

# Artificial Intelligence-based threat detection and prevention methods for securing Internet of Things devices

Gavxar Turdieva<sup>\*a</sup>, Firuza Sadikova<sup>a</sup>, Komiljon Qobilov<sup>b</sup>, Gulchiroy Ruziyeva<sup>a</sup>  
<sup>a</sup>Bukhara State University, 11, M. Iqbol Street, Bukhara, Uzbekistan

## ABSTRACT

This article discusses methods for early threat detection and prevention using artificial intelligence to ensure the security of Internet of Things devices. Numerous scientific studies by scientists on this topic and the experimental methods used are studied and analyzed. Ways to improve the security of Internet of Things devices using Artificial intelligence -based systems such as machine learning and deep learning, the impact of network attacks on Internet of Things devices, anomaly detection using artificial intelligence, anomaly prevention, mitigation of the effects of attacks, and promising solutions for cyber threat management are analyzed. The most important methods for preventing and detecting threats are analyzed and proposed, such as anomaly detection, attack type classification, predictive analysis, real-time analysis, adaptability to resource-constrained devices, and vulnerability detection in the network. As a result of research and analysis, an Internet of Things security architecture is developed and described that uses artificial intelligence technologies to improve security and detect threats. The results of the study are aimed at promoting advanced research and the development of practical software solutions for using artificial intelligence -based systems to ensure the security of Internet of Things devices used in various fields.

**Keywords:** cybersecurity, artificial intelligence, machine learning, cybersecurity systems, security protocols, data protection, encryption algorithms, authentication methods, cyber threats, Internet of Things devices, network security, intrusion detection systems, internet of Things standards

## 1. INTRODUCTION

The Internet of Things is a new technology that enables communication via the internet between electronic devices and sensors to simplify human life. The Internet of Things has seen a progression and a significant growth of communication and software technologies, which has shaped everyday life, leading the world into a new era of "Smart Things,"<sup>5</sup> where millions of objects are connected to one and other by sharing, communicating, and sensing information[1]. Internet of Things uses smart devices and the internet to offer innovative solutions to problems in business, government, and private sectors. The Internet of Things is billions of physical objects or "things" connected to the Internet, collecting data and exchanging it over the Internet with other devices and systems. IoT is an innovation that unites various intelligent systems, frameworks, and devices. Today, Internet of Things has already become an important part of our lives.

The concept of Internet of Things was developed in 1999 by a member of the Radio-Frequency Identification developer community and has recently become relevant to the practical world mainly due to the growth of mobile devices, embedded and ubiquitous connectivity, cloud computing, and data analysis. [4]

Internet of Things devices can range from small, simple household kitchen appliances to complex industrial equipment. Each Internet of Things component has a unique identifier, and they have the ability to transmit data even without human intervention.

Internet of Things devices are most common in the transportation industry, manufacturing, and utilities. Additionally, they have numerous applications in agriculture, infrastructure, and home automation.

\* gavharturdiyeva7@gmail.com

According to a 2024 analysis, there are currently over 15 billion Internet of Things devices connected worldwide. The number of active Internet of Things devices is expected to double by 2030. In society, approximately 2 out of 3 devices use Internet of Things. According to the latest available data, there are approximately 17.08 billion Internet of Things devices connected worldwide. This figure is expected to almost double by 2030, reaching 29.42 billion [5].

Several factors contribute to the rapid spread of the Internet of Things.

First of all, technological progress has led to the development of sensors, microchips and wireless communication technologies, which has made it possible to create many cheap Internet of Things device options. The widespread use of cloud computing services has made it possible to store, process and analyze large amounts of data received from Internet of Things devices. With the help of this data, it is possible to increase efficiency, reduce costs and create new services in various industries, including manufacturing, transport, healthcare and agriculture. In addition, the availability of mobile internet and the widespread use of smartphones have also contributed to the development of Internet of Things. Smartphones are a convenient interface for managing Internet of Things devices and receiving data from them. The acceleration of information flow and the awareness of businesses and consumers about the benefits of the Internet of Things are also an important factor in the popularization of Internet of Things devices. Companies are able to optimize operations, create new sources of income and improve customer relations with the help of Internet of Things.

Finally, Internet of Things support policies from governments and standardization efforts also contribute to the development of the Internet of Things ecosystem.

With the popularization of Internet of Things devices in various fields and the growing security threats to them, the issue of protecting Internet of Things devices from attacks is becoming increasingly relevant. Many Internet of Things devices, particularly cheap and simple ones, are not sufficiently secure from a security point of view. These devices do not support complex security protocols, use default passwords, or are not password-protected at all. As a result, such Internet of Things devices become targets for cyberattacks.

Security threats in Internet of Things devices can affect not only the devices themselves but also the entire network system. Attackers can discover vulnerable Internet of Things devices, create botnets from them, steal data, or carry out Distributed Denial of Service attacks. In such cases, serious damage can also be done to privacy issues related to the collection and transmission of personal data by Internet of Things devices.

Taking security measures for Internet of Things devices and using artificial intelligence systems has become one of the urgent tasks of today. In ensuring the security of Internet of Things devices, threat detection based on artificial intelligence is a much more advanced and effective approach than traditional methods. It has the ability to detect anomalies, adapt to changing threats, and optimize resources. Artificial intelligence-based systems constantly monitor the behavior of Internet of Things devices and quickly detect unusual activities, issuing warnings for their elimination. In addition, artificial intelligence can learn and adapt using machine learning algorithms, which ensures continuous improvement of security measures and provides important advantages in the fight against emerging threats. However, when applying artificial intelligence in IoT systems, a number of problems must be addressed, such as the availability of a high-quality dataset for training artificial intelligence models, the reliability of algorithms, and privacy issues.

## **2. TYPES OF THREATS TO INTERNET OF THINGS DEVICES AND METHODS OF THEIR DETECTION USING ARTIFICIAL INTELLIGENCE**

As society becomes more technologically advanced, the number of types of the Internet of Things is also growing. These mainly include the following areas:

- Internet of Things for data transmission. This type of Internet of Things devices transmits data over the Internet, such as sensors in thermometers or temperature control devices.
- Smart things for the home. These include "Smart Home" systems, such as smart lamps, thermostats, and surveillance cameras. These devices provide user convenience and help save energy.
- Internet of Things devices in healthcare. Medical devices for monitoring a patient's condition, such as smartwatches that measure heart rate, or remote patient monitoring systems.

- Internet of Things devices in trade. These include Internet of Things devices that automate workflows in retail outlets, such as devices for monitoring supply chains and controlling inventory.
- Internet of Things devices in industry. Internet of Things devices are used to optimize industrial processes, monitor equipment, and effectively manage services.
- Internet of Things devices in transport and automobiles: These devices are used in intelligent vehicles, in logistics, and as sensors that optimize transport systems.
- Smart cities based on Internet of Things: Cities that use innovative Internet of Things solutions to improve infrastructure and public services. Such cities are called "smart cities" and aim to improve quality of life, efficient use of resources, and ensure sustainable development.

Threat types for Internet of Things devices are presented in the following Table 1:

Table 1. Threats to Internet of Things devices.

| Types of threats targeting Internet of Things devices | Adverse consequences of threats   | Threat prevention measures  |
|---|---|---|
| Distributed Denial of Service                         | Blocking Internet of Things devices/networks can lead to devices being disconnected from the network or slowing down.   | Network traffic filtering, rate limiting, anomaly detection   |
| Man-in-the-Middle                                     | Reads and steals data between Internet of Things devices, can manipulate device behavior.   | End-to-end encryption, use of secure communication protocols (Transport Layer Security) /(Secure Sockets Layer) |
| Eavesdropping   | Unauthorized access to personal information through unsecured channels, eavesdropping on transmitted data.  | Secure encryption, use of Virtual Private Network   |
| Brute-force Attacks                                   | Guessing and stealing weak passwords through automated attempts, appropriation of personal data, modification and manipulation of device functions.   | Strong password policy, account lockout, successful authentication mechanisms                                   |
| Firmware Tampering                                    | May lead to unstable operation of devices, including the shutdown of home security systems, smart light control, and other devices. Devices will not be able to receive available updates and security patches. | Strong authentication, firmware encryption, secure boot, digital signatures, regular updates.                   |
| Device Hijacking                                      | Attackers seizing control of devices to perform malicious tasks, control smart home systems, security cameras, or industrial equipment.   | Access control lists, multi-factor authentication   |
| Data Injection  | Entering incorrect data to hack or deceive systems  | Data verification, access filtering   |
| Replay Attacks  | Reusing existing data packets obtained for action imitation can lead to malicious actions such as disabling surveillance cameras or opening doors.  | It is essential to use timestamps, session tokens, strong authentication and encryption systems.                |
| Malware:  | Access to and control over devices can be gained by deploying malware on them. This creates opportunities for attackers who want to control devices, steal data, or use them.                                   | Strong and complex passwords Two-Factor Authentication, software updates, installing security patches           |

Threat and vulnerability detection has reached enormous proportions and is becoming a problem for perimeter protection and human-controlled information and communication technologies data systems. Cyberattacks are becoming much more complex and very destructive, and the risks of such dangerous technologies falling into the hands of malicious actors and competitors are also increasing [5].

Threat and vulnerability detection has reached enormous proportions and has become a problem for protecting the perimeter and data of human-managed information and communication technologies systems. Cyberattacks are becoming increasingly sophisticated and destructive, and the risk of such dangerous technologies falling into the hands of attackers and competitors is increasing.

It is necessary to identify threats targeting Internet of Things devices in advance and take measures to prevent them. The use of artificial intelligence systems to prevent threats is becoming a necessity.

Artificial intelligence methods, such as machine learning, anomaly detection, and predictive analytics, are increasingly being used to monitor, identify, and respond to potential threats in real time. These technologies help identify patterns of unusual behavior, predict potential vulnerabilities, and automate responses to reduce risks.

The integration of artificial intelligence and the Internet of Things creates a new technological ecosystem called Artificial Intelligence of Things. The combination of these two technologies expands the functionality of internet of things devices, turning them from simple data collectors into autonomous systems capable of analyzing, learning, and making decisions in real time. The creation of Artificial Intelligence of Things has opened up new ways to develop automation with the possibility of using internet of things infrastructures in various industries [7].

Artificial intelligence -powered threat detection in internet of things security is a far more advanced and effective method compared to traditional approaches. This approach involves the use of machine learning and deep learning algorithms to identify and prevent various attacks coming through internet of things devices.

This approach includes the following key aspects.

1. Anomaly Detection: Artificial intelligence algorithms can learn normal network traffic activity and identify deviations that may indicate malicious activity [3].

Artificial intelligence algorithms are trained to detect unusual actions (anomalies) in the operation of internet of things devices. These actions differ from typical user actions and are flagged as a potential threat. For example, unusually high data transmission, unusually high energy consumption, unusually frequent connections, and other anomalies can be detected.

This method creates a profile of the normal operation of an internet of things device and then identifies actions outside this profile as anomalies. The profile based on normal activity can be created using data collection and statistical methods or machine learning algorithms.

For anomaly detection, algorithms such as One-Class Support Vector Machine for One-Class Classification, Isolation Forest, Autoencoder, Local Outlier Factor type algorithms, and deep learning methods such as Recurrent Neural Network are used. The advantages of this method are its robustness to dataset imbalance and good results in detecting new types of attacks. However, there can be many false positives.

2. Classification of attack types: Artificial intelligence algorithms can be trained to classify different types of attacks (Distributed Denial of Service, Structured Query Language injections, man-in-the-middle, etc.). This helps to apply effective protection measures against each type of attack. This requires a set of labeled threats for training. Algorithms such as Decision Trees, Random Forests, support vector machine, Cable News Network, Recurrent Neural Network are used in this method. Advantages: allows you to determine the type of threat and take appropriate measures. However, large amounts of data are required, and difficulties may arise in detecting new types of attacks.

3. Predictive analysis: Artificial intelligence algorithms analyze data to predict future attacks. This allows for proactive protection measures and helps prevent attacks.

Time series analysis models AutoRegressive Integrated Moving Average, Long Short-Term Memory and neural networks can be used in predictive analysis. Advantage: provides proactive protection. However, the accuracy of the forecast is not guaranteed.

4. Real-time analysis: An Artificial intelligence -based security system receives and analyzes data from internet of things devices in real time. This provides a quick response and faster elimination of attacks.

5. Adaptability to devices with limited resources: Most internet of things devices have limited resources. Therefore, Artificial intelligence algorithms should be adaptable to these devices and require fewer resources. This requires the use of lightweight models and efficient computing technologies.

6. Detection of network vulnerabilities: Artificial intelligence algorithms can be used to detect network vulnerabilities. For example, the task is to find an insecure password, outdated software, and other various vulnerabilities. This method can detect security vulnerabilities in internet of things devices and use static and dynamic code analysis, fuzzing, and other methods.

Machine learning algorithms can be applied to detect vulnerabilities based on code analysis results. Advantage: helps prevent potential threats. However, detection of all vulnerabilities is not guaranteed.






| ARTIFICIAL INTELLIGENCE METHODS FOR ENSURING IOT SECURITY   |  |
|---|--|
| Technique   | Application in <b>internet of things</b> Security  |
|  Machine Learning                  | <b>Used for detection, classification, and prediction of anomalies in network traffic.</b>   |
|  Deep Learning                     | <b>Pattern recognition is used to analyze complex and fuzzy data. For example, deep neural networks provide high accuracy in attack detection.</b> |
|  Natural Language Processing (NLP) | <b>Threat detection from logs and texts. Used to analyze messages from internet of things devices.</b>   |
|  Predictive Analytics              | <b>Predicting potential security incidents.</b>  |
|  AI-driven Automation              | <b>Automated threat response and mitigation.</b>   |

Figure 1. Artificial intelligence methods for ensuring internet of things security.

The choice of security method depends on the type of data, device resources, required accuracy, and other factors. Often, the best results come from a combination of several methods. In addition, a large and high-quality dataset is needed to train and evaluate the Artificial intelligence model.

### 3. ARTIFICIAL INTELLIGENCE -BASED METHODS FOR PREVENTING IOT DEVICE THREATS

Creating an automated security policy for internet of things devices using artificial intelligence involves assessing existing attack surfaces and protecting against vulnerabilities. Artificial intelligence optimizes the operation of internet of things devices, enhancing their functionality. Automation of processes is essential for improving internet of things security and addressing internet of things -related incidents. Developing and implementing an automated security policy to protect internet of things devices using artificial intelligence requires consideration of technical and organizational aspects.

The process of developing an automated security policy to protect internet of things devices using artificial intelligence includes several components:

Inventory and classification (Internet of things discovery): This is the process of collecting information about connected devices on the network, at this stage the type of device and its characteristics are determined. Scans the network to identify all internet of things devices. Classification is carried out according to functions, vulnerabilities, level of access, and criticality.

Telemetry collection and activity monitoring: the process of collecting data on the activity and status of devices, telemetry may include device performance indicators, such as performance, resource utilization, and other parameters. Main tasks: monitoring network activity, device telemetry, logs, security incidents.

Sending data for analysis: The collected data is sent for analysis for further processing. This may include sending to cloud data storage, transferring to a specialized analysis server, or using special APIs for integration with analytical platforms. It is important to ensure the security and integrity of data during transmission, using encryption and other protection methods.

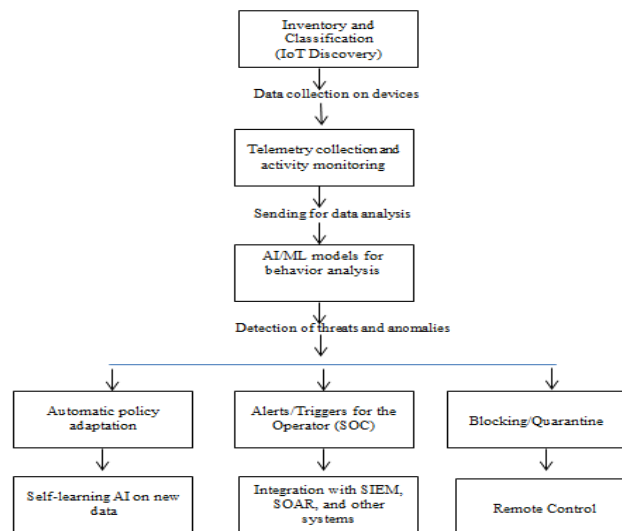


Figure 2. Artificial intelligence -enhanced internet of things security architecture.

Using Artificial intelligence/Machine Learning models for analysis: applying artificial intelligence and machine learning algorithms to analyze data and identify patterns in device behavior. These models can be used to detect anomalies, predict future actions, and optimize system performance. In particular, the following methods can be used for analysis:

- Clustering allows grouping devices with similar behavior to identify common trends and patterns. For example, identifying groups of devices with high network load or devices that are frequently attacked. Algorithms such as K-means, Density-based spatial clustering of applications with noise, and hierarchical clustering are often used for this.
- Classification allows determining to which class a device belongs based on its behavior. For example, classifying a device as "normal," "suspicious," or "compromised." Algorithms such as decision trees, random forest, logistic regression, and support vector machines are very well suited for solving classification problems.
- Anomaly detection allows identifying cases where a device's behavior deviates from the established baseline. You can use distance-based methods (e.g., Local Outlier Factor), density-based methods (e.g., Density-Based Spatial Clustering of Applications with Noise), or one-class classification methods (e.g., One-Class support vector machine).
- Time series forecasting allows predicting the future behavior of a device based on the analysis of its historical data. For example, the Autoregressive Integrated Moving Average model can predict the energy consumption of a server for planning optimal resource allocation. Recurrent neural networks (recurrent neural networks), in particular Long short-term memory, are also popular for processing sequential data.
- Analysis based on association rules involves searching for rules and relationships between different types of device behavior. For example, identifying a link between increased network traffic and the launch of a specific application.
- The choice of a specific Artificial intelligence/Machine Learning model depends on the type of data available for analysis, the task at hand, and the required accuracy. It should be noted that successful application of these models requires careful data preparation, selection of optimal algorithm parameters, and constant monitoring of their performance. In addition, it is necessary to consider the ethical aspects associated with the analysis of device behavior and ensure the confidentiality of user data.

**Threat and anomaly detection:** Based on analysis, potential threats and anomalies in device operation are identified. Artificial intelligence creates a profile of normal IoT device operation and identifies any activity that deviates from this profile as an anomaly.

**Automatic policy adaptation:** Reducing risks by automatically changing management policies in response to detected threats.

Alerts/triggers for Security Operation Center operator: When threats are detected, the system sends notifications or triggers to the Security Operation Center operator so that they can respond to incidents in a timely manner.

Blocking/Quarantine: The ability to isolate or block devices that pose a threat to prevent the problem from spreading.

AI self-learning on new data: The system continues to learn from new data, improves its models, and increases the efficiency of threat detection.

Integration with Security information and event management, Security Orchestration, Automation and Response and other systems: Collected data and analysis results can be combined with other security management systems (Security information and event management, Security Orchestration, Automation and Response) for deeper analysis and automation of security processes.

Remote management: The ability to remotely manage devices, allowing you to respond to incidents and manage devices in real time.

As a result of research and training, methods for ensuring the security of internet of things devices using artificial intelligence, detection, prevention, and elimination of threats were studied.

The most important method for preventing threats using artificial intelligence to ensure the security of internet of things devices is proactive anomaly detection and response method. This is more important than other methods because it allows you to identify attacks before they occur.

An important feature of proactive anomaly detection is that internet of things environments are very diverse and dynamic, devices are also very diverse, and these devices have various vulnerabilities, which makes it difficult to fix many devices.

Proactive anomaly detection uses artificial intelligence to learn the normal behavior of devices and systems, and then immediately detects deviations even for unknown (zero-day) threats. This provides early threat detection, faster protection, and minimal human intervention, which is critical to expanding internet of things security.

The following common anomalies can be detected using artificial intelligence:

- When anomalies are detected in equipment operation, unusually high processor or memory activity, or resource usage, can be identified.
- Network anomalies are identified by unusual traffic patterns, such as sudden spikes in sending or receiving data, and by attempts to access devices from unfamiliar Internet protocol addresses.
- In data anomalies, records that deviate significantly from expected values (e.g., temperature, pressure, etc.) can be identified.
- Unusual authentication or login attempts, incorrect Application Programming Interface requests, or processes using outdated protocols can be identified.
- Anomalies can be identified, such as changes in device settings that do not comply with security policies, i.e., open ports, changes in the firewall.

A proactive method for anomaly detection and response is carried out as follows:

1. The data collection and preparation process involves collecting and cleaning data from various sources, such as sensor data, device log files, network traffic. In this case, necessary characteristics are identified, such as network traffic volume, device power consumption, connection time, number of requests, and other characteristics. This data is used to create a profile of normal operation.
2. In the process of creating a normal activity profile using the collected data, a statistical model of the device's normal operation is created, and the model includes average values, standard deviations, correlations, and other statistical indicators. Machine learning algorithms such as One-Class support vector machine, Isolation Forest, Autoencoders can be used. In this process, the model is trained on normal data and then checked to see if new data coming from the device matches this model or not.

3. In the anomaly detection process, real-time data is compared with the normal activity profile. If the data does not match the profile, that is, an anomaly is detected, the system issues a warning. Various restrictions can be applied to detect anomalies.

4. In the process of automated response, the system automatically responds when an anomaly is detected.

The reaction may include the following:

- Disconnecting the device from the network.
- Updating the firewall.
- Adding an entry to the security log.
- Notifying the administration.
- Removing malware.
- Restoring the device.

5. The model is constantly updated over time based on new data. This ensures the system's adaptability to emerging threats.

Using proactive anomaly detection and Artificial intelligence -based response methods to ensure the security of internet of things devices has the following advantages:

- Allows preventing attacks before they occur.
- Allows responding to threats without human intervention through automated response.
- Has adaptability, that is, the ability to adapt to new threats.

Proactive anomaly detection using artificial intelligence is crucial because it proactively detects the unknown, constantly adapts and takes action before damage spreads, and protects internet of things devices without constant manual intervention.

## **4. CONCLUSION**

Methods for preventing and eliminating threats to internet of things devices using artificial intelligence have been analyzed. The analysis showed that proactive anomaly detection and a response method using artificial intelligence yield positive results in preventing threats. Artificial intelligence plays an important role in ensuring the security of internet of things devices, but it is not a perfect solution for detecting and preventing threats, and this system has its limitations.

As a final conclusion, the following can be noted:

- Artificial intelligence significantly improves the security of internet of things devices, but does not provide a complete guarantee. Using artificial intelligence for proactive threat detection, anomaly detection, and attack response is much more effective than traditional methods. However, artificial intelligence models can also make mistakes and may find it difficult to adapt to unknown attacks. In this case, artificial intelligence is only part of the security system and must be supplemented with other security measures for complete protection against threats.
- Full data quality assurance is essential in artificial intelligence models. High-quality, balanced, and sufficient data is necessary for effective artificial intelligence model training. Lack of data or its low quality reduces the accuracy and reliability of the model.
- Most internet of things devices have low resources, i.e., limited computing power, memory, and energy. Therefore, it is important to choose simple artificial intelligence models and energy-saving algorithms that match the resources of the devices. These problems can be solved using Edge computing technologies.



- It is important to protect data privacy in artificial intelligence models and minimize the impact of the artificial intelligence system itself on security. Technologies such as differential privacy and federated learning help solve these problems.
- Given the constant emergence and change of threats to internet of things devices, it is necessary to constantly monitor and update artificial intelligence models.

In conclusion, artificial intelligence systems can greatly help in preventing threats associated with internet of things devices. However, when creating an effective security strategy, the use of artificial intelligence should be combined with other security measures, such as using strong complex passwords, regularly updating software, using security protocols, and applying other security systems. Artificial intelligence is only part of the security system and is most effective when used in combination with other methods.

## REFERENCES

- [1] Abed, A. K. and Anupam, A., Review of security issues in Internet of Things and artificial intelligence-driven solutions, *Security and Privacy*, 6(3), e285, 1-18 (2023).
- [2] Humayun, M., Securing the Internet of Things in artificial intelligence era: A comprehensive survey, *IEEE access*, 12, 25469-25490 (2024).
- [3] Lyapunsova, E. V. and Arm Azhi Aziz Salih, Using Artificial Intelligence to Improve Network Security: Anomaly Detection Strategies and Implementation Prospects, *Izvestiya TulGU, Technical Sciences*, 3, 131-135 (2024).
- [4] Keyur K. Patel and Sunil M. Patel, Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges, *International Journal of Engineering Science and Computing*, 6122-6131 (2016).
- [5] Artamonov, V. A. and Artamonova, E. V., Artificial intelligence and security: problems, misconceptions, reality and future, *Russia: trends and development prospects*, 17-1, 685-594 (2022).
- [6] Patel, K.K. and Patel, S.M., Internet of Things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges, *Int J Eng Sci Comput*, 6(5), 6122-6131 (2016).
- [7] Saidovna, T. G., Opportunities of Artificial Intelligence in Ensuring the Security of IoT Devices, *Miasto Przyszłości*, 59, 200–206 (2025).