

Internet of Things-Enabled Smart City Infrastructure for Enhancing Urban Safety and Operational Efficiency in Saudi Arabia under Vision 2030

Abdulrahman Alshaikhali^{1*} 

¹Independent Researcher

*Corresponding Author

Abdulrahman Alshaikhali

Independent Researcher

Article History

Received: 19.08.2026

Accepted: 13.10.2026

Published: 14.10.2026

Abstract: Saudi Arabia is speeding up the digital transformation of its urban infrastructure as it works to achieve safer cities, greater efficiency, and objectives set out in Vision 2030. The Internet of Things (IoT) is important since it connects distributed sensors, connected assets, communication networks, edge and cloud platforms, and analytics to operational control. This study looks at how smart-city infrastructure enabled by IoT can improve urban safety and operational efficiency in Saudi Arabia, without assuming that the simple deployment of technology will lead to public value. A structured integrative review of 30 peer-reviewed studies published between 2020 and 2025 was carried out covering the topics of Saudi smart-city development, IoT architectures, edge computing, digital twins, mobility, water, energy, cybersecurity, governance, and citizen participation. The analysis reveals two main pathways for impact. The first is a safety pathway in which sensing, situational awareness, anomaly detection, incident coordination, and robust communications reduce the time taken to detect and respond to incidents. The second is an efficiency pathway in which continuous monitoring, predictive analytics, adaptive control, and asset intelligence cut down delays, minimise resource losses, lower energy consumption, and prevent unnecessary maintenance. It is also found that interoperability, cybersecurity, data governance, institutional coordination, and the establishment of measurable performance benchmarks are essential prerequisites for turning IoT capabilities into real outcomes at the city level. The paper suggests a layered Saudi IoT smart-city framework that links physical assets to decision-making intelligence and operational action, along with an outcome model that connects technical capabilities to safety, efficiency, resilience, and quality of life. The review concludes that the best alignment with Vision 2030 will be achieved when IoT investments are designed around verifiable urban problems, an interoperable architecture, risk-based governance, and outcome-oriented indicators rather than on the number of devices or on isolated pilot projects.

Keywords: Internet of Things (IoT); Smart Cities; Urban Safety; Operational Efficiency; Saudi Arabia; Vision 2030; Edge Computing; Digital Twins; Predictive Analytics.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0) which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

1. INTRODUCTION

The urban development taking place in Saudi Arabia is happening at the point where fast metropolitan growth, major infrastructure initiatives, digitisation, and a national strategy which

focuses on quality of life and economic diversification are coming together. Under these circumstances, smart-city infrastructure goes beyond being simply a matter of purchasing technology; it becomes an operational issue concerning how cities are able to

Citation: Alshaikhali, A. (2026). Internet of Things-Enabled Smart City Infrastructure for Enhancing Urban Safety and Operational Efficiency in Saudi Arabia under Vision 2030. *Glob Acad J Econ Buss*, 8(5), 1911-1921.
<https://doi.org/10.36348/gajeb.2026.v08i05.075>

detect conditions, interpret the data, co-ordinate their various institutions, and act on the information quickly enough to enhance everyday services. As a result, recent research carried out in Saudi Arabia has shifted from viewing smart cities as merely a series of digital projects to developing frameworks that link technology with governance, sustainability, participation, and measurable urban performance [21–24]. Further studies into urban development in Saudi Arabia indicate that planning systems have to take account of growth while also dealing with pressure on mobility, demand for infrastructure, environmental stress, and the uneven delivery of services [23]. In this context, IoT acts as a practical nervous system for the city: networked sensors and devices monitor the physical environment, communication networks transmit the data, computational platforms combine the different data streams, and applications support decision-making in the areas of transport, water, energy, buildings, public safety, and municipal operations [1–12].

Smart city systems that are based on the Internet of Things are appealing since they allow a range of dispersed urban assets to be turned into systems that can be observed and reacted to. For example, a traffic signal can be included in an adaptive corridor if the number of vehicles passing is continuously measured; a water supply network can be handled more effectively when pressure, flow, and quality are monitored in near real time; a building will be able to cut back on unnecessary energy consumption when the levels of occupancy and the state of the equipment are used to set its control schedules; and a public-safety operation can enhance its situational awareness when environmental sensors, cameras, connected devices, and the systems used to record incidents all contribute to a common operational picture. Reviews of Internet of Things-enabled cities always point to sensing, communications, data platforms, analytics, and application services as the key technical components, while also highlighting the persistent issues of heterogeneity, scalability, security, privacy, and interoperability [1–13]. Edge computing has become especially important for applications where latency is a concern since it brings processing closer to the devices and thus reduces the need for distant cloud resources [3–7].

It is important to make this distinction since smart-city discussions can take on a technology-focused character. The fact that connected devices have been installed does not in itself mean that risk has decreased or that efficiency has improved. The entire operational process has to be maintained from the stage of sensing through to decision-making and action, and the results must be compared with a clear baseline. A leakage sensor has little worth if the alerts

it generates are not given priority, forwarded, and responded to; adaptive traffic control has little significance if reliable detection does not affect the timing of the signals; and an urban camera network does not necessarily lead to safer conditions if there are weak data integration, privacy controls, and emergency coordination. Research into digital twins supports this systems approach by demonstrating that urban value is achieved when dynamic physical data are linked to analytical models that assist in planning and operations rather than simply producing visual replicas [15–26].

In light of this, the present review pays particular attention to the IoT-enabled smart-city infrastructure in Saudi Arabia with a view to improving urban safety and operational efficiency in accordance with Vision 2030. The review makes three contributions. The first is to distinguish between the technical architecture and the outcome pathways, making it clear how sensing, connectivity, edge intelligence, platforms, analytics, and control mechanisms contribute to various urban functions. The second is to combine safety and operational efficiency, two outcomes which are usually looked at separately in the various sectoral literatures even though they often rely on the same data and communications infrastructure. The third is to establish an implementation approach that is tailored to Saudi Arabia, in which interoperability, cybersecurity, governance, evidence quality, and institutional response capacity are regarded as enabling conditions rather than as secondary issues.

2. Aim and Objectives

This review seeks to provide a well-supported explanation of the way in which IoT-enabled smart-city infrastructure can enhance urban safety and operational efficiency in Saudi Arabia and at the same time contribute to the wider set of transformation goals linked to Vision 2030. Instead of merely listing the various smart-city technologies, the review looks at the mechanisms by which IoT alters urban operations and at the conditions which decide whether these mechanisms lead to believable results.

The analysis is based on four objectives. The first is to draw together the latest evidence regarding the architectural elements needed for a city-wide IoT system, covering sensing, communications, edge and cloud computing, interoperability, analytics, digital twins, and operational applications. The second involves looking at safety features such as continuous monitoring, early warning systems, anomaly detection, reduction of traffic risk, coordination during incidents, and ensuring resilient service continuity. The third objective is to assess the efficiency mechanisms in the areas of mobility, water,

energy, buildings, parking, and asset maintenance. The fourth deals with identifying the priorities for implementing IoT in Saudi Arabia, focusing on governance, citizen participation, cybersecurity, data quality, performance measurement, and scalable deployment. These objectives underpin a review framework which evaluates the value of IoT based on operational mechanisms and measurable results rather than simply on the number of connected devices.

3. REVIEW METHODOLOGY

This study used a structured integrative review approach since the subject area involves engineering, urban planning, public management, sustainability, cybersecurity, and infrastructure operations. A review that focused solely on technical aspects would fail to take account of the constraints faced by institutions, whereas one that was entirely oriented towards planning would not be able to explain the operational mechanisms by which IoT influences safety and efficiency. The method thus involved both the identification of relevant evidence and the synthesis of the material thematically along with comparisons based on mechanism.

The peer-reviewed publications dated from 2020 to 2025 were the ones included in the review corpus. The searches were based on combinations of the following terms: "Internet of Things", "IoT", "smart city", "Saudi Arabia", "Vision 2030", "urban safety", "operational efficiency", "smart mobility", "smart water", "smart energy", "edge computing", "digital twin", "cybersecurity", "interoperability", "governance", and "citizen participation". Evidence was given priority if it fulfilled at least one of three conditions: being directly relevant to the development of smart cities in Saudi Arabia; being closely related to the architecture of IoT or the mechanisms of urban operations; or providing empirical or review evidence on safety, efficiency, security, water, mobility, energy, or urban digital twins. The final body of evidence consisted of 30 studies, all of which had been published within the time period in question and could all be traced back via a DOI.

The review did not regard all publications as being equally valid evidence regarding city-level effects. It used conceptual papers to establish the architectures and governance conditions; it employed review papers to spot recurring technologies, challenges, and application areas; and it referred to empirical or implementation studies to show the operational mechanisms and performance pathways. By making this distinction, the review lowered the risk of treating conceptual potential as actual observed impact. When assessing institutional, planning, governance, and participation conditions,

particular importance was given to papers that were focused on Saudi Arabia [18-27]. International studies were included in the review where they dealt with transferable mechanisms such as edge computing, smart-water monitoring, adaptive traffic management, digital twins, and cybersecurity [3-30].

The analysis was carried out in four stages. In the first stage, each study was assigned a code based on the urban domain, technical layer, operational mechanism, outcome type, and implementation constraint. In the second stage, the coded information was combined to form a layered architecture which comprised physical sensing, communication, edge/cloud processing, data and interoperability services, analytics, and operational control. In the third stage, the outcome pathways were separately drawn up for the areas of urban safety and operational efficiency; the safety aspect involved hazard detection, situational awareness, authentication, cyber resilience, incident management, mobility safety, and continuity, while the efficiency aspect included reduced delay, lower resource loss, energy optimisation, predictive maintenance, smarter parking, improved water management, and more efficient service coordination. In the fourth stage, the cross-cutting enablers were determined by comparing the cases where technically similar systems resulted in different levels of operational value.

The entire analysis was based on a mechanism-first approach. An IoT intervention was regarded as operationally meaningful to the extent that the literature showed a link between a sensed condition and subsequent data processing, a decision or a control action, and a relevant service outcome. This is more rigorous than considering the deployment of sensors or the extent of network coverage as proof of smartness. For instance, mobility sensing only becomes important when it leads to changes in signal control, route guidance, parking allocation, or incident response; similarly, smart-water instrumentation is significant only when it allows for leakage detection, pressure management, water-quality intervention, or maintenance prioritisation [10-20]. This same logic was used in the cases of energy, public safety, and building systems.

4. IoT Infrastructure as an Urban Operational System

The existing literature suggests that the IoT infrastructure should be understood in a layered manner with each technical level carrying out a specific operational function. At the physical level, sensors, meters, cameras, connected controllers, vehicles, building systems, and environmental devices all generate observations of the city. At the communication level, wired and wireless networks

transmit these observations while having to meet different demands regarding range, bandwidth, energy use, reliability, and latency. The fact that cellular networks, 5G, Wi-Fi, low-power wide-area networks, and local industrial or building protocols all coexist means that a smart city is by nature heterogeneous [5-12]. This heterogeneity can only be dealt with if the systems are designed using interoperable interfaces and clear service requirements rather than relying on a single network technology.

It is the edge and cloud layers that decide where the data are processed. Edge computing is especially useful in those cases where response time, bandwidth, reliability, or privacy means that frequent journeys back and forth to the cloud are not desirable. For example, a traffic junction, a safety camera, a group of industrial sensors, or an important facility can carry out local filtering and event detection before sending only the relevant information on to the central systems [3-7]. Although cloud resources are still necessary for citywide storage, for carrying out cross-domain analytics, for training models, for analysing historical trends, and for co-ordinating between different agencies, the actual architecture used is therefore hybrid in nature: the local systems maintain a high level of responsiveness while the central city platforms offer integration and long-term intelligence. Research into trustworthy edge services also indicates that distributing the services leads to both security and orchestration problems, and so resilience has to be built into the way services are placed and into access control rather than being taken for granted [7].

The data and interoperability layer is located above the computation layer. IoT systems can only generate value to the extent that observations can be understood across different devices and across organisational boundaries. As a result, standardised data models, semantic structures, shared identifiers, time synchronisation, metadata, and application programming interfaces are just as important as the sensors themselves. The City Data Hub study shows

how standard-based platforms can reduce fragmentation and enable data exchange between different smart-city services [4]. This is particularly relevant in the case of Saudi municipalities and in giga-project environments where transport, utilities, buildings, security, and public services may be provided by various public and private organisations. If there are no common data rules, then each successful pilot project will end up being another isolated system.

Analytics turn integrated data into operational intelligence. The methods used include threshold setting and statistical detection as well as machine learning, deep learning, forecasting, optimisation, and the use of digital twins. Reviews of IoT and AI indicate that analytics can be used to carry out detection, classification, prediction, and control in the areas of transportation, environmental monitoring, energy, healthcare, and surveillance [1-24]. Digital twins enhance this ability by keeping dynamic virtual models of assets or urban systems which can then be used for simulation, testing of different scenarios, and operational coordination [15-26]. Their value is most evident when the models stay linked to real-time data and decision-making processes; otherwise, they may end up being nothing more than sophisticated visualisation environments lacking a definite operational function.

The last stage is action. Whether or not operational control is automated, is only partly automated or requires human approval depends on the level of risk. Examples of this include altering the timing of traffic signals, sending out maintenance requests, isolating a fault, adjusting the building controls, giving warnings to operators, rerouting vehicles, or escalating an incident. Although this stage is often neglected in smart-city designs which focus on technology, it is precisely here that the benefits are realised. That is why Figure 1 shows the IoT not as a stack ending with analytics, but as a closed operational loop in which action modifies physical conditions and new sensing confirms the result.

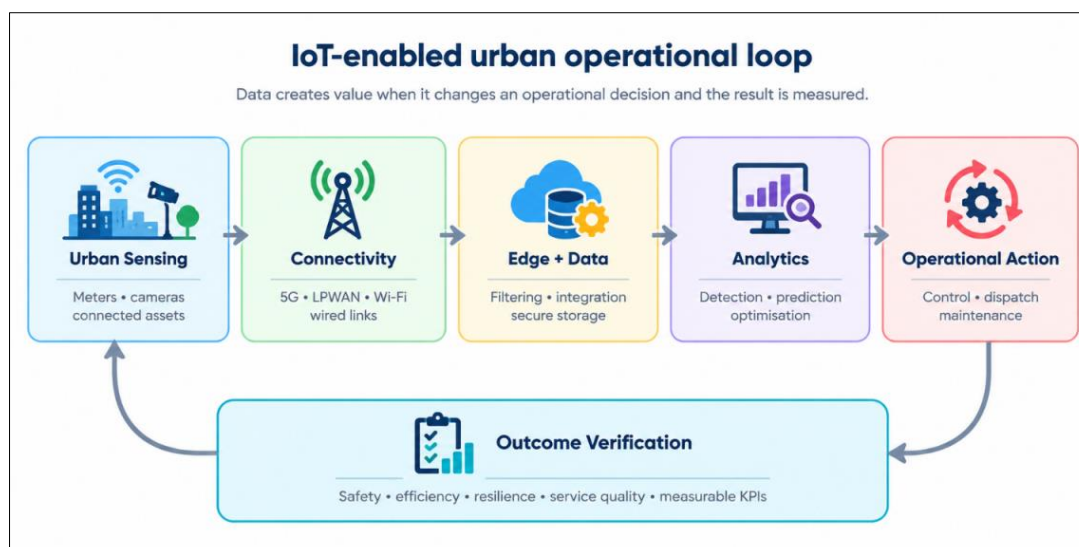


Figure 1: Layered IoT-enabled urban operational architecture linking sensing, analytics, action, and outcome verification

5. Urban Safety Pathways

Urban safety is a multifaceted result which includes road safety, public-space security, emergency response, the reliability of infrastructure, protection against environmental hazards, cyber-physical protection, and the continuity of essential services. The main contribution of IoT is to reduce information delays. Unlike traditional safety systems which usually rely on periodic inspections, human reports, or isolated control rooms, connected sensing alters this approach by enabling abnormal conditions to be identified earlier and passed on to those responsible for taking action. The safety benefits that IoT provides therefore depend on how fast and how trustworthy the entire detect-interpret-decide-respond process is.

Mobility serves as a clear example of this. Adaptive traffic management systems make use of cameras, loops, connected devices, or other types of detectors to estimate the level of traffic flow and congestion, upon which analytical models can then adjust signal settings or routing advice [14-25]. Even though reducing congestion is generally presented as an efficiency goal, smoother traffic can also help to decrease risky interactions, secondary accidents, and delays in emergency responses. Smart parking can likewise reduce the amount of traffic caused by people searching for parking spaces and can enhance access control in areas that are densely populated [10]. In Saudi cities, where road travel is still of great importance, combining traffic sensing with incident detection and corridor management provides a direct link between operational efficiency and safety.

The safety of public spaces and infrastructure relies on having a good awareness of the situation drawn from a variety of data sources.

Cameras based on IoT technology, environmental sensors, access-control devices, acoustic sensors, structural monitors, and connected alarms can together provide a unified view of emerging risks. Although deep-learning and IoT technologies have been described in terms of their use in surveillance and the detection of anomalies, they also warn that their performance is dependent on the quality of the data, the available computing power, the reliability of communications, and responsible governance [1-24]. Digital twins can also assist in incident management by combining real-time data with spatial context and the workflows of the relevant agencies. Wolf *et al.*, demonstrate how a city's digital twin can support multi-agency incident management by integrating diverse information into a common operational environment [16]. The main takeaway for Saudi emergency management is that it should not aim to copy a particular platform but instead should plan for cross-agency information sharing before a crisis happens.

Safety also involves the reliability of essential utility services. Smart water systems are able to pick up on unusual pressure, flow, or quality conditions, which enables operators to identify leaks, contamination risks, or a decline in service earlier than would be possible with periodic monitoring [8-20]. The same principle can be applied to electricity networks, district cooling systems, street lighting, and other critical building systems. With predictive sensing deterioration can be detected before failure occurs, and condition-based maintenance can direct crews to the assets that pose the highest operational risk. These capabilities are especially important in areas where climate conditions and demand place heavy loads on the infrastructure.

Cybersecurity goes hand in hand with physical safety since the integration of urban infrastructure increases the potential for attacks. Weaknesses in authentication, the use of insecure devices, the presence of compromised credentials, inadequate segmentation, and unprotected data exchanges can turn efficient technologies into operational weaknesses. Recent reviews of the authentication systems of smart cities and of AI-powered cyber defence highlight device identity, secure communication, anomaly detection, and privacy-preserving methods as essential controls [28-30]. For Saudi smart-city initiatives this means that cyber risk should be taken into account at the planning and purchasing stages, and throughout the entire lifecycle device onboarding, patchability, credential management, logging, segmentation, incident response, and the responsibilities of suppliers should all be specified.

The safety model that is most effective is therefore one that is layered and robust. It is necessary for devices to keep on operating as far as possible when there is network degradation; critical alerts should be given priority in terms of communication; edge processing should offer a local backup option; the central systems should combine information from different areas; and the various agencies should practice how information translates into decisions. Measurement of the outcomes should concentrate on detection time, response time, the length of an incident, service restoration, trends regarding near-misses, system availability, and the number of false alarms rather than on the number of sensors installed. Using these indicators makes it possible to audit the safety benefits and helps to tell the difference between operational improvements and the accumulation of technology.

6. Operational Efficiency Pathways

The degree of operational efficiency in a smart city refers to the amount of time, energy, water, labour, infrastructure capacity, and financial resources needed to achieve a given service level. Efficiency can be improved through the use of IoT since constant observation lessens the uncertainty regarding when, where, and why resources are being used. The most beneficial applications don't just involve gathering more data; rather, they use that data to substitute fixed schedules and reactive methods with operations that respond to demand or are based on conditions.

Transport is perhaps the most evident area of application. Adaptive traffic control can modify the timing of signals in response to observed demand, and connected parking systems can guide drivers to vacant parking spaces thereby reducing unnecessary traffic circulation [10-14]. Further research into IoT-

assisted intelligent transport systems emphasizes real-time monitoring, vehicle-infrastructure interaction, route information, and incident-aware control as ways of improving network performance [25]. In the case of Saudi metropolitan areas, the operational value should be assessed by means of corridor travel time, intersection delay, reliability, parking search time, public-transport punctuality, and incident clearance rather than by making general statements about "smart mobility". Only by integrating with metro, bus, pedestrian, logistics, and event-management systems can a more comprehensive picture of mobility be obtained than can be achieved using road sensors alone.

Water efficiency is just as important. Research into smart water systems shows that the requirements for monitoring vary depending on the application: leakage detection, water quality, pressure control, consumption analysis, and network optimisation function at different spatial and temporal resolutions [19, 20]. This has a direct effect on the design of systems in Saudi Arabia. The instrumentation to be used should be chosen on the basis of the decisions that operators need to make, not just because a communication technology is available. An application involving pressure management may call for frequent and reliable observations in the field, whereas long-term consumption analysis can afford with lower reporting rates. When sensors are linked with hydraulic models, alert systems, and work-order systems, water utilities will be able to achieve targeted inspections and maintenance, which could lead to a reduction in non-revenue water and the avoidance of unnecessary field work.

Energy efficiency can be achieved at many different levels. IoT devices are capable of aiding building automation, providing for occupancy-aware control, enabling demand management, and allowing asset monitoring, while analytics can be used to forecast loads and detect abnormal consumption. Research into smart-city energy optimisation shows how IoT data can be combined with optimisation techniques in order to decrease the use of resources, although the application of the algorithmic results to performance at a city scale relies on the equipment, the controls, the baselines, and the operating behaviour [11]. Edge processing can likewise help to reduce communication overhead in the case of dense deployments of devices, but the edge nodes themselves bring about energy and management costs. Efficiency therefore has to take into account the entire architecture rather than improving one layer at the expense of shifting the costs to another.

Municipal asset management offers a more efficient approach. Instead, traditional maintenance

methods tend to switch back and forth between fixed preventive maintenance schedules and reactive repairs. Thanks to the Internet of Things, condition-based maintenance is possible by keeping an eye on factors such as vibration, temperature, power quality, occupancy, structural behaviour, or the state of the equipment. Maintenance can then be prioritised on the basis of the estimated probability of degradation or failure and the operational consequences. Digital twins can further this process by connecting real-time asset data with the asset's geometry, its maintenance history, simulation results, and service dependencies [15-26]. In large developments in Saudi Arabia, where new infrastructure is being built on a large scale, it is more effective to design the assets for digital lifecycle management from the very beginning of commissioning than to try retrofitting disconnected monitoring at a later stage.

Efficiency is also due to coordination between different domains; for example, a city might improve traffic conditions locally at the expense of emergency access, or it might lower the energy used in buildings even though this reduces thermal comfort. The purpose of an integrated smart-city platform is not to centralise all control functions but rather to make the dependencies between different areas clear. By using shared data it is possible to see how mobility, energy, water, public events, weather, and maintenance influence one another. Research into interoperability has shown that common data models and interfaces are essential for this kind of coordination [4]. It is then up to the governance structure to decide which body has the authority to take action and to determine how conflicting objectives are resolved.

Table 1: IoT mechanisms, measurable efficiency outcomes, and safety/resilience safeguards

Urban domain	IoT mechanism	Operational indicators	Safety / resilience safeguards
Mobility	Traffic/parking sensing; adaptive control	Delay, travel-time reliability, parking search time	Incident detection, emergency access, pedestrian/road-user risk
Water	Flow, pressure and quality sensing; analytics	Non-revenue water, response time, inspection productivity	Contamination alerts, service continuity, failure detection
Energy/buildings	Smart meters; occupancy/condition sensing; control	Energy intensity, peak demand, equipment runtime	Thermal safety, critical-load continuity, abnormal-condition alerts
Public safety	Cameras, environmental sensors, connected alarms	Dispatch productivity, information latency	Detection time, response time, false-alarm burden, recovery time
Assets	Condition monitoring; predictive maintenance	Maintenance cost, downtime, work-order efficiency	Failure probability, availability, restoration time

7. Vision 2030 Alignment, Governance and Scalable Implementation

The Vision 2030 plan provides a strategic framework within which smart infrastructure can contribute to quality of life, digital government, enhanced investment attractiveness, improved infrastructure performance, and more efficient public services. Yet, as the literature on Saudi smart cities shows, the transition from having ambitious goals to achieving measurable results relies on governance capacity and institutional coordination [18-29]. IoT should thus be seen as a shared operational capability since its design connects the national digital foundations with the public services duties at the city level.

A model for a scalable implementation starts off with defining the problem. Every initiative must state the urban condition to be improved, name the operational owner, indicate the decision that will be affected by the new data, set out the baseline to be used in measuring improvement, and identify the

risks resulting from the extra connectivity. This order prevents technology-driven pilot projects from succeeding technically while still lacking a way of being incorporated into regular operations. It also enhances the procurement process since the system requirements can be given in terms of latency, uptime, interoperability, data quality, security, and service outcomes.

Accountability should therefore be set up throughout the entire data lifecycle. The fact that someone owns a device does not mean that they also own the data, and data access can involve various municipalities, utilities, transport agencies, security organisations, developers, and technology suppliers. There needs to be clear guidance regarding collection, classification, retention, sharing, secondary use, the disclosure of incidents, and deletion. In Saudi Arabia, research into smart governance stresses the importance of institutional capacity, transparency, digital participation, and integrated decision-making [27]. These principles

can be put into practice through the establishment of data stewardship roles, the use of common metadata, ensuring auditability, and the creation of cross-agency operating agreements.

Interoperability must be treated as a strategic requirement; although rapid urban development may lead to a need for quickly deploying systems, proprietary integration can result in long-term dependence and costly duplication. Platform designs should include documented interfaces, reusable identity and access services, consistent event semantics, and the ability to port historical data. When vendor-specific systems are needed, they should be connected to a city's integration layer via controlled interfaces so that a gradual replacement can take place and no future service has to depend on a single technical ecosystem.

Just as much importance should be given to cybersecurity as to resilience. The connected infrastructure must be divided on the basis of its criticality, device identities should be managed over the entire course of their lifecycle, support for software and firmware updates should be provided, and operational monitoring should be capable of picking up any unusual communication or device behaviour. There should be redundancy in edge and cloud services that is suitable to the consequences of a failure of the service. In the case of systems where the consequences are severe, safe local modes should still be available if central connectivity is lost. Security controls should also be measured by means of patch compliance, authentication coverage, incident rates, recovery time, and test results rather than relying solely on policy documentation [7-30].

Another condition for scaling involves the participation of citizens and stakeholders. Alamoudi and others claim that in order to implement smart and sustainable cities in Saudi Arabia it is necessary to have structured participation rather than relying solely on a technology-oriented method [22]. Since citizens act as both users of services and, in many instances, as data subjects, involvement is relevant to the use of the Internet of Things. It can help in selecting the problems to be addressed, identify obstacles to usability, uncover unintended consequences, and enhance trust. This is especially important in relation to applications such as surveillance, mobility, sensing in public spaces, and data sharing, since the perceived legitimacy of the technology can affect its adoption.

In the end, scaling should be based on evidence. A valuable pilot study is one that examines both the technical performance and the full operating model—that is, who gets the alert, what action is taken, how exceptions are managed, whether the data are reliable, how cybersecurity is maintained, and whether the results are improved. Once pilots have been successful, they can be incorporated into reference architectures and procurement guidelines. Figure 2 outlines this progression from IoT capability through to operational mechanism, governed implementation, measurable outcomes, and feedback for use in future investments. As part of Vision 2030, this evidence loop can help make sure that digital infrastructure becomes an enduring capability for city management rather than a series of disconnected demonstrations.

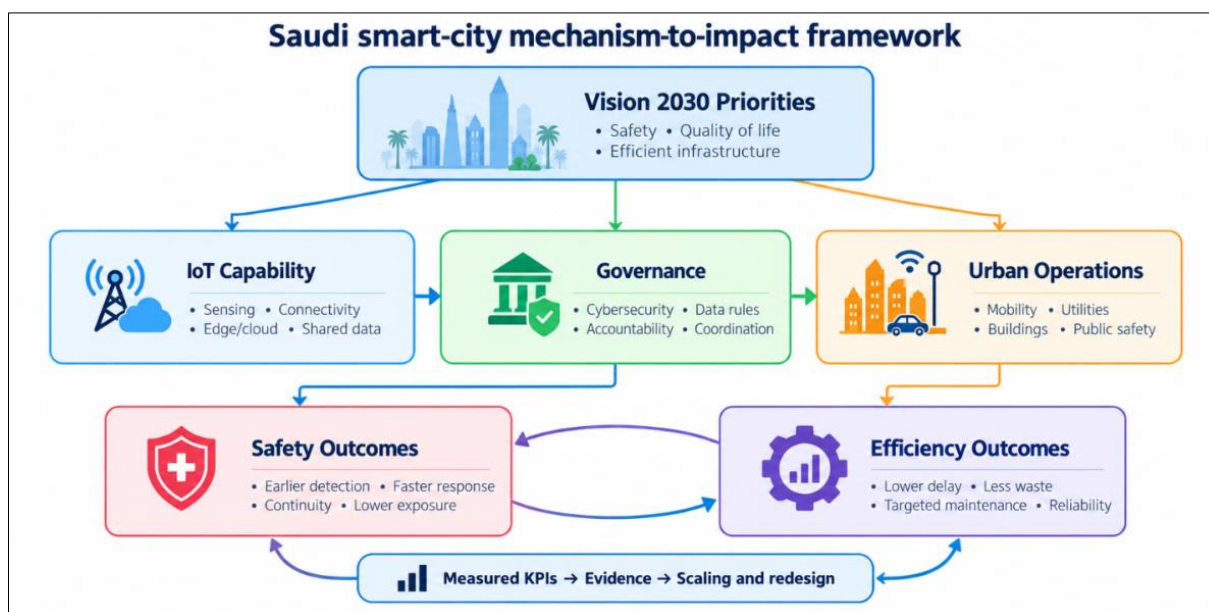


Figure 2: Mechanism-to-impact framework for scaling IoT-enabled smart-city infrastructure under Vision 2030

Table 2: Principal implementation risks and governance controls for Saudi IoT smart-city programmes

Risk	Operational consequence	Priority control
Fragmented platforms	Isolated data and duplicated infrastructure	Common APIs, semantic models, integration layer, data portability
Cyber-physical attack surface	Service disruption, unsafe control, data compromise	Device identity, segmentation, secure updates, logging, incident response
Weak evidence design	Technology deployment mistaken for impact	Defined baselines, service KPIs, stable boundaries, post-deployment evaluation
Vendor dependency	High lifecycle cost and constrained replacement	Interface requirements, portability clauses, lifecycle documentation
Institutional fragmentation	Slow response and unclear accountability	Data stewardship, cross-agency operating agreements, named process owners
Low public trust	Reduced adoption and legitimacy	Purpose limitation, transparency, access controls, stakeholder engagement

8. Challenges, Research Gaps and Future Agenda

There are still some research and implementation gaps. To begin with, there is stronger evidence regarding the performance of subsystems than there is concerning the causal impact at a citywide level. While many studies show that a model, a sensor network, or a control strategy functions under specific conditions, fewer demonstrate how the benefits continue over the years, between different agencies, and in the face of changing urban conditions. Saudi research should therefore go ahead and carry out longitudinal evaluations making use of stable baselines and consistent service indicators.

Secondly, achieving cross-domain interoperability is still technically and institutionally challenging. Although IoT platforms are able to share data, the various organisations may apply different definitions, identifiers, security classifications, and operating priorities. Future research should look at semantic interoperability and governance together, including how data can be shared by the transport, utilities, public safety, and planning sectors without leading to uncontrolled access.

Thirdly, cybersecurity research should become more aligned with the realities of operational technology. Although authentication, anomaly detection, federated learning, and advanced analytics provide useful controls [28, 29], cities also need practical evidence regarding device patching, supplier access, the integration of legacy systems, recovery procedures, and the management of cyber-physical consequences. The testbeds in Saudi Arabia could assess security architectures under conditions of high temperature, heavy event loads, communications disruption, and a mix of legacy and new infrastructure.

Fourthly, there needs to be a more clear evaluation of the outcomes of digital twins. Although current research has shown considerable promise in the areas of simulation and urban coordination [15–26], further research should clarify the difference

between visualisation, analytical forecasting, and closed-loop operational control. It should investigate which of the twin functions actually lead to a reduction in maintenance costs, an improvement in incident response, or an increase in infrastructure availability, and also determine what level of data quality is necessary to maintain those benefits.

Fifth, more attention should be paid to human factors. Operators may become overwhelmed by the number of alerts, dashboards, and model outputs. Even if a system is technically accurate it can still fail when information is presented without clear priority, explanation, or defined responsibility. Future research therefore needs to include workload, trust, decision latency, training, and organisational learning as performance variables. Systems aimed at the general public should also have considerations for accessibility, transparency, and provide mechanisms for feedback.

The research that Saudi Arabia carries out should eventually be directed towards achieving specific, measurable objectives in the field of urban development, such as safer roads, quicker recovery from incidents, reduced water loss, more reliable assets, lower energy intensity, improved mobility during events, and more resilient digital services. By carrying out comparative studies in Riyadh, Jeddah, Makkah, Madinah, Dammam, and in the newer developments, it would be possible to determine which architectural patterns are suitable for transfer and which need to be adapted to local conditions. This type of research would help to build up the body of evidence required to transform IoT from being merely a technology into a well-disciplined tool for urban management.

9. CONCLUSION

Smart-city infrastructure that is equipped with IoT technology can make Saudi cities safer and more operationally efficient if it is designed as a complete urban management system rather than

merely as a set of connected devices. The evidence examined indicates a consistent process: sensing decreases uncertainty, connectivity transfers the observations, edge and cloud platforms turn the data into useful information, analytics detect patterns or predict conditions, and operational systems turn this intelligence into action. Safety is enhanced when this chain reduces the time it takes to detect and respond to situations, improves situational awareness, aids in the coordination of incidents, and helps to protect essential services. At the same time, efficiency is improved when the same chain allows for adaptive mobility, targeted maintenance, management of water loss, energy optimisation, and a more accurate allocation of municipal resources.

The main limitation is not the availability of IoT technology but rather the ability to integrate diverse systems, to secure the growing cyber-physical environments, to manage data across different institutions, to ensure reliable performance, and to demonstrate that the implementations actually lead to improved outcomes. Although Saudi Arabia's Vision 2030 offers strong motivation for investment, substantial value will only be achieved through outcome-oriented governance. Projects must start by identifying specific urban problems and establishing clear baseline measurements, make use of interoperable and resilient architectures, assign responsibility for operations, and proceed with scaling only when there is evidence to support it.

In terms of research, the next stage involves a more in-depth assessment of the actual operating systems in the Saudi cities. Longitudinal studies should link the technical indicators to the outcomes relating to service delivery, safety, resilience, and cost, taking into account factors such as climate, event surges, the level of maturity of the infrastructure, and institutional differences. As for practical applications, the main focus should be on developing a reusable architecture and governance model which will enable various agencies and suppliers to innovate without causing the urban digital environment to become fragmented. In this way, IoT can become a lasting component of the nation's urban capabilities: one that contributes to safer public spaces, more reliable infrastructure, faster decision-making, greater resource productivity, and tangible improvements in the quality of life in urban areas.

REFERENCES

1. Ben Atitallah, S.; Driss, M.; Boulila, W.; Ben Ghezala, H. Leveraging Deep Learning and IoT big data analytics to support the smart cities development: Review and future directions. *Computer Science Review* 2020, 38, 100303. <https://doi.org/10.1016/j.cosrev.2020.100303>
2. Bibri, S.E.; Krogstie, J. The emerging data-driven Smart City and its innovative applied solutions for sustainability: The cases of London and Barcelona. *Energy Informatics* 2020, 3, 5. <https://doi.org/10.1186/s42162-020-00108-6>
3. Khan, L.U.; Yaqoob, I.; Tran, N.H.; Kazmi, S.M.A.; Dang, T.N.; Hong, C.S. Edge-Computing-Enabled Smart Cities: A Comprehensive Survey. *IEEE Internet of Things Journal* 2020, 7, 10200-10232. <https://doi.org/10.1109/JIOT.2020.2987070>
4. Jeong, S.; Kim, S.; Kim, J. City Data Hub: Implementation of Standard-Based Smart City Data Platform for Interoperability. *Sensors* 2020, 20, 7000. <https://doi.org/10.3390/s20237000>
5. Rong, B.; Han, S.; Kadoch, M.; Chen, X.; Jara, A. Integration of 5G Networks and Internet of Things for Future Smart City. *Wireless Communications and Mobile Computing* 2020, 2020, 2903525. <https://doi.org/10.1155/2020/2903525>
6. Guevara, L.; Auat Cheein, F. The Role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems. *Sustainability* 2020, 12, 6469. <https://doi.org/10.3390/su12166469>
7. Jararweh, Y.; Otoum, S.; Al Ridhawi, I. Trustworthy and sustainable smart city services at the edge. *Sustainable Cities and Society* 2020, 62, 102394. <https://doi.org/10.1016/j.scs.2020.102394>
8. Pasika, S.; Gandla, S.T. Smart water quality monitoring system with cost-effective using IoT. *Heliyon* 2020, 6, e04096. <https://doi.org/10.1016/j.heliyon.2020.e04096>
9. Syed, A.S.; Sierra-Sosa, D.; Kumar, A.; Elmaghraby, A. IoT in Smart Cities: A Survey of Technologies, Practices and Challenges. *Smart Cities* 2021, 4, 429-475. <https://doi.org/10.3390/smartcities4020024>
10. Fahim, A.; Hasan, M.; Chowdhury, M.A. Smart parking systems: comprehensive review based on various aspects. *Heliyon* 2021, 7, e07050. <https://doi.org/10.1016/j.heliyon.2021.e07050>
11. Humayun, M.; Alsaqer, M.S.; Jhanjhi, N.Z. Energy Optimization for Smart Cities Using IoT. *Applied Artificial Intelligence* 2022, 36, 2037255. <https://doi.org/10.1080/08839514.2022.2037255>
12. Bellini, P.; Nesi, P.; Pantaleo, G. IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies. *Applied Sciences* 2022, 12, 1607. <https://doi.org/10.3390/app12031607>
13. Whaiduzzaman, M.; Barros, A.; Chanda, M.; Barman, S.; Sultana, T.; Rahman, M.S.; Roy, S.; Fidge, C. A Review of Emerging Technologies for IoT-Based Smart Cities. *Sensors* 2022, 22, 9271. <https://doi.org/10.3390/s22239271>
14. Lilhore, U.K.; Imoize, A.L.; Li, C.-T.; Simaiya, S.; Pani, S.K.; Goyal, N.; Kumar, A.; Lee, C.-C. Design

- and Implementation of an ML and IoT Based Adaptive Traffic-Management System for Smart Cities. *Sensors* 2022, 22, 2908. <https://doi.org/10.3390/s22082908>
15. Lehtola, V.V.; Koeva, M.; Oude Elberink, S.; Raposo, P.; Virtanen, J.-P.; Vahdatikhaki, F.; Borsci, S. Digital twin of a city: Review of technology serving city needs. *International Journal of Applied Earth Observation and Geoinformation* 2022, 114, 102915. <https://doi.org/10.1016/j.jag.2022.102915>
16. Wolf, K.; Dawson, R.J.; Mills, J.P.; Blythe, P.; Morley, J. et al. Towards a digital twin for supporting multi-agency incident management in a smart city. *Scientific Reports* 2022, 12, 16221. <https://doi.org/10.1038/s41598-022-20178-8>
17. Ferre-Bigorra, J.; Casals, M.; Gangolells, M. The adoption of urban digital twins. *Cities* 2022, 131, 103905. <https://doi.org/10.1016/j.cities.2022.103905>
18. Alshuwaikhat, H.M.; Aina, Y.A.; Binsaedan, L. Analysis of the implementation of urban computing in smart cities: A framework for the transformation of Saudi cities. *Heliyon* 2022, 8, e11138. <https://doi.org/10.1016/j.heliyon.2022.e11138>
19. Oberascher, M.; Rauch, W.; Sitzenfrei, R. Towards a smart water city: A comprehensive review of applications, data requirements, and communication technologies for integrated management. *Sustainable Cities and Society* 2022, 76, 103442. <https://doi.org/10.1016/j.scs.2021.103442>
20. Mezni, H.; Driss, M.; Boulila, W.; Ben Atitallah, S.; Sellami, M.; Alharbi, N. SmartWater: A Service-Oriented and Sensor Cloud-Based Framework for Smart Monitoring of Water Environments. *Remote Sensing* 2022, 14, 922. <https://doi.org/10.3390/rs14040922>
21. Aldegheishem, A. Assessing the Progress of Smart Cities in Saudi Arabia. *Smart Cities* 2023, 6, 1958-1972. <https://doi.org/10.3390/smartcities6040091>
22. Alamoudi, A.K.; Abidoye, R.B.; Lam, T.Y.M. Implementing Smart Sustainable Cities in Saudi Arabia: A Framework for Citizens' Participation towards Saudi Vision 2030. *Sustainability* 2023, 15, 6648. <https://doi.org/10.3390/su15086648>
23. Almulhim, A.I.; Cobbinah, P.B. Can rapid urbanization be sustainable? The case of Saudi Arabian cities. *Habitat International* 2023, 139, 102884. <https://doi.org/10.1016/j.habitatint.2023.102884>
24. Alahi, M.E.E.; Sukkuea, A.; Tina, F.W.; Nag, A.; Kurdthongmee, W.; Suwannarat, K.; Mukhopadhyay, S.C. Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart City Scenario: Recent Advancements and Future Trends. *Sensors* 2023, 23, 5206. <https://doi.org/10.3390/s23115206>
25. Ahmad, K.; Khujamatov, H.; Lazarev, A.; Usmanova, N.; Alduailij, M.; Alduailij, M. Internet of Things-Aided Intelligent Transport Systems in Smart Cities: Challenges, Opportunities, and Future. *Wireless Communications and Mobile Computing* 2023, 2023, 7989079. <https://doi.org/10.1155/2023/7989079>
26. Wang, H.; Chen, X.; Jia, F.; Cheng, X. Digital twin-supported smart city: Status, challenges and future research directions. *Expert Systems with Applications* 2023, 217, 119531. <https://doi.org/10.1016/j.eswa.2023.119531>
27. Aldegheishem, A. Assessing progress towards smart governance in Saudi Arabia. *Humanities and Social Sciences Communications* 2024, 11, 759. <https://doi.org/10.1057/s41599-024-03235-7>
28. Ali, J.; Singh, S.K.; Jiang, W.; Alenezi, A.M.; Islam, M.; Daradkeh, Y.I.; Mehmood, A. A deep dive into cybersecurity solutions for AI-driven IoT-enabled smart cities in advanced communication networks. *Computer Communications* 2024, 108000. <https://doi.org/10.1016/j.comcom.2024.108000>
29. Alqahtany, A.M. Smart Cities as a Pathway to Sustainable Urbanism in the Arab World: A Case Analysis of Saudi Cities. *Sustainability* 2025, 17, 1525. <https://doi.org/10.3390/su17041525>
30. Alotaibi, A.; Aldawghan, H.; Aljughaiman, A. A Review of the Authentication Techniques for Internet of Things Devices in Smart Cities: Opportunities, Challenges, and Future Directions. *Sensors* 2025, 25, 1649. <https://doi.org/10.3390/s25061649>