Artificial Intelligence of Things (AIoT): Integration Challenges and Security Issues

Andrii Stanko[1,*,†] , Oleksii Duda[2,†],Andrii Mykytyshyn[1,*,†] , Oleg Totosko[1,†] and Rostyslav Koroliuk[1,†]

[1] *Ternopil Ivan Puluj National Technical University, Ruska 56, 46001 Ternopil, Ukraine*

Abstract

AIoT stands for Artificial Intelligence of Things and refers to the synergy between Internet of Things and artificial intelligence, where new frontiers are opening for developing intelligent autonomous systems. The integration of AI and IoT enables devices to operate beyond mere data collection and transmission by analyzing data in real time, making independent decisions, and adapting to environmental changes. However, AIoT has several deployment challenges, each potentially being limiting factors against the potential of AIoT and security or privacy of data. Some of the most important integration challenges for AIoT involve the discussion of device and protocol compatibility on one hand and vast amounts of data on the other, latency, and power consumption. The article further discusses the complexity brought in by a multitude of heterogeneous hardware and software platforms, making standardization and inter-operability between systems difficult. Much attention is given to the problems of security, as AIoT systems are becoming gradually vulnerable to possible cybersecurity attacks, which include unauthorized access to data, loss, or leakage. The article also covers the potential threats regarding the privacy and security of AI algorithms, including data poisoning attacks and manipulations with machine learning models. Any of these might be solved by developing secure mechanisms for authentication and authorization, advanced encryption methods, and attack-resistant AI models. Finally, the article points out the relevance of standardization and the development of international protocols with the aim of guaranteeing interoperability and security of the AIoT systems. Distributed computing, including edge computing, is also fundamental to the decrease in latency and increase in efficiency for the processing of data. The next section shall discuss the need for compliance with legislation on the protection of personal data and privacy and the application of security principles in the whole Cycle of creation and operation of an AIoT system. This paper presents the overall landscape of current challenges and security issues related to the field of AIoT and provides guidelines for researchers, developers, and practitioners on how to integrate AI and IoT efficiently.

Keywords

AIoT, artificial intelligence, integration, protocols, cybersecurity, standardization, data privacy.

BAIT'2024: The 1st International Workshop on "Bioinformatics and applied information technologies", October 02-04, 2024, Zboriv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

stanko.andrjj@gmail.com (A. Stanko); oleksij.duda@gmail.com (O. Duda); mikitishin@gmail.com (A. Mykytyshyn); totosko@gmail.com (O. Totosko); rkorolyuk@gmail.com (R. Koroliuk).

0000-0002-5526-2599 (A. Stanko); 0000-0003-2007-5761 (O. Duda); 0000-0002-2999-3232 (A. Mykytyshyn); 0000-0001-6002-1477 (O. Totosko); 0000-0002-7700-1774 (R. Koroliuk).

1. Introduction

One of the important challenges in integrating AI and IoT is interoperability between disparate devices with different communication protocols. IoT connotes a number of devices from various manufacturers; many of these may have their individual hardware platforms, operating systems, and protocols [1-10]. This leads to a seriously diverse ecosystem where coming up with united solutions enabling devices to effectively provide mutual support.

Hardware heterogeneity means that these devices have different computational powers, memory, and energy resources. Some of them are capable of complex AI algorithms, while others are simple in structure. All this constitutes a big challenge in developing software with which such diverse devices can provide the needed functionality realization [10,53,54,55].

The communication protocols also vary, starting from short-range wireless technologies, including Bluetooth and Zigbee, up to their long-range protocols like LoRaWAN. Others include MQTT, CoAP, and HTTP, among others, which in one way or another have certain advantages and limits. Since there is no preference for the use of a common standard, it becomes hard to integrate devices into applications and could demand additional gateways or protocol converters [11].

Furthermore, the format and model of information are not the same in all devices, which may be an issue during the processing and analysis of the collected information. AI algorithms require relevant and consistent data in order to learn and operate effectively. Such differences in data format only lead to errors or inaccuracies in the models, thereby leading to poor performance [12]. The overriding of some of such challenges calls for the standardization of protocols and data formats. Thus, the adoption of open standards and participation in international standardisation organisations will contribute to systems being interoperable.

The use of middleware serves for abstraction from peculiarities of devices and unification of interaction interface. Certainly, interoperability issues will be improved only in the case of collaboration between manufacturers and developers. An open platform, an ecosystem that allows co-design and knowledge sharing, could really accelerate the integration processes: based on this, a development of semantic technologies and ontologies will enable unification of data models, enabling semantic interoperability among systems [13]. It follows, therefore, that interoperability in devices and protocols forms one critical factor toward ensuring that this integration of AIoT is successfully done. This involves standardization of approaches, collaboration, and innovation both from the perspective of software and hardware.

The AIoT model is subject to constant threats, as shown in Figure 1.

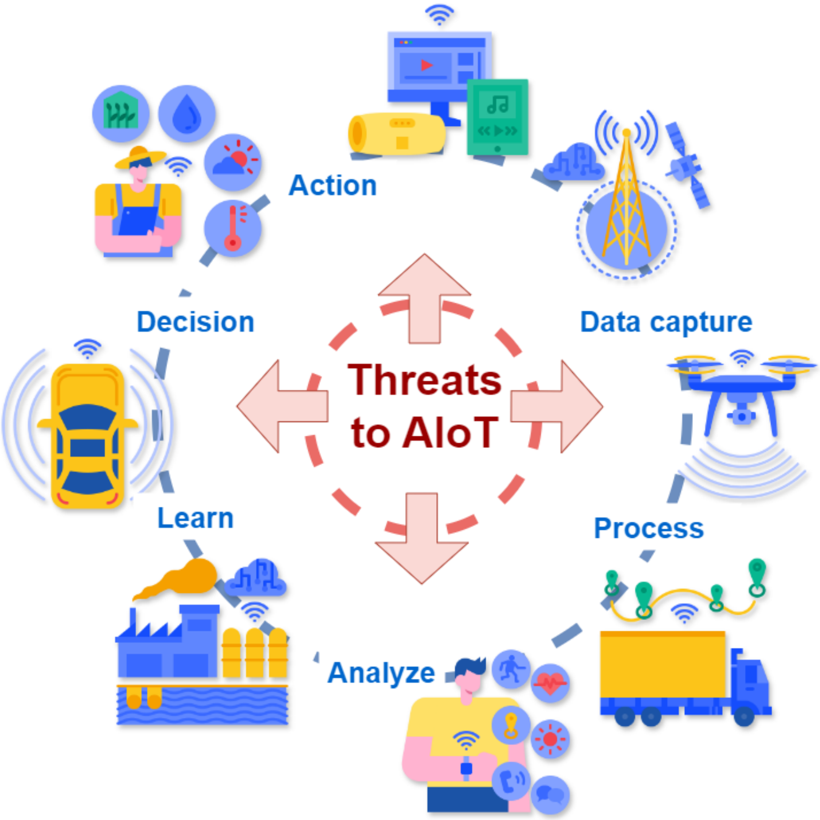

Figure 1: Threats to the elements of the AIoT model.

2. Processing large amounts of data

The integration of AI and IoT generates such huge volumes of data that processing and analysis introduce serious challenges. IoT devices constantly collect data from the environment, sensors, and users that needs to be processed as quickly as possible for real-time decisions. Traditional methods are becoming inefficient and resource-intensive while processing this amount of data. One of the main difficulties is the deficit of computational resources at the IoT device level. Because of these power and memory limitations, most of them cannot run complex AI algorithms. Transferring all collected data to be processed by cloud services may lead to network overload, delays, and swelling security risks [14,56,57].

In such circumstances, edge computing is becoming crucial. Data processing closer to, or even on the device itself, reduces latency and decreases the loads on networks [15]. That will enable preliminary analysis, filtering of the data, and instant decisions without sending data to remote servers. The distributed data processing systems-Hadoop or Spark-can be efficiently implemented and managed. They allow scaling of computing resources and processing of data in parallel, possibilities that significantly speed up the pace of analysis [16]. Optimising the transmission of data by compressing it, aggregating and filtering reduces the amount of information traveling across the network [17]. Such a feature has a particular added value for networks with limited bandwidth or for devices powered with limited power supply.

Another crucial factor during the processing of extensive volumes of data is power consumption. Sometimes, running complex AI algorithms is power-consuming, and IoT devices may not have this power every time. So, energy-efficient algorithm development and the use of some special hardware-like neuromorphic processors-will reduce the power consumption [18]. Besides data security, privacy is another critical issue concerning big data. The data may be used to carry sensitive or personal information; therefore, protection from unauthorized access is required in terms of data. Encryption, anonymization, and access control should be implemented for security [19]. Compliance with legal and regulatory requirements in terms of data processing and storage should not be omitted. An organization should be aware of which law and standards are applicable, if any, such as the general data protection regulation, and design proper policy and procedure accordingly [20].

In general, big data processing in AIoT needs a blend of technical solution, resource optimization, and security management. Meeting these challenges effectively will allow the full exploitation of AIoT's potential and ensure successful implementations either in industry or everyday life.

3. Delays in data transmission

Data latency is a major barrier to AIoT integration, as it can negatively impact system performance, especially for systems operating in real-time. Instant information exchange and fast decision-making are essential for many AIoT applications, including industrial control systems, medical devices, and autonomous vehicles. Many factors, such as limited network bandwidth, heavy traffic, or distance between devices and data centres, can cause delays [21].

In typical IoT systems, data is often sent to cloud servers for processing, which can cause significant delays, especially if network resources are limited. In mission-critical applications where milliseconds can matter, this is not always acceptable. For example, delays in traffic management systems can lead to accidents [22].

The emergence of edge computing, which processes data closer to the data source at the network edge, offers a solution to this problem. Since the data does not need to be transported over long distances for processing, it reduces latency. Real-time pre-analysis, filtering and decision-making can be performed by edge devices, which send only the data that is needed for further analysis or long-term storage to the centre [23].

In addition, because 5G and other high-speed network technologies have higher bandwidth and lower latency, they can significantly reduce data latency. New AIoT applications now have prospects that were previously impossible due to network limitations [24].

Optimising the data transfer protocol is another important factor. Using lightweight protocols such as MQTT or CoAP, which are designed specifically for the Internet of Things, helps to reduce overhead and speed up transmission. These protocols can function well even in low-bandwidth networks because they are designed to work in resource-constrained environments [25]. However, there are circumstances where delays are unavoidable even with these technologies. In such situations, it is crucial that AI algorithms are able to work with old or missing data and are resilient to delays. This requires the creation of systems that can operate autonomously for a certain period of time, as well as algorithms that can predict or fill in missing data [26].

Thus, minimising data delays is essential for successful AIoT integration. This requires a comprehensive strategy that includes the creation of adaptive AI algorithms, optimisation of transmission protocols, and the introduction of new network infrastructure technologies. This is the only way to guarantee the efficient and reliable operation of AIoT solutions in real time.

4. Energy consumption

Another point in implementation that arises as a challenge pertains to power consumption: most IoT devices are either powered on batteries or at very low levels of power input. Adding AI functionality to devices from these classes increases the need for power significantly and amply necessitates recharging the battery more often [27].

Devices with limited resources of energy mostly are unable to perform the complex algorithm calculations required by AI. This therefore constrains the possibilities of integrating AI at the device level, and hence, one has to make a trade-off between functionality and energy efficiency. Another approach is the use of specialized hardware that has been optimized for low-power AI jobs. For instance, neuromorphic processors or Application-Specific Integrated Circuits designed to execute particular AI operations could cut energy costs by an order of magnitude [28].

In addition to that, there needs to be energy-efficient machine learning algorithms and models. This includes developing lightweight models with fewer parameters, using techniques like quantization and pruning to match a model's size without significant loss of accuracy, and low-power modes of operation [29].

Employing edge computing will further help in reducing energy consumption by avoiding the continuous transfer of large volumes of data to the cloud, which is itself an energy-intensive process. Besides, edge devices can carry out simple processing of data and transmit only information needed to the centre [30]. System-level energy management includes dynamic CPU frequency control, hibernation, and resource optimization, which can be developed based on different operating systems. It is also possible to make workloads predictable with the help of intelligent algorithms and include automatic adjustment of energy consumption depending on current needs. It is also important to consider renewable energy sources for the devices powered with solar or kinetic energy. This will help to enhance the autonomy of devices and reduce their dependence on traditional power sources [31]. Generally, energy consumption in AIoT is a multifactor problem that requires both hardware and software solutions. Improving energy efficiency will expand the capabilities of AIoT and contribute to sustainable development in technologies [32].

5. Security issues in AIoT

5.1. Cybersecurity

Most AIoT systems run physical processes and are capable of processing highly sensitive information. These threats, in the field, such as unauthorized access to systems, data leakage, or physical harm, have a great influence. One of the major threats involves unauthorized access to AIoT devices and networks. This means access to the system through exploited software vulnerabilities, poor passwords, or no encryption, attackers would successfully get hold of it, after which they can steal information, disrupt devices, or use them as a part of a botnet to attack other systems [33]. In order to avoid such menace, you need to implement a strong authentication and authorization mechanism. That includes, but is not limited to, the use of strong passwords, multi-factor authentication, security certificates, updating of credentials, etc. In addition, one should not forget about secure key management and usage of cryptographic techniques while 'on the move' and while 'at rest' [34]. One more profound security aspect is data encryption. The use of modern cryptographic algorithms for data encryption makes any kind of interception of information and unauthorized access impossible. This includes data transmitted by means of a network and data stored in devices or the cloud [35]. Another critical issue is the protection against harmful software updates: this means, in other words, the proper implementation of adequate update mechanisms that verify for the integrity and authenticity of new software versions before installing the same. Detection and anomaly monitoring of system behavior enable early detection, thereby allowing timely intervention to counter cyber threats. Use AI to analyze network traffic and device behavior as a means to determine suspicious activities and potential attacks [36]. Table 2 provides an overview of the main security risks associated with AIoT and effective security practices. It also emphasises the importance of a comprehensive approach to security that includes technical, organisational and educational measures.

5.2. Data privacy

In most instances, it is grossly observed that these AIoT systems collect and process personal information of users, which gives way to a series of grave privacy issues, we have proposed a Table of Security Risks in AIoT and Corresponding Protection Methods (Table 1). Improper handling of such data can result in breaches of privacy, discrimination, or other negative consequences. Therefore, privacy necessarily demands compliance with legislation, such as the General Data Protection Regulation (GDPR) by the European Union, and ethical data processing principles should be implemented [37]. User consent to collect and process data in a system means the need for transparency over what data is collected and how it is used. Users should be empowered with a say as regards the use of their data. Data anonymization and pseudonymization provide privacy protection by eliminating or masking personal information. Results from these enable data use for analytics and AI without revealing the individual users' identities [38]. Moreover, access to personal information should only be provided to those who have been authorized, and such data must be protected well enough from unauthorized access [39]. Potential vulnerabilities can be detected and eliminated only through regular audits and security checks [40].

Table 1
Security Risks in AIoT and Corresponding Protection Methods

Security Risk	Description	Protection Methods
Excessive Data Collection	Attackers may gain access to devices or networks using vulnerabilities or weak passwords.	- Implement strong authentication and authorization - Use multi-factor authentication - Regularly update credentials
Lack of Transparency in Data Processing	Overloading the system with requests to disrupt its operation.	- Implement mechanisms to detect and block DoS attacks - Use firewalls and intrusion prevention systems (IPS)
Improper Data Storage and Transmission	Inserting malicious or incorrect data to distort AI models' operation.	- Validate and verify training data - Use anomaly detection methods - Develop robust AI algorithms resistant to attacks
Unauthorized Access to Personal Data	Manipulating input data to cause AI models to produce incorrect outputs.	- Implement defenses against adversarial examples - Regularize and enhance model robustness - Monitor AI outputs for anomalies
Lack of Right to Erasure ("Right to be Forgotten")	Installing malicious software through counterfeit updates or components.	- Verify integrity and authenticity of updates - Use digital signatures - Control suppliers and partners

5.3. AI algorithms security

The AI algorithms used in the AIoT systems can be targeted by various forms of attacks. For instance, poisoning attacks are performed by manipulating input or training data with the intent of skewing the model's output. In turn, it would result in incorrect decisions that, within the context of AIoT, can have serious consequences [41].

Another type of threat is that of attacks through the injection of crafted input data, causing the model to make mistakes or generate certain results. They are called adversarial example attacks. For such types of threats, attack-resistant AI models need to be developed. It includes regularization, integrity checks of training data, monitoring abnormal model behavior, and providing explainable AI mechanisms to clear up how the model makes its decisions [42].Besides, it's relevant to ensure security in infrastructures where AI algorithms are executed on the servers, databases, and networks against cyber threats. This is highly in contrast to routine cybersecurity training of staff, as well as the development and application of security policies [43].

Thus, security issues in AIoT are multifaceted and require a comprehensive approach. Ensuring cybersecurity, data privacy protection, and the security of AI algorithms are critical for user trust and the successful implementation of AIoT technologies in various spheres of life [44].

6. Solutions

The workable integration of AIoT into life is impossible without solving such problems as interoperability, processing of data, security, and meeting the regulatory requirements comprehensively. Below we consider the basic ways of solving listed problems.

6.1. Standardisation

Interoperability between the huge number of devices and systems is a key role that standardisation plays in AIoT. Interoperability issues arise due to the lack of standards common for the market unification; this seriously complicates integration of newer technologies. The use of common applied communication protocols, data formats, and interfaces will make the devices of different manufacturers intercommunicate easily. ISO, IEEE, IETF, and many international organizations are working on the development of standards related to IoT and AI. For example, the IEEE 2413 standard defines an architecture for IoT that promotes interoperability and security [45].

Standardization will enhance the security of AIoT. Security standards allow for the definition of the necessary level of protection against diverse cyber threats, such as IEC 62443 for industrial systems. Their adoption minimizes any weaknesses and inspires more user confidence in AIoT technologies [46]. Besides contributing to various standardization processes, which give organizations an opportunity to have their say in developing the industry and ensuring that standards meet the organization's needs, manufacturers and developers must work together with the regulators. They constitute a vital part of successful standardization processes that are the major interoperability barriers.

6.2. Distributed data processing

Distributed data processing is an efficient approach to managing large amounts of information in AIoT systems. The use of:

- Edge computing for data processing near devices with reduced latency and network load. This is invaluable for real-time applications like autonomous vehicles or industrial control systems [47].
- Fog computing provides complementary services by introducing data processing closer to the cloud, reducing the distance between devices and data centers. Fog nodes can conduct some initial processing, aggregate data, and enhance another layer of security.
- Cloud computing remains essential for large data storage over the long term and power-intensive AI workloads, including machine learning model training. Combining edge, fog, and cloud creates a comprehensive system that maximizes resource utilization and reliability [48].

6.3. Secure software

The basic protection against cyber threats of AIoT systems is to develop secure software. Security integration at all development phases, from design to testing, makes it possible to address vulnerabilities before attackers can exploit them. Security by Design principles involve embedding security mechanisms within the system architecture. Employ strong authentication and authorization, use the latest cryptographic algorithms to encrypt data, and ensure information integrity [49]. Regularly downloading and installing software updates and patches is crucial. Detecting anomalous behavior through security monitoring tools helps to quickly respond to and contain threats. Security testing, including penetration testing and code analysis, is essential for identifying vulnerabilities [50].

6.4. Regulation and legal compliance

Compliance with laws and regulations is extremely important in the successful operation of AIoT systems. Personal data protection laws (e.g., GDPR in the European Union, CCPA in California) significantly raise the requirements for assessments when collecting and processing personal information. Organizations must be transparent about the data they collect and its intended use, while also seeking explicit user consent [51]. It is critically important to enact and enforce data processing rules by specifying policies and procedures, as well as appointing oversight personnel, such as a privacy officer. Another key aspect is adherence to ethical principles in AI development and usage, including preventing unlawful surveillance, safeguarding against algorithmic bias, and ensuring that AI decisions are open to inspection [52].

Conclusions

Artificial intelligence of things (AIoT) is a powerful convergence of two of the leading technologies of our time: Internet of Things (IoT) and artificial intelligence (AI). The combination of IoT data collection and transmission capabilities with intelligent AI algorithms opens up new horizons for innovation in various fields, including industry, healthcare, transport, and everyday life. However, the integration of these technologies is accompanied by a number of challenges that require careful analysis and resolution.

One of the main challenges is device and protocol compatibility. The variety of hardware, operating systems and communication protocols makes it difficult to interoperate between devices from different manufacturers. The lack of common standards leads to market fragmentation and increases the complexity of system integration. This problem can be solved through active standardisation, participation in international organisations and cooperation between manufacturers and developers.

Processing large amounts of data is another critical aspect. IoT devices generate huge amounts of information that need to be processed and analysed efficiently. Distributed data processing, including the use of edge and fog computing, can optimise the use of computing resources and reduce latency. The integration of different computing layers creates a flexible and scalable architecture that meets the requirements of different applications.

Security issues in AIoT are extremely important. The growing number of connected devices increases the potential risks of cyber threats. Developing secure software that takes into account security principles at all stages of the life cycle is essential to protect systems from attacks. The use of modern authentication methods, encryption and regular software updates help to improve security.

Regulation and compliance are essential to ensure confidentiality and protection of personal data. Compliance with international and local laws, such as GDPR, as well as the implementation of ethical principles in the development and use of AI, contribute to user trust and the successful implementation of AIoT technologies.

This article analyses in detail the main challenges of AIoT integration and suggests ways to overcome them. Standardisation, distributed data processing, secure software development, and legal compliance are key components of a comprehensive approach to addressing the challenges.

Recommendations for future research and practice include:

- Active engagement in standardisation processes to promote interoperability and interoperability of systems.
- Developing new technologies and data processing methods that increase the efficiency and scalability of AIoT.
- Improving cybersecurity through the implementation of advanced security methods and ongoing staff training.
- Adherence to ethical standards and legislation governing data processing and use to ensure user privacy and trust.

Artificial intelligence of things has the potential to radically change various aspects of our lives, increasing efficiency, comfort and safety. However, in order to realise this potential, it is necessary to overcome the existing challenges and ensure that AIoT technologies are developed responsibly and ethically. Collaboration between academia, industry, government organisations, and society at large is key to a successful AIoT future.

References

[1] Grzesik, P., & Mrozek, D. (2024). Combining Machine Learning and Edge Computing: Opportunities, Challenges, Platforms, Frameworks, and Use Cases. «Electronics», 13(3), 640.

[2] Fagbohungbe, O., Reza, S. R., Dong, X., & Qian, L. (2022). Efficient Privacy Preserving Edge Intelligent Computing Framework for Image Classification in IoT. «IEEE Transactions on Emerging Topics in Computational Intelligence».

[3] Gudnavar, A., & Naregal, K. (2023). Edge Computing in Internet of Things (IoT): Enhancing IoT Ecosystems through Distributed Intelligence. «AIoT and Big Tech in Industry Applications», 2(3), 001.

[4] Yan, S., Zhang, P., Huang, S., Wang, J., Sun, H., Zhang, Y., & Tolba, A. M. (2023). Node Selection Algorithm for Federated Learning Based on Deep Reinforcement Learning for Edge Computing in IoT. «Electronics», 12(11), 2478.

[5] Garg, S., Kaur, K., Kaddoum, G., Prasad, G., & Aujla, G. (2021). Security in IoT-Driven Mobile Edge Computing: New Paradigms, Challenges, and Opportunities. «IEEE»

[6] Song, J., Gu, T., & Mohapatra, P. (2021). How BlockChain Can Help Enhance The Security And Privacy in Edge Computing? «Proceedings of the 22nd ACM International Conference on Mobile Computing and Networking».

[7] Ganesh, D., Suresh, K., Kumar, M. S., Balaji, K., & Burada, S. (2022). Improving Security in Edge Computing by using Cognitive Trust Management Model. «IEEE International Conference on Electronics and Communication & Aerospace Technology».

[8] Zheng, J., & Zhang, Y. (2024). RSHS: A Blockchain Consensus Mechanism for Edge Computing-Supported Agri-IoT Systems. «IEEE TNSM».

[9] Yan, S., Zhang, P., Huang, S., Wang, J., Sun, H., Zhang, Y., & Tolba, A. M. (2023). Node Selection Algorithm for Federated Learning Based on Deep Reinforcement Learning for Edge Computing in IoT. «Electronics», 12(11), 2478.

[10] Liu, Y., Hassan, K. A., Karlsson, M., Pang, Z., & Gong, S. (2019). A Data-Centric Internet of Things Framework Based on Azure Cloud. «IEEE Access».

[11] Rubí, J. N., & Gondim, P. (2020). IoT-based platform for environment data sharing in smart cities. «International Journal of Communication Systems».

[12] Ji, G., Woo, J., Lee, G., Msigwa, C., Bernard, D., & Yun, J. (2024). AIoT-Based Smart Healthcare in Everyday Lives: Data Collection and Standardization From Smartphones and Smartwatches. «IEEE Internet of Things Journal».

[13] Rubí, J. N., & Gondim, P. (2020). Interoperable Internet of Medical Things platform for e-Health applications. «International Journal of Distributed Sensor Networks».

[14] Tulkinbekov, K., & Kim, D. (2022). Blockchain-Enabled Approach for Big Data Processing in Edge Computing. «IEEE Internet of Things Journal».

[15] Ezeugwa, F. A. (2024). Evaluating the Integration of Edge Computing and Serverless Architectures for Enhancing Scalability and Sustainability in Cloud-based Big Data Management. «Journal of Engineering Research and Reports».

[16] Yang, L. (2024). Heterogeneous Internet of Things Big Data Analysis System Based on Mobile Edge Computing. «International Journal of Distributed Sensor Networks».

[17] Bajić, B., Suzić, N., Morača, S., Stefanovic, M., Jovicic, M., & Rikalovic, A. (2023). Edge Computing Data Optimization for Smart Quality Management: Industry 5.0 Perspective. «Sustainability».

[18] Samriya, J. K., Kumar, M., & Gill, S. (2023). Secured data offloading using reinforcement learning and Markov decision process in mobile edge computing. «International Journal of Network Management».

[19] Shen, Z., Jin, J., Zhang, T., Tagami, A., Higashino, T., & Han, Q. (2022). Data-Driven Edge Computing: A Fabric for Intelligent Building Energy Management Systems. «IEEE Internet of Energy Magazine».

[20] Garg, S., Singh, A., Kaur, K., Aujla, G., Batra, S., Kumar, N., & Obaidat, M. (2019). Edge Computing-Based Security Framework for Big Data Analytics in VANETs. «IEEE».

[21] Devi, K. V. R., Koithyar, A., Lakhanpal, S., Parmar, A., Sethi, V. A., & Ftaiet, A. A. (2023). Edge Computing and 5G Integration for Real-time Analytics in Interoperable Smart Grids. «IEEE International Power and Energy Conference».

[22] Shaik, R., Raju, D., Behera, P. C., Changala, R., Mary, S. C., & Balakumar, A. (2024). Real-Time Anomaly Detection in 5G Networks Through Edge Computing. «IEEE».

[23] Jain, P., Pateria, N., Anjum, G., Tiwari, A., & Tiwari, A. (2024). Edge AI and On-Device Machine Learning For Real Time Processing. «International Journal of Innovative Research in Computer and Communication Engineering».

[24] Spicher, N., Klingenberg, A., Purrucker, V., & Deserno, T. (2021). Edge computing in 5G cellular networks for real-time analysis of electrocardiography recorded with wearable textile sensors. «IEEE EMBC».

[25] Li, X., & Ye, B. (2021). Latency-Aware Computation Offloading for 5G Networks in Edge Computing. «Security and Communication Networks».

[26] Shanthakumar, C. S. T., Harish, N., Eshanya, & Giridharan, A. (2023). Internet of Things and Edge Computing for Real Time Applications. «IEEE IITCEE».

[27] Liu, Y., Chen, Y., Ye, W., & Gui, Y. (2022). FPGA-NHAP: A General FPGA-Based Neuromorphic Hardware Acceleration Platform With High Speed and Low Power. «IEEE Transactions on Circuits and Systems I: Regular Papers».

[28] Liu, C., Yang, Z., Zhang, X., Zhu, Z., Chu, H., Huan, Y., Zheng, L., & Zou, Z. (2023). A Low-Power Hybrid-Precision Neuromorphic Processor With INT8 Inference and INT16 Online Learning in 40-nm CMOS. «IEEE Transactions on Circuits and Systems I: Regular Papers».

[29] Zhang, Q., Cui, M., Liu, Y., Chen, W., & Yu, Z. (2024). Low-Power and Low-Cost AI Processor with Distributed-Aggregated Classification Architecture for Wearable Epilepsy Seizure Detection. «IEEE Transactions on Biomedical Circuits and Systems».

[30] Ren, J., Yu, Z., Xing, T., Cui, H., Chen, Y., & Guo, B. (2023). EnergySense: A Fine-Grained Energy Analysis Framework for DNN Processing with Low-Power Ubiquitous Sensors. «IEEE Southwest Symposium on Image Analysis and Interpretation».

[31] Rácz, A., Veres, A., Hága, P., Borsos, T., & Kenesi, Z. (2022). A Full-Stack Neuromorphic Prototype Architecture for Low-Power Wireless Sensors. «IEEE Global Communications Workshops».

[32] Liu, S., Wu, Z., He, Z., Chen, W., Zhong, X., Guo, B., Liu, S., Duan, H., Guo, Y., Zeng, J., & Liu, G. (2024). Low-Power Perovskite Neuromorphic Synapse with Enhanced Photon Efficiency for Directional Motion Perception. «ACS Applied Materials & Interfaces».

[33] More, P., Sakhare, S. R., & Mahalle, P. (2023). Identity-Based Access Control in IoT: Enhancing Security through Mutual Cryptographic Authentication and Context Awareness. «IEEE International Conference on Mobile Networks and Wireless Communication».

[34] Nandhini, M., & Sumalatha, V. (2023). SSS-EC: Cryptographic based Single-Factor Authentication for Fingerprint Data with Machine Learning Technique. «IEEE».

[35] Chubaievskyi, V., Lutska, N., Savchenko, T., Vlasenko, L., & Synelnyk, K. (2023). Enhanced Cryptographic Security of Aggregated Digital Signatures through Utilization of a Unified Authentication Framework. «Cybersecurity».

[36] Ahmad, S., Arya, S. K., Gupta, S., & Dwivedi, S. (2023). Study of Cryptographic Techniques Adopted in Blockchain. «IEEE ICIEM».

[37] Issaoui, A., Örtensjö, J., & Islam, M. S. (2023). Exploring the General Data Protection Regulation (GDPR) compliance in cloud services: insights from Swedish public organizations on privacy compliance. «Financial Innovation».

[38] Razak, S. A., Mohd Nazari, N. H., & Al-dhaqm, A. (2020). Data Anonymization Using Pseudonym System to Preserve Data Privacy. «IEEE Access».

[39] Davari, M., & Bertino, E. (2019). Access Control Model Extensions to Support Data Privacy Protection based on GDPR. «IEEE Big Data».

[40] Marques, J. F., & Bernardino, J. (2020). Analysis of Data Anonymization Techniques. «International Conference on Data Science, E-learning and Information Systems».

[41] Zhang, J., Song, B., Han, B., Liu, L., Niu, G., & Sugiyama, M. (2023). Assessing Vulnerabilities of Adversarial Learning Algorithm through Poisoning Attacks. «arXiv».

[42] Zheng, H., Zhao, J., & Tan, W. (2022). An Adversarial Defense Algorithm Based on Triplet Network and Voting Decision. «IEEE ICUS».

[43] Bouaziz, A., Nguyen, M.-D., Valdés, V., Cavalli, A., & Mallouli, W. (2023). Study on Adversarial Attacks Techniques, Learning Methods and Countermeasures: Application to Anomaly Detection. «International Conference on Information Systems Security and Privacy».

[44] Ali, M., Hu, Y.-F., Luong, D., Oguntala, G., Li, J.-P., & Abdo, K. (2020). Adversarial Attacks on AI based Intrusion Detection System for Heterogeneous Wireless Communications Networks. «IEEE DASC».

[45] Katrakazas, P., Kallinolitou, T., Markopoulou, S., & Chronopoulou, A. (2022). A Toolchain and Interoperability Framework to enhance privacy and individual control at the Edge. «IEEE ISC».

[46] Prokhorenkov, D. (2022). Alternative Methodology and Framework for Assessing Differential Privacy Constraints and Consequences From a GDPR Perspective. «IEEE».

[47] Liu, Y., Hassan, K. A., Karlsson, M., Pang, Z., & Gong, S. (2019). A Data-Centric Internet of Things Framework Based on Azure Cloud. «IEEE Access».

[48] Tulkinbekov, K., & Kim, D. (2022). Blockchain-Enabled Approach for Big Data Processing in Edge Computing. «IEEE Internet of Things Journal».

[49] Song, J., Gu, T., & Mohapatra, P. (2021). How BlockChain Can Help Enhance The Security And Privacy in Edge Computing? «ACM International Conference on Mobile Computing and Networking».

[50] Ezeugwa, F. A. (2024). Evaluating the Integration of Edge Computing and Serverless Architectures for Enhancing Scalability and Sustainability in Cloud-based Big Data Management. «Journal of Engineering Research and Reports».

[51] Issaoui, A., Örtensjö, J., & Islam, M. S. (2023). Exploring the General Data Protection Regulation (GDPR) compliance in cloud services: insights from Swedish public organizations on privacy compliance. «Financial Innovation».

[52] Khalid, M. I., Ahmed, M., & Kim, J. (2023). Enhancing Data Protection in Dynamic Consent Management Systems: Formalizing Privacy and Security Definitions with Differential Privacy, Decentralization, and Zero-Knowledge Proofs. «Sensors».

[53] Stukhliak, P., Martsenyuk, V., Totosko O., Stukhlyak, D., Didych, I. (2024). The use of neural networks for modeling the thermophysical characteristics of epoxy composites treated with electric spark water hammer. CEUR Workshop ProceedingsVolume 3742, CITI 2024. Ternopil 2nd International Workshop on Computer Information Technologies in Industry 4.0, Pages 13 – 242024.

[54] Yasniy, O., Mykytyshyn, A., Didych, I., Kubashok, V., & Boiko, A. (2023). Application of artificial intelligence to improve the work of educational platforms. In ITTAP (pp. 605-609).

[55] Zhukovskyy, V., Shatnyi, S., Zhukovska, N., & Sverstiuk, A. (2021). Neural Network Clustering Technology for Cartographic Images Recognition. In IEEE EUROCON 2021 - 19th International Conference on Smart Technologies. IEEE EUROCON 2021 - 19th International Conference on Smart Technologies. IEEE.

[56] Martsenyuk, V., Klos-Witkowska, A., Sverstiuk, A., Bahrii-Zaiats O., Bernas, M., Witos, K. (2021). Intelligent big data system based on scientific machine learning of cyber-physical systems of medical and biological processes. CEUR Workshop Proceedings, 2864, pp. 34–48.

[57] Duda, O., Mykytyshyn, A., Mytnyk M., Stanko, A. (2023). Information technology sets formation and "TNTU Smart Campus" services network support. In 2nd International Workshop on Information Technologies: Theoretical and Applied Problems 2023, Ternopil, pp. 93-105.