

Article

Artificial Intelligence-Driven Threat Detection in Sustainable Smart Cities: A Case Study for Saudi Urban Infrastructure

Abdullah M. Algarni ^{1,*}  and Vijey Thayanathan ²

¹ Computer Science Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia

² Department of Computer Engineering, Institute of Inner City Learning, Birmingham Campus, University of Wales, Birmingham B1 2RA, UK; v.thayanathan@uwtsd.ac.uk

* Correspondence: amsalgarni@kau.edu.sa

Highlights

Please indicate how your work links to systems science via your contributions to systems practice, theory, and/or methodology.

- Proposes a systems-level AI-based Threat Detection Mechanism (ATDM) that integrates anomaly detection, threat management, cybersecurity policies, and emerging quantum-enabled technologies across interconnected smart city domains.
- Provides a conceptual methodology for linking cybersecurity, energy efficiency, resilience, and sustainability within Saudi urban infrastructure, demonstrated through a conceptual case study based on Jeddah and the 15 priority indicators of the IMD Smart City Index 2026.

What are the main findings and/or the implications of the main findings?

- The conceptual analysis indicates that integrating AI-driven threat detection with IoT, 6G, and quantum-enabled security mechanisms can provide a holistic foundation for improving cybersecurity resilience and supporting sustainable smart city operations.
- The framework establishes a theoretical basis for future quantitative validation of security, energy efficiency, latency, and sustainability performance, while identifying the need for comprehensive datasets integrating smart city indicators with AI- and quantum-enabled cybersecurity features.

Abstract

Artificial Intelligence-driven detection mechanisms present both opportunities and challenges in modern systems, particularly within smart cities that rely on complex operational technologies. In the context of Saudi urban infrastructure, rapidly evolving and multidimensional cyber threats require advanced, energy-efficient security solutions. This research proposes an Artificial Intelligence-based Threat Detection Mechanism designed to proactively identify and mitigate cyber threats while maximizing energy efficiency and minimizing cost and system complexity. Purpose: The proposed theoretical framework focuses on securing sustainable smart cities by integrating Artificial Intelligence-based anomaly detection with quantum-enhanced algorithms to address high-dimensional and emerging cyber threats across interconnected urban systems. The Artificial Intelligence-based Threat Detection Mechanism enables early and proactive threat detection across sustainable smart city networks, including connections to external and global infrastructures, ensuring continuous monitoring, resilience, and service continuity. Methods: The methodology emphasizes the development of energy-efficient Artificial Intelligence models



Academic Editor: Jinzhi Lu

Received: 7 June 2026

Revised: 5 August 2026

Accepted: 12 August 2026

Published: 14 August 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

and quantum protocols, incorporating intelligent risk assessment, adaptive calibration, and automated response mechanisms. In addition, the framework introduces distributed security hubs to enhance cybersecurity robustness and scalability. Anticipated Results and Conclusions: Anticipated outcomes include improved security management policies, automated threat detection and response, and adaptive protection against evolving cyber risks. The proposed framework provides a scalable and cost-effective solution aligned with sustainability objectives. Ultimately, this research contributes a proactive and intelligent framework for securing smart city ecosystems, supporting long-term development goals and aligning with Saudi Vision 2030.

Keywords: artificial intelligence-based threat detection; sustainable smart cities; urban infrastructure; Saudi Vision 2030; Internet of Things cybersecurity; anomaly detection; quantum technologies; energy efficiency

1. Introduction

The rapid evolution of sustainable smart cities represents a transformative shift in urban living, driven by the convergence of cutting-edge technologies. These urban environments rely heavily on an integrated framework of the Internet of Things (IoT), Artificial Intelligence (AI), and big data to optimize resource efficiency and environmental monitoring [1]. By leveraging data-driven decision-making, smart cities can significantly enhance urban mobility, reduce congestion, and streamline public transit systems [2]. Central to this progress is the deployment of diverse IoT architectures across public safety and urban automation sectors [3]. Figure 1 illustrates a threat-free, security-managed, and security-efficient smart city architecture driven by emerging technologies (ETs), where smart security, supported by cybersecurity, serves as a fundamental enabler for achieving the Sustainable Development Goals (SDGs) in Saudi urban areas. The SDGs are represented through four interconnected smart systems that are integrated within the Smart ET Ecosystem (e.g., Intelligent IoT and 6G), forming a unified platform for sensing, communication, and data integration [4]. These interconnected SDG processes and communication links must be protected to maintain secure and sustainable smart cities (SSCs). Within this ecosystem, the AI-based Threat Detection Mechanism (ATDM) can strengthen cybersecurity by enabling real-time data fusion, anomaly detection, and predictive analysis across smart healthcare, transportation, energy, and residential systems. This integrated architecture with ATDM enhances cross-domain situational awareness, supports the timely detection and mitigation of cyber-physical threats, and improves the resilience and sustainability of smart city services with future SDGs. Furthermore, the transition toward AI-driven cloud security serves as a strategic enabler for digital transformation, ensuring that the digital services and infrastructure supporting these cities remain resilient against emerging cyber threats [4,5].

As urban centers become increasingly interconnected, the “attack surface” for cyber threats expands, creating complex security challenges. The pervasive nature of sensing and connectivity in modern telecommunications and sensor networks necessitates robust governance frameworks to protect against inherent vulnerabilities [6]. Current research highlights that the rising interconnectivity of urban digital ecosystems exacerbates risks related to safety, security, and privacy [7]. To combat these risks, novel intrusion detection systems based on AI and network analytics are being developed to mitigate threats targeting networked IoT infrastructure [8]. These efforts extend to exploring quantum-resilient systems that protect against future decryption threats while enhancing operational efficiency in smart city environments [9,10]. Protecting the underlying Cyber-Physical Sys-

tems (CPSs) is now a critical priority for maintaining the safety of transport and mobility networks [11,12].

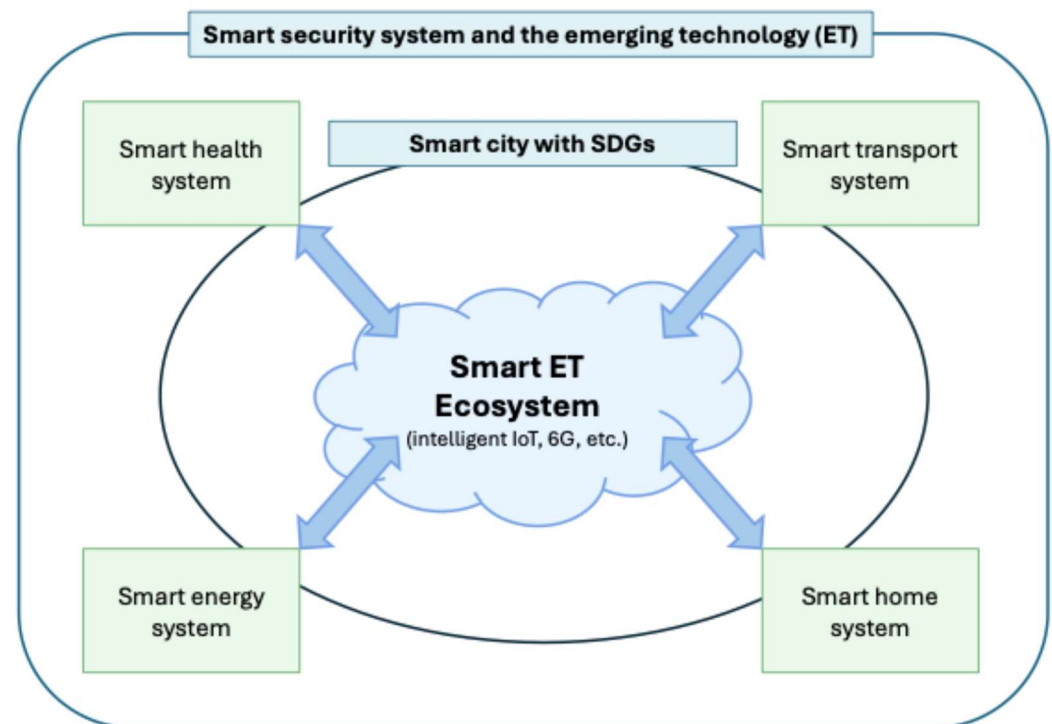


Figure 1. Smart ecosystem of ET and services for SSC.

Traditional security measures define that the measurement involves conventional methods of protecting against attacks and threats in computer network infrastructure or real-world environments, including smart cities. The limitations of traditional security measures against sophisticated, automated attacks have made AI-driven solutions a necessity in modern threat detection. Conceptual frameworks for AI-driven anomaly detection utilize machine learning to identify deviations in massive urban data streams in real-time [13]. Beyond security, AI integration improves public safety through predictive policing and automated response mechanisms [14]. Global case studies demonstrate that AI's influence spans governance, economy, and environmental monitoring, fostering a more sustainable and inclusive urban life [15,16]. Despite barriers such as algorithmic bias and implementation costs, AI remains vital for optimizing energy grids and reducing emissions [17,18]. Emerging 6G and cloud-based AI security frameworks are expected to further enhance the scalability and efficiency of urban analytics, ensuring long-term infrastructure robustness [19–22].

Within Saudi Arabia, the pursuit of smart urban development is a cornerstone of Vision 2030, which seeks to build technologically resilient cities. Sophisticated technologies like blockchain, IoT, and AI are being deployed to align urban growth with national sustainability objectives [23,24]. Flagship mega-projects like NEOM serve as a global paradigm for sustainable living, acting as a live laboratory for AI-powered construction and resource management [25,26]. These developments are supported by innovative financial instruments, such as green municipal bonds, which fund low-carbon infrastructure [27]. In cities like Riyadh, the integration of smart mobility and AI-driven data analytics is already reshaping the transportation landscape, reflecting a broader commitment to modernized, efficient urban governance [28].

Despite these advancements, a significant research gap exists regarding localized security frameworks tailored to the unique regulatory and physical landscape of Saudi

Arabia. Deploying smart applications requires balancing maximum security with cost-effectiveness, as service providers and users alike demand energy efficiency (EE) and low-cost protection systems. Traditional models often overlook the specific environmental and infrastructural conditions of Saudi urban centers. There is an urgent need to understand how AI-driven threats might specifically disrupt the future of Saudi smart cities and why an anomaly detection and threat management (AD&TM) framework is essential in this context. This research addresses the problem by investigating the trade-offs between security performance and resource consumption within a specialized Saudi case study. In this research, we manage our analysis according to the following research questions:

- RQ1. How can an ATDM be designed to improve cybersecurity for sustainable smart city infrastructure?
- RQ2. How can AI-driven anomaly detection be integrated with existing intrusion detection systems to support proactive cyber threat management?
- RQ3. What role can emerging technologies, including quantum-inspired techniques, play in enhancing future smart city cybersecurity frameworks?
- RQ4. How can the proposed conceptual framework support the resilience and sustainability of Saudi smart city infrastructure?

The primary objective of this research is to enhance security solutions for smart cities by providing professionals with AI-based tools to manage evolving threats. Specifically, the study aims to:

- Develop a conceptual ATDM for securing sustainable smart city infrastructure.
- Propose an AI-driven anomaly detection architecture that complements conventional intrusion detection systems through proactive threat detection and management.
- Investigate the potential integration of emerging technologies, including quantum-inspired techniques, within future AI-enabled cybersecurity frameworks for smart cities.
- Demonstrate the applicability of the proposed framework through a conceptual case study based on Saudi urban infrastructure.

The main advantage of integrating quantum technologies into smart cities lies in achieving minimal energy consumption and maximum security. Key aspects include:

- Data security management using quantum-safe architectures.
- Emerging drone technologies equipped with quantum sensors for smart city monitoring.
- Post-Quantum Cryptography (PQC) for drones operating within smart cities.
- The use of the Variational Quantum Eigensolver (VQE) across remote quantum machines.

These advancements are expected to enhance urban infrastructure and smart city domains through energy-efficient AD&TM. According to [29–31], quantum-safe architectures, quantum sensors, PQC and VQE are considered briefly for different applications, including drones and smart cities. Further, energy management is discussed with quantum technology, which enhances secure communication and services in smart cities.

This paper contributes to the development of AI-driven threat detection in sustainable smart cities through a case study that identifies key research challenges in SSC services within the context of Saudi urban infrastructure. It evaluates the strengths and limitations of the proposed AI-driven model, defines the requirements for AD&TM implementation, and provides actionable insights for researchers and urban planners to develop resilient security frameworks for future smart city environments.

The rest of this paper is organized as follows. Section 2 reviews the literature on sustainability, cybersecurity, and existing frameworks for smart urban infrastructure. Section 3 presents the proposed AI-driven threat detection framework, including its design, architecture, and quantum-enabled threat detection mechanisms for enhancing security in sustainable smart city environments. Section 4 presents the results of conceptual experi-

ments conducted using data derived from the IMD Smart City Index 2026, based on the 15 priority smart city indicators for Jeddah, Saudi Arabia. This section also discusses the cybersecurity implications of these indicators within Saudi urban infrastructure. Section 5 provides a discussion and analysis of the results, highlighting the potential improvements in security, resilience, and sustainability achieved through the proposed framework, together with additional security-related considerations. Section 6 discusses the limitations of the proposed framework, examines emerging challenges associated with AI-driven threat detection and the long-term sustainability of next-generation smart cities, and outlines future research directions. Finally, Section 7 concludes the paper by summarizing the main findings and contributions of the proposed ATDM.

2. Literature Review

AI is a pivotal element in the establishment of sustainable smart cities, where the amalgamation of IoT, intelligent grids, and interconnected infrastructure creates extensive and vulnerable attack surfaces. For Saudi Arabia's ambitious urban initiatives, safeguarding these systems is essential to ensuring long-term resilience and operational continuity. Moving beyond static defenses, AI-driven threat detection offers real-time, adaptive capabilities to analyze intricate data, recognize sophisticated non-linear threats, and autonomously mitigate risks, thereby preserving the integrity and availability of vital urban services.

The SSC must adopt a vision of a sustainable management system that encompasses education (e.g., food, health, housing), energy (e.g., generation, protection, storage, and consumption), and employment (ensuring that at least one member of each family is employed). These three Es are essential for maintaining SSCs, where AI-driven architectures should be deployed to enhance urban cyber-resilience, EE, digital health, and related services.

This study employs a structured narrative literature review rather than a systematic literature review (SLR). Unlike an SLR, which follows a predefined protocol for identifying, screening, appraising, and synthesizing all available evidence, a structured narrative review provides a flexible and transparent approach for identifying and critically evaluating representative studies to establish the theoretical foundation of a conceptual framework. Accordingly, the objective of this review was to identify the most relevant literature on AI-driven cybersecurity, sustainable smart cities, and emerging technologies rather than to perform an exhaustive evidence synthesis.

Relevant publications were identified through searches of six major scientific databases: IEEE Xplore, Scopus, Web of Science, ScienceDirect, SpringerLink, and MDPI. These databases were selected because they provide comprehensive coverage of research in Artificial Intelligence, cybersecurity, smart cities, sustainability, and engineering. Representative Boolean search queries included ("smart cities" OR "sustainable smart cities") AND ("cybersecurity" OR "intrusion detection" OR "anomaly detection") AND ("artificial intelligence" OR "machine learning"), together with additional search terms such as Internet of Things (IoT), 6G, quantum computing, Post-Quantum Cryptography (PQC), sustainability, Saudi Vision 2030, and emerging technologies. Multiple combinations of these keywords were used to retrieve relevant studies published primarily between 2020 and 2026, while retaining earlier seminal works where necessary.

The retrieved publications were screened through a three-stage process consisting of duplicate removal, title and abstract screening, and full-text assessment. Publications were included if they addressed AI-driven cybersecurity, anomaly detection, intrusion detection systems, sustainable smart cities, IoT, 6G, or quantum-enabled security; were published in peer-reviewed journals, reputable conference proceedings, or authoritative technical reports; and provided conceptual, methodological, or technical contributions relevant to the proposed ATDM. Publications were excluded if they were duplicate records,

outside the scope of the study, lacked sufficient technical or methodological detail, or were non-peer-reviewed sources without significant technical contributions.

Following the full-text assessment, the selected studies were classified into thematic categories, including AI-driven threat detection, cybersecurity frameworks, sustainable smart city infrastructure, IoT and 6G communications, quantum technologies, Saudi smart city initiatives, and identified research gaps. This thematic analysis formed the basis of the comparative review presented in Section 2 and supported the development of the proposed ATDM conceptual framework. Although the literature selection process was conducted systematically to improve transparency and reproducibility, a formal PRISMA protocol was not adopted because this study presents a structured narrative literature review rather than a systematic literature review.

The background section is organized to provide a logical progression from the broad context of sustainable smart cities to the specific research problem addressed in this study. It first discusses the sustainability and cybersecurity in smart infrastructure, emphasizing the need for resilient urban systems. The review then discusses AI-driven architectures for cyber-resilience and intelligent threat detection, followed by an overview of hybrid Quantum Artificial Intelligence (Q-AI) as an emerging approach for future cybersecurity enhancement. The discussion subsequently focuses on Saudi Arabia by highlighting the role of Saudi Vision 2030 in advancing digital transformation and smart city initiatives. Finally, existing research on smart cities in Saudi Arabia is reviewed to identify current developments, challenges, and research gaps. This progression establishes the theoretical foundation for the proposed ATDM and its application to sustainable Saudi urban infrastructure.

2.1. The Nexus of Sustainability and Cybersecurity in Smart Infrastructure

The integration of advanced digital technologies into urban planning has evolved beyond functional convenience to become a prerequisite for environmental and operational sustainability. This section explores the necessity for secure, resilient, and energy-efficient systems within the smart city paradigm. As urban centers increasingly rely on interconnected IoT and 6G networks, robust AI-driven cybersecurity mechanisms are imperative to safeguard critical services against emerging cyber-physical threats. Aligning security with sustainability objectives ensures operational reliability, optimized resource management, and long-term infrastructure stability.

2.1.1. Frameworks for Sustainable Urban Ecosystems

The conceptualization of modern smart cities relies on the synergy between ecological goals and digital fortification. This interplay begins with the digital representation of physical assets to maximize resource efficiency. Reference [32] presents a systematic review exploring the integration of AI-powered Digital Twins and IoT technologies to foster sustainable building environments and smart city ecosystems. By enabling real-time mimicking and optimization of urban infrastructure, this technology facilitates data-driven decision-making essential for zero-energy goals and urban resilience. This resilience is further bolstered by predictive capabilities. Reference [33] explores the transformative role of AI-powered predictive modeling in supporting sustainable urban development, focusing on critical applications such as infrastructure optimization, energy management, and climate adaptation. While these models forecast trends to enhance resource allocation, the authors emphasize that ethical governance and transparent safeguards are necessary to mitigate algorithmic bias and ensure equitable outcomes.

To handle the computational demands of such systems, recent research suggests a fusion of high-performance analytics. Reference [34] proposes a framework for

climate-resilient smart cities and energy systems by leveraging the convergence of High-Performance Computing (HPC), big data, and Edge AI. This integration utilizes hybrid deep learning to enhance renewable energy forecasting, shifting urban management from reactive to proactive stances to reduce fossil fuel reliance. Similarly, Reference [35] proposes a comprehensive AI framework designed to enable carbon-free urban environments by integrating diverse datasets, including air quality metrics and infrastructure durability. By employing automated machine learning, this framework drives informed decisions in disaster management and green technology integration, serving as a critical enabler for carbon neutrality.

Reference [36] examines the use of AI, blockchain, and big data to improve urban sustainability through optimized energy management, transportation, and resource utilization. Likewise, Reference [37] demonstrates that integrating IoT sensing, AI analytics, and automated logistics can enhance waste management, reduce operational costs, and improve the sustainability of smart city infrastructure.

2.1.2. Governance, Security Challenges, and Risk Management

Despite the operational benefits of these sustainable ecosystems, their expansion introduces significant security and management complexities. References [38,39] highlight the role of IoT technologies in smart city infrastructures and emphasize the importance of addressing security challenges through secure communication, governance, and intelligent management mechanisms. This necessitates structured oversight, as Reference [40] systematically reviews the integration of Artificial Intelligence into smart infrastructure management, exploring the technical strategies and implementation frameworks necessary for sustainable urban planning. This study highlights the importance of predictive maintenance and ethical public participation in smart city governance to ensure equitable infrastructure deployment.

The broad scope of these transformations is captured in meta-analyses of the field. Reference [15] provides a comprehensive review of AI's transformative impact on smart city infrastructure, synthesizing findings from over 92 publications across six key pillars: governance, economy, mobility, environment, living, and people. This research identifies success factors for resilient ecosystems, emphasizing data interoperability and human–AI collaboration. Despite these advancements, a persistent gap remains between innovation and protection. Reference [41] provides a thorough systematic review of the intersection between urban digitalization and security, synthesizing existing literature to identify critical vulnerabilities, threats, and mitigation measures within smart cities. The authors argue that while sustainability is often prioritized, a unified security framework is frequently lacking, necessitating a socio-technical approach that balances functionality with privacy.

Quantifying these risks is essential for strategic defense. Reference [42] proposes a mathematical approach to cybersecurity risk assessment within smart city infrastructures, providing systematic techniques for identifying and evaluating security threats across multiple urban domains. This methodology allows for the calculation of cyberattack impacts, enabling prioritized investment in risk-based protective measures. Finally, the evolution of these defense strategies must be continuous. Reference [43] provides a systematic literature review on cybersecurity risk management within smart cities, synthesizing global methodologies to identify current research gaps and best practices. By evaluating localized perspectives and governance models through 2024, this research establishes a comprehensive foundation for managing threats in increasingly complex, interconnected, and sustainable urban landscapes.

Reference [44] highlights the importance of integrating continuous risk assessment and decision-support systems to improve urban resilience and smart city risk management.

Similarly, Reference [45] proposes an AI-driven Digital Twin framework based on multi-objective reinforcement learning to optimize energy efficiency, service latency, and security compliance under smart city governance constraints.

2.2. AI-Driven Architectures for Urban Cyber-Resilience

The evolution of smart cities into hyper-connected ecosystems necessitates a shift from traditional security models toward AI-driven architectures capable of providing proactive cyber-resilience. Central to this transition is the integration of advanced learning paradigms. Reference [46] examines the transformative potential of machine learning (ML) and Deep Reinforcement Learning (DRL) in shaping the future of smart cities, focusing on how these technologies can be evolved to address emerging urban challenges and improve quality of life. By utilizing data-driven intelligence for smart grid security and 5G optimization via Unmanned Aerial Vehicles (UAVs), this research establishes a predictive roadmap for resilient urban environments.

To achieve this resilience, the literature emphasizes the convergence of physical and digital layers. Reference [47] proposes a hybrid AI-IoT framework that integrates Digital Twin technologies to enable proactive urban infrastructure management in smart cities. This architecture leverages federated learning and lightweight edge inference to facilitate real-time monitoring and predictive maintenance, significantly reducing response times for critical systems like traffic and pipeline management. Such proactive measures are vital because, as Reference [48] examines, the modern cybersecurity landscape of smart cities is characterized by an expanding attack surface where the increasing interconnectivity of urban services heightens infrastructure vulnerability. This research advocates for the integration of predictive defense measures and robust regulations to safeguard data integrity and ensure long-term service reliability.

The effectiveness of these architectures depends heavily on the ability to process massive datasets. Reference [49] examines the integration of data-driven cybersecurity within smart cities, emphasizing the critical role of big data analytics in protecting urban assets. While IoT sensor streams provide essential security intelligence, the authors note that managing high-volume data scales and maintaining privacy remains a significant challenge. This technical foundation is further explored by Reference [50], which examines the critical cybersecurity vulnerabilities inherent in the IoT and physical infrastructure of smart cities, emphasizing the urgent need for robust protective solutions. By evaluating requirements across communication protocols and architectural layers, the study identifies the multi-layered defense strategies necessary to fortify essential systems such as smart grids and water management networks.

Despite the advancement of these systems, the reliability of threat detection remains a primary concern in complex networks. Reference [51] focuses on enhancing the accuracy of threat detection in smart cities by investigating network anomalies and identifying opposing decisions or contradictory threat assessments. By resolving discrepancies between conflicting data points, this research reduces false positives and improves the reliability of AI-based monitoring. Complementing this, Reference [52] provides a high-level overview of the cybersecurity landscape in smart cities, identifying critical vulnerabilities and emerging challenges within interconnected digital ecosystems. This overview serves as a strategic foundation for understanding the future research directions required to combat evolving global threats.

Reference [53] proposes an edge-AI architecture that combines Convolutional Neural Network (CNN)-Transformer and Long Short-Term Memory (LSTM) models for real-time anomaly detection and predictive failure analysis in smart transportation systems. Their

results demonstrate that AI-based edge intelligence can achieve accurate threat detection with low latency, supporting secure smart city infrastructure.

In addition, the implementation of specialized security tools is paramount for operationalizing these resilient architectures. Reference [8] introduces a novel intrusion detection system (IDS) specifically engineered to address the unique security requirements and complexities of modern smart city environments. By focusing on securing data flow across both the application and network layers of critical infrastructure, this sophisticated solution provides a robust mechanism for defending the interconnected components of the digitalized city against increasingly advanced cyber threats. Together, these studies illustrate that a resilient urban infrastructure requires a synergy of AI, big data analytics, and specialized intrusion detection frameworks. To improve the threat intelligence framework, such as ATDM, the application of Generative Adversarial Networks (GANs) in network IDS can be considered to improve the SSC.

Figure 2 illustrates the 6G network as the core communication backbone enabling AI-driven smart city services. It integrates heterogeneous IoT paradigms—including IoT for smart homes, medical IoT (mIoT) for smart healthcare, and vehicular IoT (vIoT) for smart transportation—into a unified, high-capacity infrastructure. These IoT-based smart systems support the SDGs, SSCs, and smart security, which fundamentally relies on cybersecurity. Although 6G technology is still evolving, it is regarded as one of the key enabling technologies for future SDG implementation and SSC development in Saudi urban areas. The 6G layer supports URLLC and large-scale data aggregation from distributed devices. Through continuous interaction with users via IQN systems, the architecture facilitates AI-driven threat detection using real-time data analytics, anomaly detection, and cross-domain correlation. Furthermore, the proposed ATDM, integrated with 6G and IoT technologies, strengthens the robustness of cybersecurity solutions deployed in smart systems, thereby enhancing the security, resilience, and sustainability of smart city operations. According to [54], the role of 6G will enhance smart city facilities through many evolving technologies, including all types of IoT.

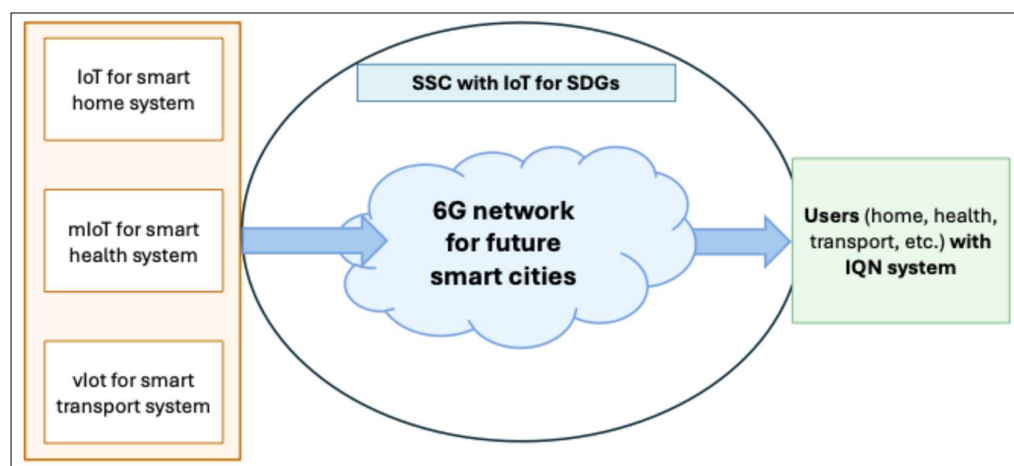


Figure 2. Smart city facilities with 6G network and IoT.

2.3. Universal Intelligence with Hybrid Q-AI

SSC faces numerous challenges arising from population growth and evolving lifestyles. In computer science, universal intelligence can be applied to manage the complex intelligence requirements of systems deployed in smart cities. It represents a theoretical framework for the management, maintenance, and measurement (3Ms) of intelligent systems in future smart cities. The integration of universal intelligence with hybrid Quantum-AI (Q-AI) technologies can not only reduce the overall operational costs for smart city stake-

holders but also support the sustainability of critical requirements such as security, energy efficiency, and resource management.

Over the coming decade, AI is expected to evolve toward universal intelligence capabilities that enable users and service providers to make informed decisions under dynamic environmental conditions. For example, the effects of global warming continue to influence temperature patterns in many smart cities, including urban areas across Saudi Arabia. Quantum channels incorporated into SSC development can further enhance the universal intelligence framework and its 3Ms. Through these channels, threats can be detected efficiently when entangled pairs are established and maintained between the source node (v_s) and destination node (v_d). Depending on the severity of threats and cyberattacks, the entanglement routing rate may vary and can be determined using the quantum routing scheme (Q_{RS}), as expressed in Equation (1).

$$Q_{RS} = \max_{(v_s, v_d) \in D} \sum P_{(v_s, v_d)} 1_{\{\varepsilon_{(p,q)} = 1 \forall (p, q) \in P_{(v_s, v_d)}\}} \quad (1)$$

The above-mentioned equation [55] represents the quantum routing scheme, which can be considered to improve the security when threats are identified in the quantum channels. In Equation (1), $P_{(v_s, v_d)}$ is the entanglement path connecting the source–destination pair, and $\varepsilon_{(p,q)}$ denotes the entanglement status between the quantum nodes p and q . The size of D depends on the window of the source–destination pair at the time.

2.4. Strategic Integration with Saudi Vision 2030

Many Saudi cities have been ranked among the top 100 smart cities for 2026 [56], including Riyadh (ranked 24), Hail (33), Mecca (50), Jeddah (55), Al Khobar (64), Medina (67), AlUla (85), and Hafar Al Batin (100). The realization of sustainable smart cities in Saudi Arabia is inextricably linked to the strategic objectives of Vision 2030, which mandates a transition toward a digitally empowered and secure economy. This transformation is not merely a technical endeavor but a socio-technical one, requiring the alignment of human expertise, organizational governance, and technological innovation. Reference [57] addresses the human element of security by evaluating cybersecurity competency within Saudi Arabia using a fuzzy decision-making approach to manage the complexity and ambiguity of skill development. By establishing a mathematical framework to identify training gaps and prioritize resource allocation, this research provides a strategic roadmap for building the human expertise necessary to defend the Saudi's expanding digital infrastructure.

At the organizational and economic levels, the integration of security must occur early in the innovation lifecycle. Reference [58] explores the unique IoT security challenges faced by Saudi startups, positioning these emerging organizations as a critical engine for the Saudi's economic growth and digital transformation. The study advocates for a security-by-design approach, enabling startups to mitigate vulnerabilities without compromising innovation velocity. Such resilience at the grassroots level of the private sector is complemented by advancements in the public sector. Reference [59] conducts a multi-case analysis of the Saudi digital government, examining the motivations, enablers, and technical challenges involved in transitioning traditional public services into automated, AI-driven platforms. This analysis highlights the importance of integrated national infrastructures and clear policy elements in eliminating service duplication and ensuring successful technology adoption. To deploy the information security policies, cybersecurity frameworks, such as the National Initiative for Cybersecurity Education (NICE) Framework, can be considered with the AI-driven IDS.

The success of these digital initiatives is ultimately determined by citizen engagement and trust. Reference [60] investigates the psychological and technical barriers influencing the adoption of AI-enabled public services among Saudi residents, with a specific focus on cybersecurity, data privacy, and trust. Identifying these factors as primary mediators for technology acceptance, the authors provide actionable recommendations for developing transparent government services. This need for transparency is reinforced by technical safeguards in cloud environments. Reference [5] provides a strategic technical framework linking AI-powered cloud security and anomaly detection directly to the objectives of Saudi Vision 2030. By positioning proactive threat detection as a non-negotiable enabler for digital transformation, this research demonstrates how intelligent automation maintains the data sovereignty and public trust essential for the Saudi's digitization goals.

Governance and compliance serve as the structural backbone for these AI-driven advancements. Reference [61] bridges the gap between Artificial Intelligence and formal IT governance, offering a strategic roadmap for Saudi organizations to integrate AI while remaining compliant with international standards such as ISO/IEC 38500 and the COBIT 2019 framework. This ensures that AI implementations are both ethically governed and technically secure. Furthermore, the broader landscape of technology adoption in the public sector shows a clear trend toward automation. Reference [62] conducts an extensive analysis of the adoption of emerging technologies—such as AI, cloud computing, and IoT—within the Saudi public sector, mapping these advancements directly against the strategic objectives of Vision 2030. Utilizing the PRISMA methodology, the study identifies that while the pandemic accelerated the transition to smart platforms, meticulous planning and robust governance remain critical to overcoming cultural and organizational hurdles.

Achieving national-level digital resilience requires a collaborative, multi-stakeholder approach. Reference [63] presents a comprehensive case study identifying the key success factors required to establish cybersecurity excellence and digital resilience within Saudi Arabia. The resulting roadmap emphasizes the synergy between government regulation, private sector cooperation, and advanced technological defense. This collaborative spirit is essential for optimizing urban drivers. Reference [64] conducted a thorough systematic literature review to examine the strategic integration of Artificial Intelligence in optimizing smart city drivers, such as public safety and healthcare quality. By proposing a conceptual model for collaborative ecosystems, the study provides a roadmap for maximizing urban efficiency. Collectively, these studies suggest that for Saudi Arabia to achieve its smart city ambitions, it must harmonize technical defense with rigorous governance and a profound focus on human-centric security.

2.5. Current Research on Smart Cities in Saudi Arabia

The accelerated urbanization of Saudi Arabia, driven by the ambitious goals of Vision 2030, necessitates the incorporation of advanced digital technologies to manage complex city-states such as The Line in NEOM. As these centers evolve into sustainable smart cities, their dependence on networked IoT sensors, cloud-based governance platforms, and automated utilities markedly increases the national cyber-attack surface. While contemporary research has examined the socio-economic advantages of these technologies, a significant gap persists between high-level policy frameworks and the technical execution of resilient, AI-driven security architectures. Protecting essential infrastructure from non-linear threat vectors while achieving sustainability objectives remains an unresolved challenge in existing literature.

Table 1 provides a comprehensive review of the current research landscape on Saudi smart cities, which focus on governance, adoption, sustainability planning, or conceptual AI roles. While extensive literature exists on adoption models [65], social impacts [66],

and NEOM-specific Digital Twins [67], there is a noticeable lack of specialized, AI-driven threat detection tailored for sustainable urban infrastructure resilience across Saudi Arabia. For instance, although References [65,68,69] emphasize the importance of security, they do not provide specific AI detection models. Furthermore, while Reference [70] suggests that smart home strategies could scale to smart infrastructure, it lacks a unified framework that aligns threat detection with environmental sustainability—such as demonstrating how preventing a grid cyber-attack directly avoids energy waste. This gap inspired the proposed framework for Saudi urban infrastructure.

To provide a structured comparison of existing Saudi smart city research, the studies summarized in Table 1 were evaluated across five dimensions that are directly relevant to the proposed AI-based Threat Detection Mechanism (ATDM): (i) the urban infrastructure layer addressed by the study, (ii) the principal AI or cybersecurity contribution, (iii) the scope of the Saudi case study or application domain, (iv) the relationship between the study and sustainability objectives such as energy efficiency, resilience, governance, or resource optimization, and (v) the remaining research gaps and limitations. These dimensions were selected because they collectively capture the technical, operational, and sustainability-related factors required to assess AI-driven cybersecurity frameworks for sustainable smart city infrastructure.

The studies summarized in Table 1 were selected as representative contributions to the fields of smart city cybersecurity, AI-based intrusion detection, and sustainable urban infrastructure. The publications were identified through a structured search of major scientific databases, including IEEE Xplore and Web of Science, using combinations of keywords such as smart cities, cybersecurity, Artificial Intelligence, intrusion detection systems, IoT security, Saudi smart cities, and sustainability. The selected studies were chosen based on their relevance to the research objectives, methodological contribution, publication quality, and applicability to the proposed ATDM framework. Rather than providing an exhaustive survey, Table 1 establishes the theoretical foundation of this study by highlighting representative contributions, current research gaps, methodological limitations, and sustainability aspects, including resilience. These findings define the scope of the present study and help identify future research challenges and opportunities for SSCs and their supporting infrastructure.

Table 1. Summary of existing studies on AI-based threat detection and sustainability for Saudi smart cities.

Ref.	Urban Layer	Main Contribution	Case Study Scope	Sustainability with ATDM	Research Gaps & Limitations
[65]	Application: Behavioral	Developed the Cybersecurity-UTAUT model for adoption; no concrete AI detection model	Saudi smart cities	Social: User trust should be considered with ATDM	Focuses on conceptual and survey-based, not technical threat detection. Lacks technical validation
[66]	Application: Socio-cultural and service layer	Conceptual AI roles for addressing social issues and promoting SDGs	Cultural and social urban of Saudi smart cities	High: Directly aligns AI with some SDGs, which support societies in SSC	No operational AI models and lacks focus on threat detection or cyber-risks
[67]	Perception: Digital Twins	AI and Digital Twin integration for urban sustainability optimization	NEOM city in Saudi Arabia	High: Digital Twins can be considered to improve the ATDM and SSC environment	Cybersecurity and threat detection not addressed
[68]	Network: Cybersecurity and digital forensics	Impact analysis of digital forensics on city security; no specific AI model	Future Saudi smart cities	Resilience: Continuity of digital services; implicit sustainability link	Largely descriptive overview; lacks specific AI model

Table 1. Cont.

Ref.	Urban Layer	Main Contribution	Case Study Scope	Sustainability with ATDM	Research Gaps & Limitations
[69]	Perception: IoT and user layer	AI-powered behavioral and trust-based adoption model for smart home devices	Saudi smart homes	Trust: The ATDM in the individual home allows us to maintain SSC through indirect sustainable adoption of IoT	Focuses on awareness rather than technical threat detection or AI models
[70]	Perception: IoT/smart	Proactive forensic meta-model for smart homes	Saudi smart homes and the residential sector will create the SSC with AD&TM	Operational: Indirect sustainability through resilient homes and long-term device reliability	Limited to smart homes, not critical city-level infrastructure or urban threat management
[71]	Cross-Layer: Governance and services	XAI impacts applied to Saudi smart cities	Applied study on Saudi cities	Governance: Support transparency in AI decision-making	No focus on real-time anomalies or cybersecurity operations
[72]	Application: E-government	Analysis of E-government role on smart city initiatives; no AI model	Saudi National perspective	Economic: Effectiveness in the administration of public resources must be maintained in SSC with AD&TM	Limited focus on the technical cybersecurity or AI-based detection mechanisms
[73]	All Layers: Multi-domain smart city assessment	Benchmarking Saudi cities' progress via a maturity framework; no AI model	Only focuses on four Saudi cities: Riyadh, Makkah, Jeddah, and Medina	Urban: The future SSC should have equitable infrastructure development to maintain the Saudi multi-domain SSC	Does not address cyber threats or AI-driven monitoring
[74]	All Layers: Strategic	Strategic analysis for advanced digital technologies	NEOM city and Qiddiya in Saudi	Strategic: To maintain the smart transport system, the explicit low-carbon technology pathways should be used within the SSC	No AI-based cybersecurity frameworks
[75]	Network: Infrastructure and services	Conceptual AI-driven solutions for urban services	NEOM and Riyadh in Saudi	Industrial: Protecting the infrastructure's longevity	Lacks deep data on cybersecurity threat or AI threat-detection models

ATDM is considered in Table 1 with the threats which affect the Saudi urban infrastructure, but these threats can be detected and managed using AD&TM. Figure 3 illustrates a representative application of the proposed ATDM within the healthcare domain. The figure was originally developed by the authors in our previous work [76] and is reproduced here to demonstrate how the conceptual ATDM architecture can be applied to one of the critical services within SSCs. As illustrated, healthcare systems are vulnerable to evolving threats, cyberattacks, and associated risks, highlighting the need for robust AD&TM capabilities. Within the proposed ATDM, AD&TM enables proactive monitoring, anomaly detection, threat analysis, and mitigation, thereby improving the security and resilience of healthcare services. Although healthcare is presented as an illustrative example, the underlying ATDM architecture is generic and can be extended to other smart city sectors, including transportation, energy, public safety, and other critical infrastructures. Together with the integrated architectures presented in Figures 1 and 2, the proposed framework is expected to strengthen cybersecurity while supporting broader sustainability objectives, including improved energy efficiency, resilient service delivery, and secure Saudi urban infrastructure.

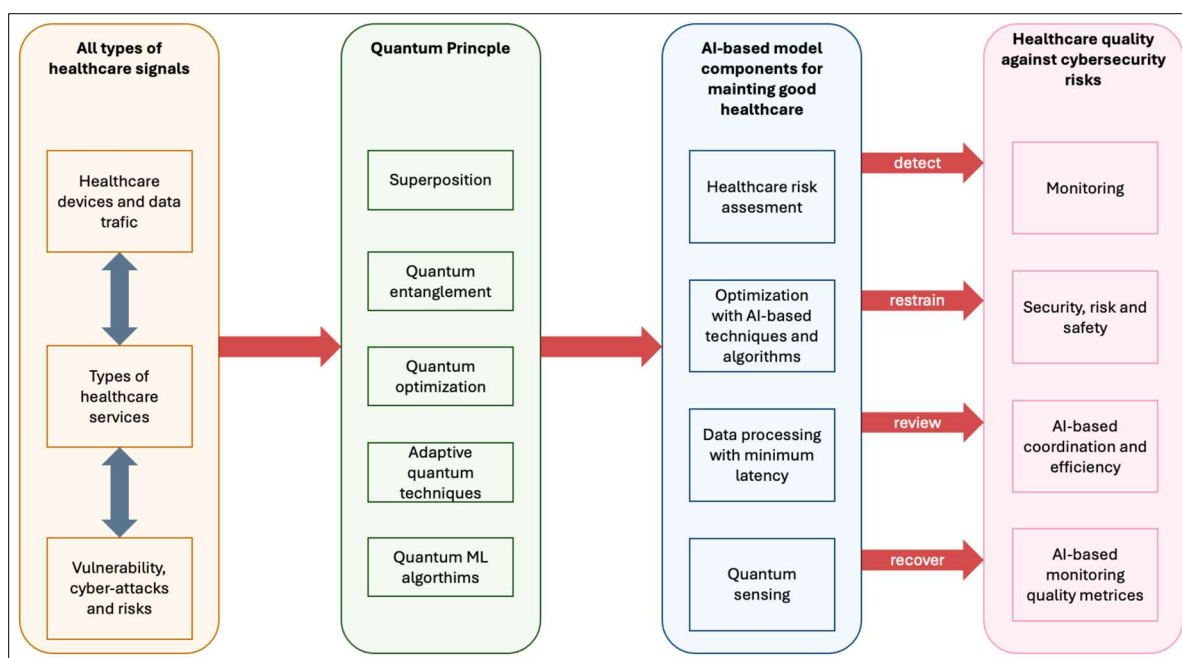


Figure 3. ATDM-based model for secure and sustainable healthcare. Reprinted from Ref. [76].

3. Materials and Methods

Although the case study serves as the primary research approach, a range of methods and techniques are analyzed to address emerging AI-driven threats and cyber-attacks. While multiple solutions can be derived from existing approaches, this study focuses on identifying the most effective methods to achieve maximum security and EE.

An AI-driven proactive model is considered the most suitable approach for detecting evolving cyber threats in SSCs. The proposed AD&TM incorporates specialized AI algorithms, energy-efficient cybersecurity techniques, and quantum-inspired technologies to identify, analyze, and mitigate threats affecting smart city services. Furthermore, the framework envisions multiple security hubs to enhance both security and energy efficiency across SSC environments.

AI-driven cybersecurity techniques will be employed to evaluate preliminary models aimed at improving the sustainability of smart cities within the context of this case study. To ensure robustness, all identified requirements of the AD&TM will be validated using appropriate analytical and simulation tools. Theoretical insights derived from the case study will guide the selection, design, and implementation of an optimal model for future SSC systems.

The ATDM can be developed using an appropriate mathematical model, such as that described in Equation (1). In this case study, the equation has not been implemented or evaluated in detail; however, it can be integrated into a Q-AI framework for future investigation.

To achieve the research objectives, Saudi smart city requirements, representative use cases, and security enhancement strategies are considered to support the sustainability of next-generation SSCs. Table 2 presents example technical concepts and enabling technologies for future security management. According to [77,78], anomaly detection (AD) is a fundamental component of security management for identifying attacks against enterprise systems and critical infrastructures. Accordingly, integrating anomaly detection (AD) with threat management (TM) provides the conceptual foundation of the proposed ATDM.

Table 2. Methods of improving security in Saudi urban infrastructure.

Security Management of Saudi Urban Infrastructure	Examples of Technical Concepts and Materials with the AD&TM Method	Expected Solutions for the Next-Generation SSC
Sustainability	IoT networks	Sensors for road traffic, automation of energy monitoring
Smartness of hubs	Data centers	Continuous hub monitoring for securing all types of data
Network infrastructure with Internet	IQN	Securing continuous services
Technological innovation	Hybrid Q-AI	A hybrid approach with quantum and AI for automating threat intelligence
Quantum communication channels	Quantum routing scheme	Managing universal intelligence in threat detection

To further clarify the case study methodology and the data requirements for the proposed framework, the following considerations are presented. According to [79], the 15 characteristics required for this research case study were considered. Although this study is not an actual empirical case study, references [80,81] provide the necessary guidance for identifying and collecting the data and information required to investigate an SSC in the context of Saudi urban areas.

Although we intended to collect datasets covering all 15 priority areas [79], no comprehensive dataset currently exists that integrates these characteristics with AI- and quantum-enabled IDS features. Future studies can utilize such datasets to perform data collection, preprocessing, exploratory data analysis, statistical analysis, and predictive modeling.

The lack of comprehensive datasets encompassing all 15 priority characteristics, together with the assumptions associated with the proposed analytical models and quantum-based developments, represents a key limitation of this study.

To demonstrate the applicability of the proposed framework, conceptual experiments were conducted using data derived from the IMD Smart City Index 2026 for Jeddah, Saudi Arabia. The analysis considered the 15 priority smart city indicators identified by the IMD survey across key urban domains, including health and safety, mobility, governance, opportunities, and quality of life [56,79]. These indicators were used as representative variables to examine the relationship between sustainability objectives, cybersecurity requirements, and the proposed ATDM. The resulting conceptual analysis, presented in this study, illustrates the potential impact of AI-enabled intrusion detection and emerging technologies on improving the security, resilience, and operational efficiency of sustainable smart city services. Because no comprehensive dataset currently integrates all 15 priority indicators with AI- and quantum-enabled IDS features, these results should be interpreted as a conceptual demonstration that establishes the foundation for future quantitative validation.

3.1. Proposed Framework with AI-Driven Design and Architecture

An AI-driven strategy can employ multiple threat detection approaches to enhance the security of smart cities and their infrastructure, including communication systems. AI-based IDSs can significantly reduce the time required to identify and respond to security incidents while continuously adapting to emerging threats and changes in urban environments. By strengthening anomaly detection and threat management capabilities, these systems contribute to the resilience and sustainability of SSCs.

The proposed framework incorporates the ATDM, which is dependent on the AD&TM. In addition, the framework integrates security policies, advanced IDS technologies, and ETs to provide a comprehensive cybersecurity solution for SSCs.

Furthermore, the framework leverages AI-driven designs and architectures enhanced by quantum-based techniques. The integration of AI and quantum technologies enables the efficient exploration of multiple solution spaces, reducing the complexity of system design and optimization. Quantum-enabled proactive mechanisms further reinforce cybersecurity, while adaptive threat detection capabilities help address the challenges posed by evolving cyber threats and rapidly advancing technologies.

3.2. Quantum-Enabled Threat Detection Mechanism

The AI-driven design and architecture must be secured using effective threat mitigation mechanisms. Quantum-enabled approaches can further enhance security in smart cities and their infrastructure.

The proposed framework, along with those mentioned above, enhances ATDM through quantum-enabled threat mechanisms. Hybrid Q-AI can identify attacks during data transmission and traffic management within SSC. Quantum key management enables service providers to secure traffic autonomously. PQC algorithms protect sensitive patient records when mIoT is integrated into SSC medical services. Additionally, quantum-secure identity solutions can be used to detect threats in biomedical applications, such as risks associated with cloneable digital security.

Figure 4 presents a multi-layered theoretical framework for AI-driven threat detection in secure smart cities facilitated by ET. The framework integrates several functional layers, including a 6G-enabled ET infrastructure, an expanded IoT layer—encompassing mIoT and vIoT—and a suite of smart city application services, all unified under an intelligent security management system. At the edge, smart monitoring and communication devices continuously generate high-velocity data, which is processed through AI-driven detection mechanisms that incorporate machine learning algorithms, robust cybersecurity frameworks, and standardized protocols. This synergy enables real-time anomaly detection, intrusion identification, and cross-layer threat correlation. Ultimately, the framework supports end-to-end security orchestration in SSC, bolstering system resilience and enabling adaptive responses across heterogeneous smart urban environments.

The implementation of the proposed method and approaches is illustrated through the flowchart (Figure 5), which outlines the key steps required to reach the solutions of the case study. Information security policies and best practices derived from established cybersecurity frameworks, such as the NIST Cybersecurity Framework and the NICE Cybersecurity Workforce Framework (NCWF), can be integrated with other recommended frameworks such as the ATDM and the AD&TM to enhance the IDS and other security solutions.

Secure AI-driven anomaly detection and threat management systems with information security policies based on the cybersecurity frameworks (NIST, NICE, etc.) can be considered to design, develop and implement the ATDM. Further, communication protocols are also considered in the flowchart for AI-based IDS deployment in smart cities, to secure information shared between the distributed IDS components.

Figure 5 shows the development procedure of the AI-based IDS designed for detecting evolving threats in the future Saudi urban infrastructure of smart cities. This flowchart allows us to achieve the aim through the proposed objectives, which include the efficient ATDM with maximum EE, minimum latency and information security policies.

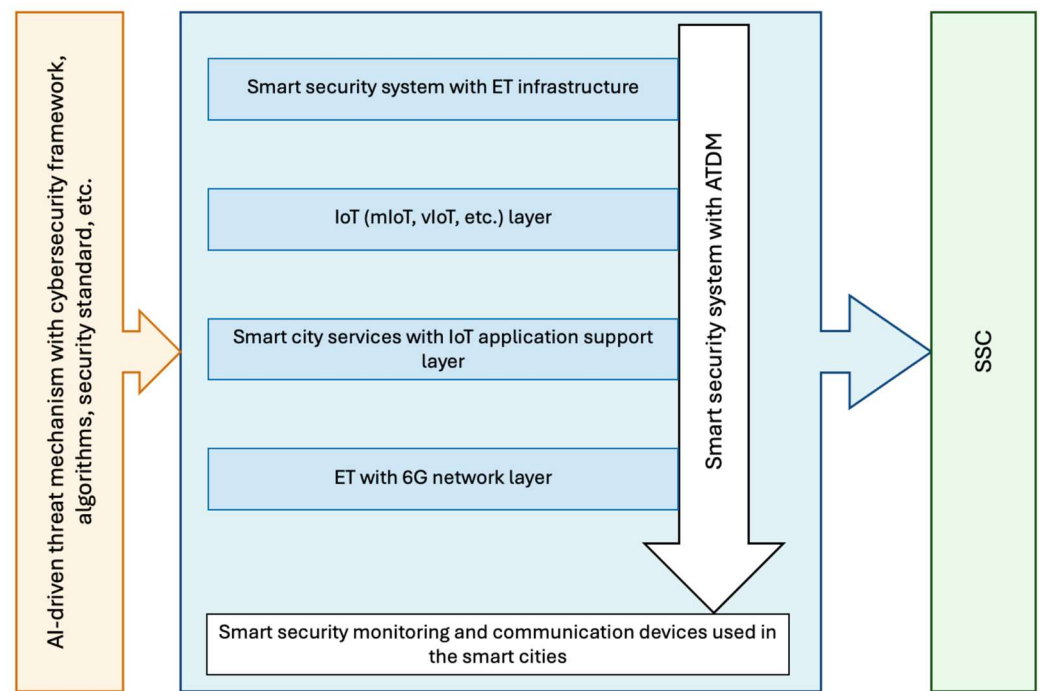


Figure 4. Theoretical framework with ET for secure smart cities.

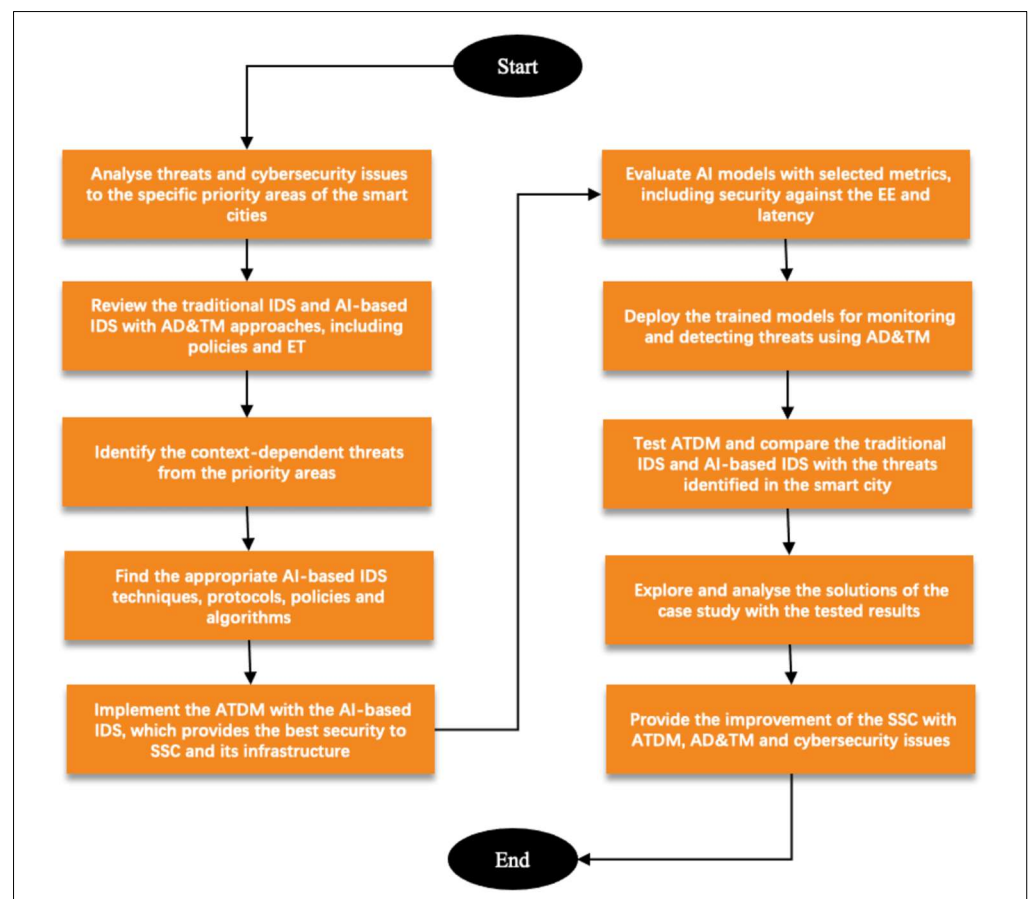


Figure 5. Proposed framework flowchart with AI-based IDS designed for smart city systems.

Since this study proposes a conceptual framework rather than an implemented intrusion detection system, reproducibility refers to the framework development methodology rather than the replication of experimental results. Figures 4 and 5 present a replicable

research process by outlining the required materials, framework design, and theoretical development steps, thereby enabling other researchers to reproduce and extend the proposed approach. Furthermore, the proposed framework is based on well-established CNN methods, which employ standardized mathematical operations, shared filter weights, and reproducible feature-learning mechanisms that have been widely adopted in AI-based IDSs and network intrusion detection systems (NIDSs). These characteristics further support the reproducibility and future implementation of the proposed framework.

To maximize secure routing in the network infrastructure of the SSC, routing optimization (Q_{RO}) for IDS is given in Equation (2).

$$Q_{RO} = \underset{i}{\operatorname{argmax}}(w_s S + w_t T + w_q Q_i + \dots + w_q Q_n) \quad (2)$$

where S is the security score, and T is the trust value of the risk management based on the cyber threats and attacks. The quality of quantum channels (Q_i to Q_n) may be considered to improve the services of the smart city. The number of channels ($i = 1$ to n) can be used to provide the service when several users are involved. Also, w_s , w_t , and w_q are the weights of the routing optimization equation. In the CNN-based IDS, the Q_{RO} may be employed to improve accuracy of detection.

3.3. Technical Specification of the Proposed ATDM

As illustrated in Figure 3 (ATDM-based model for secure and sustainable system (one of the systems in the smart cities)), the proposed ATDM processes heterogeneous signals generated by the ET smart infrastructure. For instance, a healthcare system can be illustrated as one of the systems for the technical specification of the proposed ATDM. The input data, represented in the first module of Figure 3, include network traffic, IoT-enabled medical sensor data, communication logs, system events, operational telemetry, and other cybersecurity-related information collected from interconnected healthcare devices and services. From these inputs, the ATDM extracts features related to evolving cyberattacks and security threats affecting healthcare-related SDGs, including abnormal network behavior, intrusion attempts, malware, denial-of-service attacks, insider threats, and zero-day attacks.

The extracted features, including communication patterns, packet statistics, authentication events, protocol information, temporal behavior, and technical constraints associated with quantum protocols, security algorithms, and intelligent sensing devices, are processed through data preprocessing, feature extraction, anomaly detection, threat classification, risk assessment, and automated response modules. The framework employs the AI models, particularly CNN and Support Vector Machines (SVMs), where CNN performs multi-layer feature learning and non-linear data transformation to identify both known and previously unseen attacks. The detected anomalies are classified using adaptive decision thresholds based on the operational characteristics of the ET environment, enabling more effective detection of evolving and zero-day threats than conventional signature-based IDSs. Furthermore, the proposed framework incorporates a NIDS to strengthen network security by identifying and responding to malicious traffic within the smart healthcare infrastructure.

Although the ATDM architecture and processing workflow are presented conceptually, this case study does not include a complete simulation or experimental evaluation. Consequently, the proposed framework has not yet been quantitatively validated or compared with existing approaches, and its performance should be regarded as a conceptual demonstration pending future empirical validation using real-world datasets.

3.4. Preparation of Figures

The conceptual diagrams presented in this manuscript were created using Microsoft PowerPoint, while the charts and graphical analyses were prepared using MATLAB R2024a. All figures were produced by the authors based on the proposed framework and the referenced literature.

4. Results

The primary goal of the proposed research is to analyze SSCs, their security benefits, and their resilience through the integration of AI and quantum technologies, supported by a case study. The research evaluates approaches for addressing AI-driven threats and attacks identified within the case study and demonstrates their potential benefits for SSC users and service providers. Compared with existing solutions, AI-based proactive systems—particularly the proposed research and ATDM—are expected to provide significant advantages by improving the robustness of protection measures while achieving high levels of security and EE. In addition, the research contributes to the advancement of AI- and quantum-enabled security concepts and establishes foundational principles for their implementation in next-generation SSC architectures.

Although empirical evidence suggests that the factors presented in Table 3 can contribute to reducing overall costs, these benefits have not been validated within the scope of this conceptual case study and should therefore be regarded as potential rather than confirmed outcomes. IDSs play a vital role in securing the network infrastructure of sustainable smart cities in Saudi urban areas. AI-based IDSs and NIDSs, particularly those employing CNNs and other deep learning techniques, can significantly enhance the detection of emerging cyberattacks and security threats. Compared with traditional machine learning methods, CNN-based IDSs automatically learn discriminative features from high-dimensional data, thereby improving detection accuracy, adaptability, and resilience. Consequently, CNN-based approaches have been widely adopted to strengthen IDS and NIDS solutions for addressing cybersecurity, privacy, and data protection challenges in smart city environments. Specifically, NIDS plays a critical role in the modern smart city infrastructure of the future Saudi urban areas, because the dimension of future network communication will be modified to a cubic network architecture with multiple layers [82].

Table 3. Conceptual evaluation of the proposed ATDM framework.

Empirical Consideration	Potential Challenge	Expected Benefit
Energy cost vs. cybersecurity	Energy consumption and operational costs in SSCs continue to increase.	Advanced AI-based cybersecurity can improve infrastructure protection while reducing operational costs in the ET environment.
Digital healthcare vs. data security	The reliability of digital healthcare services depends on secure and trustworthy data transmission.	Improved data security can enhance the accuracy, reliability, and integrity of digital healthcare services.
AI-based SDGs vs. AI-based IoT security	The rapid expansion of IoT devices increases the cybersecurity risks associated with AI-driven SDG applications in smart cities.	Secure AI-enabled IoT infrastructures can support the reliable achievement of healthcare-related SDGs in SSC.
Agricultural energy vs. security management and AI-based IoT security	Agricultural industries use energy for their farming tools and systems, but many cyber-attacks occur during the operations.	Security management of the energy sources and harvesting can be improved by using IoT security and AI-based security management.

The expected outcomes of the proposed research within SSC and its services include:

- Establishing theoretical and technical foundations to improve measurements related to SSC security issues, encouraging further research on ATDM using AI techniques and quantum technologies.
- Developing practical AI-based security monitoring tools for SSC services, based on AI algorithms and quantum protocols.
- Extending existing software-based protocols to support intelligent security solutions in SSC environments.
- Enhancing predictive measurement capabilities for current features used in SSC and their services.

In addressing AI-driven challenges, the solutions identified through the case study and the ATDM framework, supported by quantum-enabled proactive mechanisms, are expected to contribute to technological innovation in SSCs.

Figure 6 shows the improvement in Saudi urban infrastructure (Jeddah city as an example) when ATDM is employed alongside evolving ET. Future SSCs will focus on many features; however, we illustrate 15 features [79] currently used in Saudi SSCs. All features depend on ET and evolving cyberattacks, which affect overall systems and infrastructure in Saudi smart cities.

Although the 15 features shown in Figure 6 are considered within Saudi urban smart cities, the implementation of the ATDM can enable service providers to strengthen security solutions across the current Saudi urban infrastructure. In response to evolving threats and emerging challenges, future SSCs in Saudi Arabia are expected to incorporate enhanced security measures and proactive protection strategies.

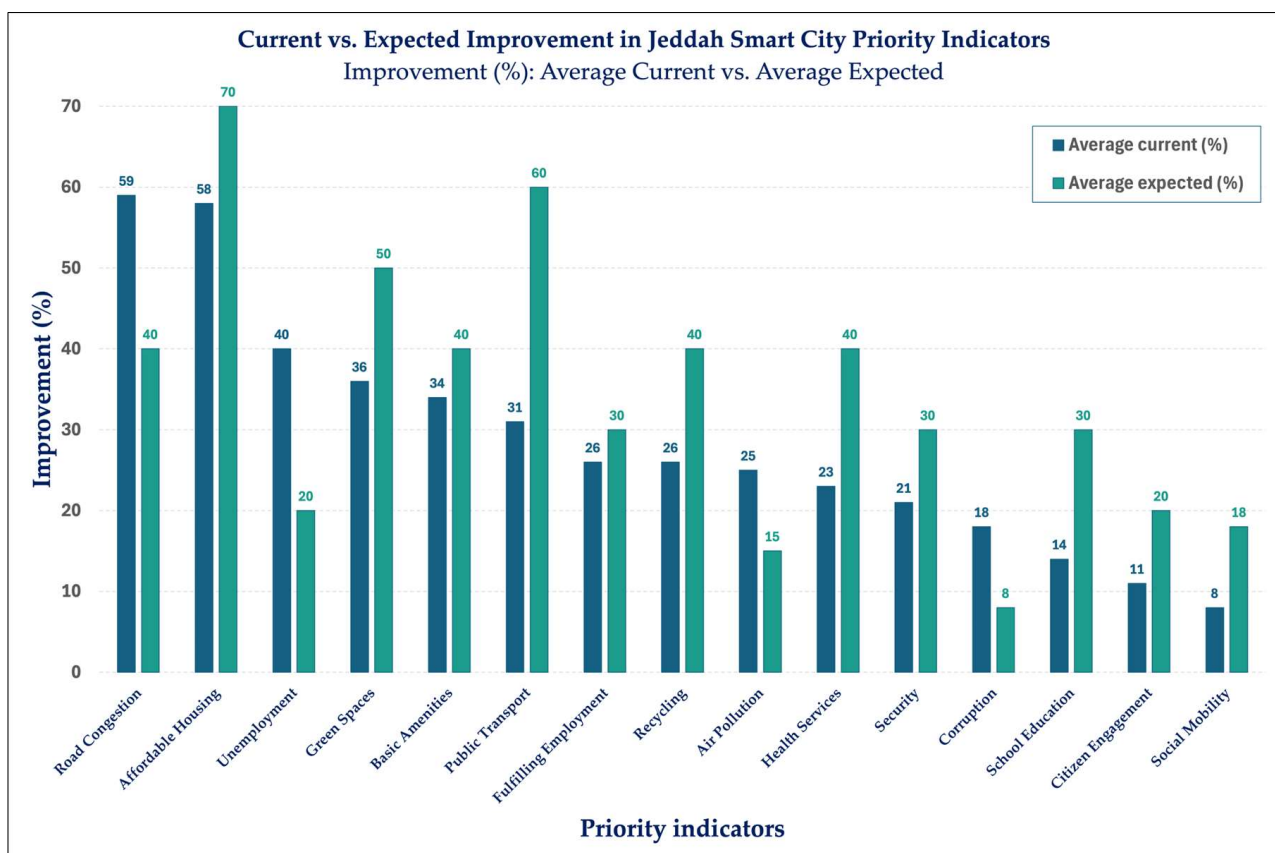


Figure 6. Comparison of current and expected SSC features with ATDM for a Saudi urban smart city (Jeddah).

Table 4 presents a qualitative comparison between representative AI-based intrusion detection approaches and the proposed ATDM. The comparison is intended to illustrate differences in architectural capabilities, security mechanisms, and integration with emerging technologies rather than to report experimentally measured performance. According to [83], SVMs and CNNs have been extensively studied for improving the security performance of IDSs. Therefore, these baseline models were selected for integration into the proposed ATDM, as they represent the traditional machine learning and deep learning paradigms, respectively. In particular, CNN-based IDS approaches were selected because they have demonstrated promising performance in previous studies [83]. The reviewed CNN-based IDS approaches are categorized into four groups: (1) standalone CNN models; (2) CNNs combined with Recurrent Neural Networks (RNNs), such as LSTM or Gated Recurrent Unit (GRU) networks, for temporal feature extraction; (3) CNNs integrated with deep learning techniques other than RNNs; and (4) CNNs combined with machine learning, fuzzy logic, Fourier transform, clustering, or evolutionary algorithms to further enhance intrusion detection performance.

Table 4. Qualitative comparison of AI models with the IDS and priority areas.

AI Models	Description of Models and IDS	Overall Improvement
AI-1	Traditional SVM and IDS without priority areas	Depends on the IDS architecture
AI-2	The SVM and IDS with the priority area	Depends on the IDS, threat types and priority areas
AI-3	Traditional CNN and IDS without priority areas	Depends on the IDS architecture
AI-4	The CNN and IDS with the priority area	Depends on the IDS, threat types and priority areas
AI-5	The ATDM with proposed research	Depends on the ET (quantum technology), policies, IDS and priority areas

Figure 7 shows the EE with conventional IDS (basic), AI-based IDS with ET (emerging quantum approaches) and ATDM involved with AI-based IDS, ET and policies of cybersecurity, such as those given in the NIST framework. To increase the EE, Equation (1) and policies recommended in NIST can be considered within the ATDM.

Figure 8 shows the latency with conventional IDS (basic), AI-based IDS with ET (emerging quantum approaches) and ATDM involved with AI-based IDS, ET and policies of cybersecurity, such as those given in the NIST framework. Although the complexity of the proposed approach is high, the latency can be reduced when quantum technology is deployed during the development of the proposed framework with ATDM, which includes the cybersecurity policy.

Critical sectors such as roads, housing, transport, and healthcare services can be monitored continuously (24/7) using AI-based quantum sensors, thereby improving threat detection and prevention capabilities. Smart housing systems should rely on secure, trustworthy, and reliable Internet connectivity to minimize vulnerabilities arising from malicious links, fraudulent websites, and cyberattacks. The integration of IQN can further enhance the identification and mitigation of such threats. Similarly, security risks affecting public road services remain significant and should be minimized to establish safer and more resilient urban environments.

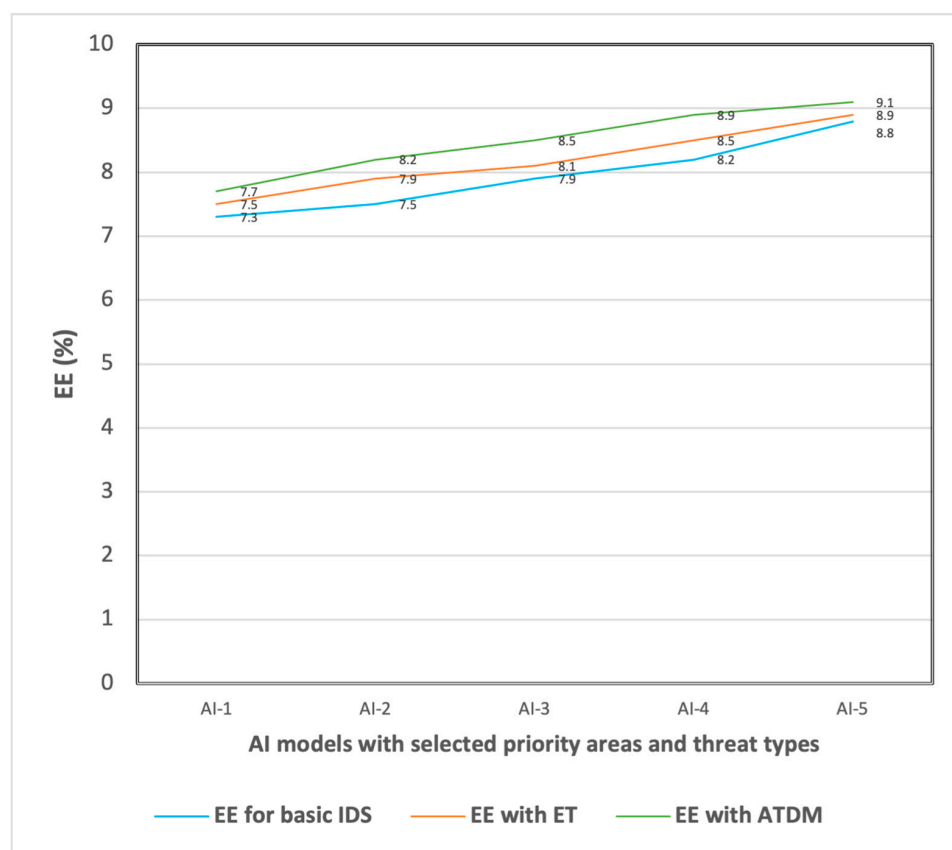


Figure 7. Comparison of EE with different AI-based IDS models.

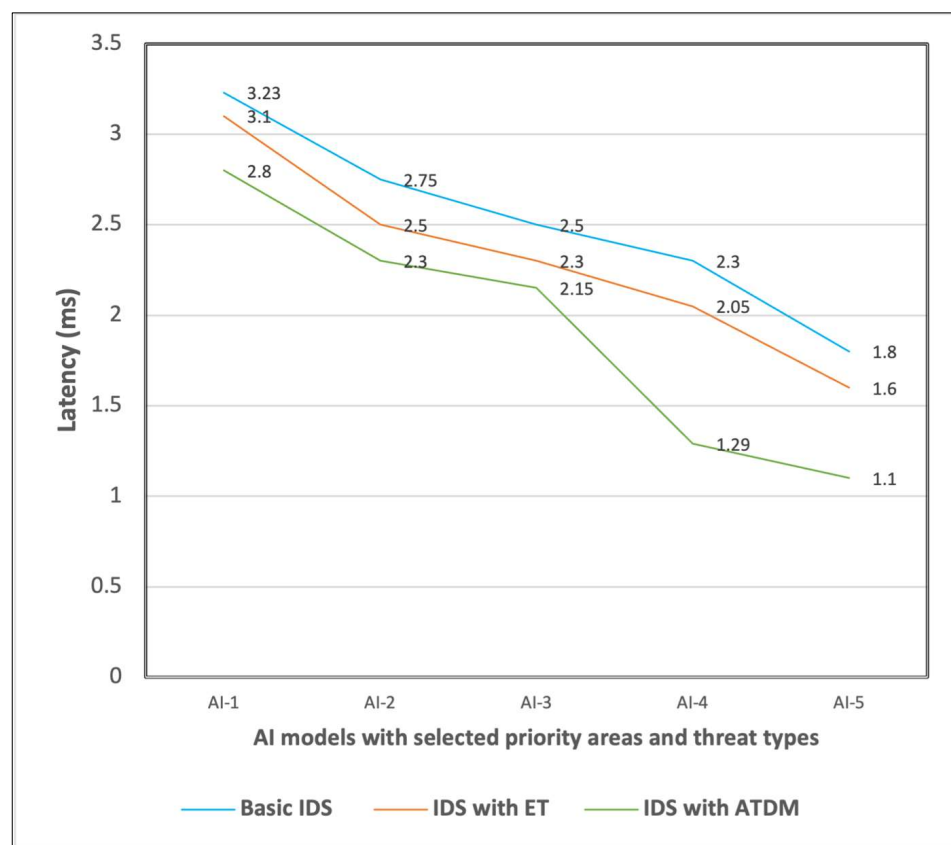


Figure 8. Comparison of latency with different AI-based IDS models.

Real-time anomaly detection of 15 priority data traffic and scalable IDS in smart cities requires actual datasets. To validate the ATDM with AI-based IDS models, more complex data of 15 priority areas and traffic patterns in all services can be tested. The traditional signature-based and AI-driven IDS methods have been compared in these results.

As AI and AI-based systems become increasingly integrated into SSCs, concerns regarding employment and workforce transformation may arise. To address these challenges, Saudi smart cities should promote citizen engagement and workforce development programs that equip individuals with relevant skills for emerging job opportunities. Advanced AI systems can also support workforce management by matching individuals to suitable roles based on their skills, qualifications, and availability.

In the future, AI is expected to play a significant role in mitigating complex threats within SSCs while reducing operational costs and maximizing sustainable security. Furthermore, next-generation AI systems integrated with Q-AI technologies can enhance energy management through secure communication and intelligent control of energy resources. Workforce challenges may also be addressed through AI-driven recruitment and decision-support systems, which can improve candidate identification, skill matching, and selection processes while reducing inefficiencies associated with conventional approaches.

Table 5 presents a set of recommended solutions for selected SSC cases within the Saudi urban infrastructure. These solutions are intended to enhance security management and minimize or remove evolving threats. Furthermore, their implementation can contribute to improving the overall security and resilience of next-generation SSC.

Table 5. Solutions of case examples with the threat detection methods.

SSC with Saudi Urban Infrastructure	Remarks on the Results with the AD&TM Method	Threat Detection Methods for the SSC
IoT sensors and devices	Offering secure services using IoT networks	AI-based secure IoT systems
Health, finance, etc.	Investigating threats and risks quickly, proactively and accurately	Automation algorithms for continuous security monitoring
Energy infrastructure and integration	High latency and delay are experienced during energy distribution and operation	Quantification with quantum, AI and AI-based cybersecurity
Transportation, including autonomous vehicles	Regarding road traffic issues and real-time data handling	Quantum cryptography and hybrid Q-AI algorithms for proactive issues
Citizen engagement for social and other peaceful environments, such as preventing high pollen problems	Availability of accessing all necessary information, including E-learning quantum routing scheme	Secure quantum routing scheme using secure quantum communication channels

The impact on each feature may vary depending on the type and severity of the threats encountered. By integrating the proposed framework with the AD&TM, hybrid Q-AI technologies, and Equation (1), smart cities can achieve a higher level of sustainable security across the 15 features considered in this case study.

Although Table 5 presents general solutions for the case study, several illustrative examples are also provided. Availability is one of the CIA components in cybersecurity that determines whether cyber threats attack the quantum channel or any communication channel to access the information (E-learning) about the pollution.

5. Discussion and Analysis

As shown in Figure 9, which was developed based on the Saudi Vision 2030 program, the IMD Smart City Index 2026, and the literature reviewed in Section 2, future SSCs are expected to increasingly integrate quantum technologies, which are likely to play a signifi-

cant role in the development of next-generation urban environments. These technologies have the potential to enhance various smart city services, particularly energy management systems, where real-time optimization, secure communication, and intelligent decision-making are essential for achieving sustainability goals. The proposed ATDM framework contributes to this vision by enhancing the robustness of cybersecurity through CNN-based IDSs integrated conceptually with AI and quantum-enabled threat detection mechanisms. The theoretical analysis indicates that the proposed framework can improve energy efficiency, security resilience, and overall system performance compared with conventional IDS approaches.

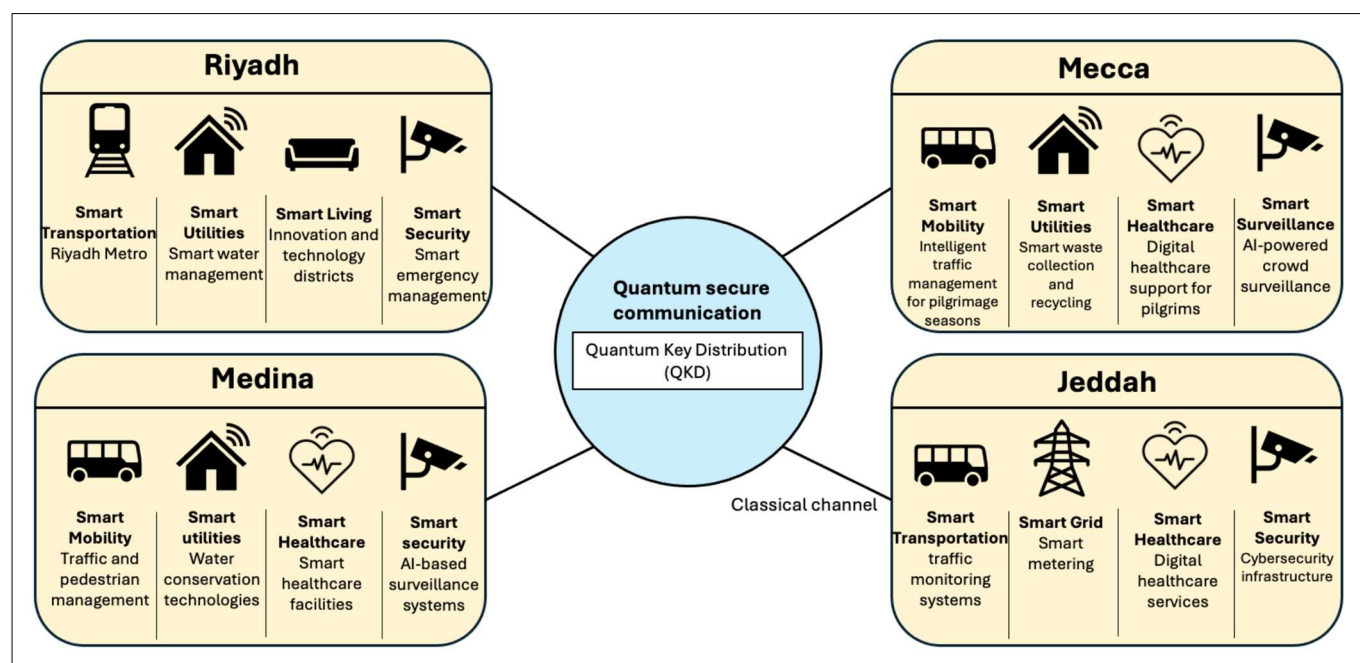


Figure 9. AI-powered quantum security management for the Saudi smart cities.

The findings of this conceptual case study are consistent with previous studies that identified AI-driven intrusion detection as an essential component of future smart city cybersecurity. However, unlike many existing studies that focus primarily on individual technologies, such as AI-enabled intrusion detection, Digital Twins, IoT security, or digital forensics, the proposed ATDM integrates these capabilities within a unified conceptual framework that also incorporates sustainability objectives and emerging quantum technologies. For example, previous studies summarized in Table 1 mainly investigate specific aspects of smart city security, including AI-based monitoring, Digital Twin applications, smart home security, explainable AI, and governance. In contrast, the proposed framework combines AI-driven anomaly detection, threat management, cybersecurity policies, and quantum-enabled technologies to provide a holistic conceptual architecture for sustainable smart city protection in Saudi urban infrastructure.

Enhancing future security and energy efficiency in SSC will be the ultimate finding of this research. With evolving and emerging technologies, not only the security facilities but also the green energy and emission reduction benefits of renewable energy and low-carbon transformation will be improved in future findings of smart cities.

Compared with conventional AI-based intrusion detection studies that primarily evaluate machine learning or deep learning models, such as SVM- and CNN-based IDSs [83], the proposed framework extends these approaches by conceptually integrating PQC, quantum communication, intelligent security policies, and sustainability objectives. Although the

framework has not yet been experimentally validated, it establishes a theoretical foundation for future quantitative evaluation of secure and sustainable smart city infrastructures.

At the core of this vision, AI serves as the enabling engine of SSCs, while service providers in the four selected cities act as operational entities that manage and coordinate smart city functions, including transportation, energy, healthcare, and public services. In this context, service providers represent quantum-enabled operational components responsible for initiating, coordinating, and maintaining the smartness of the city infrastructure.

To support these intelligent operations, large-scale data collection and analysis are required across multiple domains, including smart transportation, smart grids, healthcare, and surveillance. As a result, AI systems demand substantial computational and data-processing resources due to the massive volume of data generated by interconnected urban infrastructure. To address these requirements, hyperscale data centers can be deployed to provide the storage, processing, and analytical capabilities needed for AI-driven applications and services.

The relationship between cybersecurity and the SDGs is fundamental to future SSCs because secure and reliable data are essential for the operation of smart city services. The proposed ATDM does not directly improve sustainability through energy generation or environmental interventions; rather, it contributes indirectly by enhancing the security, availability, and resilience of critical services, including transportation, healthcare, smart grids, water distribution, and IoT infrastructures. AI-based models, particularly CNN and CNN-based IDS, together with emerging technologies such as quantum routing and quantum optimization, are conceptually integrated into the ATDM to proactively detect evolving cyber threats. By mitigating cyberattacks that may increase service disruptions, energy waste, operational costs, and resource inefficiencies, the proposed framework can support more efficient utilization of urban resources and improve the long-term sustainability of smart cities. Furthermore, the proposed quantum routing equations and AI-based security models provide a conceptual foundation for future quantitative evaluation using measurable sustainability indicators, including cybersecurity performance, energy consumption, and resource efficiency across SDG-related smart city applications.

At the application level, LSTM networks can be employed in smart buildings within SSCs. When combined with AI and quantum technologies, LSTM-based systems can enhance intelligent monitoring, prediction, and decision-making processes. Such capabilities enable smart buildings to respond more effectively to changing environmental conditions, optimize resource utilization, and improve operational efficiency.

From a security perspective, quantum-based threat modeling can be utilized to anticipate, analyze, and mitigate future cyber threats and attack scenarios. As smart city infrastructures become increasingly interconnected, proactive threat detection mechanisms will be essential for maintaining security and resilience. According to [84], the authors proposed a privacy-preserving and secure framework based on a blockchain-enabled, quantum-inspired complex Convolutional Neural Network for IoT-driven smart cities. Their findings demonstrated that cyberattacks and security threats can be effectively detected and mitigated through the integration of quantum-inspired technologies, blockchain mechanisms, and advanced AI techniques.

The findings also highlight the close relationship between cybersecurity and sustainability. Sustainable smart cities require reliable and adaptive cybersecurity solutions to ensure the continuous availability, integrity, and confidentiality of critical urban services. AI-based CNN IDSs, supported by emerging technologies, can improve resilience against evolving cyber threats while maintaining efficient resource utilization and reducing operational costs. As summarized in Table 3, these conceptual findings suggest that stronger cybersecurity can contribute to lower energy costs, more reliable digital healthcare services,

and secure AI-enabled IoT infrastructures that support the achievement of the SDGs. Furthermore, future applications such as the Agricultural Energy Internet (AET) may benefit from secure and energy-efficient smart city infrastructures by reducing energy consumption and strengthening agricultural sustainability.

Emerging technologies such as AI-Radio Access Networks (AI-RANs) and quantum communication are expected to further strengthen future SSC infrastructures through intelligent automation, adaptive networking, and proactive cybersecurity. These technologies represent promising future research directions once mature implementations and real-world datasets become available.

The proposed framework has several strengths. It provides an integrated AI- and quantum-based cybersecurity architecture that aims to maximize security while minimizing energy consumption and operational costs, thereby supporting both the smartness and sustainability of SSCs. However, the framework also has limitations. The rapidly evolving nature of cyber threats, emerging technologies, and changing environmental conditions requires continuous adaptation, while the lack of comprehensive real-world datasets limits empirical validation of the proposed approach.

To evaluate the effectiveness of the proposed ATDM, measurable Key Performance Indicators (KPIs) can be employed in future implementations. Monitoring security performance by analyzing normal and anomalous operational behavior can support the early detection of cyber threats and provide a quantitative basis for assessing the resilience of SSCs. The measurable KPIs considered in this study include the number of security incidents, patch management compliance, vulnerability remediation time, employee security awareness and training completion, and detection latency. Furthermore, when the proposed routing optimization model in Equation (2) is applied to optimize latency and other technical constraints, these KPIs are expected to improve, thereby enhancing the overall cybersecurity performance, operational resilience, and resource efficiency of SSCs and their network infrastructure.

Overall, the combination of AI, quantum technologies, advanced data analytics, and intelligent threat detection mechanisms provides a promising foundation for the development of secure, resilient, and sustainable smart cities. These technologies can enhance operational efficiency, strengthen cybersecurity, and support the long-term sustainability objectives of future Saudi urban infrastructure. The conclusions presented in this study are supported by the conceptual framework, literature review, and theoretical analysis. However, expectations regarding quantitative performance improvements, energy savings, and quantum-enabled capabilities remain future research objectives that require empirical implementation and validation. In summary, the key observation of this work is that integrating AI, cybersecurity, sustainability, and emerging technologies provides a promising pathway toward resilient, energy-efficient, and secure Saudi smart cities capable of addressing evolving cyber threats while supporting long-term sustainable development.

6. Limitations, Challenges, and Future Work

Although AI-driven threat detection mechanisms are well defined for future applications, human behavior remains one of the most challenging aspects, as it cannot be fully predicted, detected, or controlled. If AI technologies are misused, AI-driven threats may expand in scope and evolve into more complex forms. This represents a significant future challenge, potentially increasing both cost and energy consumption in smart cities. For example, conflicts driven by human decisions—such as tensions and wars—highlight limitations that AI and other technologies cannot address. While ethical values and moral considerations are widely studied in cybersecurity, their practical application to real-world issues, particularly those involving human behavior, remains limited.

6.1. Limitations

There are several limitations associated with the proposed ATDM. The framework has not been implemented or experimentally evaluated using benchmark intrusion detection datasets or operational smart city environments. Consequently, it has not yet been validated using standard cybersecurity performance metrics, such as accuracy, precision, recall, F1-score, false positive rate, detection latency, computational overhead, or energy consumption. The illustrative Saudi smart city case study is intended to demonstrate the applicability of the proposed framework rather than provide empirical evidence; therefore, the presented analyses, figures, and comparisons should be interpreted as conceptual illustrations and expected outcomes rather than experimentally verified results.

In addition, comprehensive datasets covering all 15 priority areas of sustainable smart cities are currently unavailable, particularly those involving the integration of AI-based IDSs, quantum technologies, sustainability indicators, and evolving cyber threats. As a result, comprehensive sustainability validation, including quantum sustainability validation (QSV) and other quantitative validation procedures, could not be performed. Furthermore, the proposed quantum-inspired techniques, routing models, and optimization approaches were not implemented or evaluated using quantum algorithms, communication protocols, or quantum hardware, and should therefore be regarded as conceptual enhancements and future research directions rather than operational components of the ATDM.

Furthermore, implementing AI-driven security mechanisms in sustainable smart cities also presents several practical challenges. Variations in human behavior within smart homes, differences in community behavior across cultural contexts, and the dynamic nature of emerging technologies make the design of universally effective AI-based threat detection systems difficult. Moreover, the current study does not investigate implementation-related issues such as scalability, computational complexity, deployment cost, interoperability with existing smart city platforms, privacy preservation, or regulatory compliance. Although CNN-based IDSs have demonstrated advantages over conventional machine learning methods by automatically learning complex features and improving intrusion detection performance, their effectiveness within the proposed ATDM remains to be validated using real-world smart city datasets. Finally, because the proposed framework was developed specifically for sustainable smart city infrastructure, further validation across diverse urban environments, infrastructure scales, and cybersecurity scenarios is required before its general applicability can be established.

6.2. Challenges with AI-Driven Architectures

Energy consumption and associated costs continue to rise with modern lifestyles, as reliance on advanced technologies increases. In smart cities, smart homes tend to adopt intelligent technologies and appliances that often depend on green energy sources. However, several challenges must be considered in this context.

Light and Heat: Direct sunlight can be harvested and converted into usable energy through technologies such as solar concentrators, large mirrors, and lenses. However, the efficient capture, storage, and distribution of this energy remain significant challenges within smart city infrastructures. The adoption of such technologies has the potential to reduce overall energy costs while improving the sustainability of energy management systems.

Quantum Computing in IoT-Enabled Smart Cities: Pollen monitoring and the establishment of low-pollen or pollen-free zones should be considered to enhance the quality of life in SSCs. Detecting pollen levels in and around smart homes is important for protecting public health, particularly for individuals with allergies and respiratory conditions. The integration of quantum computing techniques with IoT sensors can further enhance the detection and monitoring capabilities of the AD&TM.

Hybrid Q-AI for Next-Generation SSCs: The integration of quantum and AI technologies through a Q-AI approach can significantly improve the detection and prediction capabilities of future systems deployed in next-generation SSCs. In addition to cyber threats, emerging environmental challenges such as pollen exposure, heat waves associated with global warming, and other natural hazards should be incorporated into future threat management strategies. Addressing these challenges will contribute to strengthening the resilience, security, and sustainability of Saudi urban infrastructure and smart cities.

6.3. Future Work

Future research will focus on implementing and validating the proposed ATDM using both publicly available benchmark intrusion detection datasets and real-world operational datasets collected from the priority areas of sustainable smart cities. The proposed framework will be compared with conventional and state-of-the-art AI-based intrusion detection approaches, including SVM-, CNN-, Random Forest-, Transformer-, and hybrid AI-based IDS models. Performance will be evaluated using standard cybersecurity metrics, such as accuracy, precision, recall, F1-score, false positive rate, and detection latency, together with sustainability-oriented indicators, including energy consumption, energy efficiency, service availability, resource utilization, mean time to recovery (MTTR), computational overhead, CPU utilization, network bandwidth efficiency, and operational costs. These evaluations will provide a comprehensive quantitative assessment of how AI-driven threat detection contributes to the resilience and long-term sustainability of smart city infrastructure.

Future work will also investigate the deployment of AI-RAN within Saudi smart city infrastructure to reduce the latency and overall complexity when CNN is used for the IDS within the existing network of the smart cities. When AI-RAN is deployed instead of the existing network, smart city developers will be able to remove the legacy network and systems used within the Saudi urban areas. Further, AI-RAN will allow the smart city developers to improve the overall cost because the following key technical constraints simplify the overall infrastructure. They are energy efficiency, secrecy rate, privacy, latency, etc., which support the use of emerging technology. In addition, the integration of quantum routing, quantum optimization, quantum key management, and other quantum-enhanced cybersecurity techniques will be explored as these technologies mature. Since the quantum components presented in this study remain conceptual, comprehensive implementation and quantitative validation of quantum-enhanced ATDM architectures using operational smart city environments remain important directions for future research. Future studies will also address data security, governance, regulatory compliance, and interoperability to support the practical deployment of secure, resilient, and sustainable smart city infrastructures.

7. Conclusions

A conceptual case study of Saudi urban infrastructure should consider both general and domain-specific solutions to support the future development of SSCs. While sustainable security is the primary focus of this study, the proposed research also contributes to strengthening security solutions and improving the resilience of smart city environments. Through the proposed framework and AI-based tools, evolving threats can be proactively predicted and mitigated, thereby contributing to the sustainability, resilience, and security of smart city environments.

To directly address the research objectives, the findings of this study provide the following answers to the research questions.

RQ1. How can an ATDM be designed to improve cybersecurity for sustainable smart city infrastructure?

The proposed ATDM is designed as a conceptual framework that integrates AI-driven anomaly detection, intelligent IDSs, cybersecurity policies, and emerging technologies within a unified architecture. The framework enables proactive identification, classification, and management of evolving cyber threats while supporting the resilience and sustainability of smart city services. In this conceptual framework, the ATDM allows the security providers of smart city services to add possible security algorithms and techniques according to evolving technologies.

RQ2. How can AI-driven anomaly detection be integrated with existing intrusion detection systems to support proactive cyber threat management?

The proposed framework conceptually integrates AI-driven anomaly detection with conventional IDS technologies through intelligent feature extraction, anomaly detection, threat classification, risk assessment, and automated response mechanisms. This integration improves the capability of IDSs to identify both known and previously unseen cyber threats while supporting continuous security monitoring across heterogeneous smart city infrastructures.

RQ3. What role can emerging technologies, including quantum-inspired techniques, play in enhancing future smart city cybersecurity frameworks?

The study identifies emerging technologies, including PQC, quantum communication, quantum sensing, and hybrid quantum-AI techniques, as promising enabling technologies for future smart city cybersecurity. These technologies have the potential to strengthen secure communications, improve threat detection capabilities, enhance intelligent decision-making, and support secure, energy-efficient smart city services. Under the global trend of energy efficiency and security guidance with emerging technologies, the green energy and emission reduction benefits of renewable energy, low-carbon transformation, etc., will be better in future smart cities.

RQ4. How can the proposed conceptual framework support the resilience and sustainability of Saudi smart city infrastructure?

The proposed conceptual framework supports the resilience and sustainability of Saudi smart city infrastructure by integrating AI-driven cybersecurity, anomaly detection, threat management, sustainability objectives, and emerging technologies into a unified architecture aligned with Saudi smart city priorities. Although the framework has not been experimentally validated, it establishes a theoretical foundation for future implementation, simulation, and quantitative evaluation using real-world datasets.

Based on these findings, several general recommendations should be considered before deploying SSCs in Saudi Arabia and elsewhere:

- **Security with Energy Management:** Sustainability metrics, such as the EE of security implementations, smart energy systems, and techniques like LSTM for minimizing energy consumption, should be integrated and secured.
- **Threat Detection in Global Connectivity:** As SSCs rely heavily on global connectivity for commercial and infrastructural development, ATDM can be employed alongside quantum technologies to secure global data traffic.
- **Proactive Cybersecurity Solutions:** Hybrid Q-AI combined with Digital Twin technologies can enable proactive identification of risks and cyberattacks, thereby enhancing urban infrastructure management.
- **AI-Driven Solutions with 3Es:** The integration of the three Es (e.g., energy, efficiency, and economy) highlighted in the literature is essential for maintaining SSC, supported by mechanisms such as autonomous quantum key management.

After establishing SSC infrastructures, the following recommendations can further strengthen cybersecurity and resilience:

- **Maximum Security at Minimum Cost:** The integration of AI and quantum technologies can provide optimized, cost-effective security solutions for smart cities in Saudi Arabia and beyond.
- **Threat-Free SSC Environment:** Proactive monitoring systems can detect and mitigate threats before they reach critical infrastructure boundaries.
- **AI-Driven Proactive Mechanisms:** Advanced approaches such as proactive forensic meta-models and threat hunting using GANs can further strengthen security capabilities.
- **Managing the 3Es with AI-Driven Threat Mechanisms:** Effective integration of AI-driven threat detection with sustainability goals ensures balanced management of energy, efficiency, and economic factors.

Overall, this research establishes a comprehensive conceptual foundation for integrating AI-driven cybersecurity and emerging quantum technologies into sustainable smart city environments. Although the proposed framework has not yet been experimentally validated, it provides a replicable theoretical basis for future research involving real-world datasets, simulation studies, quantitative performance evaluation, and practical implementation within Saudi Arabia and other next-generation smart city initiatives.

Author Contributions: Conceptualization, A.M.A. and V.T.; data curation, V.T.; funding acquisition, A.M.A.; investigation, A.M.A. and V.T.; methodology, V.T.; resources, A.M.A. and V.T.; supervision, A.M.A.; validation, A.M.A. and V.T.; writing—original draft preparation, A.M.A. and V.T.; writing—review and editing, A.M.A. and V.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, grant number IPP: 852-611-2026.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: The authors gratefully acknowledge the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, Saudi Arabia, for funding this project and for providing technical support.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AET	Agricultural Energy Internet
AD&TM	Anomaly Detection and Threat Management
AI	Artificial Intelligence
AI-RANs	AI-Radio Access Networks
ATDM	AI-based Threat Detection Mechanism
CPSs	Cyber-Physical Systems
DRL	Deep Reinforcement Learning
EE	Energy Efficiency
ETs	Emerging Technologies
GANs	Generative Adversarial Networks
GRU	Gated Recurrent Unit
HPC	High-Performance Computing
IDS	Intrusion Detection System

IoT	Internet of Things
IQN	Integrated Quantum Network
LSTM	Long Short-Term Memory
mIoT	medical IoT
ML	Machine Learning
MTTR	Mean Time To Recovery
NCWF	NICE Cybersecurity Workforce Framework
NICE	National Initiative for Cybersecurity Education
NIDS	Network Intrusion Detection System
PQC	Post-Quantum Cryptography
Q-AI	Quantum-AI
RNN	Recurrent Neural Network
SDG	Sustainable Development Goal
SLR	Systematic Literature Review
SSCs	Sustainable Smart Cities
UAVs	Unmanned Aerial Vehicles
URLLC	Ultra-Reliable Low-Latency Communication
vIoT	vehicular IoT
VQE	Variational Quantum Eigensolver
XAI	Explainable AI

References

1. Bibri, S.E.; Alexandre, A.; Sharifi, A.; Krogstie, J. Environmentally sustainable smart cities and their converging AI, IoT, and big data technologies and solutions: An integrated approach to an extensive literature review. *Energy Inform.* **2023**, *6*, 9. [\[CrossRef\]](#) [\[PubMed\]](#)
2. Yusuf, O.; Rasheed, A.; Lindseth, F. Leveraging Big Data and AI for Sustainable Urban Mobility Solutions. *Urban Sci.* **2025**, *9*, 301. [\[CrossRef\]](#)
3. Zaman, M.; Puryear, N.; Abdelwahed, S.; Zohrabi, N. A Review of IoT-Based Smart City Development and Management. *Smart Cities* **2024**, *7*, 1462–1501. [\[CrossRef\]](#)
4. Barakat, H.M.; Md Ali, S.H.; Xu, Z.; Murad, S.S.; Soltani, M.D.; Yussof, S.; Oraibi, B.-A.M. Wireless and Emerging Technologies to Meet E-Government Demands: Applications, Benefits, and Challenges. *Information* **2026**, *17*, 225. [\[CrossRef\]](#)
5. Kayani, M.A. AI Driven Cloud Security and Anomaly Detection in Saudi Arabia: A Strategic Enabler of Vision 2030 Digital Transformation. *Sci. Prepr.* **2025**. [\[CrossRef\]](#)
6. Adeleke, O.J.; Jovanovich, K.D.; Ogunbunmi, S.; Samuel, O.; Kehinde, T.O. Comprehensive Exploration of Smart Cities: A Systematic Review of Benefits, Challenges, and Future Directions in Telecommunications and Urban Development. *IEEE Sens. Rev.* **2025**, *2*, 228–245. [\[CrossRef\]](#)
7. Elmaghraby, A.S.; Losavio, M.M. Cyber security challenges in Smart Cities: Safety, security and privacy. *J. Adv. Res.* **2014**, *5*, 491–497. [\[CrossRef\]](#) [\[PubMed\]](#)
8. Houichi, M.; Jaidi, F.; Bouhoula, A. Cyber Security within Smart Cities: A Comprehensive Study and a Novel Intrusion Detection-Based Approach. *Comput. Mater. Contin.* **2024**, *81*, 393–441. [\[CrossRef\]](#)
9. Khatoon, A.; Riaz, R. Quantum Computing Impacts on Smart City Cybersecurity Through Resilient Defense Framework. *Ubiquitous Technol. J. Prepr.* **2025**, *1*, 23–31. [\[CrossRef\]](#)
10. Reddy, N.R.; Dalton, G.A.; Swathi, K.; Subrahmanyam, D.V.S.S.; Kranthi, G.L.; Nagaraju, G. Secure quantum-resilient smart city communication networks using QSC-Net with MF-MBO-based energy-aware task scheduling. *Sci. Rep.* **2026**, *16*, 12534. [\[CrossRef\]](#) [\[PubMed\]](#)
11. Oliha, J.S.; Biu, P.W.; Obi, O.C. Securing the smart city: A review of cybersecurity challenges and strategies. *Eng. Sci. Technol. J.* **2024**, *5*, 496–506. [\[CrossRef\]](#)
12. Thayanathan, V.; Yazdani, J. *Secure Cyber-Physical Systems for Improving Transportation Facilities in Smart Cities and Industry 4.0*; IGI Global: Hershey, PA, USA, 2019. [\[CrossRef\]](#)
13. Zeng, H.; Yunis, M.; Khalil, A.; Mirza, N. Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity. *J. Innov. Knowl.* **2024**, *9*, 100601. [\[CrossRef\]](#)
14. Koormala, H.C.; Reddy, K.K.; Balusa, V.S.; Jillapalli, N.; Hanafiah, M.M. Enhancing urban safety: AI-driven security solutions for smart cities. In *Information Security Governance Using Artificial Intelligence of Things in Smart Environments*; CRC Press: Boca Raton, FL, USA, 2025; pp. 146–163.

15. John, J.; Raj, R.D.A.; Karimi, M.; Nazari, R.; Yanamala, R.M.R.; Pallakonda, A. Artificial Intelligence for Smart Cities: A Comprehensive Review Across Six Pillars and Global Case Studies. *Urban Sci.* **2025**, *9*, 249. [CrossRef]
16. Ullah, A.; Quddusi, S.A.; Haider, I. Incorporation of Artificial Intelligence in Enhancing Quality of Life in Smart Cities. *Am. J. Artif. Intell.* **2024**, *8*, 48–54. [CrossRef]
17. Wolniak, R.; Stecula, K. Artificial Intelligence in Smart Cities—Applications, Barriers, and Future Directions: A Review. *Smart Cities* **2024**, *7*, 1346–1389. [CrossRef]
18. Abbass, M.; Uzma, A.; Rana, J.; Syed, M.A.; Shalom, A. AI and Machine Learning Applications in Sustainable Smart Cities. In *Sustainable Smart Cities and the Future of Urban Development*; IGI Global Scientific Publishing: Hershey, PA, USA, 2025; pp. 1–32. [CrossRef]
19. Shafik, W. Artificial Intelligence-Enabled Cybersecurity and Internet of Things Applications in Smart Cities. In *Building Tomorrow's Smart Cities with 6G Infrastructure Technology*; IGI Global Scientific Publishing: Hershey, PA, USA, 2025; pp. 301–334. [CrossRef]
20. Rakshit, I. AI-Driven Cloud Solutions for Smart City Data Analytics. *Syst. Anal.* **2025**, *3*, 27–34. [CrossRef]
21. Ojadi, J.O.; Owulade, O.A.; Researcher, N.I.; Odionu, C.S.; Researcher, U.I.; Onukwulu, E.C.; Researcher, L.I. AI-Driven Optimization of Water Usage and Waste Management in Smart Cities for Environmental Sustainability. *Eng. Technol. J.* **2025**, *10*, 4284–4306. [CrossRef]
22. Fan, W.Q.; Ismail, A.S.; Mohammed, F.; Mukred, M. AI-Driven Smart City Security and Surveillance System: A Bibliometric Analysis. In *Current and Future Trends on AI Applications*; Springer Nature: Cham, Switzerland, 2025; Volume 1, pp. 305–328.
23. Mhlanga, D.; Shao, D. AI-optimized urban resource management for sustainable smart cities. In *Financial Inclusion and Sustainable Development in Sub-Saharan Africa*; Routledge: Oxfordshire, UK, 2025; pp. 96–116.
24. 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. [CrossRef]
25. Diter, L.A. NEOM and the New Paradigm of Urban Development: Challenges, Innovations, and Global Implications for Sustainable Futures. *Arab. World Geogr.* **2025**, *28*, 228–245. [CrossRef]
26. Allouzi, M.; Aljaafreh, M. Applied Ai in Neom construction projects: The potential impact of AI in enhancing projects success. *Acta Inform. Malays.* **2024**, *8*, 32–44. [CrossRef]
27. Alhowaish, A.K. Green Municipal Bonds and Sustainable Urbanism in Saudi Arabian Cities: Toward a Conceptual Framework. *Sustainability* **2025**, *17*, 3950. [CrossRef]
28. AlQuhtani, S. Assessing the Impact of Saudi Vision 2030 on Urban Mobility Transitions: The Case of Riyadh. *Growth Change* **2026**, *57*, e70094. [CrossRef]
29. Aljebry, D.; Barnawi, A. Quantum key distribution in next-generation networks: A survey of space-based, aerial, and SDN-enabled frameworks for secure communication. *Quantum Inf. Process.* **2026**, *25*, 201. [CrossRef]
30. Ojeniyi, J.A.; Fasola, O.O.; Onyeabor, G.A.; A Mohammed, A.; Aliyu, A.A.; Ahmed, H.M.; Ndanusah, U.H. A Conceptual Review of Quantum-Enhanced Resource Allocation Strategies for Sustainable Energy Management in Smart Cities. 2026. Available online: <http://irepo.futminna.edu.ng:8080/jspui/bitstream/123456789/31794/1/AIMS-V12N1P4.pdf> (accessed on 5 June 2026).
31. Kumar, A.; Bhatia, S.; Kaushik, K.; Gandhi, S.M.; Devi, S.G.; Pacheco, D.A.d.J.; Mashat, A. Survey of Promising Technologies for Quantum Drones and Networks. *IEEE Access* **2021**, *9*, 125868–125911. [CrossRef]
32. Alnaser, A.A.; Maxi, M.; Elmousalami, H. AI-Powered Digital Twins and Internet of Things for Smart Cities and Sustainable Building Environment. *Appl. Sci.* **2024**, *14*, 12056. [CrossRef]
33. Cina, E.; Elbasi, E.; Elmazi, G.; AlArnaout, Z. The Role of AI in Predictive Modelling for Sustainable Urban Development: Challenges and Opportunities. *Sustainability* **2025**, *17*, 5148. [CrossRef]
34. Mehmood, R.; Ghadah, A.; Sarah, A.; Roba, A.; Nourah, J.; Iyad, K.; Ali, A.; Turki, A. AI-Driven High-Performance Data Analytics for Climate-Resilient Smart Cities and Energy Systems. 2025. Available online: <https://ssrn.com/abstract=5383916> (accessed on 5 June 2026).
35. Salhi, A.; Algarni, F.; Alshamrani, R.; Althbiti, A.; Ismail, A.; Hassan, B.M. Leveraging artificial intelligence to enable sustainable urban development through the creation of smart and environmentally friendly carbon-free cities. *Sci. Rep.* **2025**, *15*, 35791. [CrossRef] [PubMed]
36. Pei, R.; Chen, M.; Liu, Z. Identifying Key Digital Enablers for Urban Carbon Reduction: A Strategy-Focused Study of AI, Big Data, and Blockchain Technologies. *Systems* **2025**, *13*, 646. [CrossRef]
37. Krúpová, S.; Koman, G.; Soviar, J.; Holubčík, M. The Role of Business Models in Smart-City Waste Management: A Framework for Sustainable Decision-Making. *Systems* **2025**, *13*, 556. [CrossRef]
38. Salih, S.; Abdelmaboud, A.; Husain, O.; Motwakel, A.; Elshafie, H.; Sharif, M.; Hamdan, M. IoT in urban development: Insight into smart city applications, case studies, challenges, and future prospects. *PeerJ Comput. Sci.* **2025**, *11*, e2816. [CrossRef] [PubMed]
39. Thayananthan, V.; Algarni, A. Internet of Things based 5G Infrastructure for Securing Transportation Facilities in Smart Cities. *Int. J. Comput. Appl.* **2019**, *181*, 26–33. [CrossRef]

40. Almulhim, A.I. Integrating Artificial Intelligence into Smart Infrastructure Management for Sustainable Urban Planning. *Technologies* **2025**, *13*, 481. [CrossRef]
41. Laufs, J.; Borrión, H.; Bradford, B. Security and the smart city: A systematic review. *Sustain. Cities Soc.* **2020**, *55*, 102023. [CrossRef]
42. Kalinin, M.; Krundyshev, V.; Zegzhda, P. Cybersecurity Risk Assessment in Smart City Infrastructures. *Machines* **2021**, *9*, 78. [CrossRef]
43. Alshehri, J.; Alhamed, A.; Rahman, M.M.H. A systematic literature review on cybersecurity risk management in smart cities. In *2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC)*; IEEE: New York, NY, USA, 2024; pp. 407–412. [CrossRef]
44. Vito, D.; Tammara, D.; Vermiglio, C.; Zarone, V. Risk Management and Urban Resilience: Literature and Practice. *Systems* **2026**, *14*, 459. [CrossRef]
45. Alharbi, S. MORL-SGF: A Governance-Aware Multi-Objective Reinforcement Learning Framework with Digital Twin Policy Validation for Sustainable Smart Cities. *Systems* **2026**, *14*, 294. [CrossRef]
46. Srihith, I.V.D.; Kumar, I.V.S.; Varaprasad, R.; Mohan, Y.R.; Srinivas, T.A.S.; Sravanthi, Y. Future of Smart Cities: The Role of Machine Learning and Artificial Intelligence. *South Asian Res. J. Eng. Technol.* **2022**, *4*, 110–119. [CrossRef]
47. Alourani, A.; Alam, M.; Ali, A.; Khan, I.R.; Samal, C.K. Hybrid AI-IoT Framework with Digital Twin Integration for Predictive Urban Infrastructure Management in Smart Cities. *Comput. Mater. Contin.* **2025**, *86*, 1–32. [CrossRef]
48. Almeida, F. Prospects of Cybersecurity in Smart Cities. *Future Internet* **2023**, *15*, 285. [CrossRef]
49. Mohamed, N.; Al-Jaroodi, J.; Jawhar, I. Opportunities and challenges of data-driven cybersecurity for smart cities. In *2020 IEEE Systems Security Symposium (SSS)*; IEEE: New York, NY, USA, 2020; pp. 1–7. [CrossRef]
50. Mohammed, A. Cybersecurity in Smart Cities: Securing IoT and Smart Infrastructure. *J. Innov. Technol.* **2022**, *5*, 1–11.
51. Protic, D.; Gaur, L.; Stankovic, M.; Rahman, A. Cybersecurity in Smart Cities: Detection of Opposing Decisions on Anomalies in the Computer Network Behavior. *Electronics* **2022**, *11*, 3718. [CrossRef]
52. Mijwil, M.; Doshi, R.; Hiran, K.K.; Al-Mistarehi, A.-H.; Gök, M. Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects. *Mesopotamian J. Cybersecur.* **2022**, *2022*, 1–4. [CrossRef]
53. Abdallah, W.; Alghamdi, M. AIP-Urban: Edge-Enabled Deep Learning Framework for Predictive Maintenance and Anomaly Detection in Urban Traffic Infrastructure. *Systems* **2025**, *13*, 1117. [CrossRef]
54. Sharma, S.; Popli, R.; Singh, S.; Chhabra, G.; Saini, G.S.; Singh, M.; Sandhu, A.; Sharma, A.; Kumar, R. The Role of 6G Technologies in Advancing Smart City Applications: Opportunities and Challenges. *Sustainability* **2024**, *16*, 7039. [CrossRef]
55. Le, L.; Nguyen, T.N. DQRA: Deep quantum routing agent for entanglement routing in quantum networks. *IEEE Trans. Quantum Eng.* **2022**, *3*, 4100212. [CrossRef]
56. IMD, World Competitiveness Center. *IMD Smart City Index 2026*; International Institute for Management Development (IMD): Lausanne, Switzerland, 2026. Available online: <https://imd.widen.net/view/pdf/697v9hkavp/SmartCityIndex-2026.pdf?t.download=true&u=dnnfeq> (accessed on 30 July 2026).
57. Alhakami, W. Enhancing Cybersecurity Competency in the Kingdom of Saudi Arabia: A Fuzzy Decision-Making Approach. *Comput. Mater. Contin.* **2024**, *79*, 3211–3237. [CrossRef]
58. Albaqami, S.; Nekovee, M.; Khan, I. The Future of IoT Security in Saudi Arabian Start-Ups: A Position Paper. *Int. J. Adv. Comput. Sci. Appl.* **2024**, *15*, 42. [CrossRef]
59. Alshahrani, A. Adopting Emerging Technologies in Digital Government: A Multi-Case Analysis of Drivers, Enablers, and Challenges in Saudi Arabia. *Digit. Gov. Res. Pract.* **2025**, *6*, 36. [CrossRef]
60. Alqahtani, A.; Yan, J.; Vlahu-Gjorgievska, E.; Cao, C. Factors Influencing Citizens' Adoption of AI-Enabled Public Services in Saudi Arabia: The Role of Cybersecurity, Privacy, and Trust: Factors Influencing Adoption of AI-Enabled Public Services. *Digit. Gov. Res. Pract.* **2026**, *7*, 6. [CrossRef]
61. Abudaqqa, F. Artificial Intelligence for IT Governance in Saudi Arabia: Opportunities, Challenges, and Future Directions within COBIT 2019 and ISO/IEC 38500 Frameworks. *Eur. Sci. J.* **2025**, *21*, 125. [CrossRef]
62. Bendary, M.G.; Rajadurai, J. Emerging Technologies and Public Innovation in the Saudi Public Sector: An analysis of Adoption and challenges amidst Vision 2030. *Innov. J.* **2024**, *29*, 1–42.
63. Al-Zahrani, A.A.; Al-Salloum, O.I. Success Factors in Achieving Excellence in Cybersecurity (A Case Study of the Kingdom of Saudi Arabia). *Int. J. Res. Stud. Publ.* **2025**, *6*, 59–87. [CrossRef]
64. Alsabt, R.; Adenle, Y.A.; Alshuwaikhat, H.M. Exploring the Roles, Future Impacts, and Strategic Integration of Artificial Intelligence in the Optimization of Smart City—From Systematic Literature Review to Conceptual Model. *Sustainability* **2024**, *16*, 3389. [CrossRef]
65. Alhalafi, N.; Veeraraghavan, P. Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. *Smart Cities* **2023**, *6*, 1523–1544. [CrossRef]
66. Sepehri, B.; Almulhim, A.I.; Adibhesami, M.A.; Makaremi, S.; Ejazi, F. Artificial intelligence role in promoting Saudi Arabia's smart cities: Addressing SDGs for socio-cultural challenges. *Социологическое Обозрение* **2024**, *23*, 20–47. [CrossRef]

67. Youssef, H.A.H.; Omar, N.H.E.S. Applications of Artificial Intelligence and Digital Twins in Enhancing Urban Sustainability in Saudi Cities: NEOM City as Case Study. *Int. J. Adv. Res. Publ. Rev.* **2025**, *2*, 372–394.
68. Alharbe, M.A. Cybersecurity, Forensics, and Its Impact on Future Challenges in Saudi Arabia Smart cities. *Int. J. Adv. Trends Comput. Sci. Eng.* **2020**, *9*, 2464–2470. [[CrossRef](#)]
69. Alshammari, M.M.; Al-Mamary, Y.H. Building Trust and Cybersecurity Awareness in Saudi Arabia: Key Drivers of AI-Powered Smart Home Device Adoption. *Systems* **2025**, *13*, 863. [[CrossRef](#)]
70. Alsulami, M.H. A Smart Proactive Forensic Meta-Model for Smart Homes in Saudi Arabia Using Metamodeling Approaches. *Electronics* **2025**, *14*, 4319. [[CrossRef](#)]
71. Ahmed, A.S.A.S. Explainable Artificial Intelligence and Its Impact on Smart Cities (Applied Study on Saudi Cities). Ph.D. Thesis, Cairo University, Giza, Egypt, 2021.
72. Hashim, H. E-government impact on developing smart cities initiative in Saudi Arabia: Opportunities & challenges. *Alex. Eng. J.* **2024**, *96*, 124–131. [[CrossRef](#)]
73. Aldegheishem, A. Assessing the Progress of Smart Cities in Saudi Arabia. *Smart Cities* **2023**, *6*, 1958–1972. [[CrossRef](#)]
74. Bahreldin, I.; Samir, H.; Maddah, R.; Hammad, H.; Hegazy, I. Leveraging advanced digital technologies for smart city development in Saudi Arabia: Opportunities, challenges, and strategic pathways. *Int. J. Low-Carbon Technol.* **2025**, *20*, 834–847. [[CrossRef](#)]
75. Aljijakli, M.; Akkari, N. Toward AI-Driven Solutions for Smart Cities in KSA. In Proceedings of the 2025 2nd International Conference on Advanced Innovations in Smart Cities (ICAISC), Jeddah, Saudi Arabia, 9–11 February 2025; pp. 1–6. [[CrossRef](#)]
76. Algarni, A.M.; Thayanathan, V. AI-Based Model for Maintaining Good Healthcare Quality Against Cybersecurity Risks. *Systems* **2026**, *14*, 315. [[CrossRef](#)]
77. Priyadarshini, I. Anomaly Detection of IoT Cyberattacks in Smart Cities Using Federated Learning and Split Learning. *Big Data Cogn. Comput.* **2024**, *8*, 21. [[CrossRef](#)]
78. You, Z.; Zheng, Y. Security anomaly detection for enterprise management network based on attention mechanism. *Front. Phys.* **2025**, *13*, 1538605. [[CrossRef](#)]
79. International Institute for Management Development (IMD). Jeddah—Entity Profile. Available online: <https://www.imd.org/entity-profile/jeddah/> (accessed on 30 July 2026).
80. IMD. *Smart City Observatory. Smart City Index Methodology*; IMD: Lausanne, Switzerland, 2026. Available online: <https://www.imd.org/smart-city-observatory/home/methodology/> (accessed on 30 July 2026).
81. IMD. *Case Studies*; IMD Research & Knowledge: Lausanne, Switzerland, 2026. Available online: <https://www.imd.org/research-knowledge/case-studies/> (accessed on 30 July 2026).
82. Liu, G.; Huang, Y.; Li, N.; Dong, J.; Jin, J.; Wang, Q.; Li, N. Vision, requirements and network architecture of 6G mobile network beyond 2030. *China Commun.* **2020**, *17*, 92–104. [[CrossRef](#)]
83. Mohammadpour, L.; Ling, T.C.; Liew, C.S.; Aryanfar, A. A Survey of CNN-Based Network Intrusion Detection. *Appl. Sci.* **2022**, *12*, 8162. [[CrossRef](#)]
84. Singh, C.P.; Yamaganti, R.; Umrao, L.S. A privacy-preserving and secure framework using blockchain-based quantum-inspired complex convolutional neural network for IoT-driven smart cities. *Peer-to-Peer Netw. Appl.* **2025**, *19*, 3. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.