UDC 004.42 https://doi.org/10.32515/2664-262X.2025.12(43).1.20-30

Yuriy Pidlisnyi
Chernihiv Polytechnic National University, Chernihiv, Ukraine
e-mail: ypodlesny@ukr.net

Intelligent-Contextual Model for the Classification of Internet of Things Environments

This paper presents an intelligent-contextual model for classifying Internet of Things (IoT) environments, based on the comprehensive consideration of key parameters such as the level of embedded intelligence, operational context, security level, and system dynamics. The relevance of the study stems from the rapid growth in the complexity of IoT ecosystems, which are characterized by heterogeneous devices, diverse operating conditions, the need for adaptability to environmental changes, and increased security requirements. A critical analysis of existing IoT classification approaches reveals their major limitations: a narrow focus on purely technical or functional features, inadequate reflection of device behavior and intelligence, and the disregard for operational context and threat landscape.

The developed model addresses these shortcomings and enables more accurate structuring of IoT environments by taking into account their intended purpose, architectural characteristics, and ability to autonomously make decisions. It can be applied for system analysis, risk formalization, optimization of threat response mechanisms, and the design of effective cybersecurity strategies and adaptive control in dynamic environments. The proposed classification makes it possible to generalize existing IoT system types and lays the groundwork for developing new, more flexible and secure architectures. The practical significance of the results lies in their applicability across industries where intelligent data processing, contextual awareness, and resilience to cyberthreats are essential - including Industry 4.0, eHealth, intelligent transport systems, and smart cities.

Internet of Things, IoT classification, intelligent systems, security, usage context, system dynamics, adaptation, cybersecurity, intelligent-contextual model

Problem Statement. The rapid development of Internet of Things (IoT) technologies has led to the formation of an extremely diverse environment of devices, protocols, and usage scenarios. Current classification approaches, which are mostly based on the functional or technological grouping of IoT devices, often fail to consider their complexity, operating context, or potential threat levels. This complicates the development of effective management, monitoring, and cybersecurity systems in dynamic networks.

The aim of this study is to develop a new classification model for IoT environments that is based not only on functional characteristics but also incorporates the level of embedded intelligence, the degree of security, the architecture of interaction, and the application context of devices. This approach creates a foundation for the development of flexible methods for analyzing and securing dynamic IoT environments.

Analysis of Recent Studies and Publications. Despite the considerable number of studies in the field of the Internet of Things (IoT), existing classification approaches often remain limited to traditional technical frameworks. To justify the need for a new classification model, this section reviews key modern scientific works focused on intelligence, security, architecture, and the functional context of IoT.

One of the fundamental studies highlighting the influence of intelligent technologies on IoT development is [1], which provides a broad analysis of artificial intelligence methods used across various IoT subsystems. It emphasizes the importance of integrating machine learning, neural networks, and data processing into modern IoT architectures. IoT security issues are addressed in [2], where the authors stress the need to consider threat levels and operational context when designing secure systems - particularly for critical infrastructure.

Regarding IoT architecture, [3] analyzes centralized and decentralized approaches in the medical domain, illustrating the significance of architectural choices based on application context. The relevance of dynamics and device mobility is highlighted in [4], which identifies mobility, scalability, and adaptability as key characteristics of modern IoT systems.

The conducted literature review confirms the necessity of a new classification approach that reflects the multidimensional features and challenges of contemporary IoT environments.

Research Objective. To develop a new classification model for IoT environments that goes beyond functional and technical parameters and takes into account adaptivity, security requirements, interaction architecture, and usage context. This model is intended to provide a holistic systemic view for making managerial and cybersecurity decisions in dynamic IoT networks.

Main Content. To achieve the goal of developing an intelligent-contextual classification model for Internet of Things (IoT) environments, the following research tasks were formulated and consistently implemented throughout the main body of the article:

1. Analyze current approaches to IoT system classification and identify their limitations under modern challenges.
2. Define relevant classification criteria, including intelligence level, security level, interaction architecture, operating context, and system dynamics.
3. Develop a conceptual model of intelligent-contextual classification based on the defined criteria.
4. Construct a classification block diagram that formalizes the model structure and demonstrates its applicability.
5. Evaluate the effectiveness of the proposed model compared to traditional approaches, focusing on adaptivity, security, and practical value.

Task 1: Analysis of current classification approaches and identification of their limitations.

The current IoT environment is characterized by extreme diversity in devices, architectural solutions, and application scenarios. Traditional classification methods typically focus on device types, industry-specific applications, or communication protocols [5–6]. However, such approaches fail to consider the increasing importance of device intelligence, security levels, usage context, and behavioral dynamics.

Thus, existing classification models are found to be fragmented and insufficiently adaptive, confirming the need for a new classification framework.

Task 2: Identification of relevant classification criteria.

Given the shortcomings of traditional classification methods, there is a need to establish new criteria that can adequately describe the complexity, flexibility, and risks inherent to modern IoT systems. Based on the literature analysis [5–6] and typical operation scenarios, five relevant classification criteria have been identified:

a) *Level of embedded intelligence* – the device's ability to process information autonomously, learn, or make decisions;

b) *Security level* – the presence of authentication mechanisms, encryption, anomaly detection;

c) *Interaction architecture* – centralized, decentralized, or hybrid system structure;

d) *Operational context* – the application domain (industry, household, healthcare, transport, etc.) that defines risks and reliability requirements;

e) *System dynamics* – the ability to modify topology, routing, or functionality in real time.

Task 3: Development of a conceptual intelligent-contextual classification model.

Based on the defined criteria, a conceptual model of intelligent-contextual classification for IoT environments was developed. Its core idea is to combine technical (intelligence, architecture, security) and contextual (application domain, system dynamics) characteristics to provide a more accurate representation of device behavior and roles within IoT systems.

The model functions as a multidimensional classification system where each IoT device or subsystem is positioned according to five coordinates aligned with the classification criteria. For practical use, the model is formalized as the following function (1):

$$C: D \rightarrow I \times S \times A \times C_x \times D_\gamma \qquad (1)$$

where:

C - classification function;

D - the set of IoT devices or subsystems;

I - level of embedded intelligence (0 – none, 1 – basic, 2 – high);

S - security level (low, medium, high);

A - interaction architecture (centralized, decentralized, hybrid);

C_x - operational context (home, industrial, transport, medical, etc.);

D_γ - system dynamics (static, mobile, swarm/dynamic).

Task 4: *Construction of the classification block diagram.*

To facilitate the implementation of the proposed model in decision support systems, a block diagram of IoT classification was developed (Figure 1). It formalizes the logic of classification based on the five previously defined dimensions.

At the top level, the diagram presents the general concept of an "IoT system," which is further divided into five classification dimensions. Each dimension includes examples of characteristics related to the corresponding criterion:

a) *Intelligence level* – from local data analysis to machine learning and autonomous adaptation;

b) *Security level* – authentication, encryption, resistance to cyberattacks;

c) *Interaction architecture* – centralized, decentralized, hybrid;

d) *Operational context* – urban, industrial, medical environments, etc.;

e) *Dynamics* – adaptive topology, reconfiguration, scalability.

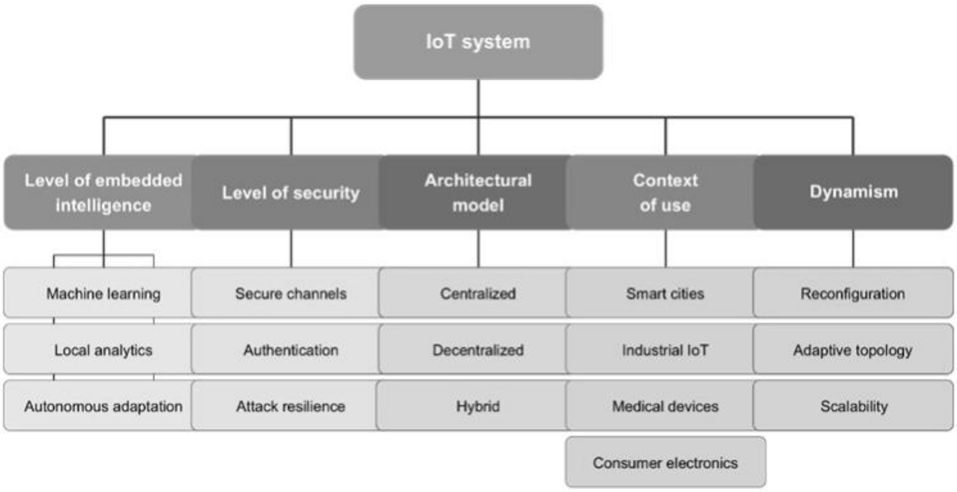

Figure 1 - Block diagram of the intelligent-contextual classification model of the Internet of Things

Source: Developed by the author

Detailed consideration of each criterion and their role in building the new classification model:

1. **Level of embedded intelligence in IoT systems:**

With the growing adoption of edge AI (artificial intelligence operating directly on the device) and federated learning (distributed training of models on multiple devices without transmitting data to a central server), IoT devices increasingly gain the capability to independently process data, make decisions, and even learn in real time [7]. This significantly reduces data processing latency, lowers network load, and enhances device autonomy. Classifying IoT systems by their level of embedded intelligence allows the identification of:

a) *Passive systems: collect and transmit data without local processing;*

b) *Analytical systems: local data processing and basic decision-making;*

c) *Adaptive systems: self-learning and functional optimization based on experience.*

2. **Security level of IoT systems**:

Information security remains a major challenge in IoT development. Depending on the level of protection, systems can be classified as:

a) *Open systems:* minimal authentication and encryption mechanisms;

b) *Basic secure systems:* use of standard security protocols such as TLS/SSL;

c) *Highly secure systems: implementation of advanced protection mechanisms, including anomaly monitoring and security neuroagents.*

The presence or absence of secure communication channels, as well as authentication and authorization policies, directly affects the system's resistance to attacks [8].

3. **Architectural Structure of IoT Systems:**

The architecture of an IoT system determines how data is processed and how devices interact. Based on this, systems can be divided into:

a) *Centralized:* data is sent to a single processing center (cloud);

b) Decentralized: data is processed locally or via peer-to-peer interaction;

c) *Hybrid:* combines local processing with centralized analysis.

This classification helps to better understand the various organizational approaches in IoT systems, which can be tailored to specific application requirements. The importance of architecture in defining protection methods and ensuring system stability has also been emphasized in studies [9], which note that the choice between centralized and decentralized systems depends on the network characteristics and data processing needs.

4. **Operational Context of IoT Systems:**

Understanding the context in which a system operates is critical for selecting the right security strategy and optimization methods. Systems can operate in various environments:

a) *Critical infrastructure* (e.g., energy, transportation);

b) Smart cities (e.g., smart homes, streets, parking systems*)*;

c) Home IoT (e.g., smart speakers, thermostats);

d) *Wearable devices* (e.g., health monitoring sensors).

The operational context is a vital component of the intelligent-contextual classification model, as it defines system-specific requirements based on function and environment. As noted in [10], for critical infrastructures such as energy or transport, it is essential to implement IoT systems that ensure high reliability and security, since failures can lead to serious social and economic consequences. The intelligent-contextual classification model allows the identification of different operational contexts to enhance adaptability and security, considering characteristics like intelligence level, security needs, and complexity of integration with other technologies.

5. **Dynamics of IoT Systems:**

Dynamics reflect the system's ability to change its structure or functioning in response to environmental changes:

a) *Static systems:* fixed sensor networks;

b) *Mobile systems:* devices that move through space;

c) *Swarm-based IoT:* collective behavior of numerous autonomous devices.

When building an intelligent-contextual classification model of IoT systems, it is important to consider not only the functional and technological aspects but also the system's ability to adapt to environmental changes, which is crucial for understanding its dynamics and security.

As noted in [11], dynamics is one of the key characteristics of modern IoT networks, which include static, mobile, and swarm-based devices capable of adapting to changing conditions. Accordingly, a well-structured classification must consider these capabilities and the various types of system adaptation to enhance effectiveness and threat resilience.

Practical Application of the Intelligent-Contextual Classification Model for IoT. The intelligent-contextual classification model for the Internet of Things is not merely a theoretical concept — it opens up broad possibilities for practical implementation across a range of applied tasks related to the management, monitoring, and security of IoT systems. Thanks to its multidimensional approach, the proposed classification model forms a methodological foundation for building intelligent risk analysis systems, adaptive security, efficient resource management, and dynamic network configuration.

Here are several key areas of its application:

1. **Intelligent Adaptation of Security Policies:** Classification of devices based on intelligence level, security, architectural characteristics, and usage context enables the creation of adaptive security policies. Instead of universal solutions for the entire system, policies can be automatically adjusted according to the type of device and its operating environment. This increases the effectiveness of protection and optimizes the use of computational resources [12].

2. **Dynamic Resource and Topology Management:** Taking into account the intelligence level and context of devices allows for dynamic changes in network topology, data routing, and distribution of computing resources in real time. This is especially important for mobile and heterogeneous IoT environments where network conditions are constantly changing [13].

3. **Context-Aware Logging and Auditing:** Intelligent-contextual classification enables the optimization of monitoring and auditing processes by collecting only the information most relevant to a given device type and its environment. This improves attack detection accuracy and reduces the load on data processing systems [14].

4. **Enhanced Monitoring Efficiency:** Classification based on threat level and environmental dynamics allows monitoring systems to focus on the most at-risk areas of the network while reducing monitoring costs in low-risk segments. This ensures more effective anomaly and cyberattack detection, even under limited resources [15].

The intelligent-contextual classification model in IoT opens new prospects for solving practical challenges in system management, monitoring, and security. Due to its ability to adapt to changing conditions and computational capabilities, this approach enables more effective network management, optimizing resource usage and enhancing threat detection accuracy. In particular, the implementation of adaptive security policies, dynamic resource and topology management, as well as improved logging and auditing, becomes critically important for reducing system load and increasing overall security.

Figure 2 illustrates the block diagram of the practical application of the intelligent-contextual classification model for IoT.

Practical significance of the proposed model. The practical significance of the developed intelligent-contextual classification model lies in its wide applicability across real-world IoT systems. Specifically, the model enables:

1. Structured system-level analysis of IoT environments based on risk levels, embedded intelligence, architecture, and dynamics;

2. The development of adaptive, context-aware cybersecurity policies tailored to device types and operational scenarios;

3. Improved efficiency in monitoring and resource allocation through dynamic network reconfiguration and intelligent prioritization of risk zones;

Application in critical domains such as smart cities, Industry 4.0, eHealth, intelligent transport systems, and wearable personal monitoring, where resilience, security, and adaptability are essential.

Task 5: Evaluation of the effectiveness of the proposed model in comparison with traditional approaches, with a focus on adaptivity, security, and practical value.

Traditional approaches to the classification of Internet of Things (IoT) devices are typically based on fixed technical or functional parameters: sensor type, data transmission protocol, energy consumption, or system role. While such classification models can be useful during the design phase and initial deployment, they exhibit significant limitations in dynamic, heterogeneous, and context-dependent IoT environments.

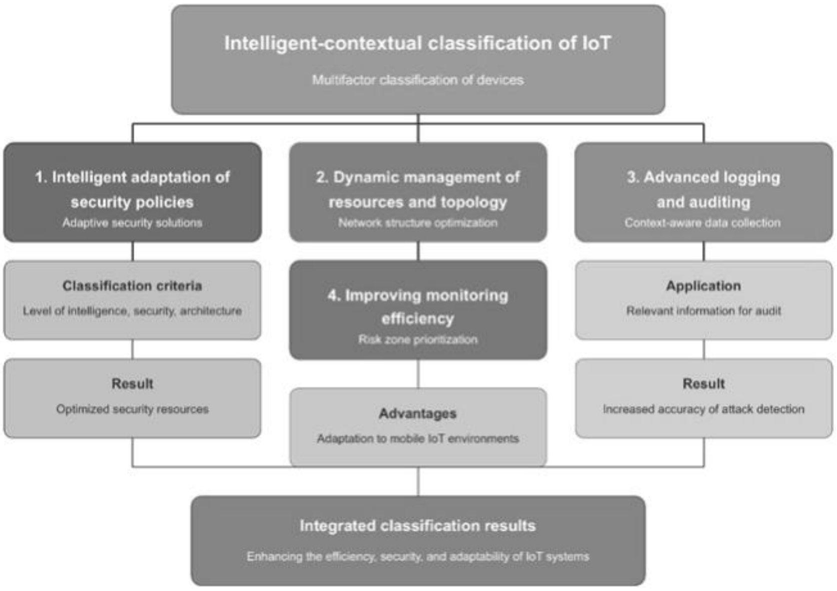
Intelligent-contextual classification of IoT
Multifactor classification of devices
1. Intelligent adaptation of security policies
Adaptive security solutions
2. Dynamic management of resources and topology
Network structure optimization
3. Advanced logging and auditing
Context-aware data collection
Classification criteria
Level of intelligence, security, architecture
4. Improving monitoring efficiency
Risk zone prioritization
Application
Relevant information for audit
Result
Optimized security resources
Advantages
Adaptation to mobile IoT environments
Result
Increased accuracy of attack detection
Integrated classification results
Enhancing the efficiency, security, and adaptability of IoT systems

Figure 2- Block Diagram of the Practical Application of the Intelligent-Contextual Classification Model for the Internet of Things

Source: Developed by the author

Table 1 presents a comparison of the proposed intelligent-contextual classification model with traditional approaches to device classification and management in IoT. This comparison highlights a number of advantages that provide greater efficiency, flexibility, and adaptability of the proposed model under modern IoT operating conditions.

Adaptability to changing environmental conditions: Traditional approaches often apply fixed policies and templates for managing devices within a network, which leads to inefficiencies in dynamic and mobile IoT systems. In contrast, the intelligent-contextual classification model considers device context and changing states, allowing the network to adapt in real time to new conditions. This reduces resource consumption and improves overall system performance.

1. **Intelligent adaptation of security policies:** Traditional approaches often apply unified security policies to all devices, which proves ineffective in highly heterogeneous IoT environments. In contrast, the proposed intelligent-contextual classification model enables the adaptation of security policies to the specific characteristics of each device, including its intelligence level, type of data processing, and current level of protection. This approach provides a significantly higher level of security by allowing the dynamic adjustment of protective mechanisms based on the device's operating context, thereby greatly reducing the risk of cyberattacks.

2. **Optimization of resource usage**: Traditional approaches generally rely on static methods of resource management, which can lead to overload in certain network segments

and inefficient use of computational capacities. The proposed intelligent-contextual classification model enables dynamic resource management, data routing, and network topology configuration based on the current state of devices and their environment. This substantially increases the overall system efficiency, particularly in mobile and heterogeneous IoT environments where operational conditions frequently change.

3. **Reduced load on monitoring and auditing systems**: By collecting only the data most relevant to a specific device and its context, the proposed classification model helps reduce the volume of information processed by monitoring and auditing systems. This not only lowers the load on computational resources but also improves the accuracy of anomaly and cyberattack detection.

Table 1 - Comparison of the Intelligent-Contextual Classification Model with traditional approaches

Criterion	*Traditional Classification*	*Intelligent-Contextual Classification (Proposed)*
Classification Parameters	Technical (device type, interface, energy consumption)	Intelligence, security level, environmental dynamics, usage context, role in the network
Adaptability	Low – does not account for environmental changes or device behavior	High – devices can change categories depending on context or threats
Security Application	Limited – uniform policies for all devices of the same type	Adaptive – security policies change based on risk level and device context
Monitoring Use	Uniform – all devices are monitored at the same level	Risk-oriented – monitoring is prioritized based on context and threat level
Support for Dynamic Management	Minimal – fixed classification, no support for flexible role reassignment	Full – dynamic changes in topology, routing, and resources based on contextual shifts
Flexibility in Scalable Systems	Limited – increasing number of devices complicates management	High – intelligent rules enable automated control of large-scale networks

Source: Developed by the author

Thus, the intelligent-contextual classification model enables more effective management of IoT systems by enhancing their security and adaptability to changing operating conditions. This makes it significantly more advantageous compared to traditional methods that do not consider such dynamic interaction with the context and the intelligence level of devices.

Challenges and Limitations of the Intelligent-Contextual Classification Model in IoT. Despite its numerous advantages, the implementation of an intelligent-contextual classification model for devices in the Internet of Things (IoT) is accompanied by several challenges and limitations that must be addressed to ensure its effective application.

1. **Heterogeneity of Devices and Limited Resources**: the IoT environment consists of a large number of devices with varying computational power, energy consumption, and supported protocols. This creates difficulties in implementing a unified classification model. Devices with limited resources may not support complex machine learning or context processing algorithms. In a systematic review [16], researchers identified 14 major challenges related to heterogeneity in IoT, including the diversity of protocols, data formats, and computational limitations of devices. These factors complicate the integration and scalability of IoT systems.

2. **Context Dynamism and Real-Time Adaptation**: device context may change dynamically, requiring systems capable of real-time adaptation. However, ensuring such

adaptability requires the development of efficient mechanisms for collecting, analyzing, and updating contextual information, which can be a complex task in environments with limited resources and high network dynamism. Study [17] emphasizes the importance of edge computing as a means to enable real-time adaptability in dynamic environments. The research also highlights the significance of context-aware management, where decisions are made based on environmental changes, workload, and device types.

3. **Lack of Standards and Limited Interoperability:** current IoT systems suffer from a lack of unified standards for representing and exchanging contextual information. This complicates integration across platforms and devices from different manufacturers. In [18], the authors emphasize the insufficient standardization in data transmission and interpretation between devices, which significantly hinders achieving full interoperability among IoT components. The study also stresses that the development of unified standards is critically important for building scalable, secure, and adaptive IoT infrastructures.

4. **Security and Privacy Issues of Contextual Data**:processing contextual information, particularly personalized data, poses privacy risks for users. In the event of a data breach or misuse, serious security threats may arise. Article [19] discusses attacks such as data recovery, model poisoning, and leakage through federated learning.

5. **Data Quality and Anomaly Handling**: inaccuracy, incompleteness, or obsolescence of contextual data can significantly impact classification accuracy. Additionally, processes for detecting and filtering anomalies require complex logic that must be both adaptive and resource-efficient [20].

Despite the vast potential of the intelligent-contextual classification model, its large-scale implementation requires overcoming a number of technical, standardization, and ethical challenges. Future research should focus on developing energy-efficient adaptive algorithms for implementing the model, establishing industry-wide standards for IoT system classification, and ensuring the privacy and protection of personalized data in dynamic and heterogeneous IoT environments.

Conclusions. The research has implemented a full cycle of developing a novel classification model for Internet of Things (IoT) environments, addressing the challenges of modern technological systems-specifically, dynamic behavior, contextual sensitivity, heterogeneity, and high security demands. In line with the stated goal, the study successfully solved **five research tasks:**

1. Modern approaches to IoT classification were analyzed, and their limitations in the context of increasing system complexity and environmental dynamics were identified.

2. Five key classification criteria were defined: level of device intelligence, security level, interaction architecture, operational context, and system dynamism.

3. A conceptual intelligent-contextual classification model was developed, integrating technical and behavioral characteristics of IoT systems.

4. A block diagram was constructed to formalize the model's logic and enable integration into applied management, monitoring, and security systems.

5. A comparative analysis with traditional approaches was conducted, demonstrating the model’s advantages in terms of adaptivity, scalability, management efficiency, and context-aware security policy implementation.

Scientific novelty of the obtained results lies in the following:

1. An intelligent-contextual classification model for IoT environments is proposed, which considers not only technical device parameters but also their intelligence level, architectural structure, application context, and system dynamism.

2. For the first time, the classification is formalized as a multidimensional function with five coordinates, enabling a unified description of complex and heterogeneous IoT networks.

3. A structural block diagram of the model is developed, allowing integration into decision support systems, monitoring tools, and adaptive control mechanisms.

4. A comprehensive comparison with traditional classification models was performed, substantiating the superiority of the proposed model in terms of adaptivity, security, and scalability.

Practical significance of the results is as follows:

1. The model can be applied for the structuring, analysis, and design of IoT environments, taking into account risk levels, dynamics, and operational context.
2. It enables the development of adaptive cybersecurity policies—security mechanisms can be automatically configured based on the device type, behavior, and application environment.
3. Resource management efficiency is improved—dynamic classification facilitates real-time optimization of routing, load balancing, and data processing.
4. The model is applicable across domains such as Smart Cities, Industrial IoT (Industry 4.0), medical sensor systems, transport, and personal wearable devices.

The intelligent-contextual classification of IoT environments opens wide prospects for further research and applied developments. In particular, future directions may include the integration of machine learning methods to enable real-time automatic classification of devices. This would support the creation of self-learning systems capable of continuously updating their security policies, routing strategies, and resource management in response to changes in device behavior and external conditions. Additionally, the model can be expanded through the use of fuzzy logic, ontological methods, or agent-based architectures, contributing to the development of autonomous, context-aware, and threat-resilient IoT systems.

List of References

1. Dixit P., Bhattacharya P., Tanwar S., Gupta R. Role of Artificial Intelligence in Internet of Things Systems: A Systematic Mapping Study. *Sensors*. 2024. Vol. 24, № 20. Article 6511. URL: https://www.mdpi.com/1424-8220/24/20/6511 (дата звернення: 28.04.2025).
2. Thibaud M., Chi H., Zhou W., Piramuthu S. Internet of Things (IoT) in high-risk environment, health and safety (EHS) industries: A comprehensive review. *Decision Support Systems*. 2018. Vol. 108. P. 79–95. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167923618300344?via%3Dihub (дата звернення: 28.04.2025).
3. Islam S. R., Kwak D., Kabir M. H., Hossain M., Kwak K. S. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*. 2015. Vol. 3. P. 678–708. URL: https://ieeexplore.ieee.org/document/7113786 (дата звернення: 28.04.2025).
4. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*. 2015. Vol. 17, № 4. P. 2347–2376. URL: https://ieeexplore.ieee.org/document/7123563 (дата звернення: 28.04.2025).
5. Dubey H., Sahoo P. K., Chahal P., Saini H. IoT Ecosystem — A survey on Classification of IoT. *EAI Endorsed Transactions on Internet of Things*. 2020. Vol. 6, № 21. Article e4. URL: https://eudl.eu/doi/10.4108/eai.16-5-2020.2304170 (дата звернення: 28.04.2025).
6. Gupta M., Abdelsalam M., Khorsandroo S., Mittal S. A Review on Internet of Things: Communication Protocols, Wireless Technologies, and Applications. In: *Internet of Things and Cyber Physical Systems*. Springer, 2022. P. 353–370. URL: https://link.springer.com/chapter/10.1007/978-981-19-2004-2_23 (дата звернення: 28.04.2025).
7. Hou Z., Ding Y., Jiao Y., Hu L., Wu D. O. A Survey of Recent Advances in Edge-Computing-Powered Artificial Intelligence of Things. *IEEE Internet of Things Journal*. 2021. Vol. 8, № 22. P. 16309–16328. URL: https://www.researchgate.net/publication/352386275_A_Survey_of_Recent_Advances_in_Edge-Computing-Powered_Artificial_Intelligence_of_Things (дата звернення: 28.04.2025).
8. Ferrag M. A., Friha O., Kantarci B., Tihanyi N., Cordeiro L., Debbah M., Hamouda D., Al-Hawawreh M., Choo K.-K. R. Edge Learning for 6G-enabled Internet of Things: A Comprehensive Survey of Vulnerabilities, Datasets, and Defenses. 2023. URL: https://www.researchgate.net/publication/371728275_Edge_Learning_for_6G-enabled_Internet_of_Things_A_Comprehensive_Survey_of_Vulnerabilities_Datasets_and_Defenses (дата звернення: 28.04.2025).
9. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*. 2015. Vol. 17, № 4. P. 2347–2376. DOI: https://doi.org/10.1109/COMST.2015.2444095 (дата звернення: 28.04.2025).
10. Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A. Security, Privacy and Trust in Internet of Things: The Road Ahead. *Computer Networks*. 2015. Vol. 76. P. 146–164. DOI: https://doi.org/10.1016/j.comnet.2014.11.008 (дата звернення: 28.04.2025).

11. Yang Z., Liu L., Zhang Y. A Survey on Security and Privacy Issues in Internet-of-Things. 2020. URL: https://www.researchgate.net/publication/316173391 (дата звернення: 28.04.2025).
12. Khan M. A., Salah K., Rehman M. H. U., Jayaraman R., Arshad J., Madhusudan G. A survey on security and privacy issues in edge computing-assisted Internet of Things. *IEEE Access*. 2020. Vol. 8. P. 82649–82674. DOI: https://doi.org/10.1109/ACCESS.2020.3003780 (дата звернення: 28.04.2025).
13. Bhajantri N., Gangadharaiah B. A Comprehensive Survey on Resource Management in Internet of Things. *Journal of Telecommunications and Information Technology*. 2020. № 4. P. 47–58. URL: https://www.researchgate.net/publication/348071565 (дата звернення: 28.04.2025).
14. Zhang Y., Deng S., Liu Y., Taheri J., Ranjan R. Context-aware security in the Internet of Things: A survey. *Journal of Network and Computer Applications*. 2021. Vol. 187. Article 103110. URL: https://www.researchgate.net/publication/354857110 (дата звернення: 28.04.2025).
15. Hassan R., Elhoseny M., Mostafa M. M., Mehmood R. Data Anomaly Detection in the Internet of Things: A Review of Current Trends and Research Challenges. *Journal of Ambient Intelligence and Humanized Computing*. 2023. Vol. 15. Article 103489. URL: https://www.researchgate.net/publication/374498472 (дата звернення: 28.04.2025).
16. Noaman A., et al. Challenges in Integration of Heterogeneous Internet of Things. *Scientific Programming*. 2022. Article ID 8626882. DOI: https://doi.org/10.1155/2022/8626882 (дата звернення: 28.04.2025).
17. Cortés A., Juan A. A., Pamos C. A review on edge computing in smart energy by means of a systematic mapping study. *Energies*. 2019. Vol. 12, № 20. Article 3877. URL: https://www.researchgate.net/publication/338245738_A_Review_on_Edge_Computing_in_Smart_Energy_by_means_of_a_Systematic_Mapping_Study (дата звернення: 28.04.2025).
18. Bandyopadhyay D., Sen J. Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications*. 2011. Vol. 58, № 1. P. 49–69. DOI: https://doi.org/10.1007/s11277-011-0288-5 (дата звернення: 28.04.2025).
19. ElZemity A., Arief B. Privacy threats and countermeasures in federated learning for Internet of Things: A systematic review. *arXiv preprint*. arXiv:2407.18096. 2024. DOI: https://doi.org/10.48550/arXiv.2407.18096 (дата звернення: 28.04.2025).
20. Chatterjee A., Ahmed B. S. IoT Anomaly Detection Methods and Applications: A Survey. *Internet of Things*. 2022. Vol. 18. Article 100168. URL: https://www.researchgate.net/publication/361621845_IoT_Anomaly_Detection_Methods_and_Applications_A_Survey (дата звернення: 28.04.2025).

References

1. Dixit, P., Bhattacharya, P., Tanwar, S., & Gupta, R. (2024). Role of artificial intelligence in Internet of Things systems: A systematic mapping study. *Sensors, 24*(20), Article 6511. https://www.mdpi.com/1424-8220/24/20/6511 (Accessed April 28, 2025).
2. Thibaud, M., Chi, H., Zhou, W., & Piramuthu, S. (2018). Internet of Things (IoT) in high-risk environment, health and safety (EHS) industries: A comprehensive review. *Decision Support Systems, 108*, 79–95. https://www.sciencedirect.com/article/abs/pii/S0167923618300344?via%3Dihub (Accessed April 28, 2025).
3. Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of Things for health care: A comprehensive survey. *IEEE Access, 3*, 678–708. https://ieeexplore.ieee.org/document/7113786 (Accessed April 28, 2025).
4. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376. https://ieeexplore.ieee.org/document/7123563 (Accessed April 28, 2025).
5. Dubey, H., Sahoo, P. K., Chahal, P., & Saini, H. (2020). IoT ecosystem: A survey on classification of IoT. *EAI Endorsed Transactions on Internet of Things, 6*(21), Article e4. https://eudl.eu/doi/10.4108/eai.16-5-2020.2304170 (Accessed April 28, 2025).
6. Gupta, M., Abdelsalam, M., Khorsandroo, S., & Mittal, S. (2022). A review on Internet of Things: Communication protocols, wireless technologies, and applications. In *Internet of Things and Cyber Physical Systems* (pp. 353–370). Springer. https://link.springer.com/chapter/10.1007/978-981-19-2004-2_23 (Accessed April 28, 2025).
7. Hou, Z., Ding, Y., Jiao, Y., Hu, L., & Wu, D. O. (2021). A survey of recent advances in edge-computing-powered artificial intelligence of things. *IEEE Internet of Things Journal, 8*(22), 16309–16328. https://www.researchgate.net/publication/352386275 (Accessed April 28, 2025).
8. Ferrag, M. A., Friha, O., Kantarci, B., Tihanyi, N., Cordeiro, L., Debbah, M., Hamouda, D., Al-Hawawreh, M., & Choo, K.-K. R. (2023). Edge learning for 6G-enabled Internet of Things: A comprehensive survey of vulnerabilities, datasets, and defenses. https://www.researchgate.net/publication/371728275 (Accessed April 28, 2025).
9. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095 (Accessed April 28, 2025).

10. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008 (Accessed April 28, 2025).
11. Yang, Z., Liu, L., & Zhang, Y. (2020). A survey on security and privacy issues in Internet-of-Things. https://www.researchgate.net/publication/316173391 (Accessed April 28, 2025).
12. Khan, M. A., Salah, K., Rehman, M. H. U., Jayaraman, R., Arshad, J., & Madhusudan, G. (2020). A survey on security and privacy issues in edge computing-assisted Internet of Things. *IEEE Access, 8*, 82649–82674. https://doi.org/10.1109/ACCESS.2020.3003780 (Accessed April 28, 2025).
13. Bhajantri, N., & Gangadharaiah, B. (2020). A comprehensive survey on resource management in Internet of Things. *Journal of Telecommunications and Information Technology, 4*, 47–58. https://www.researchgate.net/publication/348071565 (Accessed April 28, 2025).
14. Zhang, Y., Deng, S., Liu, Y., Taheri, J., & Ranjan, R. (2021). Context-aware security in the Internet of Things: A survey. *Journal of Network and Computer Applications, 187*, Article 103110. https://www.researchgate.net/publication/354857110 (Accessed April 28, 2025).
15. Hassan, R., Elhoseny, M., Mostafa, M. M., & Mehmood, R. (2023). Data anomaly detection in the Internet of Things: A review of current trends and research challenges. *Journal of Ambient Intelligence and Humanized Computing, 15*, Article 103489. https://www.researchgate.net/publication/374498472 (Accessed April 28, 2025).
16. Noaman, A., et al. (2022). Challenges in integration of heterogeneous Internet of Things. *Scientific Programming, 2022*, Article 8626882. https://doi.org/10.1155/2022/8626882 (Accessed April 28, 2025).
17. Cortés, A., Juan, A. A., & Pamos, C. (2019). A review on edge computing in smart energy by means of a systematic mapping study. *Energies, 12*(20), Article 3877. https://www.researchgate.net/publication/338245738 (Accessed April 28, 2025).
18. Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49–69. https://doi.org/10.1007/s11277-011-0288-5 (Accessed April 28, 2025).
19. ElZemity, A., & Arief, B. (2024). Privacy threats and countermeasures in federated learning for Internet of Things: A systematic review. *arXiv preprint*, arXiv:2407.18096. https://doi.org/10.48550/arXiv.2407.18096 (Accessed April 28, 2025).
20. Chatterjee, A., & Ahmed, B. S. (2022). IoT anomaly detection methods and applications: A survey. *Internet of Things, 18*, Article 100168. www.researchgate.net/publication/361621845_IoT_Anomaly_Detection_Methods_and_Applications_A_Survey (Accessed April 28, 2025).

Ю. І. Підлісний

Національний університет «Чернігівська політехніка», м. Чернігів, Україна

Інтелектуально-контекстна модель класифікації середовищ інтернету речей

У статті представлено інтелектуально-контекстну модель класифікації середовищ Інтернету речей (IoT), яка ґрунтується на комплексному врахуванні ключових параметрів, таких як рівень вбудованого інтелекту, контекст функціонування, рівень безпеки та динамічність системи. Актуальність дослідження зумовлена стрімким зростанням складності екосистем IoT, що характеризуються гетерогенністю пристроїв, різноманітністю умов експлуатації, необхідністю адаптації до змін у навколишньому середовищі та підвищеними вимогами до безпеки. Критичний аналіз існуючих підходів до класифікації IoT виявив їхні основні обмеження: вузьку орієнтацію виключно на технічні або функціональні ознаки, недостатнє врахування поведінкових характеристик та інтелекту пристроїв, а також ігнорування контексту функціонування та ландшафту кіберзагроз.

Розроблена модель усуває зазначені недоліки та забезпечує точніше структурування середовищ IoT шляхом урахування їхнього функціонального призначення, архітектурних особливостей та здатності до автономного прийняття рішень. Вона може застосовуватися для системного аналізу, формалізації ризиків, оптимізації механізмів реагування на загрози, а також проєктування ефективних стратегій кібербезпеки та адаптивного управління в динамічних середовищах. Запропонована класифікація дає змогу узагальнити існуючі типи IoT-систем і закладає підґрунтя для розробки нових, більш гнучких і захищених архітектур. Практична значущість отриманих результатів полягає в їхній придатності для використання в різних галузях, де важливими є інтелектуальна обробка даних, контекстна обізнаність і стійкість до кіберзагроз - зокрема в Індустрії 4.0, електронній охороні здоров'я, інтелектуальних транспортних системах і розумних містах.

інтернет речей, класифікація IoT, інтелектуальні системи, безпека, контекст використання, динамічність, адаптація, кіберзахист, інтелектуально-контекстна модель

Одержано (Received) 29.05.2025

Прорецензовано (Reviewed) 06.06.2025
Прийнято до друку (Approved) 24.06.2025