Risk Assessment and Risk Management Challenges in Intelligent IoT-Based Smart City Infrastructures

Abdullah Alessa, Yaseen Alduwayl, M M Hafizur Rahman
Department of Computer Networks and Communications-College of Computer Sciences and Information Technology,
King Faisal University, Al-Ahsa, 31982, Saudi Arabia

***Abstract*—Smart Internet of Things (IoT) technologies, which include artificial intelligence (AI) are increasingly being implemented in the infrastructures of smart cities to enhance the efficiency, sustainability, and service delivery of cities. Nonetheless, with the implementation of such intelligent and interconnected systems, there are complex security, privacy, and safety risks that are not easily handled against conventional risk assessment and risk management methods. Current frameworks tend to be unresponsive and centralized whereas smart city infrastructures are dynamic, decentralized, and based on autonomous decision-making elements. This incompatibility poses serious problems for the reliability and robustness of intelligent urban systems. The study contains a systematic literature review of the risk assessment and risk management issues in smart city infrastructure based on intelligent IoT. The review is based on security, privacy, safety, and risks of AI, such as adversarial machine learning, data poisoning, model drift, and failures of autonomous systems. To enhance the level of methodological transparency, the review lists the databases searched, search words, screening process, inclusion, and exclusion criteria, and the resulting list of studies selected. The comparison of the key risk assessment methods, such as the standard-based, qualitative, probabilistic, and AI-based approaches, has been made, and their advantages and weaknesses in the smart city context have been identified. The results indicate that existing frameworks are still in fragments and not always able to deal with the joint effect of the heterogeneity of IoT, AI-based decisions, cyber-physical interdependence, scalability, and governance. The study, based on this summary, offers a more defined taxonomy of risk factors and research directions towards adaptive, AI-conscious and operationally feasible risk management in smart cities.**

Keywords*—*Artificial intelligence; cybersecurity; Internet of Things; risk assessment; risk management; smart cities

ABBREVIATIONS

The following abbreviations are used in this manuscript:

IoT	Internet of Things
AI	Artificial Intelligence

I. INTRODUCTION

The concept of smart cities has become one of the key trends in the current urban development with the fast growth of digital technologies and the necessity to provide efficient, sustainable, and human-centered services. The fundamental aspect of smart city projects is to implement Intelligent Internet of Things (IoT) infrastructures wherein interrelated sensors, actuators, edge devices, and communication networks with artificial intelligence (AI) approaches are used to assist automated monitoring, automated decision-making, and automated control in the urban domain. The systems have become common in transportation management, intelligent energy grids, healthcare services, environmental monitoring, security services, and protection of critical infrastructure [1], [2].

The smart city systems based on intelligent IoT are highly distributed data-driven and adaptive ecosystems compared to traditional urban infrastructures. They keep gathering real-time data using heterogeneous sources and use machine learning and optimization algorithms to facilitate autonomous or semi-autonomous behavior. Although this intelligence has greatly contributed to better operational efficiency and quality of services, there are also complex security, safety, and privacy risks that are totally different to those that exist when the information system is normal [3]. Consequently, this has made proper risk assessment and risk management, an important issue towards long-term reliability and trustworthiness of smart city infrastructures.

A. Background and Motivation

Smart cities are driven by issues that are not limited to the world but are global in nature, including urbanization, population explosion, scarcity of resources, global warming, and the desire to have resilient cities in terms of population services. The amount of governments and municipalities depending on the technologies of IoT and AI to streamline urban processes, cut expenses, and enhance living standards is rising [4], [5]. As an illustrative case, smart traffic management devices dynamically change traffic lights to ease the traffic jams, smart grids regulate energy supply and demand in real-time, and smart surveillance systems assist emergency workers and curb crime with AI-assistance [6], [7], [8].

Nevertheless, the very features that render smart IoT systems appealing also contribute substantially to the scale of the attack on the urban infrastructures. The smart city environments comprise thousands or even millions of heterogeneous devices, with most possessing limited computational power and limited security features. They use wireless and public networks to communicate with each other, and usually, they use cloud and edge computing platforms to process and store data [1], [2]. Such high levels of connectivity and heterogeneity expose people to the risks of cyber threats, including unauthorized access, data breaches, denial-of-service attacks, and system manipulation.

Moreover, AI implementation brings a different category of risks which are not limited to conventional cybersecurity issues. Adversarial attack, data poisoning, model inversion and

concept drift can adversely affect the performance of machine learning models and lead to wrong decisions [9], [10]. Such failures in a smart city setting can cause digital, but also corporeal, damage, in the form of traffic accidents, power outages, incidents involving the safety of the population, and getting crucial services out of order [9], [10].

Conventional risk management models, like the NIST Risk Management Framework or ISO/IEC 27005, were initially intended to be used with fairly stable centralized information systems [11], [12]. These frameworks frequently face difficulties in managing the dynamic, autonomous and decentralized characteristics of intelligent infrastructures based on the IoT. This discrepancy inspires the necessity of a holistic and updated knowledge of the methods of risk assessment and management in the particular context of smart cities.

B. Intelligent IoT-Based Smart City Infrastructures

The concept of intelligent IoT-driven smart city infrastructures may be understood as the macro-scale level of cyber-physical infrastructures based on integrating IoT technologies with AI-powered analytics and decision-making processes. Fig. 1 shows the common notion that these infrastructures are usually comprised of four major layers, namely, the sensing layer, the communication layer, the data processing layer and the application layer [7], [6].

The sensing layer contains physical devices like sensors, actuators, cameras, and an embedded system that is scattered across the city to gather information about traffic flow, air quality, energy consumption, weather conditions and human activities. The communication layer provides the transmission of data based on heterogeneous networking technologies, 5G, LPWAN, Wi-Fi, and wired networks. The data processing layer is based on the edge computing, fog computing, and cloud computing to store and analyze the huge amount of real-time data. Lastly, the application layer provides smart services to city operators, policymakers and citizens via dashboards, automated control system, and decision support systems [1], [2].

The key difference between the intelligent IoT infrastructures and the previous smart systems lies in the wide application of AI methods, including machine learning, deep learning, reinforcement learning, and predictive analytics. The techniques can be used to allow the systems to learn using past and real-time data, adjust to environments undergoing change, and make autonomous decisions with a minimum amount of human involvement [7], [6]. Although such intelligence improves scalability and responsiveness, it also adds complexity to the systems and diminishes transparency, so it is more challenging to predict, measure, and control risks.

C. Problem Statement

Although the intelligent IoT technologies are widely implemented in the smart cities, the analytical interface between the conventional risk assessment methodology and the dynamic nature of AI-driven IoT infrastructures has a great gap. The current risk management techniques are somewhat inertial and theoretical, concentrating on the previously known threats, known vulnerabilities, and fairly fixed system parameters [3].

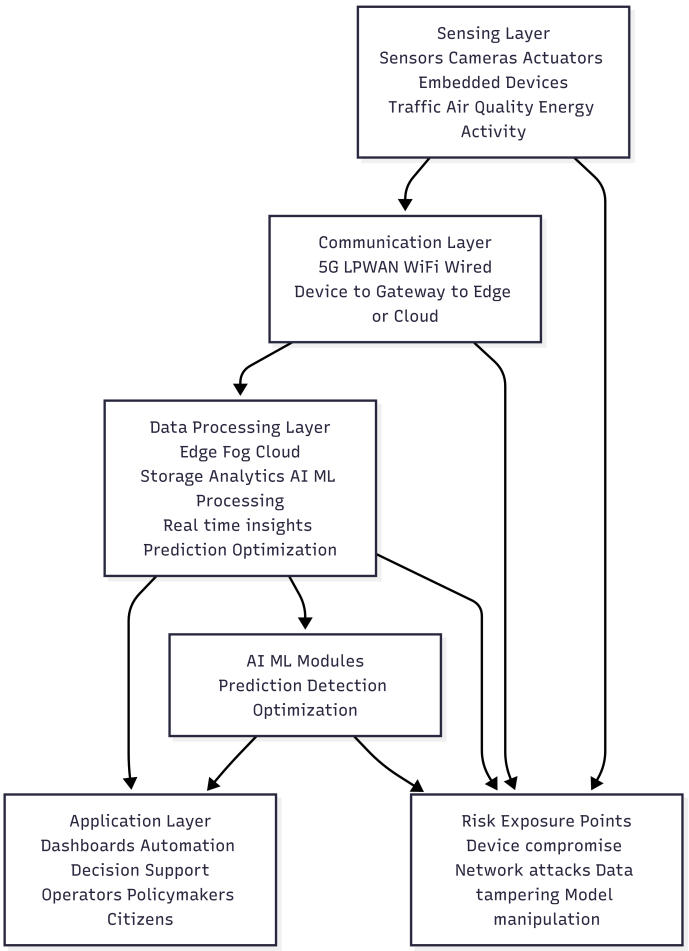

Fig. 1. Layered view of intelligent IoT-based smart city infrastructure, where AI/ML typically operates.

Conversely, smart city systems are also intelligent and they are constantly developing. They are decentralized, use autonomous decision-making algorithms, and are driven by real-time data streams and change of context. The novel and transforming risks brought about by these properties are not properly represented by the traditional models. Specifically, artificial intelligence features like machine learning algorithms present threat on adversarial manipulation, biased training, data poisoning, and unanticipated model behaviour, which may spread within interconnected urban services [9], [10]. As shown in Fig. 2, the reality of intelligent IoT smart city and the traditional risk assessment and management and the gap that addressed between them which reflect on real-world and cause impact to be cyber-physical.

In addition, intelligence IoT failures may have ripple effects on different areas of the city. A subdued traffic management system can affect emergency response, and a smart grid attack can affect the transportation system, healthcare network, and public safety networks all at the same time. This situation where a coherent and consistent knowledge of the way to evaluate and manage such interdependent risks does not exist is a grave threat to the secure and sustainable implementation of smart city infrastructures.

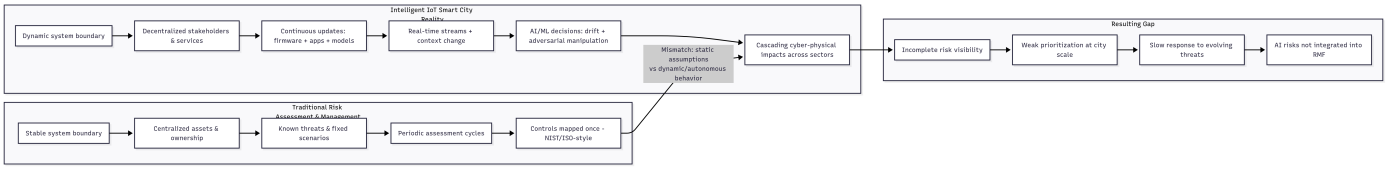

Fig. 2. Mismatch between traditional risk assessment assumptions and the dynamic nature of intelligent IoT-based smart city infrastructures.

D. Research Questions

This comprehensive and rigorous systematic study will address the following research questions to deal with the identified issues:

- RQ1: What are the major security risks and threats specific to the newer AI-based IoT infrastructure within the smart cities?
- RQ2: What are the current risk assessment methodologies and models and what are the technical and practical limitations of the models?
- RQ3: What are the particular difficulties in the process of risk management in real-time, autonomous, and decentralized urban networks?
- RQ4: What are the proposed strategies, frameworks or technologies to reduce intelligent risks in smart city settings?

These research questions will help to organize the study and conduct a full analysis of current methods, problems, and unresolved issues in the area.

E. Contributions of this Review

The review has four key contributions to the literature. First, it introduces a more precise taxonomy of risk factors that impact intelligent IoT-based intelligent city infrastructure, such as technical, AI-specific, cyber-physical, operational, and governance-related risks. Second, it gives a systematic comparison of the significant risk assessment and risk management methods that have been reported in the literature, with a focus on their applicability, strengths, and weaknesses in smart cities. Third, it pinpoints repeating research gaps, particularly in the area of adaptability, scalability, empirical validation, and addressing AI-related threats. Fourth, it outlines practical research opportunities to develop more resilient and context-based risk management approaches towards smart city systems.

F. Paper Organization

The rest of this study will be structured in the following way: Section II outlines the review methodology, which entails the review protocol, databases, search strings, inclusion and exclusion criteria, screening process, quality assessment and data extraction plan. Section III will provide a comparative discussion of the chosen works and summarize the key methodological trends and shortcomings in the literature. The key risk types, risk evaluation methods, risk management issues, and coping strategies are covered in Section IV in the context of intelligent IoT-based smart city infrastructures. Section V provides future research directions. The study ends with a conclusion in Section VI.

II. Review Methodology

The aim of this review was to help identify, analyze, and synthesize recent literature on risk assessment and risk management of intelligent IoT-based smart city infrastructures. The research approach was structured to enhance transparency and reproducibility by having a clear-cut review protocol, database selection plan, screening process, inclusion and exclusion criteria, quality evaluation plan, and thematic synthesis plan. Specifically, the review emphasized the studies that covered cybersecurity, privacy, safety, AI threats, and cyber-physical dependencies of smart cities.

A. Review Protocol

A review protocol was defined before the literature search in order to maintain methodological consistency. The protocol outlined the objectives of the review, research questions, databases to be used, search terms, inclusion and exclusion criteria, screening steps, and quality assessment criteria. The review process was informed with the existing review reporting practices that included transparent reporting of study identification, screening, eligibility assessment and final inclusion. This was done to minimize selection bias and so as to allow a better understanding and reproducibility of the review. Fig. 3 presents the review pipeline used for search, screening, quality assessment, extraction, and synthesis.

B. Search Strategy and Databases

The literature search was done in the following academic databases: IEEE Xplore, Scopus, Web of Science, ScienceDirect, SpringerLink, MDPI, and the ACM Digital Library. The choice of these databases was based on their wide scope of peer-reviewed material on smart cities, IoT, artificial intelligence, cybersecurity and cyber-physical systems.

The search focused on studies published between 2020 and 2026. Only peer-reviewed journal articles and conference papers were considered. The search terms were grouped into four concept clusters: smart cities, IoT systems, artificial intelligence, and risk management. Representative keywords included “Smart City”, “Smart Cities”, “Internet of Things”, “IoT”, “Intelligent IoT”, “Artificial Intelligence”, “Machine Learning”, “Risk Assessment”, “Risk Analysis”, “Risk Management”, “Cybersecurity”, “Privacy”, and “Safety”.

Representative Boolean search strings included the following:

- (“Smart City” OR “Smart Cities”) AND (“Internet of Things” OR “IoT” OR “Intelligent IoT”) AND (“Risk Assessment” OR “Risk Analysis”)

- ("Smart City Infrastructure") AND ("Risk Management") AND ("Artificial Intelligence" OR "Machine Learning")
- ("Smart City") AND ("Cybersecurity" OR "Privacy" OR "Safety") AND ("IoT")
- ("Intelligent IoT") AND ("Smart City") AND ("AI") AND ("Risk Management")
- ("Cyber-Physical Systems") AND ("Smart City") AND ("Risk Assessment")

The search strings were adjusted slightly to match the syntax of each database. This strategy was intended to capture both conventional IoT security risks and emerging AI-specific risks in intelligent smart city environments.

C. Inclusion and Exclusion Criteria

In order to achieve relevance and consistency, strong inclusion and exclusion criteria were used in selecting the studies.

Inclusion criteria:

- Publications of less than five years (2020-2026).
- Conference papers or peer-reviewed journal articles.
- Studies on smart cities, intelligent IoTs, or urban cyber-physical infrastructures.
- Research that deals with risk assessment, risk management, security, privacy, or safety concerns.
- Articles written in English.

Exclusion criteria:

- Studies published before 2020.
- Articles not peer-reviewed or edited or tutorials and opinion papers.
- Research centered on conventional iot that does not feature intelligent/AI-related aspects.
- Articles that are not connected with the context of urban or smart city.
- Redundant papers in databases.

The criteria were established to make sure that the studies that were selected were recent, relevant and directly connected to smart city risk assessment and risk management using intelligent IoT.

D. Study Selection Procedure

The selection of studies was done in several steps. To begin with, all databases were accessed and their records were combined into one dataset and any duplicate records eliminated. Second, the titles and abstracts were filtered through inclusion and exclusion criteria. At this point, studies that were evidently not related to smart cities, intelligent IoT systems, or risk-related issues were filtered out. Third, the entire contents of the rest of the studies were evaluated in terms of topicality and methodological appropriateness. The final review set only used studies that had directly answered the research questions.

E. Search Results and Study Selection Summary

The selection of the study is as follows: In the selected databases, a total of 465 records were initially found. Upon exclusion of 105 duplicates, there were 360 studies left to screen in terms of title and abstract. At this phase, 300 records were eliminated due to the out of scope of the review or failed to meet the inclusion criteria. The rest of the 60 studies were evaluated on full-text. Following the full-text review, 17 articles were filtered out, with 9 being not related to IoT or smart cities, 6 articles lacked a pertinent risk evaluation or risk management lens, and 2 articles were either non-English or old. This led to 43 papers included in the final review (see Table I).

TABLE I. STUDY SELECTION SUMMARY

Records identified	465
Duplicate records removed	105
Records screened	360
Records excluded after title/abstract screening	300
Full-text studies assessed	60
Full-text studies excluded	15
Final studies included in the review	45

F. Quality Assessment of Selected Studies

A structured quality assessment checklist was used in order to assess the methodological quality of the chosen works. The checklist will be based on the existing frameworks of quality assessment of studies and will consist of items like:

- Transparency of research purposes.
- Suitability of methodology.
- Sufficiency of source of data and analysis.
- Applicability to smart city risk management based on intelligent IoT.
- Coherence of findings and conclusions.

All the studies were evaluated in relation to these criteria to make sure that high-quality and relevant research only entered the synthesis. Analyses of studies that had low methodological rigor or unknown contributions were not included in the further analysis.

G. Data Extraction and Synthesis

Relevant information in each of the selected studies was collected by use of a standardized data extraction form. Data taken out comprised the year of publication, the purpose of the research, the area of application, the risk assessment or risk management strategy, essential findings, the challenges identified, and the limitations.

Thematic analysis was a qualitative approach that was used to synthesize the extracted data. The studies were categorised according to the shared themes, including types of threats, risk factors, assessment models, management framework, and AI specific issues. This methodology allowed finding patterns, similarities, and gaps within the literature, which allowed conducting the comparative analysis of the research and discuss the future directions and trends of the studies in a structured way.

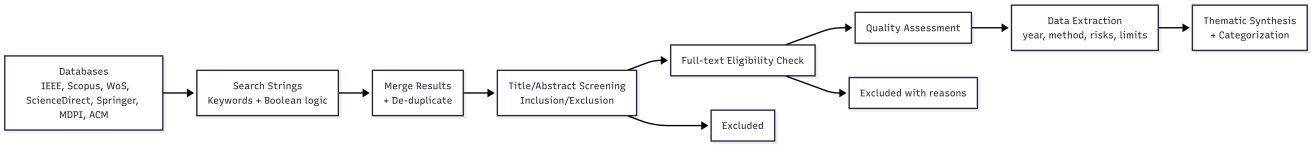

Fig. 3. Review pipeline used for search, screening, quality assessment, extraction, and synthesis.

III. Comparative Analysis of Related Work

This section presents a comparative analysis of the studies selected for the review. Its purpose is to synthesize the literature on risk assessment and risk management in intelligent IoT-based smart city infrastructures, identify common methodological patterns, and highlight unresolved issues.

A. Summary of Reviewed Studies: Objectives and Methods

The study shows that there is an increasing research interest in ensuring smart city infrastructures are secured by risk-sensitive design, as well as risk-sensitive implementation. The majority of the study seeks to determine security threats, to evaluate vulnerabilities, or to suggest frameworks to prevent risks in urban environments with the help of IoT enablers. Nevertheless, they have very different goals and methodology.

Much of the study is dedicated to IoT-based risk assessment, which highlights vulnerabilities at the device level, network security threats, and confidentiality threats to data in the context of smart city implementation [13], [1]. These works often apply conventional security analysis methods, including the threat modeling, attack surface analysis, and qualitative risk matrices, to the situation in urban IoT. Although they are useful in detecting known vulnerabilities, these methods are not always flexible to the dynamic behavior of the system.

The other body of research builds upon classical risk assessment techniques by adding context-sensitive or probabilistic methods, such as Bayesian networks, fuzzy logic, and multi-criteria decision analysis [14]. The purpose of these approaches is to better model uncertainty and interdependencies between smart city elements. Whereas these methods enhance the level of analysis, they are not usually applied at city-wide infrastructures, but applied individually to isolated subsystems, such as smart grids or intelligent transportation systems.

Recent studies are based on applying the methods of artificial intelligence and machine learning to risk assessment and management. These articles address the topic of anomaly detection, predictive risk modelling, and automated threat detection via data-driven methods [15]. Although the above ways demonstrate potential possibilities in managing large-scale and real-time-data, most of the research is still at the concept phase, with minimal implementation in real-world smart city settings.

B. Open Challenges and Research Gaps

A number of open issues and gaps in research can be identified regardless of the variety of approaches to the issue in the study. The first gap is the absence of single risk assessment frameworks that could be used to concurrently consider IoT, AI, and cyber-physical risks related to smart city infrastructures. Fig. 4 illustrate that most of the research is limited to IoT security or AI-based risks, without looking at the potential effect of the two on the interconnected urban systems [16].

The other major problem is that most of the risk assessment models are not dynamic. In traditional and semi-traditional techniques, architecture of the systems and possible attack scenarios are usually fixed and predetermined. Nevertheless, the intelligent smart city systems are constantly changing because of software updates, retraining models, mobility of device, and environmental variations. This time-varying behavior is not well represented in the study models [17], [18].

Scalability is also of great concern. Various suggested frameworks have been shown to be effective in small-scale case studies or simulations, but not in the computational and operational issues of city-wide implementation. The lack of longitudinal research also restricts the knowledge on the transformations of risks over time in smart city intelligent landscapes [1], [2].

C. Key Limitations in Current Research

The comparative analysis indicates several limitations that limit the applicability of the current research in practice. First, in most works, there is rather little attention to AI-specific threats. Although the vulnerabilities of IoT to device compromise and communication attacks are well known, the risks associated with adversarial machine learning, data poisoning, model drift, and biased decision-making are not only briefly mentioned [9], [10] but perhaps not mentioned at all.

Second, the lack of integration of physical safety effects is also a common weakness. Cyber-physical systems are smart city infrastructures, and cyber-attacks may have a direct impact on physical operations and human lives. Nevertheless, most risk assessment studies consider cyber risks individually without clearly modeling the physical or societal impact of such risk [3].

Third, most of the analyzed studies do not present standardized metrics and benchmarks of evaluation, which is why comparing outcomes of various methods can be challenging [19]. This drawback makes the process of selecting appropriate risk management tactics applied to the actual implementation of smart cities more difficult, as well as the formulation of best practices [3].

D. Comparative Analysis of Objectives, Problems, Methods, Findings, and Limitations

To support a structured comparison, the reviewed studies were analyzed across five dimensions: objective, methodology, results, key findings, and limitations [20], [21]. It is noted in

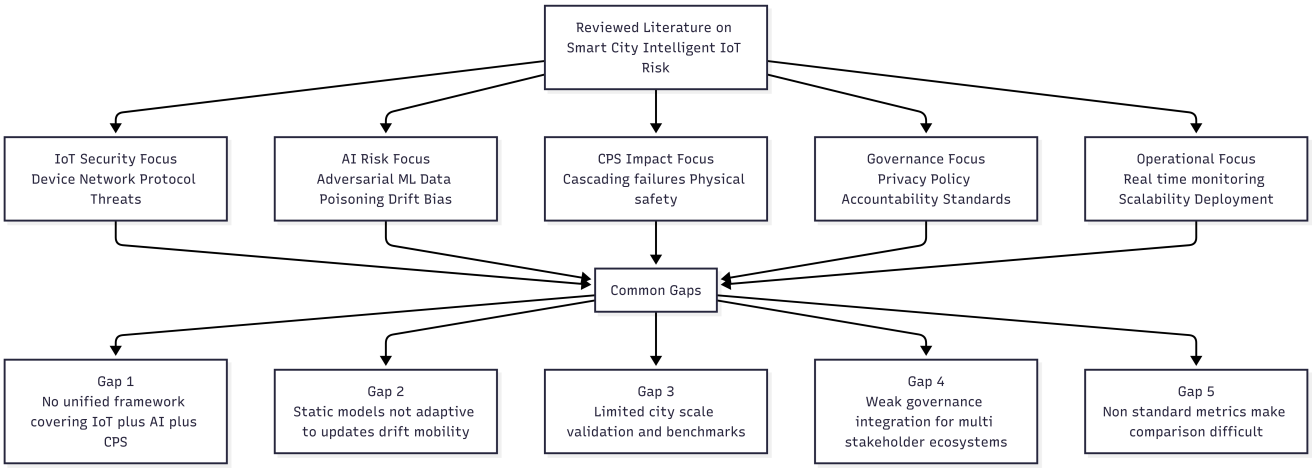

Fig. 4. High-level gap map summarizing limitations across IoT security, AI-specific risks, cyber–physical impacts, governance, and operational scalability in the study.

the analysis that even though the various studies have common objectives e.g. enhance security awareness or minimise the vulnerability of a system, the statement of the problem and the approach used to solve the problem vary significantly among the studies.

Other papers stress on preventive risk management, including secure system design and threat mitigation measures, and others reactive ones, including intrusion detection and incident response [3]. The results of the study tend to establish that intelligent IoT-based smart city systems are confronted with complex risks that cannot be counteracted with unilayer security systems.

E. Synthesized Analysis of Related Work on Risk Assessment and Management in Intelligent IoT-Based Smart Cities

The body of recent research on cybersecurity risk evaluation and management of smart city systems falls under several research strands, such as IoT security, cyber-physical systems (CPS), edge and fog computing, artificial intelligence (AI)-based defenses, governance frameworks, and standardization projects. Initial work on smart city security defines that the heterogeneity, scale and openness of urban IoT ecosystems intrinsically increase the attack surface relative to conventional enterprise systems. According to a foundation of research, smart cities combine sensing, communication, calculation, and control in multi-domain administration, and such risk spread and coordination of attacks are increasingly possible compared to single IoT implementation [22], [4], [23].

Quite a significant study is devoted to the identification of threats and taxonomies based on IoT. Various surveys and examination studies categorize threats to IoT, vulnerabilities, and attack vectors, pointing out vulnerabilities due to constrained devices, insecure communication protocols, weak identity management, and similar [6], [13], [17], [21]. These papers are useful background information but are mostly based on qualitative analysis and taxonomies. Although this sort of approach can be valuable in terms of being aware of a threat, this approach does not provide measurable risk scores regularly updated to support dynamic smart city environments. In addition, they usually consider AI as an external tool and not a part and parcel of the system that is under risk analysis.

The other important research stream deals with risk evaluation structures and methods of smart cities. A number of works can apply classical risk management rules to urban digital infrastructure and focus more on risk identification of assets, the possibility of the threat, and its consequences [24], [20]. Risk management processes and control baselines are further formalized by international standards and guidelines, such as ISO/IEC 27005 and NIST IoT cybersecurity series (NISTIR 8259, NIST SP 800-213, NIST SP 800-53) [12], [11], [1], [16]. Nevertheless, they are very technology-neutral and fixed, and do not provide much information on how risk management can be operationalized in smart city services that are highly adaptive and driven by AI or how to consider the changing threat conditions at a very high rate.

The cyber-physical aspect of smart city risk is considered in CPS-oriented study and demonstrates how cyber attacks propagate into physical disturbances of transport, energy, healthcare, and other, as well as public-safety systems [14], [25]. These publications highlight the harshness of cascading failures and interdependences between digital and physical layers. Nevertheless, the majority of CPS security research is theoretical or computer-based, not being empirically validated, real-time monitoring systems, and quantitative risk prioritization models that can be implemented by the operators of a city.

As edge and fog computing continues to spread, a number of studies explore the effect of decentralized architectures on the smart city threat environment. Mog and edge security surveys determine the new attack vectors of distributed control, data locality, and trust management [26], [27], [28]. Although these papers acknowledge the fact that risk differs at different architectural layers, they do not go further to offer the combined, city-wide risk assessment models that can be used to correlate edge-level events to system-wide impacts.

The use of AI and machine learning in security systems, in particular, intrusion detection and attack detection in IoT networks, is actively studied in recent studies [29], [9], [18]. These methods prove to be better in detecting and being more

flexible than rule-based systems. Nevertheless, they mainly assess performance based on detection-focused measures (i.e., accuracy or false-positive rates) and they do not tend to include adversarial robustness, model drift, or explainability in risk measurement. Introduced by AI as a challenge to the analysis in ENISA reports and threat analysis AI-centered, data poisoning, evasion attacks, and model manipulation have not been dealt with sufficiently in current smart city risk frameworks [7], [30], [10].

Digital twins have been suggested as the way to facilitate the simulation and anticipation of risks at a city scale and provide the opportunity to analyze failures and cyber events in a scenario [19], [8]. Although digital twins provide useful insights on the dynamic processes of complex cities, existing research points out a high level of computational overhead and lack of applicability in real-time. Besides, the majority of digital twins applications focus on operational optimization and do not include constant monitoring and control of cybersecurity risks.

It is also observed that governance, ethics, and sustainability issues are becoming more and more part of smart city cybersecurity. Ethical AI, responsible data use, and sustainable smart city development Studies investigate how technical security controls cannot be effective without open governance and accountability systems [31], [32], [33]. However, such works seldom frame ethical constraints into practice, quantifiable risk management procedures in line with operational cybersecurity interventions.

All in all, the evaluated study shows that there has been substantial development in the domain of threat identification, risk classification, and the suggestion of security systems to be implemented in the IoT systems of Smart Cities, yet, the vital gaps are observed. Current methods tend to be stagnant, inter-technologic, or limited in their coverage of detection performance. There are not many studies that offer combined, quantitative and constantly revised risk management approaches that directly consider AI-driven decision-making, cyber-physical dependencies, and real-time operational constraints. These constraints drive the necessity of a comprehensive risk evaluation and management strategy which is specific to intelligent IoT-based smart city infrastructures namely the ability to incorporate quantifiable risk indicators, AI-conscious threat management, and implementable mechanism to perform ongoing monitoring and mitigation across systems of city-scale systems.

Another study area focuses on security guidance documents, baseline requirements, and regulatory-oriented risk controls related to the implementation of IoT and smart cities. Etis and NIST IoT Core Baseline and other standards and profiles like ETSI EN 303 645 focus on minimum device and system-level capabilities, like secure boot, disclosure of vulnerability, and lifecycle management [34], [8], [35], [36]. Although these documents are necessary to set the basic security hygiene, they are mainly an outline of compliance-based controls as opposed to dynamic risk assessment processes. Consequently, they offer scanty support on the need to prioritize risks, adapt to new threat dynamics, or integrate AI-driven behaviour with current risk management procedures through intelligent smart city infrastructures.

Some works refer to blockchain based and distributed trust systems as a potential facilitator of secure and robust smart city systems. The presence of studies of blockchain integration with IoT and AI reports of enhanced data integrity, decentralization and trust management across heterogeneous stakeholders [37], [16]. Nevertheless, scalability constraints, latency overheads and energy costs that limit real time applicability at city scale are also observed in the surveyed works. Furthermore, blockchain-related solutions tend to center on ensuring the exchange of data as opposed to offering a full-fledged, end-to-end risk assessment platforms that quantify and control cyber and physical risks as well as AI-related risks.

The other new research area is the study of context aware and adaptive security systems of an IoT environment. Context-aware security models seek to adapt protection systems according to the environment, device status or usage patterns, which can enhance responsiveness in smart city contexts [15], [38]. Though they are promising, all these approaches usually run at the control or access management level and have no connection to the higher-level risk assessment processes. They, therefore, add to the local adaptation but fail to offer an uniform perspective of city-wide risk posture or long-term risk trends.

Smart city risk management is indirectly informed through research on resource management and optimization in fog environments and edge environments. Research on the allocation of resources associated with fog and on distributed computing architectures show the impact of workload distribution, latency constraints and resource contention on system performance and resilience [28], [27]. Nevertheless, security and risk considerations do not tend to be a priority or thought of as an assumed limitation; instead, they are often seen as secondary objectives. This lack of correspondence restricts the extrapolability of such works to smart city settings that are intelligent and have resource decisions that can directly affect exposure to cyber and cyber-physical threats.

Lastly, cross-cutting surveys of cyber risk and insurance-focused studies indicate that there is still a multitude of issues with data availability, risk measurement, and intersectoral comparability [3]. Such studies underscore the fact that absence of standardized and high-quality incident and loss data will retard empirical validation of risk models and diminish belief in quantitative risk assessment. It is made worse in smart city settings where a variety of stakeholders, proprietary systems and privacy restrictions further restrict information sharing. Consequently, there has been a high number of suggested smart city risk frameworks that are theoretically tested, but not operationally verified.

Overall, the study confirms that the smart city cybersecurity research is still disjointed on the technical, organizational, and regulatory levels. Although each of the strands is relevant and informative, with some providing background security measures and AI-enhanced detection, others offering governance and ethical aspects, the number of works that combine these viewpoints into a unified, implementable risk assessment and management framework are scarce. This fragmentation highlights the necessity to have an approach whereby AI-aware threat modeling, cyber-physical impact analysis, quantitative risk measures, and ongoing monitoring, are incorporated in

one, operational approach to intelligent IoT-based smart city infrastructures.

Table II shows that the reviewed studies fall into several broad categories: standards-based frameworks, qualitative surveys, probabilistic, CPS-oriented studies, AI-based detection models, adaptive security models, and governance-oriented studies. The analysis of this comparison reveals a definite trend. Standards-based frameworks offer powerful governance framework but are usually inflexible and not responsive to smart city conditions. Taxonomy-based and qualitative studies provide a wide visibility of threats, but seldom assist in dynamic prioritization. Probabilistic and AI-based methods enhance the depth of analysis, but most of them are akin to certain subsystems and are not operationally validated on a city scale. Ethics and governance research brings out issues of accountability and sustainability, yet seldom converts these issues into practicalized risk management processes. Altogether, the literature is still quite fragmented, and there is hardly any research that incorporates under one operational risk management framework the IoT, AI, cyber-physical, and governance dimensions.

IV. Discussion: Challenges and Techniques in Risk Assessment and Management

This section will be the synthesis of the major themes that were identified in the study and are organized in a way that facilitates direct answers to the research objectives and contributions of the current study. The discussion incorporates the technical, operational, and governance perspectives to assess the current state of risk management in smart city infrastructures based on intelligent Internet-of-Things (IoT) technologies.

A. Threat Landscape and Taxonomy of Intelligent Risk Factors

The environment of smart city IoT systems is highly heterogeneous and interconnected where risks come into being on various technical and organizational levels. It is possible to discuss the risk landscape presented in the reviewed literature as a five-layer taxonomy, provided by the study: device layer, network and communication layer, data processing and AI layer, application and service layer, and the governance and organizational layer.

The risks associated with device layers are insecure sensors, embedded devices, firmware vulnerabilities, weak authentication, physical tampering and device compromise. The lack of computational and security power of most IoT devices exacerbates these risks [39], [19].

Examples of network and communication-layer risks are spoofing, running insecure wireless protocols, denial of service, man-in-the-middle and interception of data across heterogeneous communication infrastructures (5G, LPWAN, Wi-Fi, edge-to-cloud).

In automated decision systems, the risks in data processing and AI-layer comprise adversarial machine learning, data poisoning, model inversion, concept drift, biased decision-making, and weak explainability [9], [10], [31].

Risks to application and service-layers involve disruption of smart transportation, energy, surveillance, emergency response and other public services. Due to interconnectedness of these services, the local failure can cause a chain effect on various functions in the city [23], [40].

Governance and organizational risks entail poor accountability, divided risk ownership, poor coordination among the stakeholders, use of nonstandardized metrics, regulatory risk, and inadequate integration of legal, ethical, and operational controls. This stratified taxonomy demonstrates that risk in intelligent smart city infrastructures cannot be confined to single, cybersecurity problems, but rather exists along technical, service, and governance planes (see Fig. 5).

B. Comparative Analysis of Risk Assessment Methodologies

The comparative analysis of the existing study shows a wide range of possible risk assessment models, as shown in Fig. 6, starting with classic qualitative matrices up to the sophisticated data-driven models. The traditional models of qualitative are commonly used due to their simplicity though do not involve the dynamic behavior of decentralized urban ecosystems [3].

More detailed models with the ability to deal with uncertainty and interdependence are available with quantitative and semi-quantitative techniques, including Bayesian networks and fuzzy logic [1], [2], [30]. Nonetheless, these approaches need quality data and in-depth domain expertise, which is often not accessible in advanced smart urban areas. Authors delve more recently into AI-powered anomaly detection and predictive modeling [9], [10]. Although such models hold potential in the real-time monitoring, they have major issues that include transparency, explainability, and susceptibility to adversarial manipulation.

Risk treatment procedures are provided in an organized manner through the use of standard frameworks, e.g. NIST RMF and ISO/IEC 27005 [11], [12]. However, this study finds a large discrepancy: such frameworks assume boundaries of systems and definite ownership of assets, which are not present in the context of decentralized and adaptive smart city conditions [3].

C. Challenges in Real-time, Autonomous, and Decentralized Management

This section summarizes major gaps and constraints that impair efficient risk management in smart city networks. One of the most critical gaps is the lack of a cohesive model that would mitigate the IoT security, AI-specific risks, and cyber-physical implications. Most existing models are not dynamic and do not consider the time varying behavior of the systems that are being continuously updated in software and retraining the models [3].

The two non-technical issues that are dominant are privacy and governance [38]. Smart cities gather sensitive behavioural information and therefore pose a major issue of balancing intelligent service delivery and privacy of data [3]. The absence of specific regulatory frameworks and multiple stakeholders, including the government, the private sector and citizens, also complicate governance because it becomes difficult to

TABLE II. SUMMARY AND COMPARISON OF RELATED WORKS ON RISK ASSESSMENT AND MANAGEMENT IN INTELLIGENT IOT-BASED SMART CITIES

Ref	Objective	Methodology	Results	Key Findings	Limitations
[22]	Analyze security challenges in smart cities	Conceptual analysis of IoT-based city services	Qualitative insights	Heterogeneity increases attack surface	No quantitative risk metrics; IoT-centric
[4]	Study threat modeling for smart cities	Examination study with Bayesian focus	Taxonomy of threat models	Highlights need for probabilistic modeling	No operational validation
[23]	Survey cybersecurity challenges in smart cities	Narrative study	Identified major attack vectors	Emphasizes multi-layer security	Lacks risk quantification
[6]	Study IoT cybersecurity risks	Examination study	Classified IoT risks	Shows fragmented risk handling	Static, non-adaptive
[13]	Taxonomize IoT security risks	Survey and taxonomy	Risk categories identified	Useful baseline taxonomy	No city-scale focus
[17]	Survey IoT cybersecurity techniques	Comprehensive survey	Broad coverage	Highlights attack diversity	No risk prioritization
[21]	Identify critical IoT security categories	Examination study	Security dimensions identified	Structured threat view	Lacks smart city context
[24]	Assess cyber risks in smart city infrastructure	Risk assessment framework	Conceptual risk model	Highlights infrastructure interdependencies	No real-time capability
[20]	Study smart city risk management	Examination study	Identified gaps	Confirms lack of quantitative methods	Study-only
[12]	Standardize information security risk management	Risk management standard	Prescriptive guidance	Widely applicable framework	Static, non-AI-aware
[11]	Define IoT cybersecurity activities	Guideline-based framework	Baseline controls	Strong governance focus	Not smart-city-specific
[1]	Secure IoT devices in government systems	Requirement-based guidance	Security baselines	Improves device hygiene	No risk scoring
[16]	Define security controls for systems	Control catalog	Comprehensive controls	Supports compliance	Heavyweight for real-time use
[14]	Study cyber–physical risks in smart cities	CPS security analysis	Identified cascading risks	Cyber impacts physical systems	Lacks empirical metrics
[25]	Analyze CPS threat landscape	ENISA threat analysis	Threat trends	Confirms CPS risk severity	No city-specific metrics
[26]	Survey edge-based IoT security	Architectural survey	Security design patterns	Edge reduces latency	Fragmented risk handling
[27]	Study edge/cloud IoT computing	Comparative survey	Architecture comparison	Highlights decentralization risks	No risk modeling
[28]	Study fog resource allocation	Examination mapping	Resource strategies	Resource constraints affect resilience	Security treated indirectly
[29]	Detect IoT attacks using ML	ML-based detection	Improved detection accuracy	ML effective for IoT attacks	Detection-only focus
[9]	Study AI-driven IoT security	AI-based threat analysis	Identified AI vulnerabilities	AI introduces new attack surfaces	No risk management integration
[18]	Map AI-based smart city security	Examination mapping study	Technique classification	AI widely used in defense	Ignores AI risk
[7]	Analyze cyber threat landscape	Threat intelligence report	Threat trends identified	Confirms evolving risks	Non-operational
[30]	Identify AI cybersecurity challenges	ENISA analytical report	Risk categories	Highlights adversarial ML	No mitigation framework
[10]	Identify emerging cyber threats	Conference threat analysis	Threat sources identified	AI threats increasing	High-level analysis
[19]	Study city digital twin potential	Examination study	Use cases identified	Supports risk simulation	High computational cost
[8]	Define digital twin requirements	Technical report	Deployment guidelines	Improves system understanding	Limited real-time feasibility
[37]	Study blockchain in IoT & AI	Survey	Security benefits identified	Improves trust & integrity	Scalability issues
[15]	Enable adaptive IoT security	Context-aware models	Improved local adaptation	Dynamic control	No global risk view
[3]	Study cyber risk data availability	Examination study	Data gaps identified	Quantification remains weak	Limits empirical validation
[33]	Link data-driven cities & sustainability	Evidence synthesis	Conceptual insights	Governance is critical	No security metrics
[31]	Explore ethical AI use	Ethical analysis	Normative guidance	Ethics essential for AI systems	Not operationalized
[32]	Study smart vs sustainable cities	Examination study	Sustainability gaps	Security tied to governance	No technical depth

establish risk ownership and accountability [3], [41]. The study concludes that lack of standardised metrics and benchmarks makes it a great challenge to compare the efficacy of various risk management strategies in different city-scale projects.

D. Proposed Strategies and Technologies for Risk Mitigation

In order to overcome the identified threats, the proposed study will use emerging technologies and suggest a pathway to adaptive and resilient infrastructures where Fig. 7 explain the steps of the strategies [1], [2]. Edge and fog computing is referred to as the main enablers in cutting the latency and the exposure of data since information is processed closer

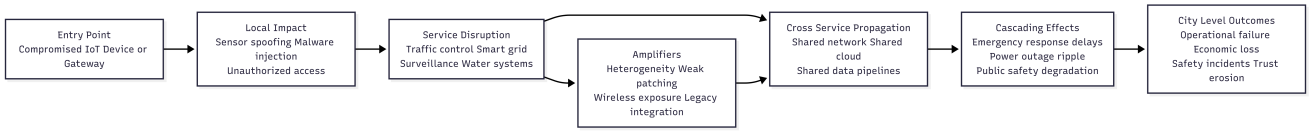

Fig. 5. Example of cascading threat propagation across interconnected smart city services, illustrating how local compromise can trigger city-wide impact.

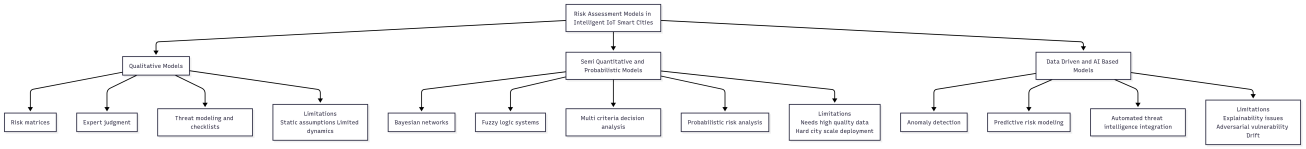

Fig. 6. Taxonomy of risk assessment models reported in the study for intelligent IoT-based smart city systems, including qualitative, probabilistic, and AI-driven approaches.

to the source. Blockchain technologies are suggested to also promote the integrity and auditability of data in distributed environments [1], [2].

The study is more and more in favor of the shift to AI-driven, self-healing security infrastructure that is able to detect anomalies automatically and reconfigure components on the fly [3]. Nevertheless, such solutions further complicate the situation and require stringent validation in order to prevent unexpected outcomes.

Last but not least, this study has added an abstract maturity map, which implies that smart city risk management needs to transform baseline, fixed controls into governance-adopted, AI-conscious, and self-corrective approaches. Risk management cannot be based on one technology, since it should combine technical controls with legal, ethical, and social factors [32].

E. Illustrative Real-World Incidents and Operational Implications

The recorded cases can be used to demonstrate that the risks listed in the literature are not merely theoretical. In the 2018 City of Atlanta ransomware attack, the fundamental operations of the city were disrupted as over a third of the city software applications were offline or partially disabled, including mission-critical services such as police and courts. In 2024, a cyberattack on Transport for London resulted in unauthorised access to a small amount of personal data of some customers, including contact details and potential bank-account information of some users. In 2025, St. Paul, Minnesota, was hit by a coordinated digital attack which the city responded to by shutting down information systems, leading to Wi-Fi disconnection in buildings, library services disrupted, and network resources suspended. Simultaneously, in 2024, U.S. federal government officials advised that disruptive attacks on water and wastewater systems were being conducted by foreign hackers, citing an example in Pennsylvania where a controller at a water facility was incapacitated. These instances demonstrate that the breakdown of digital municipal systems may lead to operational interruption, degradation of the public-services, exposure to privacy, and even safety implications among interconnected urban infrastructures.

V. Future Research Directions

The study also shows that the existing risk assessment and risk management methods are still inadequate to handle the complexity and dynamism of intelligent IoT-based smart city infrastructures. This section provides an overview of some of the most important future research directions that can be used to create more adaptive, resilient, and trustful systems of smart cities. Fig. 8 presents a staged maturity roadmap for evolving risk management in smart cities from baseline controls toward adaptive, AI-aware, and governance-aligned approaches.

A. Adaptive Risk Assessment Models

Creating adaptive risk assessment models that can address continuous modifications in smart city ecosystems is one of the research directions that are of the utmost importance. Future strategies are to be updated dynamically according to the real-time system conditions, environmental factors, and the changing threat intelligence, unlike traditional, inert systems [3].

Continuous monitoring mechanisms and exploiting the streaming data of the IoT devices, edge platforms, and operational logs should be incorporated as adaptive models. The machine learning methods can be used to perceive the new threats and update the risk estimations. Nonetheless, issues of data quality, model drift, and explainability needs to be considered in future studies as well since, in this way, adaptive assessments will be reliable and transparent [1], [2].

B. AI-Driven and Self-Healing Security Frameworks

Self-healing and AI-driven security systems are a good way of controlling risks in autonomous infrastructures of smart cities. These types of frameworks are designed to identify security events, identify root causes, and automatically implement mitigation measures with the least human intervention [3], [35].

Further studies are required in the future to combine AI-based risk management with the resilience principles of systems to allow smart infrastructures of a city to retain satisfactory levels of services even in case of attack or failure. This covers automated isolation of affected parts, dynamic rerouting of network routes, and smart recovery facilities. The

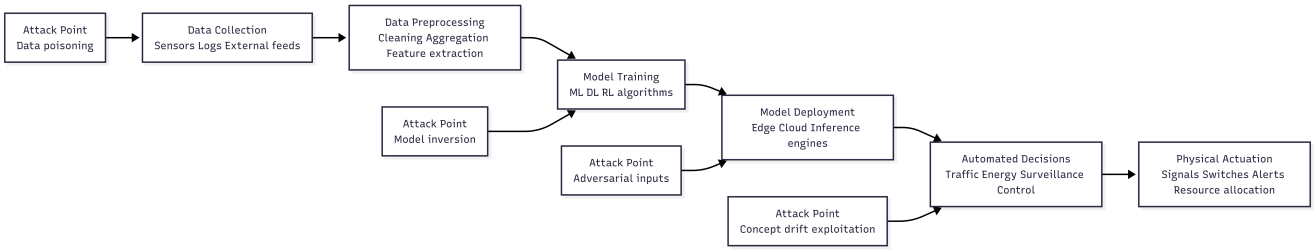

Fig. 7. AI/ML pipeline attack surface in intelligent IoT smart city systems, highlighting adversarial manipulation, data poisoning, model inversion, and drift-related risks.

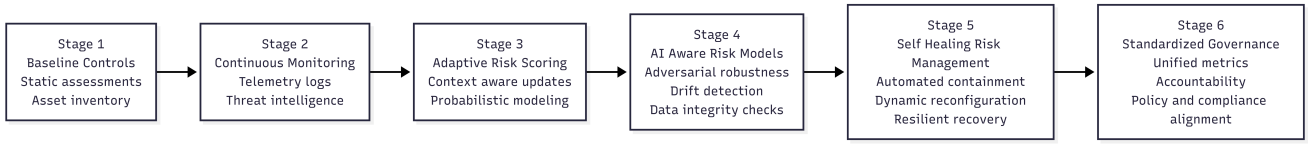

Fig. 8. Proposed maturity roadmap for evolving from baseline risk controls toward adaptive, AI-aware, self-healing, and governance-aligned risk management in smart cities.

research problem of ensuring the strength and safety of these self-healing mechanisms is still open to research [3], [8].

C. Standardization Needs for Smart Cities

Their interoperability and inability to achieve secure smart city deployments are largely due to the absence of standardized risk assessment and management practices. Future studies would help in the establishment of standards specific to domain that deal with the special features of smart IoT-based city infrastructures [3].

The standardization should encompass the technical, organizational, and governance domains, such as risk metrics, threat classification schemes, data governance models, and AI accountability needs. Finding alignment of smart city standards with the existing frameworks including NIST and ISO and extending them to cover AI-related and cyber-physical risks is also a major research priority [11], [12].

D. Practical Deployment Considerations

A gap exists between research and practical implementation to bring about risk management in smart cities. Most of the suggested frameworks and models can be tested by simulation only or through small-scale case studies which restricts their application in practice. The next generation of work would focus on big scale pilot applications and longitudinal designs which would evaluate risk changes over time [3], [42].

Also, the practical implementation should take resource availability, integration of the legacy system, regulatory requirements and coordination of stakeholders. System design should also consider the human factors with the trust of the operator in the risk management tools and the ease of use. These practical considerations will be important issues to address in order to realise the successful implementation of advanced risk management solutions in actual smart city settings [3], [43].

VI. Conclusion

Smart city IoT infrastructures can be extremely effective and efficient, highly automated, and of excellent quality of services, yet they also create complex and changing risks that do not fit the well-established methods of risk evaluation and risk management. This review has explored the recent literature that has been at the crossroads of IoT, artificial intelligence, cybersecurity, and smart city systems. The analysis revealed that current methods are still disjointed. A large amount of research is dedicated to single technical challenges, whereas less is devoted to the interaction of AI-based decision-making, cyber-physical interdependence, complexity of governance, and limitations of operations at the scale of cities.

The review also revealed that the existing frameworks tend to be lacking in flexibility, empirical testing, and standard measures to be used in actual smart city settings. Despite the fact that standards-based models offer a helpful governance framework, and AI-based methodologies enhance detection capabilities, the literature does not report common and operationally feasible frameworks that combine technical, organizational and societal aspects of risk.

The study builds on these results and proposes that future research ought to be directed at adaptive and situation-aware risk assessment model, enhanced treatment of AI-specific threats, enhanced analysis of cyber-physical impact, and more realistic validation in deployed smart city environments. A better taxonomy of risk factors and a more systematic comparison of the current strategies can help build a more robust and reliable smart city infrastructure.

Author Contribution

All authors have equally contributed. All authors have read and agreed to the published version of the manuscript.

Funding

This work was supported by the Deanship of Scientific Research, Vice Presidency of Graduate Studies and Scientific

Research, King Faisal University, Saudi Arabia under the [GRANT No. KFU261919].

Data Availability Statement

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

Acknowledgment

The authors wish to express their gratitude to the Deanship of Scientific Research, Vice Presidency of Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia.

We would like to acknowledge the anonymous reviewers who made great contributions with their brilliant scholarly intuitive comments and sagacious recommendations to improve the quality and clarity of this study.

Conflicts of Interest The authors declare no conflicts of interest.

References

[1] M. Fagan, J. Marron, J. Brady, Kevin G., B. B. Cuthill, K. N. Megas, R. Herold, D. Lemire, and B. Hoehn, "IoT device cybersecurity guidance for the federal government: Establishing IoT device cybersecurity requirements," National Institute of Standards and Technology (NIST), NIST Special Publication 800-213, 2022. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-213

[2] K. N. Megas, M. Fagan, K. Scarfone, and M. Smith, "IoT device cybersecurity requirement catalog," National Institute of Standards and Technology, Tech. Rep. NIST SP 800-213A, 2021. [Online]. Available: https://www.nist.gov/publications/iot-device-cybersecurity-guidance-federal-government-iot-device-cybersecurity

[3] F. Cremer, B. Sheehan, M. Fortmann, A. N. Kia, M. Mullins, F. Murphy, and S. Materne, "Cyber risk and cybersecurity: A systematic review of data availability," *The Geneva Papers on Risk and Insurance - Issues and Practice*, vol. 47, no. 3, pp. 698–736, 2022.

[4] M. Wright, H. Chizari, and T. Viana, "A systematic review of smart city infrastructure threat modelling methodologies: A bayesian focused review," *Sustainability*, vol. 14, no. 16, p. 10368, 2022.

[5] A. Clim, A. Toma, R. D. Zota, and R. Constantinescu, "The need for cybersecurity in industrial revolution and smart cities," *Sensors*, vol. 23, no. 1, p. 120, 2023.

[6] T. S. AlSalem, M. A. Almaiah, and A. Lutfi, "Cybersecurity risk analysis in the IoT: A systematic review," *Electronics*, vol. 12, no. 18, p. 3958, 2023.

[7] M. Barros Lourenco and L. Marinos, "ENISA threat landscape 2019/2020 – the year in review," European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape Report, Oct. 2020. [Online]. Available: https://doi.org/10.2824/552242

[8] "ETSI en 303 645 v3.1.3 cyber security for consumer internet of things: Baseline requirements," European Telecommunications Standards Institute (ETSI), Tech. Rep., 2024. [Online]. Available: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

[9] W. Zhao and P. Wang, "AI-driven cybersecurity in IoT-based systems," *Sensors*, vol. 25, no. 23, p. 7254, 2025.

[10] J. Simola and T. Leppanen, "Identification of the emerging sources of cybersecurity threats," in *European Conference on Cyber Warfare and Security*, vol. 24, no. 1, 2025, pp. 794–802.

[11] M. Fagan *et al.*, "Foundational cybersecurity activities for IoT device manufacturers," National Institute of Standards and Technology, Tech. Rep. NISTIR 8259, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf

[12] *ISO/IEC 27005:2022 Information Security Risk Management*, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2022. [Online]. Available: https://blog.ansi.org/ansi/iso-iec-27005-2022-security-risk-management/

[13] M. Waqdan, H. Louafi, and M. Mouhoub, "Security risk assessment in IoT environments: A taxonomy and survey," *Computers & Security*, vol. 154, p. 104456, 2025.

[14] M. Houichi, F. Jaidi, and A. Bouhoula, "Cyber security within smart cities: A comprehensive study and a novel intrusion detection-based approach," *Computers, Materials & Continua*, vol. 81, no. 1, pp. 393–441, 2024.

[15] M. Fagan *et al.*, "IoT device cybersecurity capability core baseline," National Institute of Standards and Technology, Tech. Rep. NISTIR 8259A, 2020. [Online]. Available: https://csrc.nist.gov/pubs/ir/8259/a/final

[16] J. T. Force, "Security and privacy controls for information systems and organizations, revision 5," National Institute of Standards and Technology (NIST), NIST Special Publication 800-53, Revision 5, 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-53r5

[17] E. Dritsas and M. Trigka, "A survey on cybersecurity in IoT," *Future Internet*, vol. 17, p. 30, 2025.

[18] R. Alraddadi, M. Alshayeb, S. Mahmood, and M. Niazi, "Enhancing cybersecurity in smart and cognitive cities: A systematic mapping of AI-based techniques," *Array*, vol. 28, p. 100606, 2025.

[19] E. Shahat, C. Hyun, and C. Yeom, "City digital twin potentials: A review and research agenda," *Sustainability*, vol. 13, p. 3386, 2021.

[20] J. Alshehri, A. Alhamed, and M. M. H. Rahman, "A systematic literature review on cybersecurity risk management in smart cities," in *2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, Osaka, Japan, 2024, pp. 407–412.

[21] H. Sebestyen, D. Popescu, and R. Zmaranda, "A literature review on security in the internet of things: Identifying and analysing critical categories," *Computers*, vol. 14, p. 61, 2025.

[22] C. K. Toh, "Security for smart cities," *IET Smart Cities*, vol. 2, no. 2, 2020.

[23] J. S. Oliha and P. W. Biu, "Securing the smart city: A review of cybersecurity challenges and strategies," *Open Access Research Journal of Multidisciplinary Studies*, vol. 7, no. 1, pp. 094–101, 2024.

[24] M. Kalinin, V. Krundyshev, and P. Zegzhda, "Cybersecurity risk assessment in smart city infrastructures," *Machines*, vol. 9, no. 4, p. 78, 2021.

[25] M. Goncalves *et al.*, "ENISA threat landscape 2021," ENISA, Tech. Rep., 2021. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[26] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing based designs for IoT security," *Digital Communications and Networks*, vol. 6, no. 2, 2020.

[27] F. Andriulo, M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, "Edge computing and cloud computing for internet of things: A review," *Informatics*, vol. 11, p. 71, 2024.

[28] I. B. Lahmar and K. Boukadi, "Resource allocation in fog computing: A systematic mapping study," in *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, Paris, France, 2020, pp. 86–93.

[29] M. F. Hyder, W. Nazir, M. U. Farooq, M. Anwer *et al.*, "Attack detection in IoT using machine learning," *Engineering, Technology and Applied Science Research*, vol. 11, no. 3, pp. 7273–7278, 2021.

[30] European Union Agency for Cybersecurity (ENISA), "Artificial intelligence cybersecurity challenges," ENISA, Tech. Rep., 2020. [Online]. Available: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

[31] M. Taddeo and L. Floridi, "How AI can be a force for good," *Science*, vol. 361, no. 6404, pp. 751–752, 2020.

[32] T. Yigitcanlar, L. Kamruzzaman, M. Foth, and J. Marques, "Can cities become smart without being sustainable? a systematic review of the literature," *Sustainable Cities and Society*, vol. 45, 2025.

[33] S. E. Bibri, "Data-driven smart sustainable cities of the future: An evidence synthesis approach to a comprehensive state-of-the-art literature review," *Sustainable Futures*, vol. 3, no. 1, p. 100047, 2021.

[34] "ETSI en 303 645 v2.1.1 cyber security for consumer internet of things: Baseline requirements," European Telecommunications Standards Institute (ETSI), Tech. Rep., 2020. [Online]. Available: https://www.etsi.org/standards#303645

[35] M. Gencer *et al.*, "Profile of the IoT core baseline for consumer IoT products," National Institute of Standards and Technology, Tech. Rep. NISTIR 8425 (Initial Public Draft), 2022. [Online]. Available: https://csrc.nist.gov/external/nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.ipd.pdf

[36] M. Fagan *et al.*, "NISTIR 8259 series: Cybersecurity for IoT program," National Institute of Standards and Technology, Tech. Rep., 2021. [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series

[37] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A review of blockchain in internet of things and AI," *Big Data Cogn. Comput.*, vol. 4, p. 28, 2020.

[38] T. Xue, Y. Zhang, Y. Wang, W. Wang, S. Li, and H. Zhang, "Edge computing for IoT: Novel insights from a comparative analysis of access control models," *Computer Networks*, vol. 270, p. 111468, 2025.

[39] G. M. Abreu, A. Pan, A. E. Post, N. Malkin, and K. T. Frick, "How do cyber-risks vary across smart city technologies?" *Journal of Urban Technology*, pp. 71–91, 2025.

[40] B. Sereda and J. Jaskolka, "An evaluation of IoT security guidance documents: A shared responsibility perspective," *Procedia Computer Science*, vol. 201, pp. 281–288, 2022.

[41] M. Alowaidi, S. K. Sharma, A. AlEnizi, and S. Bhardwaj, "Integrating artificial intelligence in cyber security for cyber-physical systems," *Electronic Research Archive*, vol. 31, no. 4, pp. 1876–1896, 2023.

[42] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *Systematic Reviews*, vol. 10, no. 1, p. 89, 2021. [Online]. Available: https://link.springer.com/article/10.1186/s13643-021-01626-4

[43] N. Rieke, J. Hancox, W. Li, F. Milletari *et al.*, "The future of digital health with federated learning," *npj Digital Medicine*, vol. 3, no. 1, 2020.