UDK: 004.75:004.056:004.056.7
Student Yevhen Biezhyn
Vasyl' Stus Donetsk National University, Ukraine

CYBERSECURITY IN IOT SYSTEMS: METHODS OF DATA PROTECTION IN DISTRIBUTED NETWORKS

The Internet of Things (IoT) is reshaping the world by networking billions of devices into giant systems for the purpose of automation and data processing. Yet, the very size of IoT systems presents special cybersecurity problems. [1] Vulnerabilities in wireless protocols, insecure device authentication mechanisms, and insufficient resources to employ sophisticated encryption techniques leave IoT networks open to cyber-attacks. This report discusses theoretical aspects and practical methods of data protection that consider the specifics of distributed IoT systems.

The main threats to IoT systems

IoT devices, such as sensors, smart meters, and medical gadgets, often have limited computing power, making it difficult to implement traditional security mechanisms. For example, wireless protocols (Bluetooth, NFC or ZigBee) use weak encryption algorithms based on energy efficiency and are vulnerable to man-in-the-middle attacks. In addition, collection of user data (e.g., geolocation, biometric information) entails a risk of leakage owing to design weaknesses of IoT platforms.

Distributed IoT networks are also a target for DDoS attacks due to the enormous number of connected devices. Studies show that the number of captured IoT devices in 2024 increased by 136% compared to previous years and amounted to nineteen million devices. [2]

Innovative methods of data protection

Quantum cryptography has an answer to the secure communication of data in the form of quantum key distribution (QKD). It relies on the Heisenberg uncertainty principle, which makes it impossible to intercept keys without disturbing the quantum state of particles. Although QKD is still used in experimental IoT systems, it has the potential to protect critical infrastructure.

Distributed data storage is based on dividing information into fragments that are distributed among network nodes. This approach, which uses modular arithmetic, ensures confidentiality: even if an attacker gains access to a part of the data, he or she will not be able to recover the entire amount of information. Studies show that such systems are an effective means of ensuring the confidentiality and security of information. [3]

Practical Implementation

Integrating cybersecurity methods into IoT systems requires considering the limitations of the devices. For example, encryption algorithms need to be optimized for low-power processors. Experiments with real datasets have shown that Fed SVD (singular value decomposition federation) is more than 10,000 times faster than methods based on homomorphic encryption and has 10 orders of magnitude less error than solutions based on differential privacy, and the use of FedSVD with local data processing before transmission over the network really helps reduce the risk of confidential information leakage. [4][5]

Decentralized systems based on blockchain also demonstrate efficiency. They ensure data transparency and integrity through a distributed ledger that prevents unauthorized changes.

Additional aspects of cybersecurity in IoT systems

- Cryptographic algorithms and their adaptation to IoT

Existing IoT devices use light-weight cryptographic algorithms that trade-off between energy efficiency and security. For example, elliptic curve-based algorithms (ECC) provide a high degree of security with lower computational overhead than RSA. This is especially important for constrained devices such as sensors or wearables.

- Vulnerability analysis and countermeasures.

Research has shown that the majority of IoT devices come with pre-installed backdoors or default passwords that are easily guessable, and attackers use them as easy entry points. Automatic

software patching and multi-level authentication should, hence, be embraced to reduce attacks. AI techniques can also be utilized in identifying IoT network irregularity.

- The role of standards and regulation

The lack of unified security standards for IoT devices remains a key issue. For example, some producers overlook data encryption procedures during transmission, thus leading to massive data leaks. Global standardization, like ISO/IEC 30141, aims at bringing together security requirements; however, the implementation of the standards requires a lot of time and investment. [6]

These factors highlight the need for a comprehensive approach to cybersecurity in the Internet of Things that addresses both technical and organizational aspects.

Conclusions

Cybersecurity of IoT systems requires a synthesis of theoretical solutions (e.g., quantum cryptography) and practical technologies (hardware protection, optical networks). Further research should focus on adapting these methods to resource-limited devices and developing unified security standards. Only a comprehensive approach will ensure reliable data protection in distributed IoT networks.

References

6. A. Slonopas, "IoT Cybersecurity: Strengthening Defenses against Threats," *American Public University*, May 03, 2024. https://www.apu.apus.edu/area-of-study/information-technology/resources/iot-cybersecurity-strengthening-defenses-against-threats/

7. Forescout Technologies, Inc., "What are the riskiest connected devices right now?," *Forescout*, Jun. 27, 2024. https://www.forescout.com/blog/what-are-the-riskiest-connected-devices-right-now/?utm_source=Securitylabru

8. R. A. Chou and J. Kliewer, "Secure distributed Storage: Rate-Privacy Trade-Off and XOR-Based coding scheme," *arXiv.org*, Jan. 13, 2020. https://arxiv.org/abs/2001.04241

9. D. Chai *et al.*, "Practical Lossless Federated Singular Vector Decomposition over Billion-Scale Data," *arXiv.org*, May 19, 2021. https://arxiv.org/abs/2105.08925

10. D. Dimitrov I., M. Balunović, N. Konstantinov, and M. Vechev, "Data leakage in federated averaging," *arXiv.org*, Jun. 24, 2022. https://arxiv.org/abs/2206.12395

11. "ISO/IEC 30141:2024," *ISO*. https://www.iso.org/standard/88800.html

UDK: 331.108.2:004.7:331.101.3

Student Yevhen Biezhyn
Vasyl' Stus Donetsk National University, Ukraine

DIVERSIFICATION OF THE WORK ENVIRONMENT: THE IMPACT OF ICT ON EMPLOYEE EFFICIENCY AND SATISFACTION

In the contemporary business landscape, certain digital technologies, including collaboration tools and analytical software, are transforming diversity management in organizations. This study explores the influence of these information and communication technologies (ICT) on two aspects: communication effectiveness in diverse teams and business process effectiveness of multicultural business processes. Here, it is relevant to consider how ICT facilitates diverse team integration and enhances their productivity overall.

Diversity problems and the role of digital technologies

Research has demonstrated that diversity in the workplace, though advantageous in general, can present challenges like communication gaps, disagreements, and unequal work burden. [1]

Adoption of technology to break communication barriers is necessary. For instance, sites that incorporate translation facilities, like Microsoft Teams and Zoom, allow for automatic language exchanges, significantly enhancing mutual understanding among employees from different cultural