I. Zhmuryk, *BA student*
O. Mahdiuk, *PhD in Ped., As. Prof*
Khmelnytskyi National University

INTERNET OF THINGS SECURITY PROBLEMS

The Internet of Things (IoT) has become a key part of modern digital infrastructure allowing physical devices to connect and interact within networks. Smart home systems, wearable devices, industrial controllers, and healthcare technologies constantly collect and exchange data. This helps improve efficiency, automation, and overall performance. At the same time this rapid growth has significantly expanded the attack surface making IoT ecosystems more exposed to cybersecurity threats.

This topic is very important because IoT is widely used in critical areas such as healthcare, transportation, and industry. Unlike traditional computers many IoT devices have limited processing power, memory, and storage. Due to this decentralized topology and the resource constraints of the majority of devices, conventional security and privacy approaches are often inapplicable for IoT [1, p. 2]. As a result security is often treated as a secondary priority during the design and development stages which leads to widespread vulnerabilities.

One of the most serious problems in IoT security is weak authentication and access control. Many devices are still deployed with default credentials or without proper identity management systems. This makes it easier for attackers to gain unauthorized access with minimal effort. In addition weak or missing encryption allows attackers to intercept data during transmission using methods like packet sniffing or man-in-the-middle attacks.

Another major issue is the lack of regular firmware and software updates. IoT devices are often used in environments where updating them is difficult or rarely performed. Because of this they stay vulnerable to known security problems for a long time. Attackers actively exploit these weaknesses, infect devices, and include them in botnets. These botnets are then used to launch large-scale Distributed Denial-of-Service (DDoS) attacks. For instance, the notorious Mirai botnet malware exploits vulnerabilities of IoT devices to launch massive attacks, highlighting the devastating potential of unsecured IoT swarms [2, p. 45]. This shows that insecure IoT devices can affect not only individual users but also large networks.

The diversity of IoT systems also creates additional challenges. Devices produced by different manufacturers use different communication protocols, architectures, and standards. This diversity makes it difficult to implement a unified and consistent security policy. As a result monitoring systems and intrusion detection tools become less effective which reduces the ability to quickly detect and respond to threats.

Privacy is another critical issue in IoT environments. Many IoT devices collect personal and behavioral data all the time. In many cases, users do not fully understand how their data is collected or used. If such data is compromised it can be used for surveillance identity theft or other malicious purposes. Therefore, ensuring data confidentiality and protecting user privacy must be a fundamental requirement in IoT system design.

An additional important aspect is device identity and trust management. In large IoT environments, it is often hard to check if a device is real or has been hacked. When there is no reliable system to manage device identities, attackers can add malicious or fake devices to the network. These devices can manipulate data, disrupt communication, or act as hidden entry points for further attacks.

Scalability is another serious challenge for IoT security solutions. Traditional cybersecurity mechanisms are not always suitable due to the large number of connected devices. As networks grow, managing encryption keys, authentication, and access control becomes more complex and requires more resources. Therefore there is a need for lightweight, efficient, and scalable security solutions that can operate effectively even on limited devices.

Energy limitations of IoT devices further complicate security implementation. Many devices run on batteries or low-power systems, which limits the use of complex security mechanisms that require a lot of resources. Therefore it is necessary to find a balance between maintaining strong security and energy efficiency so that device performance and lifespan are not significantly affected.

Edge computing also introduces new security risks. While it helps reduce latency and network load by processing data closer to the source it also shifts part of the responsibility for data protection to edge devices. The hasty development of edge computing often leads to the neglect of security threats, making these platforms vulnerable to distributed denial of service, side-channel, and malware injection attacks [3, p. 1608–1609]. Ensuring data integrity and confidentiality at the edge is therefore critically important.

Artificial intelligence is playing an increasingly important role in IoT security. Machine learning algorithms can help detect anomalies, identify potential threats, and automate responses to cyber incidents. Furthermore integrating techniques like federated learning within a zero-trust environment can significantly enhance the privacy of sensitive data shared by IoT devices without centralizing the datasets [4, p. 1168]. However, attackers can also target AI systems by feeding them manipulated or misleading data. This can lead to incorrect decisions and creates new types of threats known as malicious machine learning.

Finally, the human factor remains one of the weakest points in IoT security. Users often ignore basic security practices, such as changing default passwords, updating firmware, or properly configuring devices. This significantly increases the overall vulnerability of IoT systems. For this reason raising user awareness and promoting secure behavior is a crucial part of any effective IoT security strategy.

To address these challenges a comprehensive and systematic approach to IoT security is required. This includes the use of strong encryption protocols, secure authentication mechanisms such as multi-factor authentication, and regular automated updates. It is also important to apply network segmentation and the principle of least privilege to limit the spread of potential attacks. In addition modern security models such as Zero Trust can significantly improve system resilience by ensuring continuous verification of all devices and users. Recent implementations of trusted-based Zero Trust architectures tailored for IoT at scale have shown significant improvements in processing efficiency without compromising robust access control [5, p. 114].

IoT security problems represent a complex and constantly evolving challenge in the field of cybersecurity. As the number of connected devices continues to grow there

is a need to shift from reactive to proactive security strategies. Building a secure IoT ecosystem requires cooperation between developers, manufacturers, cybersecurity specialists, and end users. Only a comprehensive and security-focused approach can effectively reduce the risks associated with IoT technologies.

REFERENCES

1. Al-Garadi, M. A., et al. A Review of IoT Security Challenges and Solutions. IEEE 8th International Japan-Africa Conference on Electronics, Communications, and Computations (JAC-ECC), 2020. P. 1–6.
2. Hussain, S. A., et al. Protecting IoTs from Mirai Botnet Attacks Using Blockchains. IEEE International Conference, 2019. P. 45–50.
3. Shi, W., et al. Edge Computing Security: State of the Art and Challenges. Proceedings of the IEEE, 2019. Vol. 107, Issue 8, P. 1608–1631.
4. Kumar, R., et al. Ensuring Zero Trust IoT Data Privacy: Differential Privacy in Blockchain Using Federated Learning. IEEE Transactions on Consumer Electronics, 2024. Vol. 71, Issue 1, P. 1167–1179.
5. Smith, A., et al. Zero Trust+: A Trusted-based Zero Trust architecture for IoT at Scale. IEEE International Conference on Consumer Electronics (ICCE), 2024. P. 112–117.