Analysis of vulnerability databases for wireless networks in the Internet of Things for threat modelling

Nurdaulet Karabayev[1], Yerik Mardenov[2*] , Tamara Zhukabayeva[3], Dina Satybaldina[4], Altynbek Seitenov[5]

[1, 2, 3, 4] Faculty of Information Technology, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

[2,5] Astana IT University, Astana, Kazakhstan

020419501012@enu.kz, emardenov@gmail.com, tamara.kokenovna@gmail.com, satybaldina_dzh@enu.kz, altynbek.seitenov@astanait.edu.kz

*Corresponding author: emardenov@gmail.com

ABSTRACT

The development of technologies such as digitalisation, the Internet of Things (IoT), cloud computing, big data, and communication networks has led to the emergence of "smart" cities. The number of IoT devices connected to urban infrastructure is steadily increasing, increasing exposure to potential cyberattacks. Therefore, analysing vulnerabilities in IoT devices used in smart city infrastructure remains a key research challenge. This study compares three widely used vulnerability sources for IoT systems-CVE, NVD, and ICS Advisories-using criteria such as data structure, machine readability, product identification, and risk metrics. The advantages and limitations of existing databases are identified in terms of their applicability for threat modelling. We propose a structured integration approach that combines CVE, NVD, and ICS Advisories into a unified dataset. In addition, a generalised schema for describing vulnerabilities of IoT devices is developed, taking into account their type and application context. The results enable the construction of a unified vulnerability dataset suitable for threat modelling and risk assessment in smart city environments.

Keywords: *IoT security, CVE database, NVD database, ICS Advisories, vulnerability analysis, threat modelling in IoT systems*

1. Introduction

The development of technologies such as digitalisation, the Internet of Things (IoT), cloud computing, big data, data analytics, and communication networks has led to the emergence of "smart" cities. Within a smart city, data from sensors and IoT devices are collected and analysed to support decision-making and infrastructure management. Although there are currently not many fully or partially "smart" cities [1], their number is increasing every year.
Along with these advantages, the increasing number of connected devices also creates new security challenges [2,3,4]. In practice, vulnerabilities in IoT devices are actively exploited in real-world attacks, such as the Mirai botnet, highlighting the need for their systematic analysis and consideration in threat modelling [5,6]. Decision-making in smart cities depends on reliable data. For this reason, it is important to analyse vulnerabilities in IoT devices. It is also necessary to detect abnormal device behaviour and consider it in threat modelling. Risk assessment and the implementation of protective measures by enhancing the functionality of nodes responsible for data analysis, decision-making, and infrastructure management within the smart city. In this work, vulnerability databases are compared to evaluate their applicability for threat modelling. In [7], a preliminary analysis of databases in the field of information security was conducted, including databases of attacks, vulnerabilities, weaknesses, exploits, and incidents; however, the analysis of data sources was limited to only one source. Unlike

Proceedings of ICICCS-2026 (Poster Papers), DMPedia Lecture Notes in Computer Science & Engineering.
ISBN: 978-81-993813-1-5

previous studies, this work examines several vulnerability databases together rather than focusing on a single source. The findings are applied to improve vulnerability analysis and support threat modelling processes.

The scientific novelty of this work lies in the development of an approach to the comparative analysis of data sources for Internet of Things devices, accounting for their applicability to threat modelling in smart city infrastructure. Unlike existing studies that are limited to analysing individual databases [9] or to analysing databases from the perspective of all vulnerabilities rather than specifically those related to wireless IoT networks [8], this work proposes a systematic comparison of various vulnerability sources, enabling consideration of the specific characteristics of the IoT ecosystem. As a result of the study, the following outcomes were identified: a comparative analysis of IoT vulnerability databases was conducted; evaluation criteria for their use in threat modelling were proposed; limitations of existing solutions were identified; and the applicability of these databases for risk analysis in smart cities was assessed. The paper is organised as follows. Section 2 presents the structure of wireless networks for the Internet of Things and formulates the problem statement. Section 3 reviews data sources for connected devices. Section 4 provides a comparative analysis of these databases and examines their applicability for threat modelling and risk assessment in smart cities.

2. Problem Statement

The infrastructure of a smart city can be represented as a tuple that includes a set of devices (D) (sensors, IoT nodes, actuators), network connections (C) (Wi-Fi, 5G, LPWAN, Ethernet, Zigbee), access points (AP), gateways and edge computing nodes (G) (gateway, hub, edge device, base station), data processing platforms (P) (cloud, data processing and storage platform, device management platform), application services (S) (transport, energy, healthcare), and users (U):

$$SC = \{D, C, AP, G, P, S, U\} \quad (1)$$

Previously, in studies [7,10], the authors defined wireless sensor networks based on a set of client and end devices (D), base stations (BS), access points (AP), and network connections (C):

$$WSN=\{D, C, AP, BS\} \quad (2)$$

Thus, WSN is a part of IoT and, in turn, a part of SC: WSN $\subset$ IoT $\subset$ SC. In this model, wireless sensor networks collect and transmit data and serve as the foundation of the Internet of Things, integrated into a broader architecture for managing urban infrastructure.

Vulnerabilities may arise in any component of SC. In [7], the authors introduced vulnerabilities into the WSN model as follows (using client devices as an example): (UD) represents client devices interacting through network connections, (UD = \sum_{i=1}^{n} ud_i), where (n) is the number of client devices, and (ud_i = {SW, WM, HW}), where (SW) is client software, (WM) is middleware, and (HW) is hardware, including NIC. Each of these sets is characterised by a name, criticality (crit), and vulnerabilities (Vuln).

The problem is to formalise the most comprehensive available source of vulnerabilities that enables the identification of vulnerabilities in SC components based on available information about them (name, version), for subsequent threat modelling and risk analysis.

Here, completeness of a data source refers not only to the availability of vulnerability information but also to the ability to establish relationships between vulnerabilities, devices, their versions, and operating conditions, which is necessary for building threat models and conducting risk assessment in distributed IoT systems.

3. Vulnerability databases of Internet of Things devices.

The NVD (National Vulnerability Database). In [7], the NVD vulnerability database was considered. It contains information about vulnerabilities as well as details on the products in which they were identified. Table 1 presents the fields used to describe vulnerabilities in the NVD, as defined by the JSON schema.

Table 1: Fields used to describe a vulnerability in the NVD

Metadata		**Descriptions**	
id	*CVE identifier*	*descriptions*	*Descriptions*
sourceIdentifier	Source of vulnerability information		
published	Publication date		
lastModified	Timestamp of last modifications		
vulnStatus	Status		
Vulnerability type (weakness)		**Vulnerable configurations**	
weaknesses	List of weaknesses	*configurations*	Vulnerable configurations
weaknesses.source	Source of the weakness	*nodes*	Nodes (products included in the configuration)
weaknesses.type	Type of weakness	*operator*	AND/OR
weaknesses. description	Description	*negate*	Negation operator
		cpeMatch	Associated CPE entry
References		**Metrics**	
references	External references	*cvssMetricV2*	CVSS version 2 metrics
references.url	*URL*	*cvssMetricV30*	CVSS version 3.0 metrics
references.source	Reference source	*cvssMetricV31*	CVSS version 3.1 metrics
references.tags	Tag (patch, exploit)	*cvssMetricV40*	CVSS version 4.0 metrics
CISA KEV fields		**Additional fields**	
cisaExploitAdd	Date added to KEV	*vendorComments*	Vendor comments
cisaActionDue	Remediation due date	*evaluatorComment*	NVD analyst comments
cisaRequiredAction	Required remediation actions		
cisaVulnerabilityName	KEV name		

Product information can be used to identify vulnerabilities related to Internet of Things devices. It should be noted that associated CPE entries (cpeMatch) are described by the following fields: vulnerable (true or false), criteria (CPE 2.3 string), matchCriteriaId (internal identifier), versionStartIncluding (the version in which the vulnerability first appeared), versionStartExcluding (the last version in which the vulnerability is not yet present), versionEndIncluding (the version in which the vulnerability is no longer present), and versionEndExcluding (the last version in which the vulnerability is still present). However, this does not allow for direct identification of the product type, i.e., distinguishing products related to the Internet of Things. Therefore, when using NVD data, it is necessary to analyse the field containing the product's CPE entry (cpeMatch). For example, the following types of products related to IoT can be identified: IP cameras, smart thermostats, gateways, routers, and smart home control hubs. Thus, when analysing the product's CPE entry (cpeMatch), the following list of keywords can be used: camera, router, gateway, sensor, thermostat, doorbell, NVR, DVR, smart, IoT. An example of a CPE entry (cpeMatch) containing the keyword "camera" is: cpe:2.3:h:hikvision:ds-2cd2142fwd_camera When working with NVD, queries can also be performed via the NVD API, which allows searching by keywords using the keywordSearch parameter. In this case, the list of keywords mentioned above can be applied. An example query for the keyword "camera" is:

https://services.nvd.nist.gov/rest/json/cves/2.0?keywordSearch=camera

The MITRE CVE (Common Vulnerabilities and Exposures) database. Similar to NVD, CVE contains information about vulnerabilities and the products in which they were identified. Table 2 presents the fields used to describe vulnerabilities in CVE, as defined by the JSON schema. Information from this database is used within NVD.

Table 2: Fields used to describe a vulnerability in CVE

Metadata		**Descriptions**	
cveMetadata.cveId	CVE identifier	containers.cna.descriptions[].value	Descriptions
cveMetadata.assignerShortName	CNA (organisation that assigned the identifier)	containers.cna.descriptions[].lang	Description language
cveMetadata.datePublished	Publication date		
cveMetadata.dateUpdated	Last updated date		
cveMetadata.state	Status		
Affected products		**Vulnerability type (weakness)**	
containers.cna.affected[].vendor	Vendor	containers.cna.problemTypes[].descriptions[].description	Vulnerability type
containers.cna.affected[].product	Product	containers.cna.problemTypes[].descriptions[].type	Classification type

containers.cna.affected[].versions[]	Versions		
containers.cna.affected[].modules	Component		
Metrics		**Impact**	
containers.cna.metrics[].cvssV3.baseScore	CVSS version 3.0 score	containers.cna.impacts[].descriptions[].value	Impact
containers.cna.metrics[].cvssV3.baseSeverity	Severity		
containers.cna.metrics[].cvssV3.vectorString	CVSS vector		
References		**Vulnerable configurations**	
containers.cna.references[].url	References	containers.cna.configurations[]	Vulnerable configurations
containers.cna.references[].tags	Type	containers.cna.cpeApplicability[]	CPE entry
Mitigation and exploitation		**Additional fields**	
containers.cna.solutions[]	Solutions	containers.cna.timeline[]	Change history
containers.cna.workarounds[]	Workarounds	containers.cna.credits[]	Researcher
containers.cna.exploits[]	Exploit availability	containers. cna.tags[]	Tags

As with NVD, product information in CVEs can be used to identify vulnerabilities in Internet of Things devices. The field containers.cna.affected.product contains an unstructured description of the product, while the field containers. cna.cpeApplicability provides a formalised representation of vulnerable products based on the CPE standard, enabling automated analysis and vulnerability correlation. However, this does not allow direct identification of the product type, i.e., distinguishing products related to the Internet of Things.

When working with CVE data, it is usually required to additionally analyse both the fields containing the product's CPE entry (containers.cna.cpeApplicability) and the unstructured product description (containers.cna.affected product). As with NVD, the following list of keywords can be used: camera, router, gateway, sensor, thermostat, doorbell, NVR, DVR, smart, IoT, or the approach proposed in [11]. The disadvantages compared to NVD include the lack of a convenient keyword search via API and the need to analyse two fields. An advantage over NVD is the presence of a field containing an unstructured product description (containers.cna.affected .product), which enables identifying IoT devices even when no relevant keyword is present in the CPE entry. For example, the CPE entry (containers.cna.cpeApplicability) "cpe:2.3:h:hikvision:ds-2cd2142fwd: does not contain any of the specified keywords, whereas the unstructured product description (containers.cna.affected.product "IP Camera" includes the keyword "Camera."

The ICS Advisories vulnerability database. This database is maintained by the Cybersecurity & Infrastructure Security Agency (CISA) in the USA. It contains official reports on vulnerabilities and threats related to industrial control systems (a subset of IoT vulnerabilities, specifically those of the Industrial Internet of Things). Each report provides an extended description of vulnerabilities (often based on CVE), tailored to industrial systems and including context, risk assessment, and mitigation recommendations. Table 3 presents the report fields used to describe vulnerabilities, defined based on the information available in the database.

Table 3: Fields used to describe a vulnerability/threat in ICS Advisories

Metadata		**Affected products**	
advisoryId	Report identifier	*vendor*	Vendor
title	Title	*product*	Product
publishedDate	Publication date	*affectedVersions*	Versions
updatedDate	Last updated date	*sector*	Sector
Vulnerability description		**Metrics**	
summary	Summary	*cvssScore*	CVSS score
technicalDetails	Technical description	*severity*	Severity level
cveList	List of CVE identifiers	*attackVector*	Attack vector
cwe	Vulnerability type (CWE)	*attackRequirements*	Attack conditions
		privilegesRequired	Required privileges
		userInteraction	User interaction
		impact	Impact
		impactType	Impact type
Mitigation measures		**Additional fields**	
mitigations	Remediation	*references*	References
patchAvailable	Patch availability	*researcherCredits*	Researcher
workarounds	Workarounds	*exploitStatus*	Exploit availability

ICS Advisories are semi-structured reports. Information from ICS Advisories can be used to identify vulnerabilities related to Industrial Internet of Things (IIoT) devices. For this purpose, the product field, which contains an unstructured product description, and the cveList field, which contains a list of CVE identifiers, can be utilised.An advantage, similar to CVE, is the presence of a field containing an unstructured product description (product), which allows IoT devices to be identified using keywords. For more accurate product identification, its version (the affectedVersions field) can also be considered. It should be noted that the list of keywords for the Industrial Internet of Things differs from that of the general Internet of Things.

It is proposed to use a controlled vocabulary of keywords that includes terms related to industrial controllers (control_devices), SCADA systems (scada_systems), network infrastructure (network_infrastructure), sensors (sensors), actuators (actuators), embedded systems (embedded_systems), and industrial protocols (industrial_protocols), taking into account their application context in control and automation systems:

IIoT_keywords = control_devices ∪ scada_systems ∪ network_infrastructure ∪ sensors ∪ actuators ∪ embedded_systems ∪ industrial_protocols,

where:

control_devices = {plc, controller, industrial controller, logic controller, rtu, remote terminal unit, dcs, distributed control system},

scada_systems = {scada, hmi, human machine interface, control system, monitoring system, supervisory system},

network_infrastructure = {industrial router, industrial switch, gateway, edge gateway, IoT gateway, industrial firewall, modem, access point, network device},

sensors = {sensor, industrial sensor, smart sensor, transmitter, meter, smart meter, data logger, measurement device},

actuators = {actuator, valve controller, motor controller, drive, inverter, relay},

embedded_systems = {firmware, embedded system, embedded device, real-time operating system, rtos},

industrial_protocols = {modbus, opc, ua, dnp3, profinet, ethernet/ip, bacnet, can bus, industrial protocol}.

For example, the unstructured product description in the ICS Advisory “Schneider Electric Modicon Controllers M241, M251, M258, and LMC058” contains the keyword “controller,” and the cveList field for this advisory includes the following CVE identifier: CVE-2025-13902.

The advantages of ICS Advisories include access to attack scenarios, remediation measures, and industry-specific context. The disadvantages include the fact that, unlike CVE and NVD, the ICS Advisories database is not provided as a standardised, machine-readable dataset, requiring the use of third-party projects or parsing methods for further analysis.Shodan IoT Exposure Data.

Although this is not a classical IoT vulnerability database, it is worth mentioning. This platform allows searching for vulnerable and misconfigured devices. Thus, when building cyberattack models, it can be used to identify potential entry points for attacks.

4. Comparative analysis of IoT vulnerability databases

The following criteria are used to compare the databases discussed in the previous section.

From the perspective of structure and formalization: the presence of a data schema and machine readability; from the perspective of completeness of vulnerability description: availability of descriptions and level of detail; from the perspective of affected products: product formalization and accuracy of version specification; from the perspective of metrics and risk assessment: availability of CVSS scoring and detailed attack parameters; from the perspective of vulnerability context: availability of information about the operating environment and linkage to infrastructure; from the perspective of recommendations: availability of information on remediation measures, patches, and workarounds; and from the perspective of suitability for automated analysis: database structure and applicability for threat modeling and machine learning. Based on the conducted analysis, the following advantages of CVE as a vulnerability database for wireless IoT networks in smart cities can be identified: (1) CVE is a global identification standard, (2) the presence of a unified identifier (CVE-ID), (3) broad coverage of vulnerabilities, and (4) integration with other systems. NVD builds on CVE data by including additional structured fields such as CPE identifiers and CVSS scores, which simplifies automated processing: (1) high level of structuring, (2) availability of CPE (accurate product identification), (3) availability of CVSS scoring (risk assessment), (4) suitability for automation, and (5) support for analytics.ICS Advisories describe vulnerabilities, often including possible attack scenarios and recommended mitigation measures. CVE mainly provides vulnerability identification, while NVD adds structured technical details. In contrast, ICS Advisories include more context and practical information about real-world systems.

The results of the comparison of the databases discussed in the previous section based on the selected criteria are presented in Table 4.

Table 4: Fields used to describe a vulnerability/threat in ICS Advisories

Criterion	**Criterion**	**CVE**	**NVD**	**ICS Advisories**
Structure	Structure	+ (Strict, JSON 5.0)	+ (Strict, JSON API)	- (Semi-structured)
Machine readability	Machine readability	+	+	- (Limited)
Description	Description	+ (Concise)	+ (Extended)	+ (Detailed)
Products	Products	- (Text)	+ (CPE)	+ (Explicit, but formalised)
Versions	Versions	+- (Partially)	+ (Strictly)	+
Standardization	Standardization	-	+ (High)	-
CWE	CWE	+- (Partially)	+	+
CVSS	CVSS	+- (Optional)	+	+ (Often)
Application context	Application context	-	-	+
Recommendations	Recommendations	-	-	+
Exploitation	Exploitation	- (Rarely)	+- (Partially)	+ (Sometimes)
Automation	Automation	+- (Moderate)	+ (High)	- (Low)

At the same time, several limitations of the databases under consideration can be identified. The limitations of CVE include: (1) lack of context, (2) limited level of detail, (3) absence of recommendations, and (4) unstructured product data. The limitations of NVD include: (1) lack of operational context, (2) absence of mitigation recommendations, (3) difficulty in identifying IoT devices, and (4) possible delays in data updates. The limitations of ICS Advisories include: (1) lack of a formalised structure, (2) limited machine readability, (3) focus on IoT (not the entire IoT domain), (4) incomplete coverage of vulnerabilities, and (5) difficulty in automated analysis.

Overall, CVE serves as a global reference system for identifying vulnerabilities, but it does not provide sufficient contextual information; NVD complements CVE with structured data, including risk metrics and formalised descriptions of affected systems, making it suitable for automated analysis; and ICS Advisories provide application context and mitigation recommendations but are characterised by a low degree of formalisation. Therefore, no single database is complete on its own, and comprehensive vulnerability analysis, especially in smart city infrastructure, requires the combined use of these sources.

This section may be organised using subheadings or combined as a unified Results and Discussion section, which is often appropriate depending on the nature of the research. The focus should be on interpreting the significance of the findings, rather than simply restating the results. Instead of conducting a broad literature review here, it's more effective to reference recent, relevant studies to draw comparisons, highlighting how the current work stands out in light of ongoing developments and challenges within the field.

5. Applicability of databases for risk analysis in smart cities

The analysis showed that none of the considered databases is complete on its own. For comprehensive vulnerability analysis, especially in urban systems, the combined use of these sources is required. The integration of vulnerability data has already been discussed in previous studies; however, this work focuses on IoT-specific scenarios [12].

This study proposes integrating vulnerabilities into a unified database specifically for wireless IoT networks.

The following method for building a unified vulnerability database for wireless IoT networks in a smart city is proposed, based on CVE, NVD, and ICS Advisories, and taking into account the recommendations of the IoT Security Foundation [13]: (1) data extraction, (2) normalisation, (3) linking, (4) enrichment, and (5) storage.

1. At the first stage, data are collected from CVE, NVD, and ICS Advisories for further processing.

2. Next, records are linked using the CVE identifier as the primary integration key, as well as additional fields such as vendor, product, and CPE.

3. After linking, the data are transformed into a unified structure to ensure consistency across sources.

4. The dataset is then extended by adding additional attributes such as device type and deployment context. For this purpose, it is proposed to use the recommendations of the IoT Security Foundation [13]. The following set of fields is proposed for describing vulnerabilities in the integrated database: advisoryId, vendor, product, productType, affectedVersions, description, cveId, cwe, severity, cvssScore, attackVector, impact, mitigation, and references.

5. Storage. It is proposed to use a graph database.It should be noted that the proposed method for integrating vulnerability databases can be extended by incorporating additional information sources, such as data on the actual locations of devices in the network (e.g., results of Internet-wide scanning) and information on misconfigurations and zero-day vulnerabilities.

This would improve the completeness of the threat model by considering not only known vulnerabilities but also potential attack entry points determined by the deployment characteristics of devices within smart city infrastructure. Using a graph database also enables the construction of interconnected threat models that capture relationships among vulnerabilities, devices, and attack scenarios.

Let us consider an example of merging records from the CVE, NVD, and ICS Advisories databases for the vulnerability CVE-2025-13902.

1. Data extraction. Table 5 presents data for the vulnerability CVE-2025-13902 extracted from CVE, NVD, and ICS Advisory.

TABLE 5 : DATA ON CVE-2025-13902 EXTRACTED FROM CVE, NVD, AND ICS ADVISORY

Information from CVE	Information from NVD	Information from ICS Advisory
{ "cveId": "CVE-2025-13902", "product": "Modicon Controller", "vendor": "Schneider Electric", "description": "Improper input validation vulnerability", "cvssScore": 8.8 }	{ "id": "CVE-2025-13902", "cpeMatch": "cpe:2.3:h:schneider:modicon_ m241:*:*:*:*:*:*:*:*", "cvssMetricV31": { "baseScore": 8.8, "vectorString": "AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H" }, "cwe": "CWE-20" }	{ "advisoryId": "ICSA-25-XXX", "vendor": "Schneider Electric", "product": "Modicon Controllers M241, M251", "cveList": ["CVE-2025-13902"], "summary": "Vulnerability in industrial controller", "impact": "Remote code execution", "mitigations": "Apply firmware update" }

2. Linking:
   Using the key = CVE-2025-13902, records from all sources are merged.

3. Normalisation:
   vendor: Schneider Electric
   product: Modicon Controller
   description: merged descriptions
   CVSS: from NVD (priority)
4. Enrichment:
   Adding IoT/IoT context:
   device_type: controller
   iot_flag: true
   domain: industrial

Final integrated record:

{
"cveId": "CVE-2025-13902",
"advisoryId": "ICSA-25-XXX",
"vendor": "Schneider Electric",

"product": "Modicon Controller",
"productType": "industrial_controller",
"affectedVersions": "M241, M251",
"description": "Improper input validation vulnerability in industrial controller",
"cwe": "CWE-20",
"cvssScore": 8.8,
"attackVector": "Network",
"impact": "Remote code execution",
"mitigation": "Apply firmware update",
"references": [
"CVE",
"NVD",
"ICS Advisory"
],
"iot_flag": true,
"deployment_context": "industrial_control_system"
}

The given example demonstrates that integrating data from CVE, NVD, and ICS Advisories enables a more comprehensive representation of a vulnerability by combining identification, formalised characteristics, and application context. This significantly enhances the applicability of the resulting database for threat modelling and risk analysis in smart-city infrastructure.

6. Conclusions

This work compares vulnerability databases used in IoT systems and analyses their suitability for threat modelling tasks. It is shown that each of the considered databases has both significant advantages and notable limitations. The CVE database provides universal vulnerability identification and broad coverage, but is characterised by limited depth of information and a lack of context. The NVD database complements CVE with structured data, including risk metrics and formalised descriptions of affected systems, making it suitable for automated analysis; however, it does not account for operational context or mitigation recommendations. In turn, ICS Advisories provide extended descriptions of vulnerabilities, including attack scenarios, industry context, and mitigation measures, but are low on formalisation and machine readability.

The results indicate that none of the analysed databases can be used independently to conduct a complete vulnerability assessment. This limitation is caused by the distributed architecture of IoT systems, device heterogeneity, and the lack of unified classification [6].

To overcome this limitation, a combined use of multiple data sources is proposed. Particular attention is given to the enrichment stage, where it is proposed to account for the device type and its application context using the recommendations of the IoT Security Foundation. This enhances the applicability of the vulnerability database for threat modelling and risk analysis.

The proposed approach can be used to build unified vulnerability datasets for smart city cybersecurity applications. Future research directions include the development of methods for automatic classification of IoT devices, the development and expansion of an ontological model of vulnerabilities, and the creation of tools for building threat models and conducting risk assessments based on the integrated database.

Acknowledgements

Grant No.BR24992852 "Intelligent models and methods of Smart City digital ecosystem for sustainable development and the citizens' quality of life improvement”

Conflict of Interest

The authors declare no conflict of interest.

References

[1] International Institute for Management Development, "IMD Smart City Index Report 2025," [Online]. Available: https://imd.widen.net/s/psdrsvpbk7/imd_smart_city_2025_report. Accessed: Mar. 24, 2026.

[2] V. Demertzi, S. Demertzis, and K. Demertzis, "An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities," Appl. Sci., vol. 13, no. 2, Art. no. 790, 2023, doi: 10.3390/app13020790.

[3] M. Houichi, F. Jaïdi, and A. Bouhoula, "Cyber security within smart cities: A comprehensive study and a novel intrusion detection-based approach," Comput. Mater. Continua, vol. 81, pp. 393–441, 2024, doi: 10.32604/cmc. 2024.054007.

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

[5] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017, doi: 10.1109/MC.2017.201.

[6] M. Antonakakis et al., "Understanding the Mirai Botnet," in Proc. 26th USENIX Security Symp. (USENIX Security '17), Vancouver, BC, Canada, 2017, pp. 1093–1110.

[7] T. Zhukabayeva, Y. Mardenov, N. Karabayev, D. Satybaldina, and D. Yedilkhan, "Vulnerability analysis and threat modeling in wireless networks of smart city infrastructure," Procedia Comput. Sci., vol. 272, pp. 588–593, 2025, doi: 10.1016/j.procs.2025.10.252.

[8] M. Rytel, A. Felkner, and M. Janiszewski, "Towards a safer Internet of Things: A survey of IoT vulnerability data sources," Sensors, vol. 20, no. 21, Art. no. 5969, 2020, doi: 10.3390/s20215969.

[9] X. Li, S. Moreschini, Z. Zhang, F. Palomba, and D. Taibi, "The anatomy of a vulnerability database: A systematic mapping study," J. Syst. Softw., vol. 201, Art. no. 111679, 2023, doi: 10.1016/j.jss.2023.111679.

[10] T. Zhukabayeva, V. Desnitsky, and A. Abdildayeva, "Wireless sensor network modeling and analysis for attack detection," Comput. Model. Eng. Sci., vol. 144, no. 2, Art. no. 2591, 2025.

[11] G. J. Blinowski and P. Piotrowski, "CVE Based Classification of Vulnerable IoT Systems," in Theory and Applications of Dependable Computer Systems, W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, and J. Kacprzyk, Eds. Cham, Switzerland: Springer, 2020, pp. 99–109, doi: 10.1007/978-3-030-48256-5_9.

[12] G. Bhandari, A. Naseer, and L. Moonen, "CVEfixes: Automated collection of vulnerabilities and their fixes from open-source software," in Proc. 17th Int. Conf. Predictive Models and Data Analytics in Software Engineering (PROMISE '21), New York, NY, USA: ACM, 2021, pp. 30–39, doi: 10.1145/3475960.3475985.

[13] IoT Security Foundation, "IoT Security Assurance Framework," [Online]. Available: https://af.iotsf.org. Accessed: Mar. 24, 2026.