frontiers | Frontiers in Computer Science

TYPE Original Research
PUBLISHED 22 July 2025
DOI 10.3389/fcomp.2025.1647179

OPEN ACCESS

EDITED BY
Muriel Figueredo Franco,
Federal University of Health Sciences of Porto Alegre, Brazil

REVIEWED BY
Kishor Kumar Reddy C.,
Stanley College of Engineering and Technology for Women, India
Santosh I. Gore,
Sai Info Solution, India

*CORRESPONDENCE
Mariya Ouaissa
m.ouaissa@uca.ac.ma

RECEIVED 14 June 2025
ACCEPTED 10 July 2025
PUBLISHED 22 July 2025

CITATION
Ouaissa M, Ouaissa M, Nadifi Z, El Himer S, Al Masmoudi Y and Kartit A (2025) A framework for cyber threat modeling and risk assessment in smart city environments.
Front. Comput. Sci. 7:1647179.
doi: 10.3389/fcomp.2025.1647179

A framework for cyber threat modeling and risk assessment in smart city environments

Mariya Ouaissa[1]*, Mariyam Ouaissa[2], Zineb Nadifi[2], Sarah El Himer[3], Yassine Al Masmoudi[4] and Ali Kartit[2]

[1]LISI, Cadi Ayyad University, Marrakech, Morocco, [2]LTI, Chouaib Doukkali University, El Jadida, Morocco, [3]Sidi Mohamed Ben Abdellah University, Fez, Morocco, [4]Laboratory of Geosciences and Environment Technics, Faculty of Science, El Jadida, Morocco

Introduction: With the rise of digital transformation, the concept of the smart city has emerged as a key pillar of modern urban development. However, as smart cities increasingly rely on the Internet of Things (IoT), cloud computing, and real-time data processing, they also face an expanded attack surface and growing cybersecurity threats.

Methods: This paper presents a comprehensive threat modeling and risk assessment approach tailored to smart city environments. It begins by identifying the core components and data flows within a typical smart city architecture covering domains such as surveillance, transportation, and healthcare. A Data Flow Diagram (DFD) is constructed to visualize the interactions and pinpoint critical assets. The STRIDE methodology, supported by the Microsoft Threat Modeling (MTM) tool, is employed to systematically uncover threats including spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. To enrich the analysis and align with real-world adversarial behavior, the MITRE ATT&CK framework is also utilized to map identified threats to known tactics and techniques. Each discovered threat is evaluated through a detailed risk assessment using the Common Vulnerability Scoring System (CVSS) and a 5 by 5 risk matrix, allowing a quantifiable estimation of impact and likelihood.

Results: The analysis revealed 21 threats across smart city domains, with spoofing, tampering, and denial of service being the most frequent. Five threats were rated as critical based on CVSS, particularly targeting cloud services and web applications.

Discussion: Furthermore, the paper introduces a dedicated case study involving the Internet of Vehicles (IoV), applying the Cyber Kill Chain model to demonstrate the progression of a cyber-attack targeting connected vehicle systems, with a focus on identifying less common yet critical ATT&CK techniques at each phase. The study concludes by proposing targeted mitigation strategies and architectural recommendations aimed at enhancing the cyber resilience of smart city infrastructures.

KEYWORDS

threat modeling, STRIDE, MITRE ATT&CK, MTM, risk assessment, CVSS, cyber kill chain adversarial tactics, techniques

1 Introduction

The concept of smart cities has become central to discussions about the future of urbanization. By leveraging Information and Communication Technologies (ICT), smart cities aim to enhance the quality of life for residents through the efficient management of urban services such as mobility, energy, security, and the environment (Bastos et al., 2024). Internet

of Things (IoT) devices and connected systems play a crucial role in monitoring and optimizing infrastructure, including public transport, street lighting, traffic flow, waste management, air quality, and telecommunications (Chen et al., 2024).

As technology advances, smart city applications are proving essential for building sustainable, efficient, and secure urban environments. These innovations support more responsive and user-oriented city management across key sectors, ultimately fostering resilient and future-ready communities (Razavi et al., 2024). However, cities face multiple and interrelated challenges, including the need to improve residents' quality of life, develop infrastructure and housing, stimulate economic activity, protect security and privacy, and reduce energy consumption and environmental impact. Addressing these demands requires sustainable and intelligent urban development strategies that strike a balance between comfort, efficiency, and ecological responsibility (Sánchez-Corcuera et al., 2019). At the same time, the very technologies that enable smart cities such as IoT, Artificial Intelligence (AI), and cloud platforms also introduce significant cybersecurity risks. The widespread use of interconnected systems and data-driven services expands the attack surface and exposes urban infrastructures to threats like data breaches, service disruptions, ransomware, and unauthorized surveillance. Ensuring the security, privacy, and resilience of these systems is therefore not only a technical challenge but also a foundational requirement for the safe and trusted development of smart cities.

In this context, the increasing reliance on interconnected community infrastructures and digital services introduces new vulnerabilities. As cities become more connected, they are also more exposed to cyberattacks targeting essential systems. At the same time, urban environments are becoming testing grounds for emerging security technologies, such as augmented video surveillance, artificial intelligence, and facial recognition. While these technologies aim to enhance public safety, they also raise significant concerns about privacy, ethical use, and potential misuse (Rasoulzadeh Aghdam et al., 2025). In our work, the proposed methodology for cyber threat modeling and risk assessment in smart cities consists of six major steps. These include smart city use case definition and security requirements, system modeling through data flow diagram (DFD), threat identification using the STRIDE methodology, mapping attacker behavior using the MITRE ATT&CK framework, risk evaluation using both CVSS and a 5 by 5 risk matrix, and finally, the formulation of targeted mitigation strategies (see Figure 1).

This paper provides a more comprehensive and systematic methodology by integrating both STRIDE and the MITRE ATT&CK framework for detailed threat classification and tactic–technique mapping. To quantify the risk levels, we conduct a rigorous risk assessment using the Common Vulnerability Scoring System (CVSS) along with a 5 by 5 risk matrix. Furthermore, we enhance the practical applicability of our model by incorporating a realistic case study in an Internet of Vehicles (IoV) environment, evaluated through the Cyber Kill Chain to enable deeper analysis of adversarial behavior across the various phases of an attack. Finally, we propose targeted mitigation strategies for each identified threat, providing a concrete and actionable security roadmap for smart city environments. The structure of this article is as follows: Section 2 provides an overview of related work. Section 3 presents a description of smart city infrastructure and applications, as well as the associated security issues. The threat modeling methodology and tools are described in Section 4. Section 5 outlines the proposed methodology. Section 6 details the results along with a discussion. Finally, conclusions are drawn in Section 7.

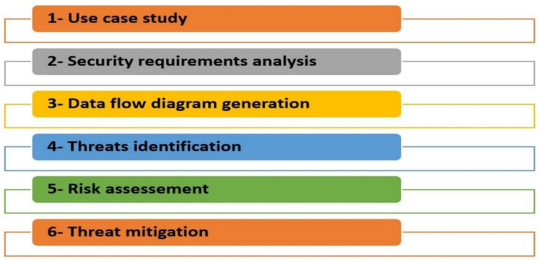

FIGURE 1
Threat modeling process for smart city system.

2 Related work

Given the importance, topicality, and richness of the subject, it has been the subject of various researches and articles, and has been tackled from different angles and approaches.

Paper (Tok and Chattopadhyay, 2023) addresses the growing concern of cyber threats targeting Smart City Infrastructure (SCI), complex systems integrating IoT, cloud platforms, and citizen services. These infrastructures, while designed to improve the quality of urban life, are vulnerable to a wide spectrum of cyber-attacks due to their scale, heterogeneity, and lack of standardized forensic readiness. To help Digital Forensic Investigators (DFI) and Law Enforcement Agencies (LEA), the authors define a standardized model of SCI using internationally recognized ISO standards. They apply the STRIDE threat modeling methodology to identify potential cyber threats, map them to cybercrime offenses and correlate them with possible evidence sources.

Authors in paper (Anwar et al., 2020) focuses on addressing security and privacy concerns in smart cities by applying Microsoft's STRIDE threat modeling methodology. As smart cities are complex systems composed of numerous interconnected components, such as smart homes, transportation systems, healthcare, energy grids, and governance—their vulnerability to cyber threats is significant. The authors break down the architecture of a smart city into manageable components, use data flow diagrams to visualize interactions, and apply the STRIDE model to systematically identify 36 security threats across four primary categories: sensing devices, communication channels, APIs/computation layers, and databases. For each threat, appropriate countermeasures are proposed.

In Koban et al. (2022), authors explore privacy and security challenges faced by users in blockchain-enabled smart city environments. Recognizing the growing reliance on technologies

Abbreviations: ATT&CK, Adversarial Tactics, Techniques, and Common Knowledge (MITRE Framework); CVSS, Common Vulnerability Scoring System; DFD, Data Flow Diagram; IoT, Internet of Things; IoV, Internet of Vehicles; MTM, Microsoft Threat Modeling (Tool); SIEM, Security Information and Event Management; STRIDE, Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.

such as IoT, AI, and blockchain within smart city infrastructures, the authors emphasize the need for a focused threat analysis from the user's perspective. Using NetObjex as a case study, the paper employs a hybrid Threat Modeling Method (hTMM), which combines Security Cards, Persona Non-Grata profiling, and the STRIDE framework to identify and classify critical threats. Through data flow and sequence diagrams, the study models interactions like device registration, verification, and payments, ultimately identifying six key user-centric threats including financial fraud, surveillance, and unauthorized data access. The work provides a structured methodology to anticipate adversary behavior and inform the design of more secure and privacy-preserving smart city systems.

The work in Wang et al. (2015) explore cybersecurity challenges within smart city systems and proposes a comprehensive framework to mitigate associated risks. It emphasizes the vulnerability of smart city infrastructures, comprising interconnected sensors, networks, and data systems; to a wide range of cyber threats such as phishing, malware, insider attacks, and weak encryption. The authors introduce the Hardware, Intelligence, Software, Policies, Operations (HiSPO) approach, which leverages hundreds of systems features to model threats and calculate a "threat factor" indicating system vulnerability. Using threat intelligence, risk assessments, and threat modeling, the study demonstrates how systematic identification and mitigation efforts can significantly lower threat levels. Real-world case studies and experimental results show that applying this methodology effectively enhances the security and resilience of smart city infrastructures.

This present article offers a more comprehensive and systematic methodology by integrating both STRIDE and the MITRE ATT&CK framework for detailed threat classification and tactic-technique mapping. Furthermore, we enhance the practical applicability of our model by incorporating a realistic case study in an internet of vehicle environment evaluated through the Cyber Kill Chain, allowing for a deeper analysis of adversarial behavior across different phases of an attack. This multi-layered approach not only strengthens the accuracy of threat identification but also provides a robust foundation for risk assessment and mitigation planning in smart city infrastructures.

3 Background

In this section, we present the infrastructure of smart city and their applications, followed by a discussion of the security challenges associated with this architecture.

3.1 Smart city infrastructure

A smart city is one that uses technology to engage its residents and link its infrastructure. A smart city can securely integrate multiple technological solutions to manage its assets, which may include local department information systems, schools, libraries, transportation systems, hospitals, power plants, law enforcement, and other community services (Singh et al., 2022). Technology shapes how city officials connect with the community and its infrastructure. Real-time monitoring systems and sensors collect data from citizens and sensors, which are then processed in real time. The information and insights gained are critical in eliminating inefficiencies and ultimately to system optimization. A smart city provides technical solutions to expose what is happening in the city, how it is changing, and how to improve the quality of life (Okai et al., 2018). However, the bulk of smart city architectures presented in the literature have four layers as shown in Figure 2: sensing layer, transmission layer, data management layer, and application layer (Bhardwaj et al., 2024).

3.1.1 Sensing layer

The primary function of this layer is to collect data from a variety of physical devices. On the one hand, data gathering is regarded as the most significant duty because it governs the rest of the operations of a smart city. However, because of the vast variability of the data, it is regarded as the most difficult assignment.

3.1.2 Transmission layer

This layer transmits data to the upper layers via a variety of communication technologies and protocols. Figure 2 depicts the various communication technologies used for smart city deployment. For example, they use access network technologies such as Bluetooth, Zigbee, Near Field Communication (NFC), M2M, RFID, and Zwave, which provide limited coverage, as well as network transmission technologies like as 4G, 5G, and Low-Power Wide Area Network (LP-WAN), which provide greater coverage.

3.1.3 Data management layer

The data management layer processes and stores the received information, which is required for the application layer's numerous services to work properly. In reality, the success of the data management layer is critical for a sustainable smart city because the performance of smart city services is dependent on data management. The primary function of the data layer is to sustain data vitality by concentrating on data purification, evolution, association, and maintenance.

3.1.4 Application layer

The application layer is the highest level of the smart city design, acting as a bridge between citizens and the data management layer. The application layer's performance has a significant impact on users' perceptions and satisfaction with smart city operations since it interacts directly with inhabitants. Citizens are concerned about the city's smart conduct, which includes smart services like weather forecasting. The application layer is made up of pieces from several domains. The application layer's key functions include smart transportation, weather forecasting, smart healthcare, and smart governance.

3.2 Smart city applications

To transform a simple city into a smart city, it is essential to implement a significant effort to integrate ICT-based solutions into key sectors of society such as governance, economy, transportation, environment, and health as illustrated in Figure 3 (Al-Ani et al., 2019; Abadía et al., 2022).

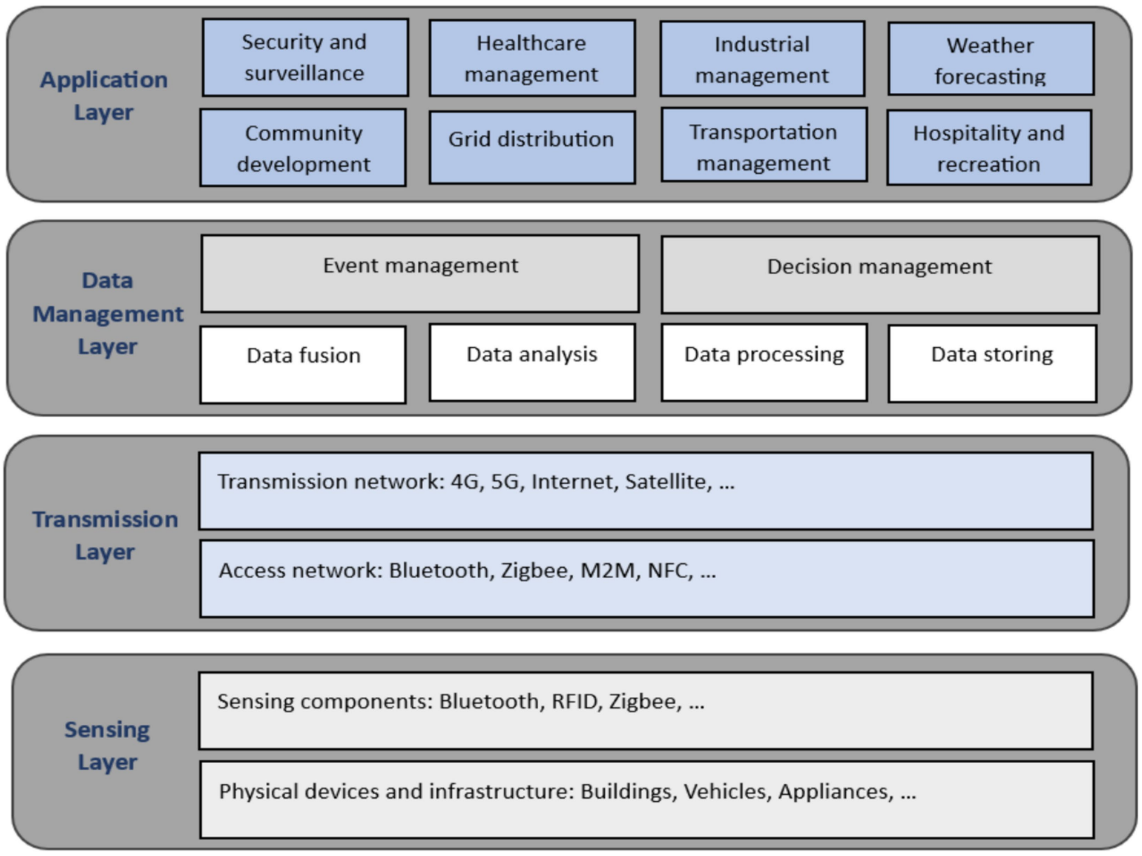

FIGURE 2
Smart city layered architecture.

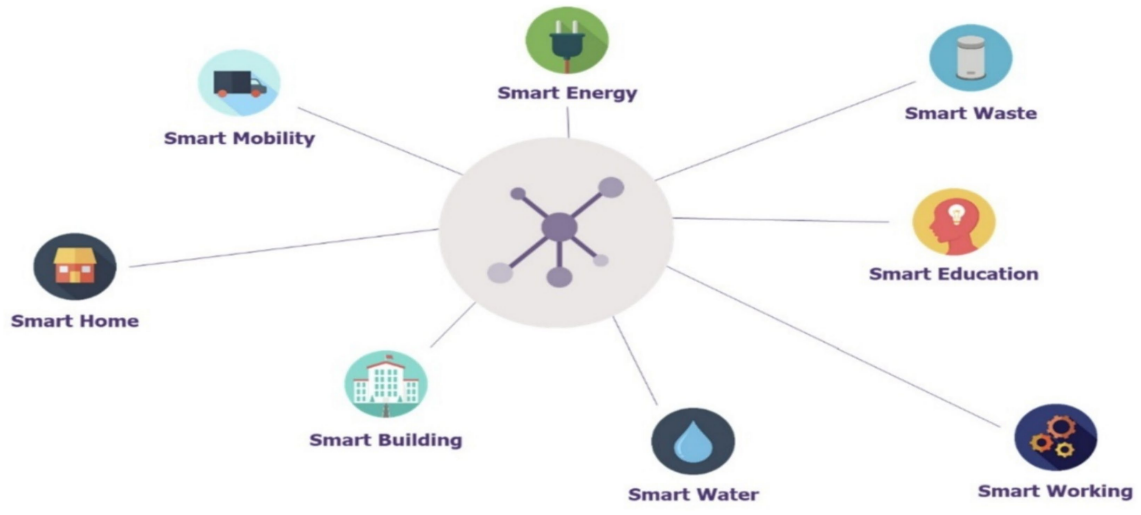

FIGURE 3
Smart city applications.

3.2.1 Smart governance

Smart governance, also known as digital governance or e-governance, aims to make governance systems more efficient, transparent, participatory, and accountable. The objective of smart governance is to transform public administrations by using ICTs to deliver more effective services and respond to citizens' needs in a faster and more personalized manner. It contributes to the creation of smart cities by promoting participatory, transparent,

and results-oriented governance, while harnessing the benefits of technological advances to improve citizens' quality of life.

3.2.2 Smart economy

The goal of the smart economy is to create an environment conducive to innovation, competitiveness, and economic sustainability. It encompasses various aspects, such as the use of artificial intelligence, data analytics, IoT and digital platforms to optimize business processes, stimulate entrepreneurship, and foster innovation.

3.2.3 Smart transportation

Smart transportation plays a crucial role in the development of smart cities by improving the mobility, safety, efficiency, and sustainability of transportation systems. The importance of smart transportation lies in its ability to reduce traffic congestion, travel times, and CO2 emissions through advanced traffic management, smart signaling, parking management, and public transportation planning systems.

3.2.4 Smart environmental elements

Smartness is an important feature of smart cities. It includes air quality, water management, green space maintenance, emission monitoring, waste collection, energy efficiency, and natural resource conservation. The main objective of a smart environment is to achieve a balance between urban development and environmental protection. This involves, for example, implementing innovative solutions for waste management, efficient use of natural resources, reducing pollution, promoting renewable energy, preserving biodiversity, and creating green spaces and urban parks.

3.2.5 Smart health

Smart health encompasses a wide range of applications and solutions, such as electronic health records, connected medical devices, mobile health monitoring apps, telemedicine, artificial intelligence in health, and health data analytics. These technologies enable the collection, sharing, and analysis of health data to facilitate diagnosis, remote patient monitoring, and more. The processing of this data leads to real-time decisions about patients' health status.

3.3 Security issues in smart city

The shift to emerging networks and IoT in smart cities increases the risk of cyberattacks. Attacks on transportation, energy, security, and water systems can cause massive disruptions to public services. These new technologies allow for the connection of an increasing number of IoT devices, but this can also open the door to a new wave of cyberattacks targeting critical government systems (Toh, 2020).

In fact, smart cities are prime targets for cybercriminals due to their connected architecture, which links thousands of interconnected systems and technologies, such as sensor networks, industrial control systems, intelligent transportation systems, and energy management systems (Mothanna et al., 2024).

They also use IoT technologies to connect thousands of devices, such as surveillance cameras, energy meters, and traffic sensors. These devices can be vulnerable to attacks due to their weak security and lack of updates.

The utilities that use these systems are the most vulnerable to cyberattacks due to the nature of their operation. As they are responsible for providing vital services such as water, electricity, and healthcare to the population, they bear a significant responsibility in terms of data availability and security. Furthermore, utilities often have aging IT systems and may lack the resources to implement effective security measures (Laufs et al., 2020).

Furthermore, utilities are often targeted by cybercriminals for political or economic reasons. For example, cyberattacks can be used to disrupt public services in a given territory or to extort money from authorities (Poleto et al., 2023).

Cybersecurity concerns in smart cities are an increasing issue, but not an insurmountable one. Cities can create a safe and resilient future for their residents by putting cybersecurity first in the planning, development, and operation of smart city infrastructure. Smart cities can use technology to improve people's lives, but strong cybersecurity measures are required to ensure that this progress occurs safely (Ismagilova et al., 2022).

Smart cities are more vulnerable to cyberattacks with potentially far-reaching implications since they rely on a broad network of IoT devices (AlJamal et al., 2024). These threats take numerous forms:

3.3.1 Data breaches

Smart city systems capture large amounts of personal and operational data, including traffic patterns, energy use, and citizen movement, making them a valuable target for hackers. Data breaches can compromise sensitive information, resulting in identity theft, financial fraud, and even blackmail.

3.3.2 Disruption of services

Hackers could disrupt services by gaining control of a smart traffic light system. They may influence traffic flow, resulting in gridlock and pandemonium. Similarly, attacks on power grids and water management systems might have disastrous results. Service disruption is a serious risk for smart city cybersecurity.

3.3.3 Ransomware attacks

Ransomware attacks encrypt important data and demand a ransom payment. This technique can have a substantial financial impact and interrupt key services such as emergency response systems and public transit.

3.3.4 Denial-of-service (DoS) attacks

DoS assaults interrupt networks with excessive traffic, blocking legitimate users. A denial-of-service attack on a smart city's control center might easily disable key infrastructure, creating widespread panic and disruption.

3.3.5 Supply chain attacks

Cybersecurity threats in smart cities go beyond directly connected gadgets. Hackers can use supply chain weaknesses to compromise software or hardware components in smart city infrastructure. This can have a cascading effect, making entire systems vulnerable.

4 Threat modeling approach for smart cities

This section presents an overview of widely used threat modeling frameworks and tools, with a particular focus on the STRIDE

methodology and the MITRE ATT&CK framework, both of which are employed in our proposed approach.

4.1 Threat modeling overview

The threat modeling framework offers a systematic approach to discovering, assessing, and addressing security threats to a system (Xiong and Lagerström, 2019). The framework aids in the identification of security hazards when designing or deploying a system or application, and it is critical in the preparation of security threat response strategies (Ouaissa and Ouaissa, 2025). Various threat modeling tools are available, including DREAD, PASTA, OWASP Threat Dragon, STRIDE and MITRE ATT&CK (Naik et al., 2024).

4.1.1 DREAD

The DREAD threat model is a risk assessment system that enables businesses to measure, compare, and prioritize the risk of security threats. The term DREAD stands for Damage, Reproducibility, Usability, Affected Users, and Discoverability. Each component contributes to a thorough assessment of potential security vulnerabilities, allowing teams to determine informed resource allocation and mitigation measures. DREAD, which was initially established as part of Microsoft's Security Development Lifecycle (SDL), has since become a widely adopted approach across a variety of sectors. Although Microsoft has since embraced alternative threat modeling methodologies, DREAD remains relevant due to its simplicity and practical application in a wide range of settings.

4.1.2 PASTA

The PASTA abbreviation stands for Process for Attack Simulation and Threat Analysis. PASTA is a seven-step threat modeling methodology that integrates business objectives and technical requirements to deliver a comprehensive risk assessment of potential threats. Unlike other threat modeling methodologies, which may focus solely on technical vulnerabilities, PASTA adopts a comprehensive approach that considers both business effect and technological concerns. This comprehensive approach makes it especially effective in company situations where security decisions must be consistent with business objectives. The PASTA methodology is iterative and flexible, allowing organizations to tailor it to their own requirements while retaining a structured approach to threat assessment. By emphasizing risk-based analysis, PASTA assists organizations in prioritizing security investments and focusing on protecting their most valuable assets.

4.1.3 OWASP threat dragon

OWASP Threat Dragon is a threat modeling tool designed to create threat model diagrams within the secure development lifecycle. Aligned with the principles of the Threat Modeling Manifesto, it helps document potential threats, define mitigation strategies, and visually represent threat model components and attack surfaces. Available as both an online and desktop application, Threat Dragon facilitates comprehensive threat analysis and security planning.

4.1.4 STRIDE

STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege. STRIDE is commonly used in cybersecurity to analyze potential security risks in applications, networks, and systems.

Each strategy aims at a specific perspective and will be more relevant and effective in some contexts than others; this paper will focus on STRIDE as a methodology. Microsoft developed the STRIDE threat model, which has emerged as one of the most effective models for proactive security planning (Das et al., 2024). The STRIDE is a systematic approach to security that encourages development teams to think like hackers in order to defend their systems before they are breached. Unlike DREAD, which primarily focuses on scoring and prioritizing threats based on impact and exploitability without offering a systematic method for discovering them, STRIDE enables a comprehensive mapping of threats to specific elements within the smart city system. While PASTA offers an attacker-centric and risk-driven methodology suitable for enterprise-level threat modeling, it requires extensive contextual and business-driven inputs, which can be complex and less adaptable in smart city infrastructure scenarios. Similarly, OWASP Threat Dragon, although user-friendly and valuable for visual modeling, is primarily a tool rather than a full framework, and it often depends on the underlying threat model being applied—such as STRIDE itself. Therefore, STRIDE was chosen for its clarity, ease of integration with data flow diagrams, and its alignment with technical threat categorization, making it particularly effective for identifying and structuring threats (Mahlous, 2023).

4.2 STRIDE method

The STRIDE model divides threats into six categories, each addressing a different component of software security risk (Table 1).

4.2.1 Spoofing

Consider digital identity theft. This entails mimicking another user or system component in order to obtain illegal access. Spoofing attacks exploit authentication methods, allowing hackers to impersonate genuine users or devices.

4.2.2 Tampering

Tampering refers to the unlawful modification of data or code. Such assaults might jeopardize data integrity by modifying files, databases, software code, deployment pipelines, or memory in live systems. Tampering with any system carries significant hazards, particularly when data accuracy is crucial for decision-making.

4.2.3 Repudiation

Threats of repudiation take advantage of accountability gaps. This type of security danger happens when a user or system refuses to complete a certain task, such as a transaction. This threat takes

TABLE 1 STRIDE model threat and security objective violation.

Threat	Security objective violation
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of privilege	Authorization

advantage of a lack of non-repudiation measures in software systems, making it harder to hold parties accountable for their behavior.

4.2.4 Information disclosure

This is the unintended disclosure of confidential or sensitive information to unauthorized people. This could be due to insufficient encryption, inappropriate access controls, or vulnerabilities in web applications.

4.2.5 Denial of service

This type of security threat attempts to disrupt service availability by overloading the system with excessive requests or exploiting system weaknesses. DoS attacks make systems unavailable to legitimate users and disrupt company operations.

4.2.6 Elevation of privilege

This happens when a hacker gains unauthorized access, typically by exploiting a system vulnerability. This can result in administrative control over a system, allowing the attacker to install malware, change system settings, or view sensitive data.

4.2.7 MITRE ATT&CK framework

The MITRE ATT&CK Framework, which stands for Adversarial Tactics, Techniques, and Common Knowledge, is a comprehensive collection of the tactics and techniques employed by cyber attackers to breach organizations' security systems. This paradigm enables cybersecurity professionals to better understand how attackers operate by giving a systematic strategy to detecting, preventing, and responding to threats (Zahid et al., 2023). There are three major editions of the MITRE ATT&CK Framework:

4.2.8 Enterprise

This iteration focuses on assaults on enterprise networks and includes Windows, macOS, and Linux operating systems, as well as cloud environments.

4.2.9 Mobile

Concentrates on attack vectors unique to mobile devices running Android and iOS.

4.2.10 Industrial control systems (ICS)

Addresses vulnerabilities to industrial control systems, which are present in vital infrastructure sectors such as power generating and manufacturing facilities.

The goal of the MITRE ATTACK framework is to strengthen the measures taken after an organization has been compromised. This allows the cybersecurity team to answer important questions about how the attacker gained access to the system and what they did once they did. As information is collected over time, a knowledge base is formed. This is a constantly expanding tool that teams can use to strengthen their defenses. Using the reports generated by MITRE ATT&CK, an organization can determine where its security architecture has vulnerabilities and determine which ones to remediate first, based on the risk each poses (Al-Sada et al., 2024).

In smart cities, where interconnected systems like transportation, healthcare, and energy rely on shared digital infrastructure, the MITRE ATT&CK framework is particularly valuable. It enables security teams to map attacks to specific tactics and techniques, enhancing threat detection and situational awareness. Given the complexity and limited visibility across smart city networks, ATT&CK supports more effective threat hunting and timely responses to protect critical services and maintain public trust (Al-Sada et al., 2023).

5 Proposed methodology

In this section, we introduce the steps of our proposed methodology, including the DFD diagram, threat identification, risk assessment, and threat mitigation.

5.1 Data flow diagram

A graphical representation of the smart city system architecture is shown using a Data Flow Diagram (DFD), as illustrated in Figure 4. The DFD simplifies the interactions between various subsystems, such as healthcare, smart homes, and vehicular system, enabling a clear understanding of how data flows between sensors, gateways, databases, AI/ML analysis units, cloud storage, and web applications. By modeling these flows, the diagram facilitates the identification of vulnerabilities and threats targeting critical components within each bounded context.

To construct and analyze this DFD, we used the Microsoft Threat Modeling tool (MTM) with Azure Threat Modeling Tool (ATMT) version 1.0.0.33. This STRIDE-based tool automatically identifies potential threats by analyzing defined elements including processes, data flows, external entities, and data stores (Hossain et al., 2023). It supports proactive security planning by proposing mitigations such as reducing, eliminating, or avoiding identified threats, thereby minimizing the potential impact of successful exploitation.

In Figure 4, circles denote processes (e.g., AI/ML analysis, gateways, databases), while rectangles represent data stores (e.g., cloud storage, internal memory). Green rounded rectangles label the direction and nature of the data flows, whether requesting, sending, or receiving data. Red dashed boxes encapsulate logical trust boundaries, including the healthcare domain, vehicle domain, user domain, and smart home domain, each representing a different functional zone of the smart city. This representation enables security analysts to trace how data traverses' different zones, assess risk exposure at each interface, and apply targeted mitigation strategies accordingly.

5.2 Threat identification

Threat identification follows the application of the threat modeling approach, as illustrated in Figure 4. A detailed threat report was generated for each component of the smart city DFD using the STRIDE threat modeling technique provided by the MTM tool. To enrich the analysis and map identified threats to real-world adversarial behaviors, the MITRE ATT&CK framework was also employed, enabling a comprehensive understanding of attacker tactics and techniques relevant to the smart city environment. Each identified

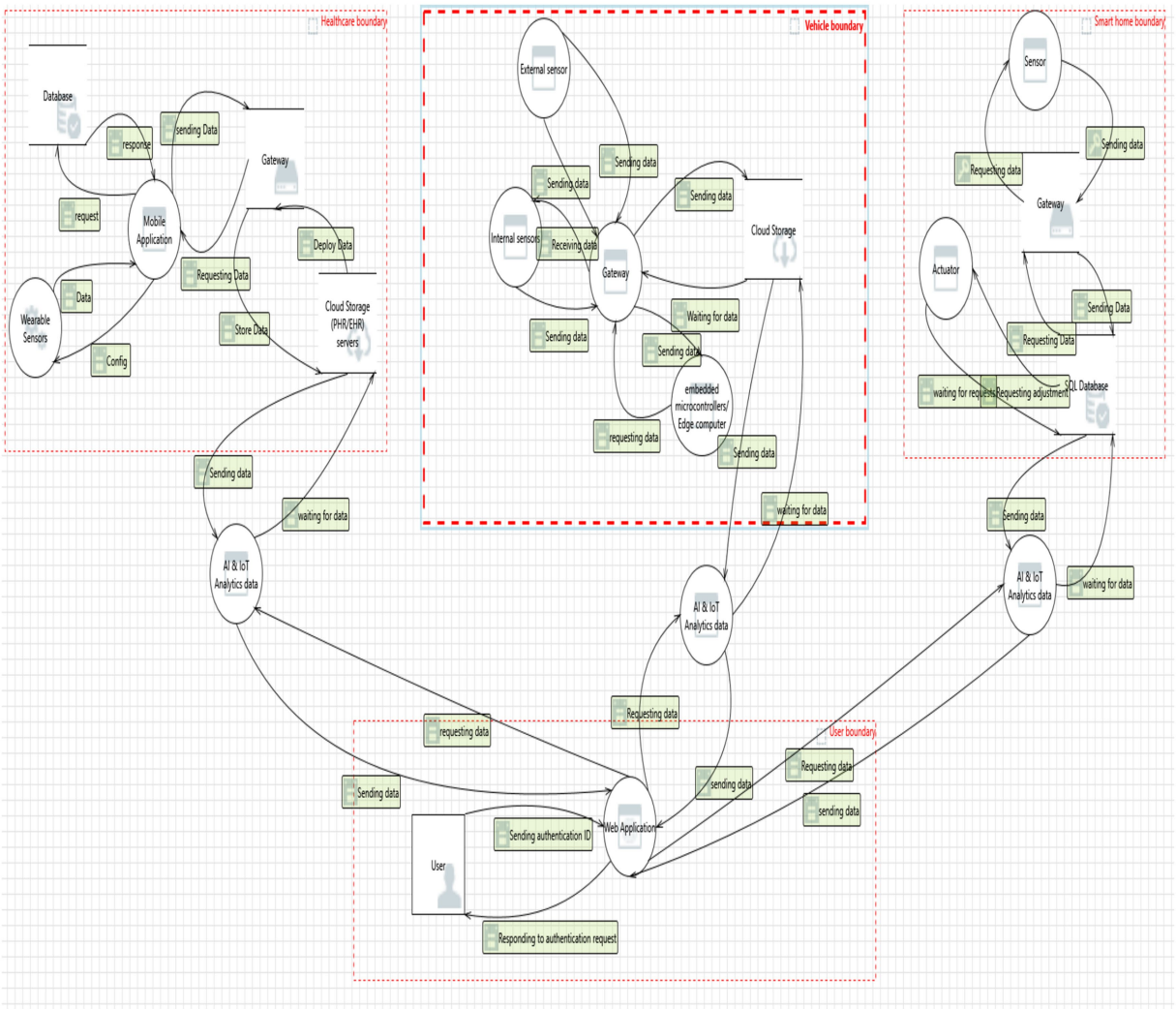

FIGURE 4
Smart city data flow diagram generated using Microsoft threat modeling tool.

threat was systematically documented and presented in sub-section 6.1 of the findings. These risks highlight how various cyber threats can compromise specific smart city assets and services. Furthermore, we described the smart city components impacted by each STRIDE threat and linked them to violations of core security principles such as confidentiality, integrity, and availability. Finally, we analyzed which threats could escalate into active attacks by classifying all discovered risks across different smart city zones, leveraging the combined insights of the STRIDE framework and the MITRE ATT&CK knowledge base.

5.3 Risk assessment

A crucial part of threat modeling in smart cities is risk assessment, which helps city planners, administrators, and cybersecurity teams efficiently prioritize and address potential risks. Threat modeling serves as a structured approach to enhancing the cybersecurity of urban infrastructures by systematically identifying and evaluating hazards. The Common Vulnerability Scoring System (CVSS) and the 5 by 5 risk matrix are two widely adopted techniques for quantifying and visualizing risks (Debnath and Xie, 2022). CVSS offers a standardized framework to assess the severity of vulnerabilities based on factors such as impact, exploitability, and environmental conditions. Meanwhile, the 5 by 5 risk matrix provides a user-friendly tool for decision-making by categorizing risks according to their likelihood and impact (Vaezi et al., 2023). When combined, these approaches enable smart city stakeholders to balance quantitative precision with practical prioritization, ensuring that mitigation efforts are focused on the most critical vulnerabilities. This study demonstrates how CVSS and the 5 by 5 risk matrix can be jointly applied to form a comprehensive risk assessment framework tailored to smart city ecosystems.

5.4 Threat mitigation

Proposing suitable mitigation strategies comes after assessing risks and detecting threats in the smart city environment. Threat mitigation

is the process of reducing or eliminating potential hazards within interconnected urban systems. We examined a number of existing approaches to develop effective mitigation measures tailored to smart city components. Based on this analysis, we selected the most appropriate solutions to protect smart city infrastructure from identified threats, as detailed in Section 6.4.

6 Results and discussion

In this section, we identify threats and conduct risk assessments using the STRIDE approach with MTM tool. As previously stated, STRIDE uses the use case to map and classify identified threats. We used the STRIDE threat modeling approach in our smart city architecture to systematically identify security flaws in domains such as transportation, healthcare and smart home. In addition, we used the MITRE ATT&CK architecture to identify threats and match them to known adversarial tactics and approaches. A detailed risk assessment was conducted for each identified threat, utilizing the CVSS and a 5 by 5 risk matrix to determine the possible impact and likelihood. Furthermore, we proposed a case study concentrating on the internet of vehicles in which the Cyber Kill Chain model was used to trace the stages of a cyberattack on vehicle systems. Based on our results, we proposed targeted mitigation methods to improve the cyber resilience of smart city systems against potential attacks.

6.1 Threats identification

In this part, we discuss all the threats identified by STRIDE tool with respect to each zone of the smart city architecture (Table 2).

The STRIDE-based threat detection identified 21 separate threats across multiple components of the smart city system, indicating critical vulnerabilities in terms of availability, confidentiality, and integrity. DoS was the most common category, particularly affecting gateways, sensors, and AI & IoT analytics, indicating the possibility of system crashes and service disruption. Elevation of privilege attacks targeted cloud storage and analytics components, indicating the possibility of illegal control via code tampering. Information disclosure threats have been detected in web applications and health data storage, raising major privacy concerns. Tampering threats represented the hazards of illegal data modification, whereas spoofing threats revealed vulnerabilities for identity theft and impersonation across users, sensors, and gateways. A single repudiation threat showed the absence of accountability procedures. The results highlight the importance of strong security measures, notably around data flows, analytics modules, and user authentication procedures, in ensuring cyber resilience in smart city infrastructures (Table 3).

The MITRE ATT&CK-based threat identification provides a detailed perspective of the strategies and tactics that attackers may use across the smart city architecture. The investigation found that execution (TA0002) and credential access (TA0006) are the most commonly used strategies, emphasizing the considerable danger of attackers exploiting client-side vulnerabilities and getting unauthorized access via weak or exposed credentials. Threats like exploitation for client execution (T1203) and valid account misuse (T1078) arise repeatedly, showing the systemic danger posed by poor authentication and software vulnerabilities. Impact-related threats (TA0040), such as endpoint and network denial of service (T1499, T1498), demonstrate the ability of attackers to impair vital services like IoT analytics and communication gateways. Data manipulation (T1565) and data collecting techniques (TA0009), such as network sniffing (T1040) and access to code repositories (T1213.003), create concerns regarding data integrity and confidentiality, especially in AI-driven systems. Threats like dynamic linker hijacking (T1574.006) and faked sensor IDs (T0858) reveal vulnerabilities in system control and data falsification. The MITRE ATT&CK mapping demonstrates the complex and multifaceted nature of cyber threats in smart cities, emphasizing the importance of defense-in-depth methods that address not only technological vulnerabilities, but also behavioral patterns and system interconnections.

6.2 Risk assessment

The official CVSS calculator was used to determine the CVSS v3.1 scores, and the MTM was used to determine the input parameters. Expert judgment and pertinent MITRE ATT&CK mappings were used to refine these values, which were based on recognized STRIDE dangers. MTM outputs, pertinent literature on smart city occurrences, and domain-specific insights were combined to estimate the 5×5 risk matrix ratings. This hybrid technique ensures a reliable and repeatable assessment by striking a balance between technical accuracy and practical relevance. In order to preserve resources and assets, lower financial losses, enhance decision-making, and other goals, risk assessment entails evaluating the threats found through threat modeling, quantifying the risks, and implementing mitigation strategies.

6.2.1 CVSS calculator 3.1

The Common Vulnerability Scoring System, which assigns a risk score on a range of 0 to 10 in ascending order based on the severity and effect of the vulnerability, can be used to evaluate the risks associated with the threats and vulnerabilities mentioned above. Table 4 presents how the score is divided according to the severity and the criticality hierarchy of the vulnerability.

Following CVSS v3.1 calculator, the score is calculated by calling up the following parameters in Figure 5 and Table 5.

We can deduce the score and severity of the threats detected in the previous stage.

The CVSS evaluation of 21 identified threats in the smart city architecture indicates a wide range of severity levels, allowing mitigation actions to be prioritized more effectively. T5 and T21 are the most severe dangers, with Critical CVSS values of 9.8. Both involve remote code execution, which enables attackers to execute commands without physical access. In smart cities, attacking T5 might jeopardize cloud services that manage health or traffic data, whereas T21 could give attackers complete control over web-based systems, allowing for data manipulation and broader attacks. These vulnerabilities pose significant real-world dangers, with the potential for cascading failures across city services. Prioritizing their mitigation is critical to maintaining urban resilience and public trust. Several more threats, such as T7, T10, T12, T14, T15, T16, and T19, have High severity scores (7.5–8.8), indicating a considerable danger of unauthorized access, data leakage, and execution flow manipulation in important components like AI analytics and cloud storage. A large number of

TABLE 2 Summary of identified cyber threats in smart city architecture based on STRIDE.

Threat's identification	Threats	STRIDE
T1	Gateways and sensors can be targeted by resource consumption attacks that can be difficult to manage, and it is sometimes a good idea to let the operating system do the work	Denial of Service
T2	Gateway may be spoofed by an attacker and this may lead to incorrect data delivered to Sensor.	Denial of service
T3	Improper data protection of Gateway can allow an attacker to read information not intended for disclosure.	Denial of service
T4	Gateway may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Gateway.	Denial of service
T5	Cloud Storage (PHR/HER) servers may be able to remotely execute code for AI & IoT Analytics data.	Elevation of privilege
T6	An attacker may pass data into AI & IoT Analytics data in order to change the flow of program execution within AI & IoT Analytics data to the attacker's choosing.	Elevation of privilege
T7	AI & IoT Analytics data may be spoofed by an attacker and this may lead to unauthorized access to Cloud Storage (PHR/HER) servers.	Elevation of privilege
T8	AI & IoT Analytics data crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Denial of service
T9	Data flowing across waiting for data may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations.	Information Disclosure
T10	User may be spoofed by an attacker and this may lead to unauthorized access to Web Application.	Information Disclosure
T11	The web server 'Web Application' could be a subject to a cross-site scripting attack.	Information Disclosure
T12	In case AI & IoT Analytics data is given access to memory, such as shared memory or pointers, or is given the ability to control what Web Application executes (for example, passing back a function pointer.), then AI & IoT Analytics data can tamper with Web Application.	Tampering
T13	An attacker may pass data into AI & IoT Analytics data in order to change the flow of program execution within AI & IoT Analytics data to the attacker's choosing.	Tampering, Elevation of Privilege
T14	Unauthorized modification of data stored in storage units	Tampering
T15	Unauthorized access to patient health data.	Information disclosure.
T16	Identity theft to access user accounts.	Spoofing
T17	An attacker could usurp the identity of the sensors to send false data.	Spoofing
T18	In user boundary, a user can deny having sent a request	Repudiation
T19	Leakage of critical data or proprietary algorithms in AI & IoT Analytics.	Information disclosure
T20	An external agent interrupts data flowing across a trust boundary in either direction.	Spoofing
T21	An attacker may pass data into Web Application in order to change the flow of program execution within Web Application to the attacker's choosing.	Spoofing

threats, including T1, T2, T4, T6, T8, T11, T13, T17, and T20, are graded as Medium (5.9–6.3), indicating DoS, spoofing, or privilege escalation efforts with restricted reach. Only one threat, T18, is rated Low (3.7), implying likely repudiation with minimal damage. This CVSS analysis emphasizes the crucial importance of layered security measures, particularly around AI analytics, cloud interfaces, and web applications, in addressing high-impact vulnerabilities across smart city infrastructure.

6.2.2 5 by 5 risk matrix

Prior to undertaking the evaluation, assets should be identified and prioritized using the 5 by 5 Risk Matrix, a helpful tool for risk assessment that combines threat impact and likelihood ranked from low to extreme. The likelihood is the possibility that the risk will materialize, whereas the impact is the severity of the consequences if the risk materialized.

According to the matrix in Figure 6, the risk is color-coded in green, yellow-low, orange, and red, and can be classified as low, medium, high, or extreme using the formula:

$$\text{Risk rating} = \text{Impact}^{*} \text{ Likelihood}$$

Using the 5 by 5 risk matrix below on the threats identified:

Based on the 5 by 5 matrix, a threat assessment was carried out, and summarized in the Table 6.

The 5 by 5 risk matrix assessment of the 21 threats reveals varied levels of urgency and mitigation. Five threats (T5, T12, T15, T20, and T21) are classified as Extreme, indicating the most important vulnerabilities with either a high probability or severe impact, particularly those affecting execution flow, cloud platforms, and AI analytics. Six threats (T4, T6, T7, T13, T16, and T17) are classified as

TABLE 3 Mapping of identified threats to MITRE ATT&CK tactics, techniques, and sub-techniques relevant to smart city systems.

Threat's identification	Threat	Tactic	Technique	Sub-technique
T1	Gateways and sensors can be targeted by resource consumption attacks that can be difficult to manage, and it is sometimes a good idea to let the operating system do the work.	Impact (TA0040)	Endpoint denial of service (T1499)	Resource hijacking (T1499.001)
T2	Gateway may be spoofed by an attacker and this may lead to incorrect data delivered to Sensor.	Credential access (TA0006)	Valid accounts (T1078)	Cloud accounts (T1078.004)
T3	Improper data protection of Gateway can allow an attacker to read information not intended for disclosure.	Credential access (TA0006)	Unsecured credentials (T1552)	Credentials in files (T1552.001)
T4	Gateway may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Gateway.	Collection (TA0009)	Data staged (T1074)	Remote data staging (T1074.002)
T5	Cloud Storage (PHR/HER) servers may be able to remotely execute code for AI & IoT Analytics data.	Execution (TA0002)	Command and scripting interpreter (T1059)	Cloud service (T1059.009)
T6	An attacker may pass data into AI & IoT Analytics data in order to change the flow of program execution within AI & IoT Analytics data to the attacker's choosing.	Execution (TA0002)	Exploitation for client execution (T1203)	—
T7	AI & IoT Analytics data may be spoofed by an attacker and this may lead to unauthorized access to Cloud Storage (PHR/HER) servers.	Initial access (TA0001)	Valid accounts (T1078)	Cloud accounts (T1078.004)
T8	AI & IoT Analytics data crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Impact (TA0040)	Endpoint denial of service (T1499)	Service exhaustion flood (T1499.002)
T9	Data flowing across waiting for data may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations.	Collection (TA0009)	Network sniffing (T1040)	—
T10	User may be spoofed by an attacker and this may lead to unauthorized access to Web Application.	Credential access (TA0006)	Valid accounts (T1078)	Application accounts (T1078.002)
T11	The web server 'Web Application' could be a subject to a cross-site scripting attack.	Execution (TA0002)	Exploitation for client execution (T1203)	—
T12	In case AI & IoT Analytics data is given access to memory, such as shared memory or pointers, or is given the ability to control what Web Application executes (for example, passing back a function pointer.), then AI & IoT Analytics data can tamper with Web Application.	Persistence (TA0003)	Hijack execution flow (T1574)	Dynamic linker hijacking (T1574.006)
T13	An attacker may pass data into AI & IoT Analytics data in order to change the flow of program execution within AI & IoT Analytics data to the attacker's choosing.	Execution (TA0002)	Exploitation for client execution (T1203)	—
T14	Unauthorized modification of data stored in storage units	Impact (TA0040)	Data manipulation (T1565)	Stored data manipulation (T1565.001)
T15	Unauthorized access to patient health data.	Credential access (TA0006)	Unsecured credentials (T1552)	Credentials in files (T1552.001)
T16	Identity theft to access user accounts.	Credential access (TA0006)	Steal application access token (T1528)	—
T17	An attacker could usurp the identity of the sensors to send false data.	Impair process control (TA0119)	Spoof reporting message (T0858)	—

(Continued)

TABLE 3 (Continued)

Threat's identification	Threat	Tactic	Technique	Sub-technique
T18	In user boundary, a user can deny having sent a request	Defense evasion (TA0005)	Indicator removal on host (T1070)	Clear windows event logs (T1070.001)
T19	Leakage of critical data or proprietary algorithms in AI & IoT Analytics.	Collection (TA0009)	Data from information repositories (T1213)	Code repositories (T1213.003)
T20	An external agent interrupts data flowing across a trust boundary in either direction.	Impact (TA0040)	Network denial of service (T1498)	Direct network flood (T1498.001)
T21	An attacker may pass data into Web Application in order to change the flow of program execution within web application to the attacker's choosing.	Execution (TA0002)	Exploitation for client execution (T1203)	—

TABLE 4 Allocation of vulnerability severity scores according to CVSS.

Severity	Score
None	0
Low	0.1 → 3.9
Medium	4.0 → 6.9
High	7.0 → 8.9
Critical	9.0 → 10.0

Very High, owing to the considerable repercussions associated with unauthorized access, spoofing, or flow manipulation, as well as their likelihood of occurrence. Another six threats (T1, T2, T9, T10, T14, and T19) are classified as High, indicating common but significant hazards that require immediate attention, such as data interception and the misuse of valid accounts. Four threats (T3, T8, T11, and T18) are classified as Medium risk, which means they pose a moderate threat but still require monitoring or preventive procedures. None of the dangers are rated Low, implying that all detected threats offer some level of operational or security risk. The matrix verifies that risks to execution integrity, sensitive data, and cloud service availability should be prioritized, particularly when the chance is high or near-certain.

6.3 Case study: security analysis of internet of vehicles

To evaluate the suggested threat modeling approach in a real-world smart city setting, we give a detailed case study of the IoV as an important and developing subsystem in modern urban environments. An attacker attempting to compromise a vehicle in an IoV environment in order to cause an impact by disrupting its route, modifying and altering its route, or spying on its movements (Taslimasa et al., 2023; Kumar et al., 2024). The diagram in Figure 7 illustrates the attack path using Cyber Kill Chain, with the type of threat for each stage of the Kill Chain provided using the STRIDE approach, and the techniques mapped to the MITRE ATT&CK Framework (Table 7) (Zhao, 2024; Fadzil et al., 2023).

This case study describes a complex multi-stage cyberattack on automobiles in a smart city's IoV ecosystem, using the Cyber Kill Chain paradigm. During the reconnaissance phase, the attacker collects intelligence by actively scanning Vehicle-to-Infrastructure (V2I) units, which might lead to information leakage vulnerabilities. The Weaponization step entails the creation of custom malware designed specifically to exploit vehicle embedded systems, highlighting tampering hazards. In the Delivery phase, the attacker utilizes a faked Road Side Unit (RSU) to launch an adversary-in-the-middle attack, injecting malware while imitating a trustworthy V2I node and demonstrating spoofing and credential access techniques. Exploiting firmware vulnerabilities during the Exploitation phase allows the attacker to escalate privileges within the vehicle's telematics computer. In the Installation step, the virus achieves persistence by embedding itself into the vehicle's multimedia system via event-triggered execution, hence sustaining tampering hazards. The Command and Control phase indicates repudiation risk because the compromised car relays location data back to the attacker's server via application layer protocols, allowing for covert control. Finally, during Actions on Objectives, the attacker impairs vehicle operations by exploiting endpoint denial of service, such as GPS jamming or navigation disabling, resulting in substantial operational effect and endangering safety. These phases demonstrate a thorough attack that employs numerous STRIDE threat categories as well as MITRE ATT&CK methods and techniques, demonstrating the importance of layered defenses in IoV smart city infrastructures.

6.4 Threat mitigation techniques

It's time to provide a list of mitigation strategies to lessen the potential harm that could result from one of the threats being exploited after they have been recognized and categorized by zones using the STRIDE approach (Table 8).

The proposed mitigation techniques effectively address the identified risks by focusing on critical security objectives such availability, confidentiality, integrity, authorization, authentication, and non-repudiation. Protocol timeouts, reconnection methods, robust encryption, authentication protocols, and redundant architectures, all contribute to ensuring continuous system operation and preventing service disruption for availability-related concerns (T1, T2, T3, T4, T8). Encrypting data in transit (T9, T16, T19), multifactor authentication (T10), input validation (T11), and tight access controls (T15), all help to protect confidentiality and prevent illegal data exposure. Data validation, memory access limitations (T12), hashing techniques (T14), and regular fuzzing and penetration testing (T13) protect against unwanted data

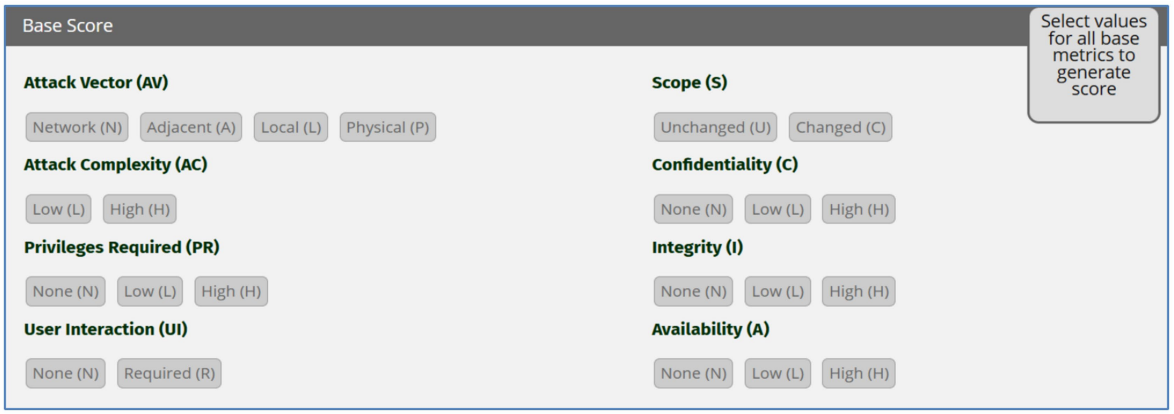

FIGURE 5
Common vulnerability scoring system version 3.1 calculator base score.

TABLE 5 CVSS v3.1 base metrics and severity ratings for identified smart city threats.

Threat	AV	AC	PR	UI	S	C	I	A	Score	Severity
T1	N	H	L	N	U	L	L	H	5.9	Medium
T2	N	L	L	N	U	L	H	L	6.3	Medium
T3	N	L	L	N	U	H	L	L	7.5	High
T4	N	L	L	N	U	L	H	L	6.3	Medium
T5	N	L	H	N	C	H	H	H	9.8	**Critical**
T6	N	L	L	N	U	L	H	L	6.3	Medium
T7	N	L	L	N	C	H	H	L	8.1	High
T8	N	L	L	N	U	L	L	H	6.3	Medium
T9	N	L	L	N	U	H	L	L	7.5	High
T10	N	L	L	N	U	H	H	L	8.1	High
T11	N	L	L	R	U	L	H	L	6.1	Medium
T12	N	L	L	N	C	H	H	L	8.8	High
T13	N	L	L	N	U	L	H	L	6.3	Medium
T14	N	L	L	N	U	H	H	L	8.1	High
T15	N	L	L	N	C	H	L	L	7.7	High
T16	N	L	L	N	U	H	H	L	8.1	High
T17	N	L	L	N	U	L	H	L	6.3	Medium
T18	N	L	L	N	U	L	L	L	3.7	Low
T19	N	L	L	N	C	H	H	L	8.8	High
T20	N	L	L	N	U	L	L	H	6.3	Medium
T21	N	L	L	N	C	H	H	H	9.8	**Critical**

Values in bold indicate threats assessed as critical based on their CVSS score and overall risk level.

tampering, ensuring integrity. System hardening, regular patching (T5), and rigorous data and process validation (T6, T7) all help to prevent authorization threats. Authentication safeguards include digital certificates, cryptographic signatures, mutual authentication with X.509 certificates (T17, T20), and token-based identity validation, such as OAuth2 (T21), which improves identity verification and access control. Finally, non-repudiation is reinforced by using audit logs and Security Information and Event Management (SIEM) solutions (T18), which provide tamper-proof documentation of user actions. While these countermeasures form a robust defense-in-depth strategy tailored to the nature and severity of each threat, it is important to recognize that some solutions such as full SIEM deployment or ubiquitous Transport Layer Security (TLS) encryption may present cost, integration, and scalability challenges, particularly for smaller municipalities or resource-constrained smart city environments. Therefore, a phased and risk-prioritized implementation is recommended to balance security effectiveness with practical feasibility.

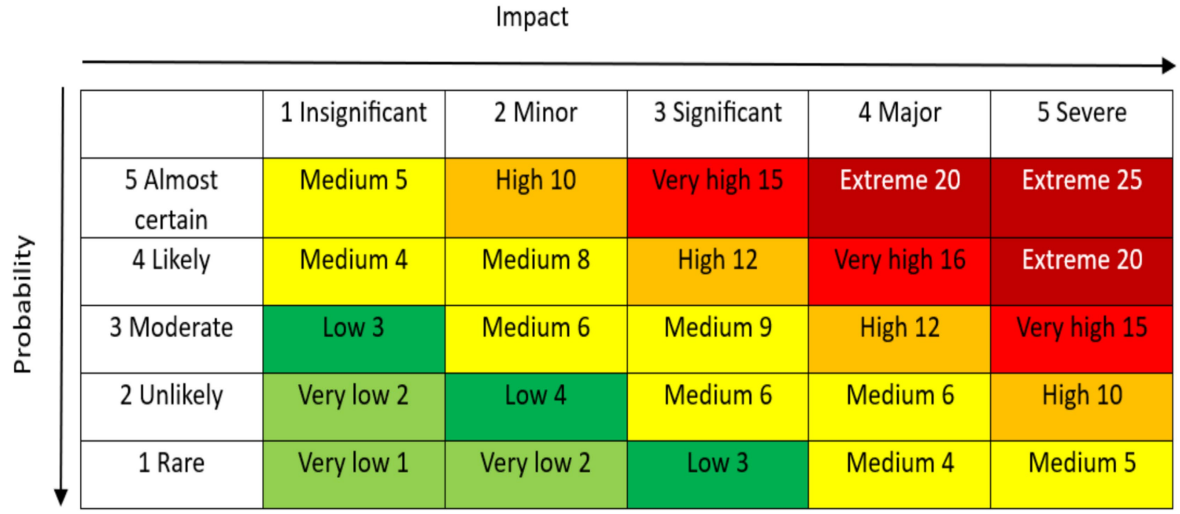

FIGURE 6
5 by 5 risk matrix.

TABLE 6 Risk evaluation of smart city threats using 5 × 5 matrix.

Threat ID	Probability	Impact	Risk rating
T1	4 (medium)	3 (significant)	High (12)
T2	3 (moderate)	4 (major)	High (12)
T3	2 (unlikely)	4 (major)	Medium (6)
T4	3 (moderate)	5 (severe)	Very high (15)
T5	5 (almost certain)	4 (major)	**Extreme (20)**
T6	4 (likely)	4 (major)	Very high (16)
T7	3 (moderate)	5 (severe)	Very high (15)
T8	2 (unlikely)	3 (significant)	Medium (6)
T9	4 (likely)	3 (significant)	High (12)
T10	3 (moderate)	4 (major)	High (12)
T11	3 (moderate)	3 (significant)	Medium (9)
T12	5 (almost certain)	5 (severe)	**Extreme (25)**
T13	4 (likely)	4 (major)	Very high (16)
T14	3 (moderate)	4 (major)	High (12)
T15	4 (likely)	5 (severe)	**Extreme (20)**
T16	3 (moderate)	5 (severe)	Very high (15)
T17	4 (likely)	3 (significant)	High (12)
T18	3 (moderate)	2 (minor)	Medium (6)
T19	2 (unlikely)	5 (severe)	High (10)
T20	5 (almost certain)	4 (major)	**Extreme (20)**
T21	4 (likely)	5 (severe)	**Extreme (20)**

Values in bold indicate threats assessed as critical based on the overall risk level using 5 by 5 matrix.

7 Discussion

This article integrates different cybersecurity frameworks and risk assessment approaches to give a thorough threat analysis of smart city infrastructure. Using the STRIDE model, important threat categories such as spoofing, tampering, denial of service, and elevation of privilege were found across many smart city components, including sensors, gateways, cloud services, and web applications. These threats were then contextualized with the MITRE ATT&CK framework, which linked attacker behaviors to real-world tactics and techniques such as credential theft (T1557), privilege escalation (T1068), and denial of service (T1499).

Spoofing and tampering have emerged as the most common risks, mostly targeting authentication and permission procedures. Spoofing is generally associated with credential access or session hijacking, whereas tampering involves illegal code or data changes that jeopardize system integrity. Furthermore, DoS and information disclosure threats jeopardize system availability and confidentiality, while elevation of privilege assaults enables unauthorized access, frequently serving as predecessors to more sophisticated incursions.

The IoV case study demonstrates how these risks develop throughout the Cyber Kill Chain. The attack lifecycle was reconstructed, starting with reconnaissance (T1595), progressing to weaponization (T1587), delivery via spoofed RSUs (T1557), firmware exploitation (T1068), persistent malware installation (T1546), command and control via application protocols (T1071), and finally service disruption via GPS jamming (T1499). This progression demonstrates how STRIDE threat categories develop at each attack stage, emphasizing the importance of layered, stage-specific responses.

To quantify risk severity, the CVSS was used. Scores ranged from medium to critical, with notably high values recorded for cloud service exploitation and online application tampering, indicating areas of immediate concern. This quantitative analysis was supplemented with a 5 by 5 risk matrix that assessed each threat's likelihood and impact. Several risks, particularly those involving privilege escalation and persistent infection, were classed as "High," "Very High," or "Extreme," requiring immediate mitigation.

The proposed mitigation techniques directly address the identified threats. Robust authentication, encryption, and input validation are advised to combat spoofing and tampering. To reduce DoS concerns, timeout setups, failover systems, and rate limiting are recommended.

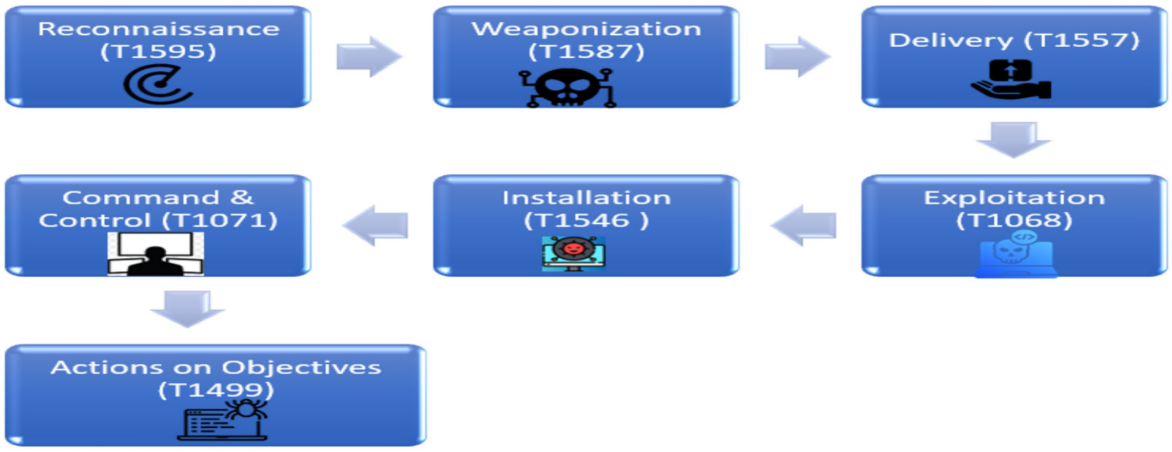

FIGURE 7
Diagram of kill chain stages of compromise for IoV system correlated with MITRE ATT&CK.

TABLE 7 Stage of compromising an IoV system using cyber kill chain, STRIDE and MITRE ATT&CK.

Cyber kill chain stage	Menace STRIDE	MITRE ATT&CK tactics	MITRE ATT&CK technique	Description
1. Reconnaissance	Information disclosure	Reconnaissance	T1595—active scanning	The attacker scans V2I (Vehicle to Infrastructure) units to identify and assess vulnerable vehicles.
2. Weaponization	Tampering	Development	T1587—develop capabilities	Creation of malware targeting the vehicle's embedded operating system.
3. Delivery	Spoofing	Credential access—collection	T1557—adversary-in-the-middle	Injection of malware via a spoofed roadside unit (RSU) posing as a legitimate V2I station
4. Exploitation	Elevation of privilege	Privilege escalation	T1068—exploitation for privilege escalation	Exploitation of a vulnerability in the telematics computer firmware.
5. Installation	Tampering	Persistence–privilege escalation	T1546—event triggered execution	The malware is permanently installed on the embedded multimedia system.
6. Command & Control	Repudiation	Command and control	T1071—application layer protocol	The compromised vehicle sends location data to the attacker's server.
7. Actions on Objectives	Denial of service	Impact	T1499—endpoint denial of service	The attacker tracks the vehicle's location, disables the navigation system or jams the GPS, causing a malfunction.

System hardening, penetration testing, and secure development techniques all help to ensure integrity. Non-repudiation requires secure logging and SIEM integration. These are consistent with the overarching security objectives of confidentiality, integrity, availability, and accountability.

8 Conclusion

This article provided a complete cybersecurity analysis of smart city infrastructure by combining various threat modeling and risk assessment methods. Using STRIDE, MITRE ATT&CK, CVSS scoring, and a 5 by 5 risk matrix, we identified and prioritized important threats to confidentiality, integrity, availability, and authentication across smart city systems. The case study in the IoV domain, which used the Cyber Kill Chain paradigm, shed light on the real-world attack lifecycle, showing vulnerabilities ranging from reconnaissance to denial-of-service that might jeopardize vehicle safety and impair city-wide transportation networks. Our results highlight the complexity and multifaceted nature of smart city cyber threats, underlining the necessity for a defense-in-depth strategy that includes robust authentication, data encryption, system hardening, and continuous monitoring. The combined usage of these frameworks not only improves threat detection and risk prioritization, but it also enables focused and effective mitigation techniques. The proposed framework provides a practical tool for policymakers and smart city planners to prioritize cybersecurity investments, guide risk mitigation strategies, and embed security-by-design principles into urban infrastructure

TABLE 8 Threat mitigation techniques for smart city case study.

Threat's identification	Countermeasure	The protected security objective
T1	Making sur that resource requests do not deadlock, and that they do timeout, by for example configuring protocols such as MQTT, CoAP or HTTP with timeouts and reconnection mechanisms.	Availability
T2	Using a standard authentication mechanism to identify the source data store, such as TLS/DTLS, digital signatures…	Availability
T3	Review authorization settings, and using robust encryption algorithms such as AES-256.	Availability
T4	Using a standard authentication mechanism to identify the destination data store.	Availability
T5	Regular updates and patches and system hardening	Authorization
T6	Strict validation of data at different levels, such as type, format, value range, length… sandboxing, logical flow control, etc.	Authorization
T7	Using a standard authentication mechanism to identify the source process.	Authorization
T8	Implement redundant architectures (clustering) and failover mechanisms, and set up quotas to limit the frequency or volume of data submitted to the system.	Availability
T9	Encrypting the data flow.	Confidentiality
T10	Use of multifactor authentication (MFA), secure cookies and session expiry	Confidentiality
T11	Validation and neutralization of user input by escaping dangerous characters, and encoding of dynamic content	Confidentiality
T12	function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.	Integrity
T13	Performing regular tests fuzzing and penetration.	Integrity, authorization
T14	Use of robust algorithms for data hashing.	Integrity
T15	Access management based on strict policies (IAM)	Confidentiality
T16	Encryption of data in transit with TLS.	Authentication
T17	Digital certificates, cryptographic signatures	Authentication
T18	Audit time-stamped activity logs with non-falsifiable evidence using solutions such as SIEM	Non-repudiation
T19	Using VPN.	Confidentiality
T20	Set up mutual authentication using X.509 certificates, to ensure that both sides of the data flow are legitimate.	Authentication
T21	Use authentication tokens or OAuth2 mechanisms to validate the identity of the communicating entities.	Authentication

planning. Future work will focus on improving the proposed framework by integrating it with operational security tools like SIEM platforms and SCADA systems, which will allow for real-time threat detection and response. We intend to validate the method in a controlled smart city testbed or simulation environment. This direction is consistent with the overall goal of establishing adaptable, resilient, and intelligence-driven cybersecurity methods that are appropriate for the complex and distributed nature of smart city infrastructures.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

MariyaO: Resources, Visualization, Funding acquisition, Data curation, Conceptualization, Writing – original draft. MariyamO: Visualization, Software, Formal analysis, Writing – review & editing, Methodology. ZN: Data curation, Formal analysis, Writing – original draft, Methodology, Resources, Software. SH: Investigation, Validation, Writing – review & editing. YM: Project administration, Supervision, Writing – review & editing, Investigation. AK: Writing – review & editing, Supervision, Validation, Project administration.

Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The authors declare that Gen AI was used in the creation of this manuscript. During the preparation of this work the authors used ChatGPT in order to improve the readability and language of the manuscript. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

Publisher's note

References

Abadía, J. J. P., Walther, C., Osman, A., and Smarsly, K. (2022). A systematic survey of internet of things frameworks for smart city applications. *Sustain. Cities Soc.* 83:103949. doi: 10.1016/j.scs.2022.103949

Al-Ani, K. W., Abdalkafor, A. S., and Nassar, A. M. (2019). Smart city applications: a survey. In Proceedings of the 9th International Conference on Information Systems and Technologies (pp. 1–4)

AlJamal, M., Mughaid, A., Bani-Salameh, H., Alzubi, S., and Abualigah, L. (2024). Optimizing risk mitigation: a simulation-based model for detecting fake IoT clients in smart city environments. *Sustain. Comput.* 43:101019. doi: 10.1016/j.suscom.2024.101019

Al-Sada, B., Sadighian, A., and Oligeri, G. (2023). Analysis and characterization of cyber threats leveraging the MITRE ATT&CK database. *IEEE Access* 12, 1217–1234. doi: 10.1109/ACCESS.2023.3344680

Al-Sada, B., Sadighian, A., and Oligeri, G. (2024). Mitre att&ck: state of the art and way forward. *ACM Comput. Surv.* 57, 1–37. doi: 10.1145/3687300

Anwar, M. N., Nazir, M., and Ansari, A. M. (2020). Modeling security threats for smart cities: a stride-based approach. In Smart Cities—Opportunities and Challenges: Select Proceedings of ICSC 2019 (387–396). Springer Singapore.

Bastos, D., Costa, N., Rocha, N. P., Fernández-Caballero, A., and Pereira, A. (2024). A comprehensive survey on the societal aspects of smart cities. *Appl. Sci.* 14:7823. doi: 10.3390/app14177823

Bhardwaj, V., Anooja, A., Vermani, L. S., Sunita, and Dhaliwal, B. K. (2024). Smart cities and the IoT: an in-depth analysis of global research trends and future directions. *Discov. Internet Things* 4:19. doi: 10.1007/s43926-024-00076-3

Chen, Z., Gan, W., Wu, J., Lin, H., and Chen, C. M. (2024). Metaverse for smart cities: a survey. *Int. Things Cyber-Phys. Syst.* 4, 203–216. doi: 10.1016/j.iotcps.2023.12.002

Das, P., Asif, M. R. A., Jahan, S., Ahmed, K., Bui, F. M., and Khondoker, R. (2024). Stride-based cybersecurity threat modeling, risk assessment and treatment of an in-vehicle infotainment system. *Vehicles* 6, 1140–1163. doi: 10.3390/vehicles6030054

Debnath, J. K., and Xie, D. (2022). CVSS-based vulnerability and risk assessment for high performance computing networks. In 2022 IEEE International Systems Conference (SysCon) (pp. 1–8). IEEE.

Fadzil, L. M., Manickam, S., and Al-Shareeda, M. A. (2023). A review of an emerging cyber kill chain threat model. In 2023 Second International Conference on Advanced Computer Applications (ACA) (pp. 157–161). IEEE.

Hossain, I., Chowdhury, N. I., and Hasan, R. (2023). How secure is AI-based coding?: a security analysis using STRIDE and data flow diagrams. In 2023 IEEE Virtual Conference on Communications (VCC) (pp. 56–61). IEEE.

Ismagilova, E., Hughes, L., Rana, N. P., and Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: literature review and development of a smart city interaction framework. *Inf. Syst. Front.* 24, 393–414. doi: 10.1007/s10796-020-10044-1

Koban, C., Falaleyeva, M., Spravtseva, M., Moiseev, R., and Khan, S. (2022). Modeling user-centric threats in Smart City: a hybrid threat modeling method. In 2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA) (pp. 1–7). IEEE.

Kumar, R., Gill, R., Singh, A., Kumar, R., Singh, D., and Al-Farouni, M. (2024). A comprehensive analysis of internet of vehicle security vulnerabilities in smart cities. In 2024 International Conference on Data Science and Network Security (ICDSNS) (pp. 1–6). IEEE.

Laufs, J., Borrion, H., and Bradford, B. (2020). Security and the smart city: a systematic review. *Sustain. Cities Soc.* 55:102023. doi: 10.1016/j.scs.2020.102023

Mahlous, A. R. (2023). Threat model and risk management for a smart home IoT system. *Informatica* 47, 51–63. doi: 10.31449/inf.v47i1.4526

Mothanna, Y., ElMedany, W., Hammad, M., Ksantini, R., and Sharif, M. S. (2024). Adopting security practices in software development process: security testing framework for sustainable smart cities. *Comput. Secur.* 144:103985. doi: 10.1016/j.cose.2024.103985

Naik, N., Jenkins, P., Grace, P., Naik, D., Prajapat, S., and Song, J. (2024). A comparative analysis of threat modelling methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. In The international conference on computing, communication, cybersecurity & AI (pp. 271–280). Springer Nature Switzerland, Cham. (2024, July)

Okai, E., Feng, X., and Sant, P. (2018). Smart cities survey. In 2018 IEEE 20th international conference on high performance computing and communications; IEEE 16th international conference on smart city; IEEE 4th international conference on data science and systems (HPCC/SmartCity/DSS) (1726–1730). IEEE.

Ouaissa, M., and Ouaissa, M. (2025). Analyzing and mitigating attacks in IoT smart home using a threat modeling approach-based STRIDE. *Int. J. Interact. Mob. Technol.* 19, 126–142. doi: 10.3991/ijim.v19i02.52377

Poleto, T., Nepomuceno, T. C. C., De Carvalho, V. D. H., Friaes, L. C. B. D. O., De Oliveira, R. C. P., and Figueiredo, C. J. J. (2023). Information security applications in smart cities: a bibliometric analysis of emerging research. *Future Internet* 15:393. doi: 10.3390/fi15120393

Rasoulzadeh Aghdam, S., Bababei Morad, B., Ghasemzadeh, B., Irani, M., and Huovila, A. (2025). Social smart city research: interconnections between participatory governance, data privacy, artificial intelligence and ethical sustainable development. *Front. Sustain. Cities* 6:1514040. doi: 10.3389/frsc.2024.1514040

Razavi, H., Titidezh, O., Asgary, A., and Bonakdari, H. (2024). "Building resilient smart cities: the role of digital twins and generative AI in disaster management strategy" in Digital twin computing for urban intelligence (Singapore: Springer Nature Singapore), 95–118.

Sánchez-Corcuera, R., Nuñez-Marcos, A., Sesma-Solance, J., Bilbao-Jayo, A., Mulero, R., Zulaika, U., et al. (2019). Smart cities survey: technologies, application domains and challenges for the cities of the future. *Int. J. Distrib. Sens. Networks* 15:1550147719853984. doi: 10.1177/1550147719853984

Singh, T., Solanki, A., Sharma, S. K., Nayyar, A., and Paul, A. (2022). A decade review on smart cities: paradigms, challenges and opportunities. *IEEE Access* 10, 68319–68364. doi: 10.1109/ACCESS.2022.3184710

Taslimasa, H., Dadkhah, S., Neto, E. C. P., Xiong, P., Ray, S., and Ghorbani, A. A. (2023). Security issues in internet of vehicles (IoV): a comprehensive survey. *Internet of Things* 22:100809. doi: 10.1016/j.iot.2023.100809

Toh, C. K. (2020). Security for smart cities. *IET Smart Cities* 2, 95–104. doi: 10.1049/iet-smc.2020.0001

Tok, Y. C., and Chattopadhyay, S. (2023). Identifying threats, cybercrime and digital forensic opportunities in smart city infrastructure via threat modeling. *Forensic Sci. Int. Digit. Investig.* 45:301540. doi: 10.1016/j.fsidi.2023.301540

Vaezi, A., Jones, S., and Asgary, A. (2023). Integrating resilience into risk matrices: a practical approach to risk assessment with empirical analysis. *J. Risk Anal. Crisis Response* 13, 252–272. doi: 10.54560/jracr.v13i4.411

Wang, P., Ali, A., and Kelly, W. (2015). Data security and threat modeling for smart city infrastructure. In 2015 international conference on cyber security of smart cities, industrial control system and communications (SSIC) (1–6). IEEE.

Xiong, W., and Lagerström, R. (2019). Threat modeling–a systematic literature review. *Comput. Secur.* 84, 53–69. doi: 10.1016/j.cose.2019.03.010

Zahid, S., Mazhar, M. S., Abbas, S. G., Hanif, Z., Hina, S., and Shah, G. A. (2023). Threat modeling in smart firefighting systems: aligning MITRE ATT&CK matrix and NIST security controls. *Int. Things* 22:100766. doi: 10.1016/j.iot.2023.100766

Zhao, L. (2024). Navigating the cyber kill chain: a modern approach to pentesting. *Appl. Comput. Eng.* 38, 170–175. doi: 10.54254/2755-2721/38/20230549