; digital twins; and security and privacy, with emphasis on blockchain-based and federated approaches. Application domains in energy, transportation, waste, water, environmental monitoring, and street lighting are reviewed. The central contribution is a conceptual cross-layer decision framework that links service requirements to connectivity selection, computation placement, and digital twin configuration under security and governance constraints. A first-order model of offloading delay and device energy illustrates the computation placement trade-off. The reviewed studies show that no single connectivity technology satisfies all urban requirements; that a field pilot of 5G exhibited significant variation in network performance; that, in simulation, a low Earth orbit (LEO) narrowband IoT constellation of 60 satellites guaranteed a minimum link availability of about 30% of the simulated period; that city-scale digital twins have been applied most often to urban planning; that a blockchain ledger does not guarantee the truthfulness of recorded sensor data; and that learning-based defenses can be evaded. An evidence classification shows that the quantitative studies examined mostly report results from simulations, benchmark datasets, or single pilots, and not from operational city deployments. Persistent challenges include interoperability, energy efficiency, scalability, connectivity reliability, and data governance. Promising directions include hybrid terrestrial and satellite connectivity, adaptive edge and cloud processing, sensor-driven digital twins on standardized data models, privacy-preserving collaborative learning, and selectively applied distributed ledgers. The survey is non-exhaustive and follows no formal systematic protocol.

PAPER INFORMATION

HISTORY

Received: 6 August 2026

Revised: 8 October 2026

Accepted: 23 October 2026

Online: 31 October 2026

MSC

68M12; 68M14; 68M20;
90B18; 68T05; 68U20

KEYWORDS

Internet Of Things;
Smart Cities;
IoT Architectures;
Edge Computing;
Digital Twins.

1 INTRODUCTION

Urban populations continue to grow, and approximately 68% of the world population is projected to live in urban areas by 2050 [1]. This growth places increasing pressure on infrastructure, energy, transportation, and public services. The

¹Corresponding author at Faculty of Applied Health Sciences Technology, Beni-Suef University, Beni-Suef City, 62511, Egypt;
E-mail: asmaa.abdelhamed@fahst.bsu.edu.eg

Internet of Things (IoT), which integrates identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols, and distributed intelligence for smart objects [2], has therefore become a central technology for urban monitoring and management [3, 4]. No single definition of a smart city is accepted, and most definitions refer to advances in information and communication technology that improve quality of life through smart services [5]. In this survey, a smart city denotes an urban environment in which physical infrastructure is instrumented with networked sensors and actuators and the resulting data streams are processed to improve efficiency, sustainability, and quality of life. This working definition is consistent with the view of a smart city as the application of information and communication technologies to create a better living experience for the urban population [6].

An early and frequently cited example is the Padova Smart City project, a proof-of-concept urban IoT deployment in which wireless nodes mounted on street light poles collected environmental data and monitored public lighting through a gateway connected to the municipal data network [3]. That work identified the noninteroperability of heterogeneous technologies as the most relevant technical obstacle to a unified urban platform [3]. Later work on open data reached a related conclusion, noting that proprietary protocols and vertically integrated systems prevent equipment and services from different vendors from being combined [7].

Since then, three developments have widened the design space. Low-power wide-area network (LPWAN) and cellular technologies offer a range of coverage and energy trade-offs for city-scale sensing [6, 8]. Edge and fog computing move processing close to data sources to reduce latency [9, 5, 10]. Digital twins couple continuously updated virtual models with physical assets [11, 12]. Each development also expands the attack surface that must be secured [13, 6].

Representative surveys, compared in Section 2, address these themes largely in isolation, so the dependencies among them receive limited attention. Examples include the effect of link behavior on digital twin update intervals and the effect of device constraints on security design.

The main contributions of this survey are as follows.

- A conceptual cross-layer decision framework is proposed as the principal contribution. It orders service requirements, connectivity selection, computation placement, and digital twin configuration under security, privacy, and governance constraints, and it is applied to two service scenarios (Section 8).
- A five-layer reference architecture for IoT-enabled smart cities is synthesized from the literature (Section 3).
- Connectivity technologies are compared using values reported in published surveys, with the differences between sources stated, and a hybrid terrestrial and satellite connectivity model is described (Section 4).
- Computation placement across the device, edge and fog, and cloud continuum is reviewed, and first-order delay and energy criteria for offloading are stated under explicit assumptions (Section 5).
- Security and privacy mechanisms are reviewed by threat, countermeasure, and residual limitation, with qualified evidence for learning-based, blockchain-based, and federated approaches (Section 6).
- An evidence classification of representative quantitative studies identifies the study type behind each reported result (Section 8.3).
- Open challenges and future research directions are consolidated (Sections 9 and 10).

The remainder of this paper is organized as follows. Section 2 compares related surveys and describes the survey methodology. Section 3 presents the layered architecture. Section 4 reviews communication and connectivity technologies. Section 5 discusses edge computing, fog computing, and digital twins. Section 6 examines security and privacy. Section 7 surveys application domains. Section 8 presents the cross-layer framework, its application, and the evidence assessment. Section 9 identifies open challenges, and Section 10 outlines future research directions. Section 11 discusses the limitations of this survey, and Section 12 concludes the paper.

2 RELATED SURVEYS AND SURVEY METHODOLOGY

2.1 Related Surveys

Table 1 summarizes representative studies and their scope. The scope statements are based on the topics stated by each source. Among the studies listed, none is stated to examine connectivity, computation placement, digital twins, and security together.

Table 1: Representative Related Surveys and Their Scope

Reference	Primary focus	Scope
[6]	Components, architectures, networking technologies, artificial intelligence, applications, and challenges of IoT in smart cities	Broad IoT coverage; digital twins are not among the stated topics
[1]	IoT features, architecture, communication infrastructure, and applications in smart cities, including smart grid, transport, and health	Digital twins and blockchain are not among the listed topics
[14]	IoT fundamentals, smart city workflows, architectures, applications, and challenges	Solutions are proposed at a conceptual level, and realization is left to future work
[15]	IoT applications in urban domains, investment trends, and urban IoT sensors with their performance metrics and power profiles	Application and sensor emphasis; digital twins and computation placement are not among the stated topics
[5]	Edge computing in smart cities: evolution of paradigms, taxonomy, requirements, and open challenges	Computing perspective; digital twins are not among the stated topics
[10]	Edge computing for IoT: architecture-based categories, latency, bandwidth, energy, overhead, and security	General IoT scope rather than city-specific; digital twins are not among the stated topics
[8]	Hybrid 5G and LPWAN architectures, security, network slicing, and satellite extension for smart cities and remote areas	Connectivity and security focus; edge computing and digital twins are not the central topics
[16]	6G technologies and their smart city applications	Prospective technologies without deployed evidence
[11]	Digital twins from smart manufacturing to smart cities	Digital twin focus; connectivity and security are not the central topics
[17]	Systematic review of 64 studies on urban digital twins, IoT, and artificial intelligence in smart city development	Digital twin focus; connectivity and computation placement are not stated topics
[18]	Digital twin applications in urban mobility, with a case study of Helsinki	Mobility focus; connectivity and security are not stated topics
[19]	Federated learning for urban sensing: attacks, defenses, incentive mechanisms, and applications	Privacy and security focus; connectivity and digital twins are not stated topics

2.2 Survey Methodology

The literature was identified through targeted searches of IEEE Xplore, ScienceDirect, SpringerLink, and MDPI using combinations of the terms Internet of Things, smart city, edge computing, fog computing, digital twin, blockchain, federated learning, 5G, and 6G. Studies were included when addressing at least one of the five themes and when the statements attributed to the source could be checked against it. English-language journal articles, conference papers, and book chapters published from 2020 to 2025 were prioritized, and earlier foundational studies were added where those studies define the concepts used here. Preprints and other sources lacking peer review were excluded. Publications from 2025 were added to update coverage, and each was checked against its abstract and bibliographic record.

Quantitative values are reported as stated by the source together with its study type. Records of search dates and of the number of screened records were not maintained, so the search is described as targeted and non-exhaustive. The survey

follows a qualitative narrative approach and not a formal systematic protocol such as PRISMA. It includes no registered search strategy, no formal risk-of-bias assessment, and no quantitative meta-analysis, and the consequences are discussed in Section 11. To prevent the conflation of different kinds of evidence, each quantitative result is labeled as originating from a literature review, a field pilot, a simulation, a benchmark dataset evaluation, a secondary analysis, or a population survey (Section 8.3).

3 LAYERED ARCHITECTURE FOR IOT-ENABLED SMART CITIES

IoT-based smart city deployments are commonly organized in layers that separate sensing, communication, computation, and application concerns [6, 1]. No universally accepted architecture exists. Three-layer (perception, transport, and application), four-layer (device, network, data management, and application), five-layer, and six-layer variants have been described [1], and a five-layer structure comprising sensing, network, middleware, application, and business layers has been reported for smart cities [6].

Figure 1 shows the five-layer structure adopted in this survey, with the perception, network, edge and fog, platform and analytics, and application layers. The structure was synthesized from the cited descriptions by renaming the middleware layer as the platform and analytics layer, adding an explicit edge and fog layer, and treating business concerns under governance. The edge and fog addition follows the distinction between cloud, fog, and edge processing models, which are not mutually exclusive and are intended to complement one another [6]. The double-headed arrows indicate bidirectional exchange between adjacent layers. Security, privacy, and governance concerns apply at several layers, so the countermeasures reviewed in Section 6 are not confined to a single layer [6]. Digital twin functions are likewise not confined to a single layer, because a reported digital twin architecture distributes edge, data management, digital twin, event management, resource management, and system management functions across edge and cloud resources [12].

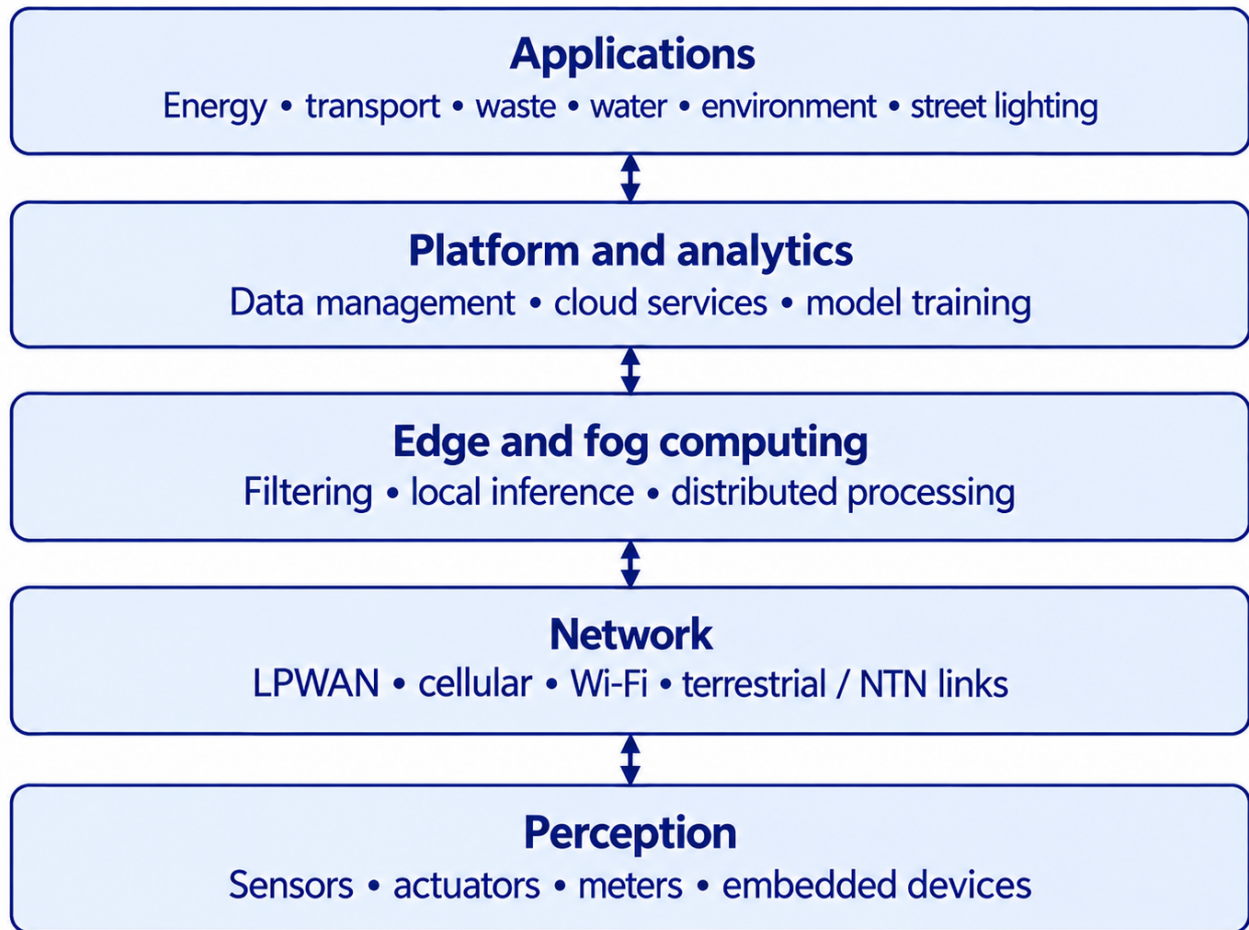


Figure 1: Layered Architecture for IoT-Enabled Smart Cities

The perception layer consists of sensors, actuators, meters, and embedded devices that observe physical quantities and

act on physical objects [6]. The network layer transports the collected data using LPWAN, cellular, Wi-Fi, and terrestrial and non-terrestrial network (NTN) links, which are compared in Section 4 [6]. The edge and fog layer localizes decision making, performs filtering and local inference, and can provide higher layers with decision options rather than raw data [6]. The platform and analytics layer provides data management, cloud services, and model training, and applies analytics, including machine learning, to aggregated data [6, 20]. The application layer delivers domain-specific services to city administrators and residents, as summarized in Section 7.

Interoperability across heterogeneous devices and vendors, identified in the Padova deployment, remains an open concern for architecture designers [3, 7]. Open standards do not by themselves yield open systems, because an open infrastructure also requires access to open data and open interfaces [7].

4 COMMUNICATION AND CONNECTIVITY TECHNOLOGIES

Communication in smart city IoT must be energy efficient because devices are often constrained in memory and processing capacity and may depend on batteries or small solar panels, which favors power-efficient protocols [7]. **Table 2** lists the technologies most often discussed for smart cities, including narrowband IoT (NB-IoT), LoRaWAN, and Sigfox, with values as reported in two surveys [6, 1]. The two sources report different figures for several technologies, and neither states whether the values are specified maxima or field measurements. The table should therefore be read as an indication of orders of magnitude and not as a performance specification.

Table 2: Reported Characteristics of Communication Technologies for IoT-Enabled Smart Cities

Technology	Spectrum	Reported data rate	Reported range
NB-IoT	Licensed cellular bands [6]	200 kb/s [6]; up to 250 kb/s [1]	1 to 10 km [6]; up to 35 km [1]
LoRaWAN	Unlicensed 433, 868, and 915 MHz [6]	Up to 50 kb/s [6]; 0.3 to 50 kb/s [1]	5 to 20 km [6]; 3 to 8 km urban and 15 to 22 km rural [1]
Sigfox	Unlicensed 433, 868, and 915 MHz [6]; 900 MHz [1]	100 b/s [6]; 10 to 1000 b/s [1]	10 to 50 km [6]; up to 50 km [1]
Zigbee	868 MHz, 915 MHz, and 2.4 GHz [6]	250 kb/s [6]	Up to 100 m [6]
Wi-Fi	2.4 and 5 GHz [6]	54 Mb/s and 6.75 Gb/s [6]	100 to 140 m [6]
4G	600 MHz to 5.925 GHz [6]	Up to 1 Gb/s [6]	Not reported
5G	600 MHz to 80 GHz [6]	Up to 20 Gb/s [6]	Not reported

A third survey, which concentrates on urban sensor electronics, gives values that differ again. It reports LoRaWAN ranges of 2 to 5 km in urban areas and up to 15 km in rural areas, sub-6 GHz 5G cells covering 1 to 2 km and millimeter-wave 5G covering 100 to 200 m in dense environments, Bluetooth Low Energy (BLE) 5 ranges of 200 to 400 m under ideal conditions, indoor Wi-Fi coverage of 30 to 50 m, and Zigbee ranges of 100 to 200 m line of sight per hop [15]. The same survey lists transmit currents for specific transceivers: 40 to 100 mA for a LoRa transceiver at 100 mW output power, 10 to 20 mA for a BLE transceiver, and 287 mA at 3.3 V, or about 947 mW, for a Wi-Fi radio [15]. These transceiver values depend on the device model and the output power. Transmit current alone differs by more than an order of magnitude between the BLE transceiver and the Wi-Fi radio, and the energy per delivered bit also depends on data rate and duty cycle, which **Table 2** does not capture.

4.1 Network Topologies and Area Networks

Three topologies are used in IoT networks: point to point, star, and mesh [6]. A star topology provides a natural aggregation point at a central node or gateway but may cause high latency and bottlenecks when many devices connect, whereas a mesh topology extends range through multiple hops and increases resilience because alternate paths remain available when a node fails [6]. Smart city networks are also grouped into home area networks, field or neighborhood area networks, and wide area networks. Home area networks are short range and use protocols such as Zigbee, Bluetooth, and Wi-Fi, whereas wide area networks use cellular services, fiber optics, and low-power protocols designed for wide-area coverage [6].

4.2 Low-Power Wide-Area Networks

NB-IoT operates in licensed cellular bands, whereas LoRaWAN and Sigfox operate in unlicensed sub-GHz bands, and Sigfox is a proprietary standard that uses ultra-narrowband transmission at very low data rates [6]. In a LoRaWAN deployment, end devices are not bound to a specific gateway, and the gateways forward data to a back-end network server that connects to the cloud [6]. As shown in **Table 2**, LPWAN technologies trade data rate for range, with reported rates between 10 b/s and 250 kb/s and reported ranges between 1 km and 50 km. Short-range technologies such as Wi-Fi and Zigbee serve home and building area networks, whereas LPWAN technologies serve wide-area sensing [6].

4.3 Fifth-Generation Networks and Hybrid Connectivity

Fifth-generation networks are expected to benefit ubiquitous sensing through high bandwidth and low latency, but population coverage of current deployments remains low, and a 2024 evaluation does not expect global coverage above 80% before 2028 [21]. That evaluation deployed an IoT solution for identifying road assets requiring maintenance on 11 waste collection trucks over six months, from June to December 2022. It found that 5G supports mobile video streaming but exhibits significant variations in network performance, which may make it unsuitable for applications that require higher data intensity or near real-time responsiveness [21]. New smart city applications are therefore expected to experience a mixture of 4G and 5G [21].

Current architectures are reported to lack flexible connectivity for many IoT applications, which has motivated hybrid architectures that provide ubiquitous connectivity in urban and underserved remote areas [8]. Reported elements of such architectures include the combination of 5G with LPWAN, the slicing of virtual networks by quality of service using software-defined networking and network function virtualization, and the use of LPWAN jointly with LEO satellites [8]. Satellite links are one form of NTN. **Figure 2** illustrates the resulting logical paths. Urban sensors reach the core network and cloud through an LPWAN gateway and cellular backhaul, whereas remote sensors with NTN-capable endpoints reach it through a LEO satellite and a ground segment. The figure is a conceptual illustration synthesized for this survey from the hybrid architectures discussed in [8], and it omits reverse control flows.

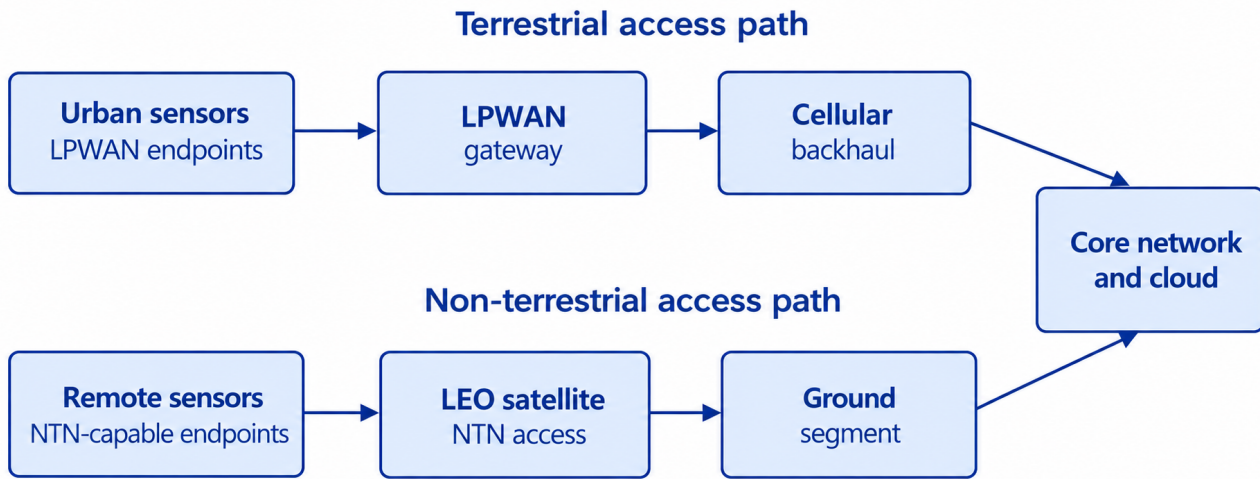


Figure 2: Hybrid Terrestrial and Satellite Connectivity Paths for Urban and Remote IoT

Quantitative evidence for the satellite path comes from simulation. A 2025 study of NB-IoT downlinks over LEO constellations at altitudes of 600 km and 1,200 km, with 24 to 60 satellites and antenna apertures of 0.4, 1, and 2 m, defined the minimum guaranteed link availability as the lowest availability observed among all end devices in the distribution region [22]. For 60 satellites at 1,200 km with 0.4 m apertures, every end device kept a valid link for at least about 30% of the 2 h simulated period, compared with 7.9% at 600 km, which is almost four times longer [22]. Physical-layer downlink rates were compared with the experienced data rate of 2 kb/s in 3GPP TS 22.261, which is defined at the application layer, and a physical-layer threshold of 3.5 kb/s was adopted to allow for protocol overhead. For the same 1,200 km configuration, 65.2% of end devices reached or exceeded 3.5 kb/s, compared with 24.4% at 600 km with 60 satellites [22]. Link availability and bit rate are therefore separate constraints, because the rates were evaluated whenever a link was available. Intermittent availability favors delay-tolerant, low-rate reporting over continuous control, and the result is a simulation outcome and not a field measurement.

4.4 Sixth-Generation Networks

Sixth-generation networks remain at an early research stage. The growth of mobile traffic expected until 2030 and the envisioned smart city use cases are reported to exceed the capabilities for which 5G was designed, and 6G is expected to meet requirements that include ultra-low latency, ubiquitous coverage, high data rates, device density, capacity, energy efficiency, and reliability [16]. The same study lists network security, data privacy, interoperability, and the digital divide among the concerns that remain to be addressed [16]. Because 6G standards are still under development, performance expectations for this technology are projections and not evidence from deployed systems.

5 EDGE COMPUTING, FOG COMPUTING, AND DIGITAL TWINS

Centralized cloud computing has inherent limitations of high latency, no context awareness, and no support for mobility, which constrain its use in real-time smart city applications, whereas edge computing extends cloud resources to the network edge and offers context awareness, low latency, mobility support, and scalability [5]. Edge and fog computing therefore place computation closer to data sources [23, 24, 10]. Fog computing was proposed as a highly virtualized platform that provides compute, storage, and networking services between end devices and cloud data centers, and its defining characteristics include low latency, wide geographic distribution, mobility support, a very large number of nodes, predominant wireless access, and heterogeneity [9].

The cloud, fog, and edge models are not mutually exclusive [6]. The cloud offers large computing and storage capacity and a central management platform, but transmitting all data to it increases network traffic and latency. Fog nodes hold local context and can aggregate data and make decisions that reduce the information flow toward the cloud. Edge devices process data at the level of the sensors themselves and therefore decide fastest on local state, but have the least capability [6].

Reported practice follows this division only partly. In a review of artificial intelligence applications for smart cities, most city service applications, such as air quality monitoring, sewer monitoring, and waste collection, were proposed as cloud systems, because data are gathered from nodes distributed across a city [6]. Edge-based designs were suggested for household load forecasting, including one that trains a recurrent neural network with federated learning, and for smart grid monitoring, where edge processing reduces delay [6]. In an agricultural comparison of edge and cloud systems for outlier detection, the cloud implementation performed much better, although the edge system showed potential for highly responsive analytics [6].

5.1 Computation Offloading

Offloading moves a task from a resource-limited device to a more capable node. A decision may result in local execution, full offloading of the whole computation, or partial offloading, in which one part of the computation is processed locally and the rest is offloaded [25]. The decision depends on user preferences, radio and backhaul connection quality, device capabilities, and the capabilities and availability of the remote resources [25]. Whether a task is executed locally, offloaded to an edge or cloudlet server, or offloaded further to a remote cloud affects latency and energy consumption in IoT networks [10]. When the components of an application depend on one another, components that need input from others cannot always be offloaded in parallel, and the dependencies can be expressed by a component dependency graph or a call graph [25].

The model below is intentionally simplified. It considers a single task, fixed effective processing and uplink rates, equal computational work at both sites, and negligible queuing and orchestration overhead, and it ignores task dependencies. Its purpose is to illustrate the delay and energy trade-off and not to provide a deployment-ready scheduling algorithm. **Table 3** lists the symbols.

Table 3: Notation Used in the Offloading Model

Symbol	Meaning	Unit
T_{off}	Delay of an offloaded task	s
$T_{\text{tx}}, T_{\text{rx}}$	Uplink transmission time and time to return the result	s
T_{proc}	Processing time at the edge node	s
T_{loc}	Local execution time at the device	s
C	Task workload	cycles
D	Input data size	bits
R, R_{min}	Uplink rate and break-even uplink rate	b/s
f_d, f_e	Processing rates of the device and the edge node	cycles/s
$P_c, P_{\text{tx}}, P_{\text{idle}}, P_{\text{rx}}$	Device power during local computation, transmission, idle waiting, and reception	W
$E_{\text{loc}}, E_{\text{off}}$	Device energy for local execution and for offloading	J

The execution delay of an offloaded task consists of the transmission duration of the offloaded data, the processing time at the edge server, and the time spent receiving the processed result, and offloading reduces the delay when local execution takes longer [25]. Following this decomposition, as shown in **Equation 1**, the delay of an offloaded task is

$$T_{\text{off}} = T_{\text{tx}} + T_{\text{proc}} + T_{\text{rx}}. \quad (1)$$

For a task of C processor cycles and D input bits, with uplink rate R in bits per second and processing rates f_d at the device and f_e at the edge node in cycles per second, the simplest closed forms, as shown in **Equation 2**, are

$$T_{\text{loc}} = \frac{C}{f_d}, \quad T_{\text{tx}} = \frac{D}{R}, \quad T_{\text{proc}} = \frac{C}{f_e}. \quad (2)$$

Offloading reduces delay when $T_{\text{off}} < T_{\text{loc}}$. If T_{rx} is neglected, this condition, as shown in **Equation 3**, becomes

$$\frac{D}{R} < C \left(\frac{1}{f_d} - \frac{1}{f_e} \right). \quad (3)$$

Equivalently, when $f_e > f_d$, the criterion defines a break-even uplink rate, as shown in **Equation 4**, above which offloading reduces delay:

$$R > R_{\min} = \frac{D f_d f_e}{C (f_e - f_d)}. \quad (4)$$

Equation 1 follows the decomposition reported in [25]. The closed forms in **Equation 2** and the criterion in **Equation 3** are first-order specializations adapted here for illustration, the criterion follows by substituting the closed forms into the inequality $T_{\text{off}} < T_{\text{loc}}$, and **Equation 4** is its algebraic rearrangement. The right-hand side of **Equation 3** is positive only if $f_e > f_d$. Offloading is favored by high link rates, capable edge nodes, and computation-heavy tasks with small input data, whereas large input data and weak links favor local execution. Local execution is also the outcome when edge resources are unavailable or when offloading does not pay off [25].

The delay criterion does not establish an energy benefit. For a battery-powered device, the energy of offloading consists of the energy spent to transmit the offloaded data and to receive the result [25], and the energy spent while the device waits for the edge node can be added. As shown in **Equation 5**, the device energy for local execution and for offloading is

$$E_{\text{loc}} = P_c T_{\text{loc}}, \quad E_{\text{off}} = P_{\text{tx}} T_{\text{tx}} + P_{\text{idle}} T_{\text{proc}} + P_{\text{rx}} T_{\text{rx}}, \quad (5)$$

and offloading saves device energy when $E_{\text{off}} < E_{\text{loc}}$. The transmit and receive terms follow the energy components described in [25], whereas the power-times-time form and the idle term are first-order assumptions of this survey. A decision that minimizes delay does not necessarily minimize energy, because the energy needed to transmit and receive the data can exceed the energy of local execution, and the device then executes locally, as in the energy-based decision example of [25]. Offloading for an energy-constrained device is therefore evaluated against both **Equation 3** and **Equation 5**.

Integration of edge computing with IoT systems has been reported to reduce latency through edge caching and data preprocessing and to reduce transmission energy by filtering and aggregating data before the data reach the cloud, whereas the heterogeneity of edge devices, variable network conditions, and resource constraints limit the uniform application of such techniques [26]. The study reports these findings qualitatively, so no numerical effect size is attributed to it here.

5.2 Digital Twins for Smart Cities

A digital twin maintains a continuously updated virtual representation of a physical asset. Digital twins have received considerable attention in industrial IoT, whereas their use in smart cities has been less common, and it has been argued that city twins should be treated differently and considered cyber-physical systems of systems because of their size and complexity [11]. Urban planning is reported as the most popular use case of city-scale twins, the use of twins in waste management appears almost nonexistent, and standardization, scale, security, and privacy remain open issues [11]. A systematic review of 64 peer-reviewed studies on urban digital twins, IoT, and artificial intelligence classifies urban digital twin applications into traffic management, urban planning, environmental monitoring, energy systems, and public services, and lists semantic interoperability, predictive modeling, data privacy, and impact evaluation among the persistent challenges [17]. A 2025 review of digital twin applications in urban mobility examines their use for predictive analytics, scenario evaluation, and decision support, and identifies key implementation challenges [18]. Time synchronization between digital twins and their physical counterparts has also been identified as a significant challenge in edge-enabled data centers for smart cities [27].

Architectures built on the edge-cloud continuum have been proposed. A modular architecture with six subsystems for edge, data management, digital twin, event management, resource management, and system management functions was demonstrated for traffic management in Issy-les-Moulineaux, France [12]. Data are stored in an NGSI-LD context broker,

events are exchanged through Apache Kafka, containers are orchestrated across edge and cloud, and a long short-term memory (LSTM) network trained on seven months of data predicts traffic intensity [12]. Sensing was simulated through the Google Distance Matrix API and not measured by deployed sensors [12]. The event management subsystem can adjust the data update interval to balance prediction accuracy against communication cost [12].

6 SECURITY, PRIVACY, AND BLOCKCHAIN-BASED SOLUTIONS

6.1 Threats and Countermeasures

The distributed and heterogeneous nature of smart city IoT creates a broad attack surface. IoT, cloud computing, and wireless communication are among the technologies raising security concerns, and attackers exploit vulnerabilities in hardware, software, and communication layers [13]. Typical security schemes may be less effective for smart city IoT, so new methods need to be developed [6]. **Table 4** summarizes the layer-wise issues and countermeasures reported in [6], extended with a classification of each countermeasure by control type and an indication of its residual limitation. The classification and the residual limitations are interpretations by this survey and not statements of the source.

Table 4: Security Issues and Countermeasures by Layer

Layer	Threat	Countermeasure reported in [6]	Control type	Residual limitation
Application	Data injection and integrity violation	Data validation, limiting data access, query parameterization, penetration testing	Preventive and detective	Depends on the coverage of the validation rules
Network	Man-in-the-middle and eavesdropping	Cryptographic protocols, authenticated protocols such as TLS and WPA2, session timeouts	Preventive	Depends on correct deployment and key management
Network	Denial of service	Checking irregular data requests, for which AI has been shown useful	Detective	Detection alone does not remove capacity limits
Network	Spoofing	Cryptography, hybrid encryption, blockchain-based validation of data exchange and device authentication	Preventive	Keys must be provisioned on constrained devices
Perception	Tampering and jamming	Software policies that alert to missing or abnormal data	Detective	Interference is detected but not prevented
System wide	Data leakage	Data anonymization, minimization, and aggregation	Preventive	Sensor data may still indicate occupancy or identity

6.2 Machine Learning for Threat Detection

Learning-based detection has been applied to infected IoT devices in smart cities. A classification accuracy of 99.31% with a low false positive rate has been reported on the NSL-KDD benchmark dataset [28]. A benchmark result of this kind does not establish performance on live city traffic, and machine learning and deep learning solutions are reported not to be resistant to evasion techniques, which must be considered against intelligent attackers [13].

6.3 Blockchain

Blockchain has been proposed to address safety, authentication, and maintenance problems in IoT systems because of its decentralized nature, including in sustainability and smart government applications [29]. It is also reported among the countermeasures in **Table 4** for validating data exchange and device authentication [6], and its integration with IoT security has been investigated [30]. The security of a public blockchain depends on the hash computing power supporting the network, and attacks such as the 51% attack, eclipse attack, Sybil attack, and distributed denial of service have been described [31].

A ledger protects recorded data but not the truthfulness of data entering it. In a blockchain-based wastewater management framework, reward tokens are issued for wastewater reuse, which can encourage tampering with the sensor data on which

the tokens depend, and anomaly detection is therefore used to identify tampered inputs [32]. The reported evaluation of that framework is a simulation analysis [32]. Blockchain-based security concerns in edge computing have also been surveyed [33].

6.4 Privacy and Federated Learning

Smart city sensors continuously collect data that may expose the daily activities of residents, and anonymization that preserves the context of the measured task is therefore required so that decision making remains possible [6]. Traditional machine learning requires the migration of data from devices to a centralized location, which raises privacy concerns, whereas federated learning performs distributed learning on the device and has been recommended where privacy is of significant interest [5]. Retaining raw data locally reduces its exposure but is not by itself a privacy guarantee, and federated learning at the edge requires on-demand computational resources [5]. A 2025 survey of federated learning for urban sensing systems addresses inference attacks, poisoning attacks, and incentive mechanisms for participants while preserving privacy, which confirms that collaborative training introduces threats of its own [19]. Data anonymization, minimization, and aggregation are listed among the countermeasures against data leakage in **Table 4** [6]. A digital twin based approach using federated learning has been reported for pandemic response planning [11], and distributed intelligence for IoT-based smart cities has been surveyed in [20].

6.5 Governance and Public Trust

A survey of 829 residents of a city in northeastern Brazil, analyzed with structural equation modeling, measured the relationships between smart governance factors (transparency, collaboration, participation and partnership, communication, and accountability) and quality of life, and it reported intense and important relations among these constructs [34]. The study supports considering governance together with technical design. However, it measured perceived quality of life and not the acceptance of IoT sensing, and it covers a single city.

7 APPLICATION DOMAINS

IoT technologies support a broad range of smart city applications. **Table 5** summarizes the domains addressed in the reviewed literature, with representative technologies and the type of evidence reported.

Table 5: Application Domains of IoT in Smart Cities

Domain	Representative technologies and functions	Evidence type	Reference
Energy management	Smart meters and real-time consumption data; fog tier between smart grid and cloud tiers	Reviews and conceptual models	[6, 9, 5]
Transportation	Vehicle communication; smart traffic lights; 5G road asset detection; twin-based traffic prediction	Reviews, a conceptual use case, a field pilot, and a prototype with simulated sensing	[6, 9, 21, 12]
Waste management	Fill-level bin sensors with route planning; collection trucks as mobile sensing platforms	Service description, review, and a field pilot	[3, 6, 21]
Water and wastewater	Water quality and leak sensing; blockchain incentives with anomaly detection for wastewater reuse	Review and simulation analysis	[6, 32]
Environmental monitoring	Air quality, noise, carbon monoxide, temperature, humidity, and vibration sensing; air pollution monitoring for traffic planning	Proof-of-concept deployment and testbed platform	[3, 7]
Street lighting	Light intensity monitoring at street light poles; network-enabled LED street lighting	Proof-of-concept deployment and a reported city system	[3, 7]

In energy systems, smart grids transmit real-time power data to utilities, which allows prediction models to support the management of power generation and the integration of different energy sources [6]. Fog computing has been described as a

natural platform for smart grid services [9], and a three-tier reference model comprising smart grid, fog, and cloud tiers has been reported [5]. In transportation, vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-pedestrian communication make smart transportation systems possible [6]. A smart traffic light interacts locally with sensors that detect pedestrians and cyclists and measure the distance and speed of approaching vehicles, coordinates with neighboring lights, and sends clustered data to the cloud for global, long-term analytics [9]. The 5G pilot and the traffic digital twin discussed in Sections 4 and 5 belong to the same domain [21, 12].

Intelligent waste containers that detect the fill level and plan truck routes can reduce the cost of waste collection and improve the quality of recycling [3]. Waste collection trucks have also been used as mobile platforms for sensing road assets [21]. In water systems, sensors can provide continual updates on water quality and detect leaks [6], and a blockchain-based framework with anomaly detection has been proposed to encourage wastewater reuse [32]. In environmental monitoring, the Padova deployment collected carbon monoxide level, air temperature and humidity, vibrations, and noise [3], and the GreenIoT platform in Uppsala supports air pollution monitoring and traffic planning [7]. The Padova deployment also monitored public street lighting by measuring light intensity at each pole [3], and a network-enabled LED street lighting system in Amsterdam has been reported to reduce the energy consumption of the city [7].

8 CROSS-LAYER SYNTHESIS AND EVIDENCE ASSESSMENT

8.1 Cross-Layer Design Framework

The preceding sections treat architecture, connectivity, computation, digital twins, and security separately, although a decision in one constrains the others. **Figure 3** outlines a conceptual decision framework synthesized from the reviewed literature that orders these decisions. It is not a validated optimization procedure. The first step defines service requirements: coverage, latency, reliability, energy budget, and data sensitivity. The second step selects connectivity among LPWAN, cellular, short-range, and non-terrestrial options according to capacity, availability, and deployment cost. The third step places computation on the device, edge, fog, or cloud, weighing transmission against processing as formalized for delay in **Equation 3** and for device energy in **Equation 5**. The fourth step configures data and digital twin functions, namely sampling, synchronization, fidelity, interoperability, and model uncertainty. Security, privacy, governance, and lifecycle cost apply to every decision, and choices are evaluated against application-specific metrics and revised using observed performance.

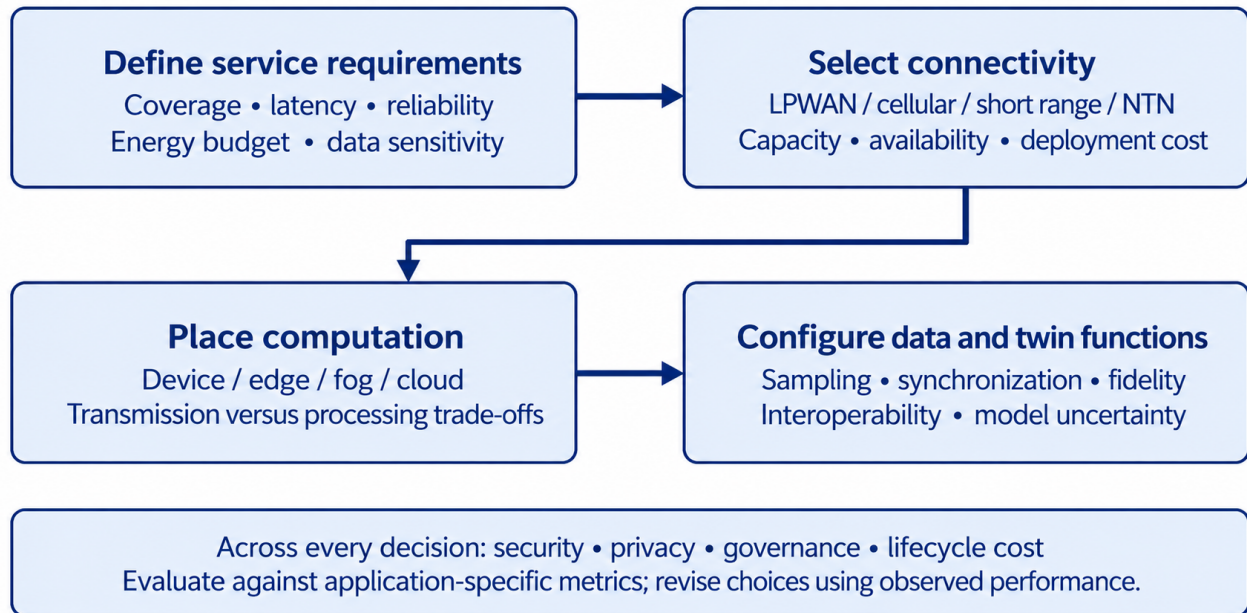


Figure 3: Conceptual Cross-Layer Design Framework for IoT-Enabled Smart Cities

Table 6 instantiates the framework for representative requirement classes and uses only findings reported in the reviewed studies. Cells marked as not addressed indicate that the reviewed studies do not cover that combination.

Table 6: Cross-Layer Design Implications for Representative Requirement Classes

Requirement class		Connectivity	Computation placement	Twin and data	Security and governance
Massive sensing	low-rate	LPWAN with low data rate and long range [6, 1]	Aggregation at fog or edge nodes reduces the information sent to the cloud [6]	Longer update intervals reduce communication cost but raise prediction error in one study [12]	Typical security schemes may be less effective; data minimization is listed against leakage [6]
Latency-sensitive control		Cellular links; measured 5G performance varied in a field pilot [21]	Local processing at fog nodes, as in smart traffic lights [9]	Twin and physical system synchronization is a significant challenge [27]	Denial of service is a reported network-layer threat [6]
Bandwidth-intensive sensing		5G supported mobile video streaming with significant variation [21]	Edge servers address cloud latency and lack of context awareness [5]	Not addressed in the reviewed studies	Migrating raw data to a central location raises privacy concerns [5]
Remote or underserved areas		LPWAN with 5G backhaul or with LEO satellites [8]; a simulated minimum link availability of about 30% for the best LEO configuration [22]	Filtering and aggregation at the edge reduce data sent to the cloud [26]	Not addressed in the reviewed studies	Endogenous security is examined for 5G and LPWAN-IoT [8]
City-wide twins and cross-department services		Heterogeneous devices connected through an edge subsystem [12]	Container orchestration across edge and cloud [12]	NGSI-LD context broker; standardization remains open [12, 11]	Governance factors relate to quality of life [34]; open interfaces avoid vendor lock-in [7]

8.2 Applying the Framework

Two scenarios assembled from the findings cited above illustrate the use of the framework. Both are constructed illustrations and not evaluated deployments.

The first scenario is citywide environmental monitoring. The Padova deployment showed street light poles carrying nodes that measured carbon monoxide level, air temperature and humidity, vibrations, and noise and reported through a gateway to the municipal network [3]. The requirement is periodic, low-volume reporting from many fixed nodes that may depend on batteries or small solar panels [7]. The reported LPWAN data rates of 10 b/s to 250 kb/s and ranges of 1 to 50 km in **Table 2** match this requirement, whereas Wi-Fi and Zigbee ranges do not cover wide-area sensing. Aggregation at fog or edge nodes reduces the information sent to the cloud [6], and the digital twin update interval balances prediction accuracy against communication cost [12]. Data minimization limits leakage of information about residents [6]. If the service later requires real-time alerts, the connectivity, placement, and update interval must be reassessed together, because a latency requirement affects all three.

The second scenario is leak detection in water networks beyond terrestrial coverage. Sensors can provide continual updates on water quality and detect leaks [6], and LPWAN combined with LEO satellites has been advocated for connectivity in remote areas [8]. In simulation, the best LEO NB-IoT configuration guaranteed a minimum link availability of about 30% of the simulated period [22], so delay-tolerant, low-rate reports suit this path better than continuous control. Filtering at the edge reduces the data sent over the satellite link [26]. Because a ledger cannot verify the truthfulness of recorded readings, sensor integrity relies on anomaly detection and not on the ledger alone [32].

8.3 Evidence Assessment

Table 7 classifies the representative quantitative studies cited in this survey by evidence type. Values are reported as stated by the sources.

Three observations follow from **Table 7**. First, among the quantitative studies listed, only the 5G evaluation reports measurements from a field deployment, and that pilot comprised 11 trucks over six months. Second, the satellite connectivity, digital twin, wastewater, and intrusion detection results derive from a constellation simulation, simulated

Table 7: Evidence Type of Representative Quantitative Studies

Reference	Evidence type	Setting	Reported outcome	Limitation
[21]	Field pilot	11 waste collection trucks, six months, road asset detection	5G supports mobile video streaming; significant performance variation	Single pilot application
[22]	Simulation	LEO NB-IoT downlink at 600 km and 1,200 km; 24 to 60 satellites; apertures of 0.4, 1, and 2 m; 2 h period	Best case (1,200 km, 60 satellites, 0.4 m): minimum link availability of about 30% versus 7.9% at 600 km; 65.2% of devices above 3.5 kb/s versus 24.4% at 600 km	Simulation only; no field measurement; physical-layer rates
[12]	Prototype with simulated sensing	Traffic prediction in Issy-les-Moulineaux; LSTM trained on seven months of data	MAE of 0.154 at 1 h and 0.744 at 6 h update intervals	Simulated sensing; units not stated
[28]	Benchmark dataset evaluation	NSL-KDD dataset	Accuracy of 99.31% with a low false positive rate	Benchmark data; live city traffic not evaluated
[32]	Conceptual framework with simulation analysis	Wastewater reuse incentives with anomaly detection	Recycling rate of 96.3% and increased reuse of 90.8% in simulation	Simulation only
[34]	Population survey	829 residents of a city in northeastern Brazil; structural equation modeling	Intense and important relations between governance factors and quality of life	Single city; perceived quality of life
[27]	Analysis	Digital twins for edge-enabled data centers	Time synchronization identified as a significant challenge	Analysis of challenges, not a deployment
[6, 1, 5, 10, 8, 11, 16, 17, 15, 18, 19]	Literature reviews	Published studies	Synthesis of reported results	No independent measurements

sensing, a simulation analysis, and a benchmark dataset, respectively. Third, the reviews synthesize reported results without independent measurements. Quantitative figures from different studies should therefore not be compared directly, because the studies differ in setting, metric definition, and evaluation type.

9 OPEN CHALLENGES

The reviewed literature points to several interrelated barriers that continue to limit large-scale deployment and the long-term sustainability of IoT-enabled smart cities. Interoperability remains a persistent concern because heterogeneous technologies are often difficult to combine [3]. Proprietary, vertically integrated systems further restrict the use of equipment and services from different vendors [7], while standardization remains unresolved for city-scale digital twins [11].

Energy efficiency presents a related constraint. Many sensing devices rely on batteries or small solar panels and therefore require power-efficient communication protocols [7]. Edge processing can reduce the computational burden on energy-constrained nodes [10], but the diversity of edge devices makes uniform optimization difficult [26]. Moreover,

offloading a task to minimize delay does not necessarily minimize energy consumption [25].

Scalability and latency also remain difficult to balance. City-scale digital twins face open questions of scale [11], while centralized cloud processing can introduce high latency [5]. Maintaining synchronization between digital twins and their physical counterparts is another significant challenge [27]. Connectivity adds further complexity: field measurements of 5G show considerable performance variation, and population coverage remains limited [21]. These limitations have encouraged interest in hybrid and satellite-assisted connectivity [8], although simulated LEO constellations still provide limited link availability [22].

Security and privacy concerns compound these technical challenges. Conventional security mechanisms may not be sufficient for smart-city IoT environments [6], and learning-based defenses can be evaded by adaptive attackers [13]. A blockchain ledger can protect recorded data, but it cannot verify the accuracy of the data entered into it [32]. Similarly, federated learning reduces raw-data exposure but remains vulnerable to inference and poisoning attacks [19].

Governance and public participation are equally important. Evidence suggests that governance factors are associated with residents' perceived quality of life [34], while the involvement of multiple communities is a defining feature of city-scale digital twins [11]. Finally, the evidence base itself remains limited: most quantitative findings in the reviewed studies come from simulations, benchmark datasets, or individual pilots rather than long-term operational deployments, as discussed in Section 8.3.

10 FUTURE RESEARCH DIRECTIONS

Six research directions follow from these challenges.

1. *Hybrid terrestrial and satellite connectivity.* Combining 5G backhaul, LPWAN access, and LEO satellite links offers a path to ubiquitous coverage in urban and remote areas [8]. Field evaluations beyond single pilots and beyond simulation are needed [21, 22].
2. *Federated learning and edge intelligence.* Federated learning at the edge has been recommended for resource management and privacy-sensitive applications [5], and decentralized deployments have been suggested to improve reliability [6]. Its privacy properties and its exposure to inference and poisoning attacks require explicit evaluation [19].
3. *6G-enabled real-time urban control.* Continued 6G development is expected to address the latency, density, and reliability requirements of smart cities, while security, privacy, interoperability, and the digital divide remain concerns [16].
4. *Selectively applied distributed ledgers.* The security of public blockchains depends on hash computing power [31], and a ledger cannot verify its inputs [32]. Restricting ledger use to integrity-critical data flows follows from these two limitations, and blockchain-related security concerns in edge computing require further study [33].
5. *Standardized, sensor-driven digital twins.* Open data models, adaptive update intervals, and deployments with measured sensing address the standardization and scale issues of city twins [12, 11, 18].
6. *Citizen-centered governance.* Research that connects governance factors to the acceptance of IoT sensing is needed, since existing evidence concerns perceived quality of life [34].

11 LIMITATIONS OF THIS SURVEY

Several limitations apply to the findings. First, this survey is a qualitative narrative synthesis and not a systematic review conducted under a registered protocol, so it includes no formal risk-of-bias assessment or quantitative meta-analysis. Second, the literature search concentrated on studies indexed by IEEE Xplore, ScienceDirect, SpringerLink, and MDPI and on publications in English, so work published elsewhere or in other languages may be underrepresented, and search dates and screening counts were not recorded. Third, the communication values in **Table 2** are compiled from secondary surveys and not from primary standards, and the sources differ. Fourth, quantitative values drawn from individual studies are reported as presented in the original sources and have not been independently validated. Fifth, several of the cited studies rely on simulated sensing, simulation-only evaluation, or benchmark data, which limits generalization to operational deployments. Sixth, the scope statements in **Table 1** are based on the topics stated by each source and do not assert that a topic is absent from its full text. Seventh, the offloading model in **Equations 1 to 5** is a first-order illustration that ignores queuing, task dependencies, and edge congestion. Finally, the conceptual framework in **Figure 3** and the control classification in **Table 4** are interpretations by this survey and have not been validated empirically. These constraints are common to narrative surveys in rapidly evolving technical fields.

12 CONCLUSION

This survey reviewed IoT-enabled smart cities across layered architectures, connectivity, edge and fog computing, digital twins, security and privacy, and application domains, and it organized the findings in a conceptual cross-layer decision framework. The literature indicates that no single connectivity technology meets all urban requirements and that hybrid combinations of LPWAN, cellular, and satellite links are being explored, although in simulation the best LEO NB-IoT configuration guaranteed a minimum link availability of only about 30% of the simulated period. Computation is distributed across device, edge and fog, and cloud tiers, and the delay and energy conditions in **Equation 3** and **Equation 5** illustrate how link rate, processing capability, and device power determine whether offloading is beneficial. City-scale digital twins remain concentrated in urban planning, and security mechanisms require attention to the truthfulness of recorded data, to the evasion of learning-based defenses, and to the inference and poisoning threats that accompany federated learning. A classification of the evidence shows that most quantitative results come from simulations, benchmarks, or single pilots. Interoperability, energy efficiency, scalability, connectivity reliability, and governance remain only partially resolved. Future progress depends on coordinated development of hybrid connectivity, federated edge intelligence, selectively applied ledgers, standardized sensor-driven digital twins, and citizen-centered governance, evaluated in operational deployments.

AUTHOR CONTRIBUTION STATEMENT

All authors contributed to the conceptualization, literature analysis, writing, and revision of the manuscript and approved its final version.

ETHICS APPROVAL AND CONSENT TO PARTICIPATE

Not applicable. This study did not involve human participants or animals.

CONSENT FOR PUBLICATION

Not applicable.

DATA AVAILABILITY

No datasets were generated or analyzed in this study. This work is a review of publicly available literature.

ACKNOWLEDGMENTS

The authors acknowledge the use of OpenAI's ChatGPT for assistance with manuscript refinement.

FUNDING

No Funding.

DISCLOSURE STATEMENT

The authors declare no conflict of interest.

REFERENCES

- [1] I. Rafiq, A. Mahmood, S. Razzaq, S. H. M. Jafri, and I. Aziz, "IoT applications and challenges in smart cities and services," *The Journal of Engineering*, vol. 2023, no. 4, p. e12262, 2023.

- [2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
- [3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.
- [4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.
- [5] L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang, and C. S. Hong, "Edge-computing-enabled smart cities: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10200–10232, 2020.
- [6] A. S. Syed, D. Sierra-Sosa, A. Kumar, and A. Elmaghraby, "Iot in smart cities: A survey of technologies, practices and challenges," *Smart Cities*, vol. 4, no. 2, pp. 429–475, 2021.
- [7] B. Ahlgren, M. Hidell, and E. C.-H. Ngai, "Internet of things for smart cities: Interoperability and open data," *IEEE Internet Computing*, vol. 20, no. 6, pp. 52–56, 2016.
- [8] E. U. Ogbodo, A. M. Abu-Mahfouz, and A. M. Kurien, "A survey on 5g and lpwan-iot for improved smart cities and remote area applications: From the aspect of architecture and security," *Sensors*, vol. 22, no. 16, 2022.
- [9] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, MCC '12, (New York, NY, USA), pp. 13–16, Association for Computing Machinery, 2012.
- [10] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the internet of things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018.
- [11] G. Mylonas, A. Kalogeras, G. Kalogeras, C. Anagnostopoulos, C. Alexakos, and L. Muñoz, "Digital twins from smart manufacturing to smart cities: A survey," *IEEE Access*, vol. 9, pp. 143222–143249, 2021.
- [12] M. Herath, M. Alvi, R. Minerva, H. Dutta, N. Crespi, and S. M. Raza, "Smart city digital twins: A modular and adaptive architecture for real-time data-driven urban management," in *2024 20th International Conference on Network and Service Management (CNSM)*, pp. 1–7, 2024.
- [13] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333, 2023.
- [14] R. Kaur, J. Singh, S. Kaur, and V. Malhotra, "Iot in smart cities: Review of iot architecture for smart cities, applications, and key challenges," in *Beyond Artificial Intelligence* (B. Soni, P. Saini, G. K. Verma, and B. B. Gupta, eds.), (Singapore), pp. 497–510, Springer Nature Singapore, 2025.
- [15] A. A. Zakaria, T. Amr, and A. A. Ragheb, "Iot in smart urban planning: A comprehensive review of applications, developments, and engineering perspectives," *IEEE Access*, vol. 13, pp. 135316–135335, 2025.
- [16] S. Sharma, R. Popli, S. Singh, G. Chhabra, G. S. Saini, M. Singh, A. Sandhu, A. Sharma, and R. Kumar, "The role of 6g technologies in advancing smart city applications: Opportunities and challenges," *Sustainability*, vol. 16, no. 16, 2024.
- [17] E. J. Sacoto-Cabrera, A. Perez-Torres, L. Tello-Oquendo, and M. Cerrada, "Iot, ai, and digital twins in smart cities: A systematic review for a thematic mapping and research agenda," *Smart Cities*, vol. 8, no. 5, 2025.
- [18] G. Torrao, J.-P. Virtanen, and E. Volanen, "Exploring digital twins for urban mobility: Applications and the case study of helsinki," in *2025 International Workshop on Intelligent Systems (IWIS)*, pp. 1–7, 2025.
- [19] A. Kapoor and D. Kumar, "Federated learning for urban sensing systems: A comprehensive survey on attacks, defences, incentive mechanisms, and applications," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 2, pp. 1293–1325, 2025.
- [20] I. A. Hashem, A. Siddiqua, F. A. Alaba, M. Bilal, and S. M. Alhashmi, "Distributed intelligence for IoT-based smart cities: a survey," *Neural Computing and Applications*, vol. 36, no. 27, pp. 16621–16656, 2024.
- [21] A. Banerjee, B. Costa, A. R. M. Forkan, Y.-B. Kang, F. Marti, C. McCarthy, H. Ghaderi, D. Georgakopoulos, and P. P. Jayaraman, "5g enabled smart cities: A real-world evaluation and analysis of 5g using a pilot smart city application," *Internet of Things*, vol. 28, p. 101326, 2024.

- [22] T. D. Le, M. Stusek, R. Dvorak, P. Palurik, P. Masek, D. Moltchanov, and J. Hosek, "Downlink coverage and bit rate performance of leo-based non-terrestrial networks for nb-iot," in *2025 17th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pp. 80–86, 2025.
- [23] W. Shi and S. Dustdar, "The promise of edge computing," *Computer*, vol. 49, no. 5, pp. 78–81, 2016.
- [24] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.
- [25] P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1628–1656, 2017.
- [26] R. R. Asaad, A. A. Hani, A. B. Sallow, S. M. Abdulrahman, H. B. Ahmad, and R. M. Subhi, "A development of edge computing method in integration with iot system for optimizing and to produce energy efficiency system," in *2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 835–840, 2024.
- [27] S. Rinaldi, S. D. Iacono, P. Bellagente, and M. Pasetti, "Analysis of time synchronization challenges in digital twins for edge-enabled data centers in smart cities scenario," in *2025 33rd Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP)*, pp. 506–511, 2025.
- [28] M. Houichi, F. Jaidi, and A. Bouhoula, "A systematic approach for iot cyber-attacks detection in smart cities using machine learning techniques," in *Advanced Information Networking and Applications* (L. Barolli, I. Woungang, and T. Enokido, eds.), (Cham), pp. 215–228, Springer International Publishing, 2021.
- [29] A. J. Obaid and M. A. Alkhafaji, "Security and privacy for iot-based blockchain technology: Review, solutions, and challenges," in *Intelligent Systems* (S. Kumar Udgata, S. Sethi, G. Ghinea, and S. K. Kuanar, eds.), (Singapore), pp. 299–313, Springer Nature Singapore, 2025.
- [30] H. Abu-tarboush, J. H. Lee, M. Al-shrouf, N. O. Maaitah, and N. A. Al-Dmour, "Blockchain and its integration with iot security," in *2024 2nd International Conference on Cyber Resilience (ICCR)*, pp. 1–4, 2024.
- [31] S. Aggarwal and N. Kumar, "Chapter twenty - attacks on blockchain working model.," in *The Blockchain Technology for Secure and Smart Applications across Industry Verticals* (S. Aggarwal, N. Kumar, and P. Raj, eds.), vol. 121 of *Advances in Computers*, pp. 399–410, Elsevier, 2021.
- [32] A. I. A. Alzahrani, S. H. Chauhdary, and A. A. Alshdadi, "Internet of things (iot)-based wastewater management in smart cities," *Electronics*, vol. 12, no. 12, 2023.
- [33] G. Archana, R. Goyal, and K. M. V. Madan Kumar, "A literature survey on block chain based security concerns in edge computing," in *2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, pp. 1–8, 2024.
- [34] J. C. F. De Guimarães, E. A. Severo, L. A. Felix Júnior, W. P. L. B. Da Costa, and F. T. Salmoria, "Governance and quality of life in smart cities: Towards sustainable development goals," *Journal of Cleaner Production*, vol. 253, p. 119926, 2020.