ELEMENTS OF INFORMATION SECURITY OF THE "INTERNET OF THINGS"

Jakhongirbek Khabibullaev
Tashkent University of Information Technologies
named after Muhammad Al-Xorazmiy

Annotation: *Due to the sharply increasing demand from users for Internet of Things (IoT) technologies, there has arisen a need for high-quality information protection of the Internet of Things network. This article examines the most important issues related to IoT information security and proposes solutions to the problems identified.*

Keywords: *Internet of Things, information security, vulnerability, security threats.*

At present, there is significant theoretical and practical interest in the impact of "machine-to-machine" interactions on the continuity and reliability of systems that support the functioning of society. Global information networks are actively developing in a direction that enables the connection of physical and virtual objects based on ICT (Information and Communication Technologies), with the aim of providing innovative services to society — for example, in the areas of shopping (contactless payments), vehicle control via smartphones, and energy consumption (reducing usage through remote monitoring using sensors and video cameras).This phenomenon has been termed the "Internet of Things."

The key features of the Internet of Things are as follows:

1. Physical objects, united in a vast computing network, can interact with each other and with the external world.
2. The IoT network involves the interaction of computers, smartphones, various powerful computing devices, and virtually any physical items.
3. The Internet of Things significantly simplifies human life, without requiring human intervention in the functioning of interconnected devices that monitor the surrounding environment using digital tools [2, p. 341].
4. The main objective of the system is to improve people's lifestyles and enhance their quality of life by fostering unity through artificial intelligence in the interaction between all members of society and governing bodies.
5. The network offers wide-ranging prospects:

- In the agricultural sector**:** The relative condition of the soil can be addressed by using sensor data on soil moisture, topsoil temperature, and plant nutrition;

- In industry**:** A reduction in scheduled equipment inspections is possible thanks to sensor readings [1, p. 157];
- In goods logistics: Package tracking along the entire delivery route simplifies its transfer from the manufacturer to the store or from the store to the customer;
- In the construction of smart homes: Conservation of water, electricity, and gas through the installation of smart meters; managing home security; programming home functions according to the specific user's needs;
- In medicine: Devices that collect and transmit data to an IT database for further analysis; real-time monitoring of patient status; automatic alerts to specialists about any changes; reduced use of high-energy-consuming medical equipment; cost savings on surgeries; health monitoring through regular tracking of physical indicators using wearable devices such as wristbands, smart clothing, and footwear;
- In retail: Targeted interaction with each network-connected customer during product searches; analysis of sales volumes; automatic price increases or reductions to maximize sales and avoid overstocking;
- In forensics: Monitoring of criminals under house arrest using biometric chips;
- In environmental protection: Monitoring of animal populations by detecting them on the Earth's surface via the radio signal emitted from a device attached to the animal;
- In transportation**:** AI will be able to independently assess traffic conditions, plan and adjust the travel route without human involvement.

One of the main problems of the Internet of Things (IoT) today is ensuring the cybersecurity of this network. This problem is caused by several factors: the rapidly changing situation in the industry; the desire of numerous individuals and organizations to gain control over the network and impose their own rules and regulations; and unrealistic forecasts. A critical role is played by technical vulnerabilities, which include: not necessarily obvious or feedback-based active influence of a subject on an object; the negative impact of a combination of conditions and factors that pose a threat to information security; and intentional malicious actions aimed at violating the availability, integrity, and confidentiality of data.

By being aware of vulnerabilities and flaws in the configuration of the system's application or control software, an individual with malicious intent can gain control over a device, embed a malicious element, or alter its program [3, p. 12].

Natural threats — such as earthquakes, fires, and floods — can also cause significant damage to computer systems. To minimize their negative impact, the best solution is to use backup systems.

Significant malicious damage to IoT systems can come from individuals both with authorized access to the network and those operating outside of it. These may include inexperienced hackers using easily accessible hacking tools, as well as professionals who are well aware of system vulnerabilities and can predict its response to specific codes and scripts.

The new generation of Internet of Things (IoT) devices already has embedded security threats, providing opportunities for attacks even by manufacturers themselves.

Malicious actions aimed at disrupting the availability, integrity, and confidentiality of data are often driven by the attacker's personal ambitions or the pursuit of financial gain. These actions can take many forms:

- Active attacks on the network to test whether an internet provider can view the data packet and determine which websites and web applications are being accessed;
- Passive attacks to search for information that is available for theft;
- Proximity-based attacks initiated from websites by compromised computers;
- Exploitation of insiders, i.e., individuals who have access to sensitive data that is unavailable to the general public.
- Intercepting or substituting messages while maintaining the hacker's anonymity in the communication channel between correspondents;
- Compromising the channel by violating transmission protocols through distortion or alteration of information;
- Gaining access to a website using credentials obtained fraudulently from a user who lacks basic network security awareness, often via a fake login page [5, p. 39].

D. Violation of personal privacy, manifested in:

- Intellectual analysis of information, allowing the identification of facts that should not be disclosed in databases;
- Obtaining confidential information about individuals or organizations through hacking or use of malicious software;
- Unauthorized eavesdropping on user conversations;
- Tracking the location and movements of users who wish to remain anonymous, using a UID;
- Password duplication attacks, by guessing combinations of letters and digits or using brute-force methods via specialized tools.

E. Unauthorized use of the network to gain financial profit by stealing intellectual property, personal data, or the set of associations and perceptions related to a product or service.

F. Attacks on the technological control mode and operational state of devices:

Denial-of-service attacks, resulting in system failure;

Control of system infrastructure through Trojans or viruses.

To date, there is not a single truly secure Internet of Things (IoT) system in the world. The main reasons for this are:

- the manufacturer's desire to minimize the cost of their product;
- the lack of necessary standards and guidelines for ensuring the information security of the network;
- the inability to authorize and authenticate many components used in the system when connected to the global network [4, p. 280].

A systematic and purposeful effort is required to create effective information security for the Internet of Things (IoT), which includes:

- monitoring device vulnerabilities during the manufacturing stage;
- applying modern standards for developing secure applications during software creation;
- creating opportunities and conditions for software updates;
- minimizing the vulnerability of hardware-dependent code by managing logistics from production to installation at the target site;
- preventing the physical capture of structures that receive and process certain types of information or generate sensory input;
- enhancing the security protection level of various perception nodes in sensor networks deployed in environments without human oversight;
- preventing sensor-related issues such as gateway node capture, data leakage, data integrity violation, power exhaustion, overloads, denial of service, installation of unauthorized devices, or unauthorized duplication of nodes;

The application of the Internet of Things in many fields is still significantly limited due to information security issues. However, a thorough analysis of the situation, achievements in this area, and expert recommendations will help address the accumulated challenges and promote the further implementation of this technology into practice.

Literature

1. Буянов Б.Я., Верба В.А. Мультиагентные модели сложных социо-технических систем // В сборнике: Системный анализ в проектировании и управлении. Сборник научных трудов XX Международной научно-практической конференции. 2016. С. 155-158.
2. Калинин А. С. Интернет вещей. Принципы, технологии, перспективы развития // Молодой ученый. 2019. № 2 (240). С. 341–342.
3. Кожевникова И. С. Тенденции безопасности интернет-вещей // Молодой ученый. 2017. № 13 (147). С. 11-14.
4. Шиков С. А., Ивлиев С. Н. Интернет вещей: новые угрозы информационной безопасности // Материалы XX науч.-практ. конференции молодых ученых,

аспирантов и студентов Национального исследовательского Мордовского государственного университета им. Н. П. Огарева. Саранск, 2016. С. 278–283.

5. Шиков С. А. Проблемы информационной безопасности интернет вещей // Вестник Мордовского университета. 2017. Т. 27, № 1. С. 27–40.