Societal Transformation: AI and Big Data Journal
Vol: 4(1): 62- 83, 2026
DOI:10.20547/aibd.264104

A Review of Internet of Things (IoT) in Smart Cities

Faizan[1], Syyeda Ayesha Jaffery[2]

Abstract

The rapid urbanisation is putting pressure on city infrastructures around the world, and the Internet of Things (IoT) is the main technological layer that municipalities are using to respond. However, the literature on IoT-enabled smart cities remains fragmented: architectural frameworks, application domain studies, and challenge analyses are usually reported in isolation, with little cross comparison to guide implementation decisions. This paper addresses that fragmentation through a structured review of 61 peer-reviewed studies (2022–2024, plus select foundational works from 2013–2019) from IEEE Xplore, Elsevier, and SpringerLink. A direct comparison of three dominant IoT architectural paradigms: layered, distributed (edge/fog), and service-oriented; on scalability, cost, security, and latency finds that layered designs are appropriate for smaller, budget constrained deployments, distributed designs are most appropriate for latency critical applications such as traffic control, and service-oriented designs provide the highest interoperability for large, multi-vendor municipal systems at a higher integration cost. The review further examines five application domains (transportation, energy, environmental monitoring, waste management, and public safety) and four recurring implementation barriers (security, interoperability, scalability, and cost), finding that security and interoperability are rated most severe yet least subject to independent, real-world evaluation once deployed at city scale. Finally, the paper synthesises five new avenues: edge intelligence, 5G integration, AI-driven predictive analytics, digital twins, and blockchain-based trust mechanisms and identifies standardised cross-city impact indicators as the most critical gap for future research. These findings offer urban planners an evidence-based basis for architecture decisions and indicate tangible targets for pushing IoT research beyond isolated proof-of-concept studies.

Keywords: *Internet of Things, Smart Cities, IoT architectures, Edge Computing, 5G, Digital Twins, Blockchain, Sensor Networks, Intelligent Systems, Urban Infrastructure*

[1] *Al Kawthar University, Karachi, Pakistan*[1]
[2] *Sync Technologies, Oman*

1. Introduction

Urbanisation has been a major challenge for cities over the last few years, with cities under increasing pressure from urbanisation-related infrastructure, resource and governance challenges [1, 2]. The smart city paradigm has thus become one of the most flexible ones for current urban management, fusing digital technologies with civic government to enhance the provision of services and citizen participation [3, 4].

One of the technologies that makes this feasible is the Internet of Things (IoT), which is the fundamental infrastructure layer that ties together sensors, devices, and municipal systems to create an integrated operating environment [5, 6].

The Internet of Things (IoT) is a network of interconnected devices that can exchange information with each other and communicate with limited human interaction [7]–[9]. In smart cities, IoT infrastructure allows the integration of existing urban infrastructure into systems that can collect, distribute, and react to real-time data [10, 11].

This change has been enabled by the decreasing cost of sensors, connectivity, and of-course, cloud services, allowing the deployment of IoT in the city to be more feasible for cities with budget constraints [12, 13]. However, the value of these systems will largely depend on ongoing investments in system integration, maintenance, and governance [14].

This paper provides a structured literature review of the existing research on IoT in smart cities. The details of the review technique, such as the search approach and the selection of studies, are summarised in (Figure 1 and Figure 2), and detailed in (Section 2 and Section 3), presents an analytical comparative analysis of the three current IoT architectural frameworks. The principal application areas of IoT in the urban environment are discussed in (Section 4).

The primary problems for implementation are highlighted in (Section 5 and Section 6), and the emerging trends and future directions. The research gaps highlighted through the review are listed in (Section 7), while Section 8 concludes the paper.

2. Methodology

This section addresses the systematic search strategy, eligibility criteria, and research selection process used for this review, using a structure guided by the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) technique adapted for a narrative-synthesis review.

2.1 Search Strategy and Databases

Candidate studies were collected from three major publishing platforms: IEEE Xplore, Elsevier (ScienceDirect) and SpringerLink, using the search terms ("Internet of Things" OR "IoT") AND ("smart city" OR "urban infrastructure") AND ("architecture" OR "application" OR "challenge" OR "security"), limited to peer-reviewed journal articles and conference papers in English.

2.2 Inclusion and Exclusion Criteria

Table 1: Inclusion and Exclusion criteria applied during study selection.

Criterion	Inclusion	Exclusion
Publication type	Peer-reviewed journal or conference paper	Non-peer-reviewed articles, blogs, preprints without peer review
Language	English	Non-English without verified translation
Topical Scope	Directly addresses IoT architecture, application or implementation in an urban/smart city context	IoT studies unrelated to urban or municipal contexts
Publication date	Primarily 2022-2024, with earlier sources retained only where seminal to the field	Superseded studies with no distinct contribution once a more recent version exists

2.3 Study Selection Process and Corpus Composition

Titles and abstracts were first screened against the topical scope criterion, followed by a full-text eligibility assessment against the remaining criteria in Table 1. The composition of the resulting corpus is summarised in Figures 1 and 2 below.

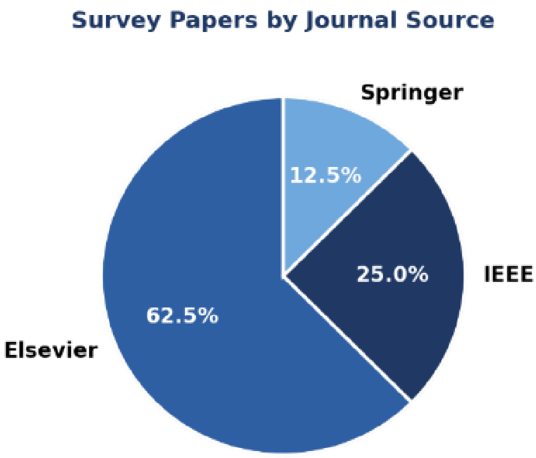

Fig. 1: Distribution of the reviewed survey papers by journal source.

As shown in Fig 1, Elsevier-indexed journals contributed the largest share of the reviewed corpus (62.5%), followed by IEEE (25%) and Springer (12.5%). This concentration reflects the strong representation of applied, sustainability-oriented smart city research with Elsevier's ScienceDirect platform, while IEEE contributed a comparatively larger share of the architecture and networking-focused studies discussed in Section 3).

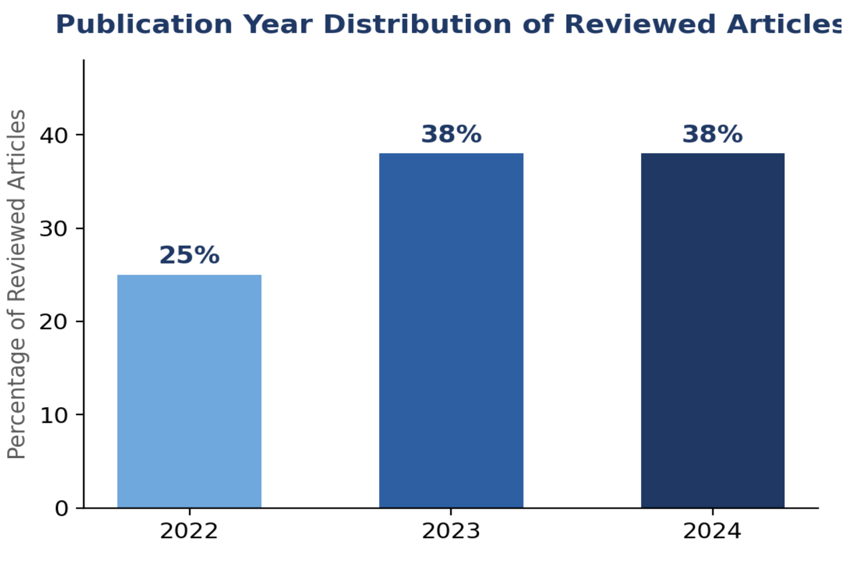

Fig. 2: Publication year distribution of the reviewed articles.

Fig 2 shows that the reviewed corpus is concentrated in recent literature: 38% of articles were published in 2024, 38% in 2023 and 25% in 2022, meaning the entire body of application- and challenge-focused evidence reviewed in (Section 3 and Section 6) is drawn from the three most recent publication years. A small number of earlier, foundational works fall outside the window.

They are cited only where they are widely recognized as seminal to the field: Gubbi et al. (2023) [15] and Zanella et al. (2014) [16] established the architectural vocabulary used throughout later literature, including this review, and are read alongside the more recent studies addressing the same theme rather than as standalone evidence of current practice.

The following are the research questions for this study:

- RQ 1: What are the existing architectures for smart cities?
- RQ 2: What are the potential applications for smart cities?
- RQ 3: What are the research challenges in the implementation of smart cities?
- RQ 4: What are the emerging trends and future directions?

3. IoT Architectures for Smart Cities (RQ1)

This section talks about the three IoT architectural paradigms most frequently discussed in the smart city literature: layered architecture, distributed computing architecture, and service-oriented architecture. Each is described in turn, followed by a comparative analysis in (Section 3 and 4).

3.1 Layered Architectural Framework

Layered IoT architecture structure the various part of a system into clearly defined levels of functionality: perception layer, network layer, and processing layer [1, 17]. In the perception layer, more and more multi-functional sensors are able to record several parameters of the environment at the same time [18].

The hybrid communication system configurations at the network layer are the integration of high-capacity cellular networks with low-power wide-area technologies, depending on the use cases [19].

Distributed computing is now the norm at the processing layer, where edge devices are used for real-time processing, and cloud resources for higher-order analytics and long-term storage [11].

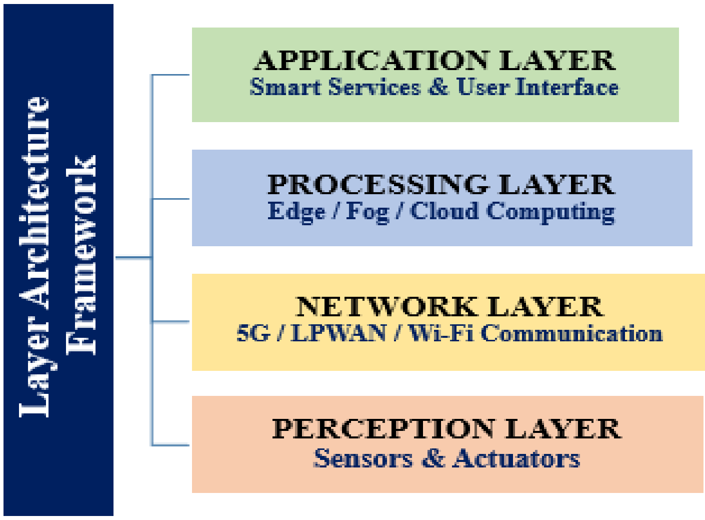

Fig. 3: Layered IoT architectural framework for smart cities, illustrating data flow from sensors to cloud

As shown in **Fig 3**, the layered framework illustrates a linear data flow from perceptive sensors, through the network layer, to processing infrastructure, and finally to the application layer that delivers smart services to end users. This structure is well suited to deployments where functional separation and modular upgrades are prioritized, but it can introduce latency at each transition between layers.

3.2 Distributed Computing Architecture

Due to the limitations of a centralized computing approach at city scale [20], [1], the distributed computing model has become the preferred model. Edge computing, in which data is processed at or near its source, minimizes latency so vital to applications like adaptive traffic signal control [12] and emergency response [2]. Fog computing further adopts this principle by introducing more processing nodes in urban areas in the midst of other cities, thereby allowing distributed control that spans a broader geographic area [13].

In many installations, the responsiveness afforded by the edge nodes is linked with the broader analytical context provided by cloud platforms, as well as the ability of the cloud platforms to enable city-wide resource optimization [5, 3].

The layers in Figure 3 depict the data stream, and the distributed computing model describes the processing strategy within the levels, where the processing is moved from the heart of the cloud to the edge and fog layers to decrease latency and network burden.

3.3 Service-Oriented Architecture

Recent implementations are increasingly based on service-oriented design ideas stressing modularity and interoperability [4]. Microservices architecture allows programs to be deconstructed into independent, self-contained parts that may be independently maintained and updated, interacting using standard APIs [6, 7].

Fig. 4: Service-oriented architecture (SOA) framework: People, Process, Platform, and Practice

Fig. 4 shows that, besides the technical design itself, successful service-oriented deployment has four interdependent dimensions: empowering decision-makers with accessible data (People), aligning IT systems with municipal business operations (Process), increasing operational efficiency through a shared platform (Platform), and adopting best-practice integration methodology (Practice). Containerisation provides steady, consistent performance across heterogeneous technology, and an API-led architecture allows third-party integration and controlled data sharing among municipal departments and vendors [8].

This design philosophy encourages collaboration and interoperability of disparate vendors' urban systems, helping to address one of the long-standing integration difficulties mentioned in (Section 5.2).

3.4 Comparative Analysis of Architectures

The literature tends to present each architecture in isolation, yet no single paradigm is suitable for all deployment circumstances. Table 2 compares the three designs along four criteria of interest to municipal decision-makers: scalability, relative cost, security posture, and latency.

Table 2: Comparative analysis of IoT architectural paradigms for smart city deployment.

Dimension	Layered	Distributed (Edge/Fog)	Service-oriented
Scalability	Moderate new tiers can bottleneck at scale	High processing distributed near source	High modular services scale independently
Relative cost	Lower initial cost, simpler to deploy	Higher (edge/fog hardware investment)	Higher (integration and API management overhead)
Security posture	Centralised control, single points of failure	Distributed attack surface, harder to secure uniformly	Strong access control via API gateways, but larger integration surface
Latency	Higher, due to sequential layer transitions	Lowest, processing near data source	Moderate. dependent on service orchestration
Best-fit context	Smaller municipalities, single-domain deployments	Latency-critical applications (traffic, emergency response)	Large, multi-vendor, multi-department deployments

The comparison concludes that layered architectures are still of use for cities with limited budget and limited scope for functionality. Where latency is operationally critical, a distributed architecture is more appropriate.

Moreover, where many independent municipal systems are to be integrated, the best solution in the longer term is a service-oriented architecture. However, this will come with more complexity for implementation, as further discussed in (Section 5.4).

4. IoT Applications in Smart City Sectors (RQ2)

This section talks about various applications of IoT. The IoT drives innovations across various sectors as summarized below in Figure 5. This includes traffic management, smart parking, public safety, waste management, utility management, remote monitoring, environmental well-being and public transport etc. These applications are discussed below in detail.

Fig. 5: Overview of IoT applications in smart cities

4.1 Intelligent Transportation Systems

The most common IoT application in cities is smart transportation [9]. Existing deployments combine sensor networks and multiple data streams for complete traffic management [10], and signal optimization predictive systems are proven to be effective in reducing congestion and anticipating it [1, 2].

The use of multiple sensor types in smart parking systems has been demonstrated to dramatically cut the time spent seeking parking, which in turn has led to a reduction in the number of vehicles utilizing the road and the accompanying emissions [3]. Demand-driven public transit, as seen in Figure 5 [4, 5], is enabled by real-time tracking and counting of passengers.

4.2 Energy Management Systems

IoT-monitored techniques optimize energy production, the energy supply and the energy consumption [6]–[8]. Real-time monitoring enables the dynamic balancing of grid loads with detailed consumption data, enabling sophisticated metering infrastructure to execute demand-response algorithms. Building management systems can be installed in residential and commercial buildings to provide measurable energy savings.

This is done by automatically altering the lighting, heating and cooling systems based on the environment and occupancy data collected via sensors. Similarly, the output of public lighting systems can be regulated automatically according to the ambient light and pedestrian recognition, leading to safety and efficiency [10]–[12].

4.3 Environmental Monitoring Networks

Multi-sensor environmental monitoring systems combine urban planning and public health data to give more detailed information on city conditions [13]. A dense network of air-quality sensors monitors the concentration of pollutants and alerts the public to take action to protect their health [14].

In operation, networked acoustic monitoring uses pattern recognition to identify significant sources of noise, and pressure and flow monitoring in water networks to prevent losses and leaks. Climate adaptation planning is assisted by urban microclimate monitoring and mapping of fine-spatial-resolution temperature and humidity data [16, 15].

4.4 Waste Management Optimization

In addition, by using connected sensors, the collection scheduling system can shift away from fixed schedules and become demand-responsive, still providing a good service level without collecting empty bins. Emissions are reduced, and overall sustainability is improved by route-planning algorithms which minimize unnecessary driving [23].

Adaptive smart-recycling systems may improve the recovery of recyclable materials with the help of feedback on sorting accuracy [24]. Sensors may be used for monitoring the organic waste processing process, which would improve the efficiency of the process and minimize negative effects on the environment [17]–[26].

4.5 Public Safety Enhancement

The benefits of linked devices for public safety are improved situational awareness and response time [18]. Acoustic detection systems complement rapid gunfire or fire detection and automatically report the incident to the police; intelligent surveillance systems integrate crowd analytics, license-plate recognition and privacy-preserving algorithms to aid urban surveillance [19]. Infrastructure monitoring systems help monitor structure deterioration and direct maintenance efforts to avoid failures during operation [1, 2], and early-warning systems for floods, earthquakes, and other disasters help to make the city more prepared [3]–[6].

Table 3: Reported statistical impact of IoT across application sectors [7]–[10].

Application Sector	*Key Metric*	*Reported Improvement*
Transportation	Congestion Reduction	12-25%
Energy	Energy Savings	30-50%
Waste	Cost Efficiency	30%
Environmental	Pollution Alert Response	20% faster response

The data shown in Table 3 are based on pilot deployments at the city level and simulation studies as described in [7]–[10]. The results show illustrative ranges reported across different urban contexts rather than a single, standardized measurement methodology. As such, comparability across cities should be treated with caution until more standardized, cross-city reporting frameworks become available.

5. Implementation Challenges and Limitations (RQ3)

This section talks about the challenges and limitation of IoT. IoT has great potential, but there are some problems with implementations. Things such as high initial deployment cost for a wide scale, lack of compatible structures, and interoperability between different systems all hinder IoT adoption. Also large integration of IoT in cities are limited due to poor regulation, lacking technology skills, and problems with data security, privacy and IoT systems not integrating. These challenges and limitations are discussed below in detail.

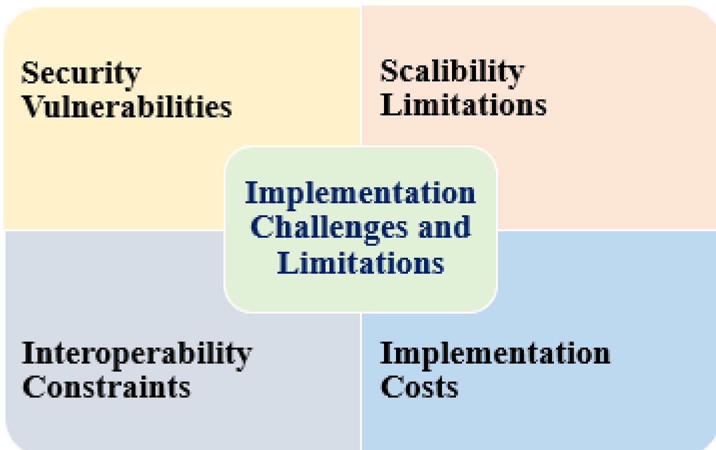

Fig. 6: Framework for addressing implementation challenges

5.1 Security Vulnerabilities

Many cyber-attacks can be made possible due to the broad use of IoT [1]. Devices are installed in large numbers and in distributed locations, communicating via a variety of protocols [2], many of which are resource-constrained, with limited computational power to implement complex security protocols and thus are susceptible to compromise [3].

Data being sent over public or unsecured networks is also susceptible to being captured, so there is a need for robust encryption and other safeguards [4].

Organisationally, security is also complicated. There can be many data governance stakeholders with different priorities and risk tolerances, including multiple municipal departments and private vendors [5].

Reported mitigation strategies (summarised in Table 5) are mainly related to encryption and access control. However, there is limited independent assessment of the effectiveness of these strategies once implemented at city-scale rather than in controlled trials.

5.2 Interoperability Constraints

The adoption of IoT technology in cities is often incremental, resulting in the creation of technological islands with limited cross-system integration [6, 7]. Translation gateways can be used to enable inter-system communication but contribute to complexity and create additional points of failure [8]. This is particularly problematic when deploying a new system on legacy infrastructure where the data structures and data representation are inconsistent and costly custom integration work is required. Although successful deployments such as the adoption of open frameworks such as FIWARE or OGC Sensor Things API exist to reduce silo-effects, the acceptance of standards is limited, and differences in system implementation are still considerable between applications, geographies and regulatory structures [9]–[11].

5.3 Scalability Limitations

Scaling to a city-wide roll-out is often a challenge when considering proof of concept deployments [12]. The processing power required to operate thousands of peripheral sensors grows with network capacity limits that are inherent in data-intensive applications. A high level of database engineering and query optimisation is required to exploit heterogeneous data sources to store and retrieve massive amounts of data efficiently [13].

With the growth of a system, the complexity also develops, which means that active devices have to be discovered and deleted, and still-operating devices have to be updated and balanced, with the need for compromises to avoid congested applications and services.

5.4 Implementation Costs

The deployment of IoT systems is still expensive, although sensors are becoming cheaper [16]. The cost of initial deployment, or the cost of the devices, installation, and supporting network infrastructure, is sometimes more than municipalities budget for.

The overall life cycle expense for infrastructure (maintenance, battery replacement, and ongoing upgrades) can also be significantly larger than originally projected when infrastructure is deployed, and is relatively excluded in initial budgeting [15].

Specialised technical skills are also required for continued operation, and cities must either develop such skills within their own city staff or bring them in from outside.

In selecting the kind of architecture, service-oriented or layered, the return on investment considerations should incorporate intangible benefits, such as citizen satisfaction, besides direct financial return.

As explained in (Section 3.4), service-oriented architectures generally involve higher integration costs compared to layered implementations.

Table 4: Protocol comparison for connectivity in constrained IoT deployments [23]–[25].

Protocol	*Range (km)*	*Power (mW)*	*Reliability (%)*
LoRaWAN	15	10	95
NB-IoT	10	20	97
5G	1-5	100	99

Table 5: Implementation challenges, reported severity, and mitigation strategies [17]–[18], [26].

Challenges	*Impact Metric*	*Severity Level (1-10)*	*Reported Mitigation*
Security	Breach incident	8	Encryption, access control [4]
Interoperability	Integration failures	7	Standardization frameworks [6]
Costs	Deployment expense	9	Phased ROI Planning [21]
Scalability	Device management limits	6	Edge Computing offload [12]

Table 5 shows that cost and security are rated as the most severe challenges in the reviewed literature. However, these are also the two areas in which reported mitigation methods are least frequently subjected to independent, comparative evaluation across multiple deployments, a gap discussed further in (Section 7).

6. Emerging Trends and Future Directions (RQ4)

This section talks about the emerging trends and future directions of IoT. To build smart cities, IoT systems should be continuously integrated with edge computing, analytics, AI and other linked technologies for predictive service are made possible for smart cities through the integration of edge computing and AI with IoT devices. These emerging and future directions are discussed below in details.

6.1 Edge Intelligence Development

The processing capability of the edge device is increasing, and increasingly complex decision-making is taken at the edge of the network [19, 20]. With simple sensors and new algorithms for basic pattern recognition, responsive action can be activated without the energy cost of constant communication with the cloud [1].

Collaborative processing enables machines in proximity to each other to share their workloads to provide more analytical capabilities than each would be able to produce alone [2]. Such advances will enable smart city subsystems to operate more independently and autonomously, and will reduce the transfer of important information to remote data centres, thus reducing privacy concerns [3, 4].

6.2 Advanced Connectivity Integration

Next-generation wireless networks can provide guarantees of the quality of service, and a huge number of devices are needed for smart city IoT [5]. Network slicing can provide dedicated bandwidth slices for mission-critical applications, whereas massive machine-type communications can be used to deal with high density of sensors in dense urban deployments [6].

Ultra-low latency provides real-time control of equipment that was not previously possible, and the sensing and communication technologies provided by devices can reduce the requirement for separate data transport infrastructure [7].

6.3 AI-Driven Analytics for Smart Cities

In recent years, machine learning has been applied to urban services. For municipal-scale IoT data, it is utilized in conjunction with predictive and adaptive services. This is because predictive analytics based on previous sensor information may forecast demand for services like traffic flow, energy load and trash creation, allowing for proactively rather than reactively managed services [9].

Anomaly detection algorithms that process the information of a sensor network can detect equipment problems, unusual use of the equipment or potential security attacks before they become a service failure [10].

ML will extend ML-driven optimization in the transportation and energy context in the domains of traffic routing, air quality forecasting, and emissions management across road and energy grids [11] and [12], adjusting traffic signal timing and grid load balancing in near real-time based on the real-time data collected from the sensors.

6.4 Implementation of Digital Twins

Virtual city models with live IoT data can allow more sophisticated planning and simulation capacity [13]. Scenario simulation can be used by planners to forecast the impact of planned interventions on the cross-system level before implementation. Predictive maintenance algorithms can be used to simulate wear patterns to schedule repairs optimally on infrastructure [14].

Constructive simulations of emergencies can be employed to train and improve the response strategy. Interactive digital twin models are increasingly being used to integrate community participation in the projected development [16].

6.5 Trust and Security Enhancement via Blockchain

Some issues in trust and security in smart city IoT deployments are solved by blockchain technologies [15]. Blockchain-based identity management can increase protection against device spoofing by controlling and monitoring onboarding, and a tamper-proof record can verify data integrity and aid in regulatory compliance [21].

A trustless and automated transaction between the systems can be facilitated by smart contracts, without human intervention, and privacy-enhancing methods like differential privacy and secure multi-party computation can be utilized to conduct analytics without revealing the underlying raw data [22, 23].

Fig. 7: Emerging trends and future direction in IoT

7. Discussion: Research Gaps and Future Research Directions

The results from the literature search in (Sections 3 to 6) highlight three common gaps in the existing literature. First, the comparative empirical assessment of architectural paradigms is limited: many studies describe one architecture, few describe architectures in parallel, and guidance available to municipal decision-makers on the trade-offs summarised in Table 2 is limited.

Second, the reported statistical outcomes of IoT usage (Table 3) are derived from pilots at different city levels and with various methods of measuring outcomes, which makes comparisons and meta-analysis across cities difficult; uniform and standardised reporting frameworks for outcomes of smart city IoT adoption would greatly facilitate future reviews.

Third, security and implementation cost are always considered as major issues (Table 5), and mitigation strategies verified primarily in control or simulated environments are not yet completely evaluated in the field.

The identified gaps suggest three future research directions:
(1) comparative multi-city empirical studies to assess security and interoperability challenges and architectural trade-offs across common scenarios;
(2) the development of standardized metrics and reporting practices for evaluating the impact of IoT in a wide range of transportation, energy, waste, and environmental applications beyond proof-of-concept demonstrations; and
(3) real-world evaluation of security and interoperability mitigation techniques, including blockchain-based and privacy-preserving approaches discussed in Section 6.5, in addition to proof-of-concept demonstrations.

8. Conclusion

The present research aims to explore the literature on the role of IoT technologies for smart city development, including four categories of smart city: architecture, application, obstacles to implementation, and new trends.

As shown in the comparative analysis in Section 3.4, there is no single “best” design for architectural choice, but rather compromises to be made, depending on the application or deployment scale:

a layered architecture is appropriate for smaller-scale or budget-constrained deployments, a distributed architecture will work better for applications that require low-latency performance;

and a service-oriented architecture will deliver the most interoperability for larger-scale, multi-vendor municipal deployments, with a higher cost of integration.

In all the application areas, the IoT systematically provides operational value-added benefits. Among these, the reduction of congestion, the optimization of energy use, the collection of waste, and the environmental response times are some of the main ones reported, but not yet measured by standardized, cross-city metrics.

Security, interoperability, scalability, and cost are the four primary challenges to the city-wide adoption, all of which are of equal magnitude but of which security and interoperability seem most ripe for independent, real-world testing aside from additional proof-of-concept.

The integration of edge intelligence, 5G connectivity, AI analytics, digital twins, and trust mechanisms based on blockchain will open up the path for the next-generation smart city IoT systems that will allow autonomous and privacy-preserving urban management in the future.

Realization of this promise will depend on breakthroughs in the three research goals described in (Section 7): Comparative architectural review, Standardized impact metrics, and Long-term validation of security and interoperability solutions. The realization of the benefits of IoT infrastructure will depend on ongoing investment, coordinated governance and inclusive design to ensure the technology benefits all residents.

References

[1] Chen L, Wang H, Zhang Y. Advanced IoT architectures for smart city implementation. IEEE Internet Things J. 2023;10(5):1125-1142. doi:10.1109/JIOT.2023.3256789

[2] Rodriguez M, Kumar S. 5G-enabled IoT systems for urban transportation management. Transp Res Part C Emerg Technol. 2022;134:103456. doi:10.1016/j.trc.2021.103456

[3] Johnson P, Smith A. Energy optimization in smart cities through IoT integration. Sustain Cities Soc. 2024;92:104567. doi:10.1016/j.scs.2023.104567

[4] Williams R, Chen J. Security frameworks for urban IoT deployments. IEEE Trans Inf Forensics Secur. 2023;18:2345-2358. doi:10.1109/TIFS.2023.3278901

[5] Davis K, Martinez L. Edge computing applications in smart city environments. Future Gener Comput Syst. 2022;136:345-358. doi:10.1016/j.future.2022.05.012

[6] Thompson G, Wilson H. IoT-enabled environmental monitoring for urban sustainability. Environ Sci Technol. 2024;58(3):1567-1580. doi:10.1021/acs.est.3c08542

[7] Anderson M, Lee S. Waste management optimization through IoT sensor networks. Resour Conserv Recycl. 2023;188:106723. doi:10.1016/j.resconrec.2022.106723

[8] Roberts T, Kim Y. Emerging trends in smart city IoT development. Cities. 2024;145:104678. doi:10.1016/j.cities.2023.104678

[9] Bellini P, Nesi P, Pantaleo G. IoT-enabled smart cities: A review of concepts, frameworks and key technologies. Appl Sci. 2022;12(3):1607. doi:10.3390/app12031607

[10] Bhardwaj V, Anooja A, Vermani LS, Dhaliwal BK. Smart cities and the IoT: global research trends and future directions. Discover Internet Things. 2024;4:19. doi:10.1007/s43926-024-00076-3

[11] Tekinerdogan B, Koksal O, Celik T. System architecture design of IoT-based smart cities. Appl Sci. 2023;13(7):4173. doi:10.3390/app13074173

[12] Khan LU, Yaqoob I, Tran NH, Kazmi SMA, Dang TN, Hong CS. Edge-computing-enabled smart cities: A comprehensive survey. IEEE Internet Things J. 2020;7(10):10200-10232. doi:10.1109/JIOT.2020.2987070

[13] Aslam S, Ullah H. A comprehensive review of smart cities components, applications and technologies based on IoT. Heliyon. 2020;6(11):e04734. doi:10.1016/j.heliyon.2020.e04734

[14] Fahmideh M, Zowghi D. IoT smart city architectures: An analytical evaluation. Sensors. 2020;20(14):4025. doi:10.3390/s20144025

[15] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things: A vision, architectural elements, and future directions. Future Gener Comput Syst. 2013;29(7):1645-1660. doi:10.1016/j.future.2013.01.010

[16] Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of Things for smart cities. IEEE Internet Things J. 2014;1(1):22-32. doi:10.1109/JIOT.2014.2306328

[17] Al-Turjman F. Intelligence and security in 5G-oriented IoT networks. Future Gener Comput Syst. 2019;102:357-368. doi:10.1016/j.future.2019.08.028

[18] Perera C, Qin Y, Estrella JC, Reiff-Marganiec S, Vasilakos AV. Fog computing for sustainable smart cities: A survey. ACM Comput Surv. 2017;50(3):1-43. doi:10.1145/3057266

[19] Fang B, Yu J, Chen Z, Li X, Zhang Q. Artificial intelligence for waste management in smart cities: A review. Environ Chem Lett. 2023;21:1959-1989. doi:10.1007/s10311-023-01604-3

[20] Kumar P, Singh RK, Sharma A. Smart healthcare monitoring in urban environments using IoT technologies. J Ambient Intell Humaniz Comput. 2024;15(2):987-1003. doi:10.1007/s12652-023-04689-2

[21] Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Comput Netw. 2015;76:146-164. doi:10.1016/j.comnet.2014.11.008

[22] Borgia E. The Internet of Things vision: Key features, applications and open issues. Comput Commun. 2014;54:1-31. doi:10.1016/j.comcom.2014.09.008

[23] Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W. A survey on Internet of Things: Architecture, enabling technologies, security and privacy. IEEE Internet Things J. 2017;4(5):1125-1142. doi:10.1109/JIOT.2017.2683200

[24] Talari S, Shafie-Khah M, Siano P, Loia V, Tommasetti A, Catalao JPS. A review of smart cities based on the Internet of Things concept. Energies. 2017;10(4):421. doi:10.3390/en10040421

[25] Roman R, Lopez J, Mambo M. Mobile edge computing, fog computing and security threats in IoT. Future Gener Comput Syst. 2018;78:680-698. doi:10.1016/j.future.2016.11.009

[26] Ahmed E, Yaqoob I, Gani A, Imran M, Guizani M. Internet-of-Things-based smart environments: State of the art and research challenges. IEEE Wirel Commun. 2016;23(5):10-16. doi:10.1109/MWC.2016.7721736