OPPORTUNITIES OF ARTIFICIAL INTELLIGENCE IN ENSURING IOT DEVICE SECURITY

Salimov Ro'zibek Nasim o'g'li,
Lecturer of the Department of Applied Mathematics and Programming Technologies, Bukhara State University.

E-mail: r.n.salimov@buxdu.uz ORCID: 0009-0005-2744-4909

ABSTRACT

IoT systems are a rapidly developing technology, and the widespread adoption of IoT devices has led to revolutionary changes across various sectors by improving connectivity and enabling intelligent operations. However, this rapid expansion has also introduced significant security challenges, as IoT devices often serve as an entry point for cyberattacks due to their diversity and varying levels of built-in security. Artificial intelligence (AI) has become an important technology in addressing these security issues, offering advanced solutions to protect IoT devices. This article examines the role of artificial intelligence in ensuring the security of IoT devices and analyzes the challenges and solutions associated with its implementation.

Keywords: IoT systems, modern technologies, energy efficiency, protocols, Internet, intelligent object, virtual world, Intel IoT Platform scheme.

INTRODUCTION

Across the world, on city streets, in homes and hospitals, billions of connected "smart" physical objects continuously collect and exchange data through the Internet, providing them with a certain level of digital intelligence and autonomy. The Internet of Things (IoT) has completely transformed the world with its innovations and has become an essential part of human daily life. IoT is widely used in offices, residential environments, and industrial sectors. It has also become a key component in areas such as healthcare management, agriculture, smart homes, smart cities, and even autonomous vehicles.

The term "IoT (Internet of Things)" was introduced by Kevin Ashton in 1999. He worked at the Massachusetts Institute of Technology (MIT) and led the Auto-ID Labs, where he first proposed the IoT concept. The development of this field is associated with the convergence of various technologies, including ubiquitous computing systems, sensors, and powerful embedded systems. Initially, the idea was related to the use of radio-frequency identification (RFID) technology for supply chain management. Over time, the concept expanded to include a wide range of other devices and applications.

According to the World Economic Forum report "State of the Connected World," the number of connected devices in the world already exceeds the number of people, and by 2025 it is predicted that 41.6 billion devices will collect and process

information about how we live, work, move across cities, operate machines, and maintain them [3].

The world has become easily interconnected thanks to IoT systems. Now it is much easier for people to work and communicate efficiently. The way devices, systems, and services interact resembles a network ecosystem.

It is important to understand how IoT devices work, how they establish communication, and how the system operates. IoT devices communicate through networks, and their main communication methods include Wi-Fi, Zigbee, and Bluetooth. These technologies enable IoT devices to transmit data to other devices. In this way, the world is becoming an increasingly interconnected system.

RESEARCH METHODOLOGY

During the process of studying this research, a number of scientific sources were used. As a result of the research, it was concluded that IoT systems (Internet of Things) continue to attract significant attention with their concept. The widespread adoption and popularity of fitness trackers and smart watches have helped people become more familiar with the term “IoT systems.”

This technology is truly revolutionizing our lives, as almost everything is becoming “smart.” Smart bracelets, agriculture, homes, cities, supply chains, manufacturing, logistics, and many other sectors are clear examples of this transformation. Therefore, some enthusiasts show great interest in studying this field in depth and gaining more knowledge. This interest may also be driven by a perceived lack of technical knowledge or information. Fortunately, today anyone interested in IoT systems can find a wide range of books suitable for different levels of technical expertise.

This article examines the main challenges of integrating artificial intelligence into IoT security, including issues of data privacy, the complexity of AI algorithms, and the need for scalable solutions. The study analyzes both the opportunities and limitations of artificial intelligence in protecting IoT devices and discusses ideas on how AI technologies can be used to build more adaptive security systems.

The conducted research emphasizes the importance of continuous research and development in artificial intelligence technologies in order to adapt to the growing and dynamic nature of IoT threats.

DISCUSSION AND RESULTS

IoT, or the Internet of Things, is a collection of physical objects capable of connecting to the internet. These objects are able to collect, exchange, and interact with each other using sensors, software, and other technologies.

The main characteristics of IoT are as follows:

1. IoT devices communicate with each other via the internet or local networks and exchange data.
2. IoT systems can process data in real time and make decisions, which enables the automation of many processes.
3. Data from the environment is collected using devices, sensors, cameras, and other equipment.

4. Collected data is analyzed and transformed into useful outcomes, for example to improve efficiency or prevent problems.

IoT devices are widely used today in the following areas:

— In the “Smart Home” sector: smart home devices such as smart lamps, thermostats, security systems, and smart doors.

— In the industrial sector: IoT solutions are used to optimize production processes and improve safety.

— In the transport sector: information exchange between vehicles and systems, for example traffic management.

— In healthcare: medical devices collect data about patients and analyze it.

IoT systems have become an integral part of our daily lives by connecting objects and providing valuable data. However, as the number of IoT devices increases, protecting them from cyberattacks is becoming a serious challenge.

According to a Check Point research report, in the first two months of 2023, the number of weekly cyberattack attempts on IoT devices per organization increased by 41% compared to 2022. Each week, approximately 54% of organizations experience attempts of cyberattacks on their IoT devices [4].

Why are IoT devices more vulnerable to cyberattacks?

In recent years, the number of IoT devices has grown significantly. According to available data, by the end of 2023 the number of IoT devices reached 16.6 billion, and by the end of 2024 it is expected to increase by 13%, reaching 18.8 billion.

Although IoT devices offer many advantages, they do not have the same level of security capabilities as laptops and workstations. In addition, their easy spread across networks creates an expanded attack surface. This is especially dangerous if the security team or IT department does not maintain accurate records of all devices in the network. The more devices connected to the internet without proper security control, the more opportunities attackers have to exploit them for unauthorized access [5].

Today, the attack surface in information security is enormous and continues to grow rapidly. Depending on the amount of data, it may contain hundreds of billions of variable signals that must be analyzed to accurately calculate risk. However, the need for human involvement in analyzing and improving cybersecurity is decreasing.

Artificial intelligence (AI)-based cybersecurity tools are emerging, helping security services reduce the risk of breaches and effectively improve security levels. AI and machine learning (ML) are becoming important technologies in cybersecurity because they can quickly analyze millions of events and detect various threats—from phishing behavior to malicious code detection and prevention of malware downloads. These technologies can also learn from past data and, over time, detect new types of attacks.

Unfortunately, despite the popularity of artificial intelligence technologies today, the use of traditional methods still continues. Unlike big data systems, cloud technologies, IoT, and other modern technologies, governments and large IT companies are actively searching for ways to transition to AI.

Artificial intelligence methods such as machine learning, anomaly detection, and predictive analytics are increasingly used for monitoring, identifying potential threats, and responding in real time. These technologies help detect unusual behavior patterns, predict potential vulnerabilities, and automate responses to reduce risks.

The integration of artificial intelligence (AI) and the Internet of Things (IoT) creates a new technological ecosystem called AIoT (Artificial Intelligence of Things). This combination expands the functionality of IoT devices, transforming them from simple data collectors into autonomous systems capable of real-time analysis, learning, and decision-making. The creation of AIoT has opened new ways to develop automation and expanded the application of IoT infrastructure in various fields.

The main advantage of AIoT is that IoT devices collect data, process it using artificial intelligence, make predictions based on it, and initiate actions without human intervention. Thanks to edge computing, this integration reduces latency and increases system reliability.

However, despite all the advantages of AIoT, there are still challenges related to data privacy and security.

If we examine the main components of AIoT, their interconnection is as follows:

IoT devices: IoT systems operate using devices such as sensors, actuators, and cameras. These devices form a network that collects and exchanges data. Function: IoT devices collect environmental data such as temperature, humidity, location, and other parameters.

Artificial Intelligence (AI): (machine learning, deep learning, natural language processing/NLU, computer vision, machine reasoning, generative AI). These technologies enable systems to analyze data, extract insights, and make decisions without human intervention. Function: AI processes data collected from IoT devices, identifies patterns, predicts outcomes, and optimizes processes.

Cloud technologies: Cloud platforms provide storage and computing resources accessible via the internet. Mission: Cloud solutions provide scalability and flexibility, enabling efficient storage of large volumes of data and execution of complex computations [6].

Data analytics: The process of extracting useful information from large amounts of data collected by IoT devices. Mission: providing analytical reports and visualizations that support decision-making and improve efficiency.

Management systems: Software designed for monitoring and managing IoT devices. Function: ensuring control over device operation, configuration, and security.

Security: Mechanisms and protocols that protect data and systems from unauthorized access and cyberattacks. Mission: ensuring information security and system integrity, as well as user safety.

These components work together to create efficient and intelligent solutions that improve quality of life and optimize processes across various sectors.

The advantages of combining AI and IoT include the ability of AI to automate repetitive tasks performed by humans, helping to optimize workflows and improve

resource efficiency. This system increases productivity, reduces labor costs, and enables faster operations.

The advantages of combining AI and the Internet of Things are as follows: the ability of AI to automate routine tasks performed by humans helps optimize work processes and improve the efficiency of resource utilization. This system increases productivity, reduces labor costs, and enables faster execution of operations.

Artificial intelligence can be applied in various areas of Internet of Things (IoT) security, including:

- Threat detection: AI can detect both known and unknown threats in real time by analyzing network traffic, system logs, and other data sources. In addition, it can identify malware and other malicious activities.
- Access control: AI improves access control mechanisms by closely analyzing user behavior on IoT devices and detecting anomalies. It can also help identify and prevent unauthorized access to IoT devices.
- User authentication: Biometric identification and multi-factor authentication are examples of user authentication systems that can be enhanced by AI. It can verify user behavior and detect violations such as login attempts from unusual locations.
- Network security: AI monitors network traffic to detect suspicious activity and potential threats. By learning from data collected from various sources such as firewalls and intrusion detection systems, it can detect attacks and respond to them in real time.
- Vulnerability detection: AI can quickly identify vulnerabilities in IoT devices and applications by analyzing code and configuration files. It can simulate attacks to reveal weaknesses and provide recommendations for security updates.
- Predictive maintenance: Using artificial intelligence to analyze historical data and patterns, it is possible to predict potential device failures and security vulnerabilities. AI can identify and address issues in advance before they become targets of cyberattacks, ensuring proactive security measures [4].

Today, one of the key challenges in ensuring the security of Internet of Things (IoT) devices is the complexity of artificial intelligence algorithms and the need for scalable solutions. This complexity can be explained as follows: in general, solving complex tasks requires modern artificial intelligence algorithms such as deep learning and powerful machine learning approaches. These algorithms have a multilayered and multi-parameter structure and require significant computational resources to achieve optimal results. This necessitates the use of advanced algorithms and optimization techniques to address high-level complexity problems. This is especially important in tasks such as classification, prediction, and natural language processing.

Next, artificial intelligence requires scalable solutions. Scalable solutions are systems that can be quickly adapted or expanded as specific needs change. For this purpose, companies and organizations need scalable AI system models that help them develop their operations and adapt to a rapidly changing market. This is done logically by adding new features or updating systems in accordance with user requirements.

Protecting Internet of Things (IoT) devices requires resources and technologies, and the computational power needed to implement AI algorithms is also related to their complexity. Scalable solutions are often provided through computer networks and cloud technologies, which enable systems to deliver the required computing power. Such scalable solutions require separate management and data storage systems, which improves the efficiency of complex algorithms.

Considering the complexity of AI algorithms and the need for scalable solutions, approaches that are compatible with modern technologies and ethical standards are extremely important.

There are significant opportunities for ensuring the security of Internet of Things (IoT) devices using artificial intelligence. AI creates both opportunities and limitations when it comes to protecting IoT devices. These can be described as follows:

Possible opportunities:

1. Cyberattack detection: AI algorithms help detect anomalous behavior by monitoring data flows coming from IoT devices and comparing them with normal patterns. This enables the rapid detection and prevention of cyberattacks (e.g., DDoS attacks).
2. Behavior prediction: Using machine learning (ML), AI can learn the behavior of IoT devices and prepare decision-making models. This enables quick action to prevent potential threats.
3. Automated response: AI systems provide mechanisms for rapid response to breaches or incidents, such as disabling devices or disconnecting connections.
4. Data analysis: AI can help identify weaknesses in systems by analyzing large volumes of data collected from IoT devices. This allows necessary measures to be taken to improve security.
5. Optimization of security protocols: AI can be used to develop new security protocols and create systems that are continuously updated to improve the efficiency of existing ones.

Limitations of using artificial intelligence in security systems:

1. The success of an AI model often depends on the quality of data. If the data is inaccurate or biased, AI algorithms may make incorrect decisions.
2. Some AI models require high computational power to operate. IoT devices often have limited resources, so powerful AI algorithms cannot always run efficiently on them.
3. Complex interactions between tools or uncertain conditions may reduce the effectiveness of AI systems. They are often not well adapted to network load and other changing factors.
4. Each part of the IoT ecosystem has its own security mechanisms. AI can protect only part of the system, while vulnerabilities in other parts may still pose a threat.
5. Privacy and ethical issues related to data collected by AI systems require clear definitions of how and for what purposes the data will be used.

Although AI offers many valuable opportunities for protecting IoT devices, its limitations and uncertainties must also be considered. Addressing these challenges requires innovative approaches and advanced technologies.

CONCLUSION

The Internet of Things (IoT) transforms everyday objects into connected devices that make life easier and enhance functionality, creating intelligent environments in cities, hospitals, and homes. From agriculture to wearable devices, IoT is changing the way people live and work, while also raising security concerns. Digital transformation driven by emerging technologies such as robotics, IoT, and artificial intelligence is known as the Fourth Industrial Revolution, and COVID-19 has further accelerated the adoption of these technologies.

To ensure the security of IoT devices using artificial intelligence, the following approaches and strategies should be considered:

1. It is necessary to maintain a high level of data quality collected from IoT devices. This requires implementing data testing and validation processes. Data should be cleaned, transformed into the required format, and anomalies should be identified and removed.
2. Many IoT devices have limited computational and energy resources, so complex AI algorithms cannot operate efficiently on them. Therefore, lightweight and high-performance algorithms (such as transfer learning) should be developed. In addition, using fog computing approaches, data should be processed not on devices themselves but on intermediate servers or computers, enabling shared computational power.
3. IoT environments often change dynamically, which can reduce the effectiveness of AI systems. This requires continuous model updates and adaptive learning approaches. It is also advisable to simulate IoT operating conditions in advance and develop optimal strategies.
4. Since IoT ecosystems consist of many different devices, ensuring their interoperability is a complex process. This can be addressed by developing standard protocols and interfaces between IoT devices and AI systems, enabling efficient integration and communication.
5. Data protection should be ensured through encryption and security protocols. Obtaining user consent and developing ethical guidelines will also contribute to effective solutions.

In general, applying modern approaches and AI-based strategies in securing IoT devices is essential. These solutions include various innovations necessary to improve system efficiency and ensure security.

REFERENCES

1. Chowdhury, Rakibul Hasan. “Advancing fraud detection through deep learning: A comprehensive review.” World Journal of Advanced Engineering Technology and Sciences, 12(2), 2024, pp. 606–613.
2. Chowdhury, Rakibul Hasan. “AI-driven business analytics for operational efficiency.” World Journal of Advanced Engineering Technology and Sciences, 12(2), 2024.
3. https://www.visionofhumanity.org/what-is-the-internet-of-things/
4. https://www.einfochips.com/blog/enhancing-iot-security-with-artificial-intelligence/
5. Turdiyeva G. S. “Network attacks and the use of NIX protection methods.” Universum: Technical Sciences, 2022, No. 2-1 (95), pp. 60–62.
6. G. G. S. Turdiyeva. “Security issues in the use of cloud platforms: risks and threats.” Intereducation and Global Research, 2024, No. 4.