УДК 004.056.55:004.312.2 **doi: 10.26906/SUNZ.2025.2.119-124**

Kuien Do[1], Iryna Klymova[1], Elen Naumova[1], Mykhailo Herevych[2], Oleksandr Yankovskyi[1]

[1] Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
[2] Uzhhorod National University, Uzhhorod, Ukraine

DATA PROCESSING AND ANALYSIS METHODS IN IOT USING MACHINE LEARNING

Abstract. Relevance. The growing integration of Internet of Things (IoT) technologies into all areas of human life – from intelligent households to smart city infrastructure – is accompanied by an exponential increase in the volume of data being collected, transmitted, and processed in real time. When combined with artificial intelligence technologies, this data becomes the foundation for making autonomous decisions, predicting user behavior, and adapting environments to the needs of specific individuals. However, it is precisely in this context that the critically important issue of personal data protection arises. Many IoT devices operate in uncontrolled environments, have limited resources for cryptographic protection, and are vulnerable to cyberattacks and unauthorized data collection. Meanwhile, artificial intelligence algorithms used to analyze this data often exhibit the "black box" problem, where it is impossible to fully explain how and why a particular decision was made based on personalized data. The lack of transparency, combined with broad access to sensitive information, threatens fundamental human rights to privacy. The relevance of this topic is driven by the need to find balanced technical solutions that enable both effective analysis of large-scale data in IoT environments and a high level of data security. In this regard, the study of modern methods for processing, analyzing, and protecting data in IoT systems, adapted to the requirements of ethical artificial intelligence and digital privacy standards, represents one of the key challenges of contemporary digital science. **The object of research**: the processes of data collection, processing, analysis, and protection in IoT systems, particularly those components related to the use of users' personal information and its processing through artificial intelligence methods. **Purpose of the article**: research of modern methods for data processing and analysis in IoT systems. The objective of the work is to identify the most effective approaches to secure data handling, characterize existing privacy threats, and assess the potential for integrating protected analytical algorithms that meet both the technical and ethical requirements of the digital environment. **Research results**. A comprehensive analysis of modern approaches to data collection, processing, analysis, and protection in IoT systems has been conducted, particularly in the context of the growing role of artificial intelligence. The technological foundations of IoT functionality were examined, key architectural components identified, and their role in creating digital ecosystems for monitoring, management, and decision-making across various sectors – from household systems to critical infrastructure – was investigated. Special attention was paid to data preprocessing methods, which help reduce information load, improve the quality of analysis, and adapt data flows to the requirements of intelligent algorithms. It was demonstrated that the use of edge processing and local-level aggregation enhances both system performance and security. The main types of databases for IoT – especially those optimized for time series – were analyzed, along with tools for handling large volumes of data in cloud and hybrid environments. **Conclusions.** Data collection methods in IoT are multilayered and closely linked to the requirements for energy efficiency, security, latency, and system scalability. The quality and reliability of the collected information form the foundation for subsequent processing, analysis, and decision-making; therefore, the selection of sensors, communication protocols, and architectural models is of strategic importance for any IoT system. Preprocessing and efficient data storage in IoT are critical stages that ensure the quality, security, and usability of information for further analysis. They determine not only the accuracy of analytics but also the stability, scalability, and compliance with regulatory standards. This creates a demand for the development of adaptive, intelligent data processing and storage systems capable of dynamically responding to changes in device operation context and user requirements. The successful implementation of secure IoT solutions requires an integrated approach that combines technical expertise, legal knowledge, and ethical responsibility.

Keywords: IoT, artificial intelligence; data processing; data analysis; privacy; personal data protection; edge computing; differential privacy; machine learning; intelligent systems.

Introduction

IoT has, over the past decade, evolved from an experimental concept into a fundamental component of modern information systems. The essence of IoT lies in creating a network of physical objects – devices equipped with sensors, communication modules, computational elements, and software – that can interact with each other, with the external environment, and with centralized computing platforms. These devices continuously generate large volumes of data about physical processes, user behavior, the condition of technical systems, or the surrounding environment. As a result, the issues of efficient data processing and analysis become extremely relevant, as they allow raw information streams to be transformed into practically valuable knowledge, recommendations, or actions.

The significance of this problem becomes particularly evident against the backdrop of widespread implementation of artificial intelligence, which greatly expands the capabilities of IoT – from intelligent control of industrial processes to autonomous management of smart city systems. However, alongside technical advantages come serious challenges. Among them is the protection of personal data, which is increasingly being processed by systems embedded in everyday human life: gadgets, vehicles, household appliances, and more. The combination of large volumes of information, automatic AI-based data processing, and distributed architecture creates risks of data leakage, unauthorized access, and misuse of personal information.

Thus, in the context of rapid digitalization and the widespread adoption of IoT, the study of data processing and analysis methods becomes critically im-

portant – not only to ensure high performance and accuracy but also to meet the requirements of confidentiality, ethical data handling, and security. IoT data processing systems must be capable of working effectively with distributed, heterogeneous, and potentially sensitive datasets while maintaining data integrity, reliability, and privacy.

The purpose of this work is a comprehensive analysis of modern methods for data processing and analysis in IoT ecosystems, considering the requirements for personal data protection, which is particularly relevant in the context of implementing machine learning in digital infrastructures. This approach allows consideration not only of the technical aspects of efficient IoT system performance but also of the legal, social, and ethical components that shape trust in technology in the digital age.

Analysis of publications. In recent years, the issue of data processing and analysis in IoT systems has become one of the central topics in the fields of applied informatics, artificial intelligence, and computer security. The analysis of scientific sources indicates active development in areas such as the optimization of computational processes at the edge, the integration of machine learning for intelligent data analysis, and the development of mechanisms for ensuring privacy in IoT environments.

One of the fundamental reviews is presented in [1], which outlines the general principles of IoT architecture and identifies key problems related to the analysis of large data streams. This publication laid the foundation for further research in the field of data processing, particularly in the context of distributed computing and cloud integration.

Research [2] focuses on the practical use of data analysis methods for managing urban infrastructure, including sensor monitoring, traffic flow analysis, and environmental control. Clustering methods, neural network approaches, and elements of predictive analytics are widely applied in this work.

A separate category includes studies devoted to the application of artificial intelligence in IoT, particularly deep learning. For example, work [3] examines classification and anomaly detection algorithms in data streams from wireless sensor networks, which are foundational for many IoT solutions.

A significant number of publications are also dedicated to privacy and information protection issues. For instance, article [4] analyzes the threats of personal data leakage and considers pseudonymization, anonymization, and differential privacy technologies. These aspects become even more important in the context of automated data processing using artificial intelligence. The authors emphasize that privacy and security issues remain key challenges for IoT. Despite the rapid adoption of IoT in critical sectors (healthcare, energy, infrastructure), the level of threats remains high due to poor device protection, limited resources, and weak security governance at various architectural levels. Several major threats are highlighted: insufficient firmware and software updates for IoT devices, the absence of effective and reliable security protocols, low user awareness of privacy risks, and real-time monitoring of active devices, which creates potential data leakage points. These factors make IoT environments vulnerable to numerous cyberattacks, certificate spoofing, node impersonation, or interception of unencrypted traffic. The proposed architecture allows for effective distribution of computational tasks and protection of data at every stage of its transmission through the system.

Modern sources such as [5,6] demonstrate a growing interest in combining IoT with machine learning, which requires new solutions for data storage, preprocessing, cleansing, and interpretation. The authors describe the synergy of artificial intelligence and IoT as a transformational approach to data processing and decision-making. It enables deeper integration of digital technologies into human life and business processes. However, alongside the advantages, this integration also brings new challenges – particularly in the context of protecting sensitive data, ensuring transparency of decisions, and the ethical use of information. For this reason, future research should focus not only on optimization algorithms but also on models for safe, responsible, and interpretable integration of artificial intelligence into the IoT environment.

In general, the analysis of scientific publications reveals a trend toward an interdisciplinary approach that combines computer science, telecommunications, applied mathematics, and cybersecurity. This approach enables the creation of not only efficient IoT data processing systems but also systems that ensure the protection of confidential information, which is a key factor in building user trust in emerging technologies.

Main part

IoT is a concept of a global network of interconnected physical objects that can collect, exchange, and process data via the Internet with no or minimal human intervention. IoT systems consist of many devices – sensors, actuators, controllers, computing modules – that interact with each other and with centralized or distributed platforms. A distinguishing feature of such systems is their ability to operate autonomously, responding to changes in environmental parameters, storing and transmitting the collected data in real time.

Unlike classical information systems, which operate within a clearly defined architecture, IoT is a dynamic, scalable environment that encompasses objects in the physical world – from household devices to infrastructure objects in industry and urban space. These objects can be mobile, distributed, limited in resources, yet still form a single digital ecosystem.

A significant advantage of IoT is the ability to obtain high-frequency and detailed data from the surrounding environment. This information is used for: monitoring the condition of systems (for example, energy networks or production equipment), optimizing resources (water supply, transport, lighting), automated decision-making (smart homes, Industry 4.0), and personalizing user interaction (healthcare, consumer services).

The integration of IoT with modern information technologies, particularly cloud computing and artificial

intelligence, has enabled a qualitatively new level of efficiency in data usage. There has emerged the possibility to implement smart systems that not only transmit information but also interpret it using machine learning algorithms, predict user behavior or environmental changes, and make optimization decisions.

In the modern information space, IoT performs a key function a link between the physical and digital worlds. This link is the foundation for building: smart cities that respond to traffic flow dynamics or environmental conditions; healthcare systems that allow continuous monitoring of patients' vital signs; logistics systems that enable real-time tracking of goods; energy systems capable of balancing loads in the grid depending on demand.

At the same time, the rapid increase in the number of connected devices (already measured in tens of billions) gives rise to a range of technical and ethical problems. Among the main ones is the security problem, since each IoT node is a potential entry point for an attacker, as well as the privacy problem, since a significant portion of the data is personalized or sensitive. These problems require new approaches to architecture, interaction protocols, data processing methods, and trust models in the IoT environment.

In conclusion, the Internet of Things is not only a technological platform for data collection, but also a strategic element of society's digital transformation. Its significance continues to grow in the context of automation, intelligence, and decentralization of control systems at all levels – from household to national.

The data collection process is a fundamental component of the functioning of any IoT system, as it is precisely through it that devices can detect changes in the surrounding environment, interact with each other, and transmit information for further analysis. The quality, volume, and structure of the collected data directly affect the effectiveness of decision-making in smart systems, especially in the context of using artificial intelligence for their interpretation. Figure 1 presents the existing data collection methods in IoT.

At the first level of data collection are sensors that can detect physical or chemical environmental parameters: temperature, humidity, pressure, motion, illumination, presence of gases, biometric indicators, etc. Sensor modules can be active – with their own power source; passive – activated by an external probing signal

Depending on the application, different types of sensors are used: temperature, motion, biometric, vibration, optical, and acoustic sensors. Data collection is provided by sensor nodes. Ready-made boards such as Raspberry Pi, Arduino, ESP32, STM32, NXP, and TI Launchpad are often used. These devices are capable not only of collecting but also of preprocessing data to reduce traffic volume.

The data collected by sensors must be transmitted to higher processing levels – either to edge devices or to the cloud. Various network protocols are used for this purpose, considering energy consumption, latency, reliability, and bandwidth limitations: MQTT, CoAP, HTTP/HTTPS, ZigBee, Z-Wave, LoRa, NB-IoT. To reduce the load on cloud services and the network, the concept of edge computing – processing data as close as possible to the point of collection – is gaining increasing importance.

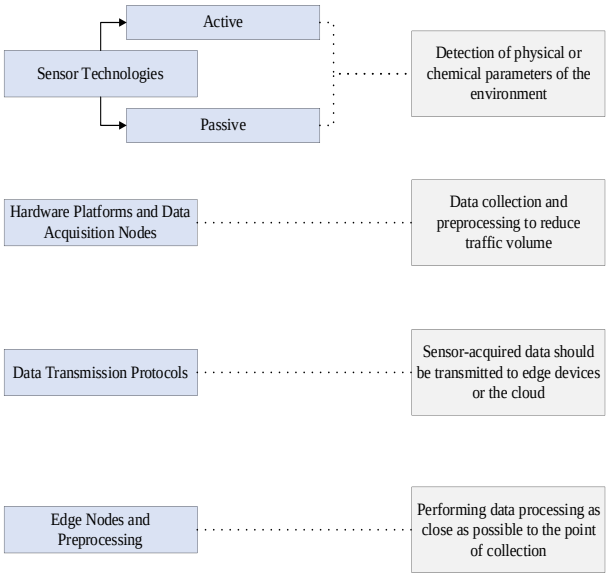

Fig. 1. Existing Data Collection Methods in IoT

Edge nodes filter out noise and data errors, perform basic analysis, and transmit only aggregated or critical data to higher levels. This helps reduce latency, decrease network load, and enhance security, as fewer incomplete or noisy data are sent to the cloud. Particular attention in modern IoT systems is paid to data protection at the collection level. Already at the sensor level, traffic encryption, device authentication, and data access control can be applied to prevent unauthorized devices from interfering with the communication channel. The data collected by IoT system sensors have no value by themselves until they are structured, cleaned, aggregated, and stored for further analysis. Since IoT data is received continuously, at high frequency, and from many sources, their preprocessing – bringing them into a consistent and analyzable format – becomes a key challenge. In this process, the data storage strategy also plays an important role: from local caching to cloud archiving. Fig. 2 presents the methods of data preprocessing and storage in IoT.

Raw data often contains noise, duplicates, incorrect or incomplete values. Therefore, at the stage of initial processing, the following methods are applied: noise filtering, missing data handling, outlier and anomaly detection, and format standardization. This stage is performed either directly on sensor nodes or on edge gateways that collect data streams from multiple devices.

To reduce the volume of information transmitted to the cloud, data aggregation is often used: calculation of averages, medians, and extreme values over a certain period; sensor data fusion; construction of synthetic indicators or indexes. Semantic data fusion from different sources is also possible – for example, combining air temperature with geolocation coordinates and video surveillance data. At the stage of preliminary intelligent processing, basic analysis algorithms can be executed: state classification, anomaly detection in the data

stream, and local storage of important events instead of the full data stream.

This reduces traffic volume, increases system autonomy, and minimizes the risks of confidential data loss.

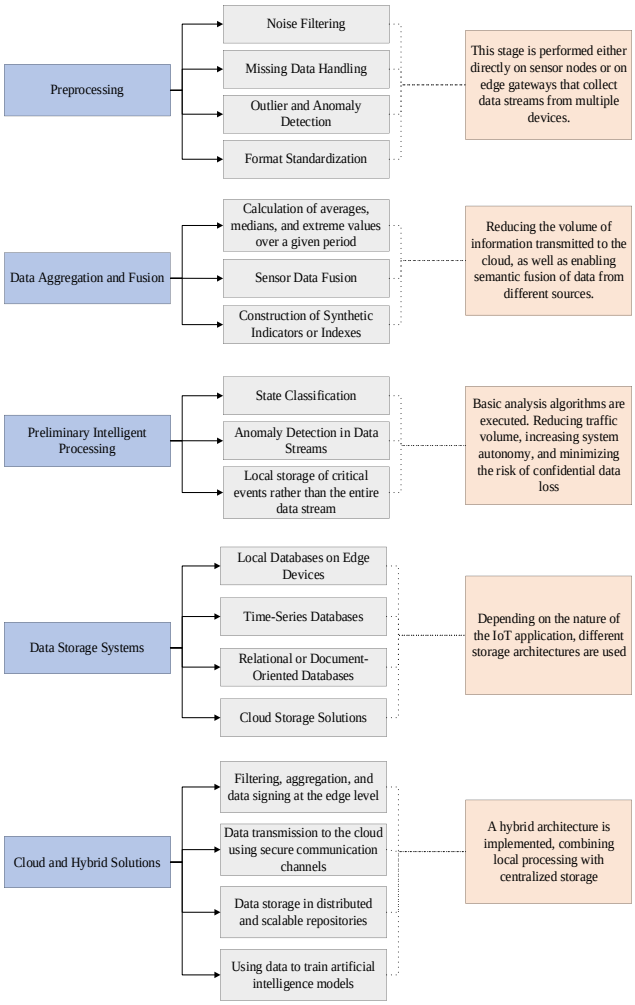

Fig. 2. Preprocessing and Data Storage Methods in IoT

Depending on the nature of the IoT application, various storage architectures are used: local databases on edge devices for caching or autonomous operation; time-series databases optimized for streaming data, with built-in time indexing mechanisms; relational or document-oriented databases for storing structured and semi-structured information; and cloud storage solutions for scalable long-term storage with backup and access to machine learning services.

Most modern systems implement hybrid architecture that combines local processing with centralized storage. In this model, data at the edge level are filtered, aggregated, and signed; transmitted to the cloud via secure channels; stored in distributed, scalable repositories; and used to train artificial intelligence models. A key requirement for data storage is protection – implementation of encryption mechanisms, access control, access logging, and compliance with GDPR standards or other local regulations.

After the stages of data collection, cleansing, and storage, the next key phase in IoT data processing is analysis – a process that enables the extraction of useful information, recognition of patterns, detection of anomalies, and formulation of well-founded decisions. Due to the large volume, speed, and diversity of data generated by IoT devices, traditional analysis methods are often insufficient. That is why statistical analysis methods, machine learning, and deep learning are at the forefront.

At the first level of analysis, descriptive statistics are used: calculation of means, variances, medians, quartiles; correlation analysis between variables; generation of histograms, time series, and trend lines. These methods help identify general trends, seasonal fluctuations, and provide initial interpretation of parameter dynamics in the sensor environment.

When there is a need to identify categories or similar groups within a dataset, classification or clustering methods are applied. Since most IoT data is time-based, time-series analysis methods play an important role: ARIMA, SARIMA, Prophet; construction of seasonal models; detection of trends and cycles; signal smoothing and change point detection.

IoT systems integrated with artificial intelligence increasingly rely on automatic learning from data. This enables training behavioral models for automatic state response; anomaly detection; real-time control parameter optimization; and interpretation of complex relationships between input parameters and outcomes. Tools for this include TensorFlow, Scikit-learn, PyTorch, Edge AI SDK, and others.

In cases involving large and complex datasets, deep learning is applied. These models work effectively in real time, if edge computing or GPU acceleration is supported.

Data visualization is an integral part of analytics: using dashboards for interactive monitoring; trend charts, heatmaps, event maps; generating reports for real-time decision-making. Also important is the implementation of interpretable models – especially in critical domains where it is necessary to explain why the system made a particular decision.

During data collection, transmission, and analysis in IoT, several privacy-related threats arise interception of unencrypted traffic, especially in wireless networks; unauthorized access to devices or processing servers; misuse of data; data leaks due to software vulnerabilities in IoT devices; man-in-the-middle attacks that allow data modification or duplication during transmission. These threats are particularly dangerous in domains such as healthcare, smart homes, and personal vehicles, where consequences can be both social and legal.

Many countries have legislative acts regulating the processing of personal data. In the context of IoT, this means that all devices and systems must have built-in mechanisms for access control, encryption, and user control over their own information.

Protecting personal data in the IoT environment is a complex task that combines legal, technical, and architectural approaches.

Given the growing autonomy of systems and their deep integration into users' personal lives, embedded data protection must be an essential part of any IoT solution.

The future of such systems lies in the combination of transparency, responsibility, and artificial intelligence capable of making ethical and well-founded decisions without threatening privacy.

In the process of modeling complex networks, the choice of an appropriate mathematical model is of critical importance. Each model has its own advantages, limitations, structural properties, and domain of effective application.

The analysis has shown that there is no universal model suitable for all types of networks. The selection of a model should be based on the core characteristics of the system under study – such as the nature of the degree distribution, the presence of a clustered structure, the dynamic nature of connections, and spatial or resource constraints. In complex applied problems, the best results are often achieved by hybrid or adaptive models that combine elements of several approaches.

Conclusions

As a result of the conducted research, a comprehensive analysis was carried out on modern approaches to data collection, processing, analysis, and protection in IoT systems, especially in the context of the growing role of artificial intelligence.

The technological foundations of IoT functionality were examined, key architectural components were identified, and their role was explored in the creation of digital ecosystems for monitoring, control, and decision-making across various domains – from household systems to critical infrastructure. Special attention was paid to data preprocessing methods that help reduce information load, improve the quality of analysis, and adapt data flows to the needs of intelligent algorithms. It was shown that the application of edge processing and local-level aggregation improves both the performance and security of systems. The main types of databases for IoT were analyzed, including those optimized for time series, as well as tools for processing large volumes of data in cloud and hybrid environments.

Data collection methods in IoT are multilayered and closely linked to the requirements for energy efficiency, security, latency, and system scalability. The quality and reliability of the collected information form the foundation for further processing, analysis, and decision-making, making the selection of sensors, communication protocols, and architectural models of strategic importance for any IoT system.

Preprocessing and efficient data storage in IoT are critical stages that ensure the quality, security, and usability of information for further analysis. They determine not only the accuracy of analytics but also the stability, scalability, and compliance with regulatory requirements.

Therefore, there is a growing need to develop adaptive, intelligent data processing and storage systems capable of dynamically responding to changing device contexts and user requirements.

Data protection mechanisms were also studied, including encryption, differential privacy, anonymization, federated learning, and access-controlled architectures. The key emphasis was placed on the need to combine effective data processing with built-in mechanisms for protecting personal information, especially in the context of system scaling and AI implementation. It was determined that the successful implementation of secure IoT solutions requires an integrated approach that combines technical expertise, legal awareness, and ethical responsibility.

Thus, the results of this work can be used to develop practical recommendations for building secure, scalable, and intelligent IoT systems focused both on data processing efficiency and on adherence to digital privacy principles.

References

1. J.Gubbi, R. Buyya, S. Marusic, M. Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. Vol.29, iss.7, Elsevier, 2013. P. 1645-1660. https://doi.org/10.1016/j.future.2013.01.010
2. Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M. (2014) Internet of Things for Smart Cities. IEEE Internet of Things Journal, 1, 2014. P. 22-32. https://doi.org/10.1109/JIOT.2014.2306328
3. M. Alsheikh; S. Lin; D. Niyato; H. Tan. Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications. IEEE Communications Surveys & Tutorials, Vol. 16, 2014. P. 1996 – 2018. https://doi.org/10.1109/COMST.2014.2320099
4. L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider. IoT Privacy and Security: Challenges and Solutions. Applied Sciences, Vol. 10(12), 2020. 17 p. https://doi.org/10.3390/app10124102
5. J.P. Singhal. A Survey on AI enabled IoT Applications. International Journal of New Media Studies, vol. 9, 2022. P. 42-46.
6. O. Aouedi, T. Vu, A. Sacco, D. Nguyen, K. Piamrat, G. Marchetto, Q. Pham. A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions. IEEE Communications Surveys & Tutorials, 2024. 56 p. https://doi.org/10.1109/COMST.2024.3430368

Received (Надійшла) 20.02.2025
Accepted for publication (Прийнята до друку) 23.04.2025

Відомості про авторів / About the Authors

Нгок До Куєн – студент кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Kuien Do – student, Department of Electronic Computers, Kharkiv National University of Radio Electronics Kharkiv, Ukraine;
e-mail: nhok.do1@nure.ua; ORCID Author ID: https://orcid.org/0009-0009-7824-3233.

Климова Ірина Миколаївна – асистентка кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Iryna Klymova – assistant of Department of Electronic Computers, Kharkiv National University of Radio Electronics Kharkiv, Ukraine;
e-mail: iryna.klymova@nure.ua; ORCID Author ID: https://orcid.org/0000-0003-0455-6180.
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57216950622

Наумова Олена Валеріївна– студент кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Elen Naumova – student, Department of Electronic Computers, Kharkiv National University of Radio Electronics Kharkiv, Ukraine;
e-mail: olena.naumova@nure.ua; ORCID Author ID: https://orcid.org/0009-0009-3561-3687.

Геревич Михайло Олександрович – доктор філософії, доцент кафедри теорії та історії держави і права, Ужгородський національний університет, Ужгород, Україна;
Mykhailo Herevych – PhD, Associate Professor of Department of Theory and History of State and Law, Uzhhorod, Ukraine;
e-mail: mykhailo.herevych@uzhnu.edu.ua; ORCID Author ID: https://orcid.org/0000-0002-0842-2828.

Янковський Олександр Аркадійович – кандидат технічних наук, доцент, доцент кафедри ЕОМ, Харківський національний університет радіоелектроніки, Харків, Україна;
Oleksandr Yankovskyi – PhD, Assistant Professor Assistant Professor of the Department of electronic computers, Kharkiv National University of radio electronics, Kharkiv, Ukraine;
e-mail: oleksandr.yankovskyi@nure.ua; ORCID Author ID: https://orcid.org/0000-0002-1268-0029.

Методи обробки та аналізу даних в IoT з використанням машинного навчання

Нгок До Куєн, І. М. Климова, О. В. Наумова, М. О. Геревич, О. А. Янковський

Анотація. Актуальність. Зростаюча інтеграція технологій Інтернету речей (IoT) у всі сфери людського життя - від інтелектуального побуту до інфраструктури «розумного міста» – супроводжується експоненційним зростанням обсягу даних, що збираються, передаються та обробляються в реальному часі. У поєднанні з технологіями штучного інтелекту ці дані перетворюються на основу для прийняття автономних рішень, прогнозування поведінки користувачів, а також адаптації середовища до потреб конкретної особи. Однак саме в цьому контексті постає надзвичайно критичне питання захисту персональних даних. Багато IoT-пристроїв працюють у неконтрольованому середовищі, мають обмежені ресурси для криптографічного захисту, а також схильні до кібератак і несанкціонованого збору інформації. Натомість алгоритми штучного інтелекту, які використовуються для аналізу цих даних, нерідко демонструють проблему «чорної скриньки», коли неможливо повною мірою пояснити, як і чому було прийнято певне рішення на основі персоніфікованих даних. Відсутність прозорості у поєднанні з широким доступом до чутливої інформації ставить під загрозу базові права людини на приватність. Актуальність теми зумовлена необхідністю пошуку балансованих технічних рішень, що дозволяють одночасно ефективно аналізувати великі масиви даних в IoT-середовищі й забезпечувати високий рівень їхньої безпеки. У зв'язку з цим, вивчення сучасних методів обробки, аналізу та захисту даних в системах IoT, адаптованих до вимог етичного штучного інтелекту та цифрових стандартів конфіденційності, є одним із ключових викликів сучасної цифрової науки. **Об'єкт дослідження**: процеси збору, обробки, аналізу та захисту даних у системах IoT, зокрема ті їхні компоненти, які пов'язані з використанням персональної інформації користувачів та її обробкою за допомогою методів штучного інтелекту. **Мета статті**: дослідження сучасних методів обробки та аналізу даних в системах IoT. Робота має на меті виявити найбільш ефективні підходи до безпечної обробки даних, охарактеризувати існуючі загрози конфіденційності та оцінити потенціал інтеграції захищених алгоритмів аналізу, які відповідають як технічним, так і етичним вимогам цифрового середовища. **Результати дослідження**. Здійснено комплексний аналіз сучасних підходів до збору, обробки, аналізу та захисту даних в системах IoT, особливо в умовах зростаючої ролі штучного інтелекту. Розглянуто технологічні основи функціонування IoT, визначено ключові архітектурні складові та досліджено їхню роль у створенні цифрових екосистем для моніторингу, управління та прийняття рішень у різних галузях – від побутових систем до критичної інфраструктури. Особливу увагу було приділено методам попередньої обробки даних, що дозволяють знизити ін-формаційне навантаження, підвищити якість аналізу та адаптувати потоки інформації до потреб інтелектуальних алгоритмів. Було показано, що застосування периферійної обробки та агрегації на локальних рівнях підвищує як продуктивність систем, так і їхню безпеку. Проаналізовано основні типи баз даних для IoT, зокрема оптимізовані для часових рядів, а також інструменти для обробки великих обсягів даних у хмарних та гібридних середовищах. **Висновки.** Методи збору даних в IoT є багатошаровими й тісно пов'язаними з вимогами до енергоефективності, безпеки, затримки та масштабованості систем. Якість і надійність зібраної інформації закладає ос-нову для подальшої обробки, аналізу й прийняття рішень, тому вибір сенсорів, протоколів та архітектурної моделі має стратегічне значення для будь-якої IoT-системи. Попередня обробка та ефективне зберігання даних в IoT – критичні етапи, що забезпечують якість, безпеку та придатність інформації для подальшого аналізу. Вони визначають не лише точність аналітики, а й стабільність, масштабованість і відповідність нормативним вимогам. У зв'язку з цим постає потреба в розробці адаптивних, інтелектуальних систем обробки та зберігання, здатних динамічно реагувати на зміну контексту роботи пристроїв і користувацькі вимоги. Успішна реалізація безпечних IoT-рішень потребує інтегрованого підходу, який поєднує технічну компетентність, правові знання та етичну відповідальність.

Ключові слова: IoT, штучний інтелект; обробка даних; аналіз даних; конфіденційність; захист персональних даних; edge computing; диференційна конфіденційність; машинне навчання; інтелектуальні системи.