2. M. A. Fazeli, H. Moghaddasi, A. Hosseini, F. Asadi, and H. Haghighi, "Application of ICT in effective crisis management: A systematic review," *Journal of Emergency Management*, vol. 19, no. 6, pp. 591–606, Nov. 2021, doi: 10.5055/jem.0612.

3. vorecol.com, "How can remote employee integration software address the challenges of crosscultural team dynamics?" https://vorecol.com/blogs/blog-how-can-remote-employee-integration-software-address-the-challenges-of-crosscultural-team-dynamics-151464

4. "AI for reducing bias in HR," Apr. 18, 2025. https://www.akoolblog.com/knowledge-base-article/ai-for-reducing-bias-in-hr

5. J. Howard, "The benefits of remote work for people with disabilities." https://www.inclusionhub.com/articles/benefits-of-remote-work

6. A. Sud, "How technology can help foster inclusivity and productivity at work," *TIME*, Aug. 12, 2021. [Online]. Available: https://time.com/6084759/technology-inclusive-productive-work/

**UDK: 004.42:004.056:004.056.5**

**Student Yevhen Biezhyn**
Vasyl' Stus Donetsk National University, Ukraine

# APPLICATION OF PARALLEL COMPUTING IN CYBERSECURITY: VULNERABILITY ANALYSIS AND DATA PROTECTION

Modern information systems face a growing number of cyber threats, which requires the development of effective protection methods. Parallel computing is a technology that allows you to simultaneously perform several data processing operations, which significantly speed up the process of analysing vulnerabilities and ensure reliable information protection. The paper discusses the theoretical ramifications of applying these technologies to cybersecurity. [1]

*Theoretical foundations of vulnerability analysis based on parallel computing*

Vulnerability analysis is a methodical process that aims to identify information system weaknesses that are capable of being exploited for unauthorized access. Concurrent computing is a useful tool for streamlining this process since it enables concurrent processing of huge volumes of data.

Dynamic analysis, which is one of the techniques employed in security audits, [1] consists of executing code and observing its behaviour to determine possible security vulnerabilities. Parallel data processing allows for such analysis at the level of the entire system, quickly detecting anomalies in real time.

In addition, parallel computing is effectively used to test systems for penetration. For example, when scanning a network, several segments can be checked simultaneously, which significantly speeds up the process of identifying weaknesses. This is especially important for large organizations where the number of network access points can be measured in thousands.

*Protecting data with parallel computing*

Parallel computing also plays an important role in direct data protection. One of the key areas is real-time encryption. Encryption is a process that requires significant computing resources, especially when it comes to large amounts of data. Parallel algorithms allow you to distribute the load among several processors, which speed up key generation and processing of encrypted data.

Another important aspect is distributed security systems. [2] Clusters or massively parallel systems (MPP) provide high availability and resistance to DDoS attacks through load distribution across a number of nodes. Such systems automatically adapt to the situation, thereby proving to be efficient in fending off various kinds of cyberattacks.

*Advantages and limitations of parallel computing in cybersecurity*

Parallel computing has several benefits that make it vital in the cybersecurity sector. To begin with, it can efficiently enhance the rate of data processing, which is central to the analysis of vast amounts of data. Secondly, it supports simultaneous processing of various tasks, hence enhancing the efficiency of security systems. [3]

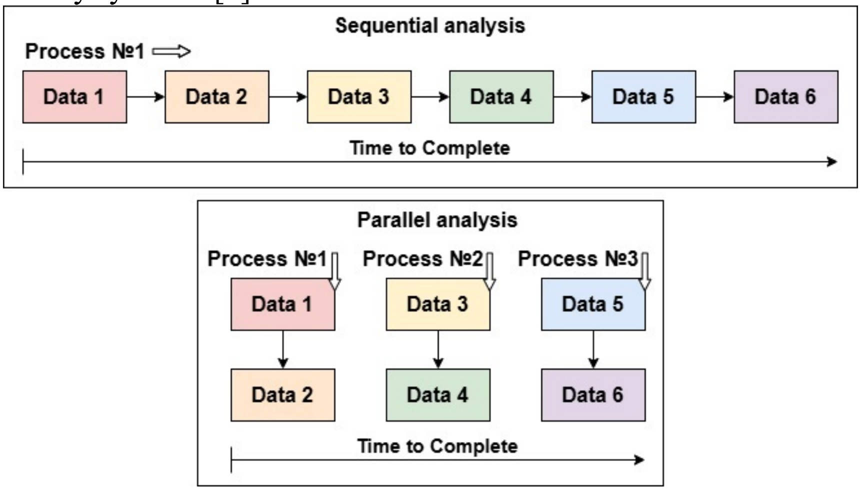

*Figure 1: An example of the dependence of the time required to process and analyse large amounts of data on dedicated processes*

There are, however, some limitations. Parallelization of most cybersecurity procedures, for instance, is typically hampered by synchronization needs or data dependencies. In addition, the implementation of parallel solutions may require significant investment in infrastructure and professional development.

*Development prospects*

The further development of parallel computing in cybersecurity is associated with integration with artificial intelligence and machine learning technologies. These technologies make it possible to automate threat detection and response processes, which are required by contemporary information systems. [4]

The other crucial domain involves optimizing the efficiency of energy consumption and forming adaptive algorithms which can execute successfully on a wide range of hardware platforms. This will make parallel computing more accessible to a wide range of organizations.

*Conclusions*

Parallelization is a powerful tool in modern cybersecurity that allows you to effectively solve the problems of vulnerability analysis, data protection, and threat response. However, it is important to consider technical, economic, and organizational aspects for their successful application. The continued expansion of this industry comes from applying new emerging technologies and developing better current solutions. The application of parallel computing can potentially greatly accelerate the processing time of huge datasets, a key necessity for systems working in real-time environments.

*List of references*

7. Lark Editorial Team, “Parallel processing,” May 26, 2024. https://www.larksuite.com/en_us/topics/cybersecurity-glossary/parallel-processing

8. “Distributed Power-Generation systems and protection,” *IEEE Journals & Magazine | IEEE Xplore*, Jul. 01, 2017. https://ieeexplore.ieee.org/abstract/document/7926394

9. A. R. Chowdhury, “How parallel testing improves your workflow?,” *LambdaTest*, Aug. 18, 2022. https://www.lambdatest.com/blog/how-parallel-testing-instantly-improves-your-workflow/

10. D. B. Johnson, “Google hopes its experimental AI model can unearth new security use cases,” *CyberScoop*, Apr. 08, 2025. [Online]. Available: https://cyberscoop.com/google-sec-gemini-experimental-ai-cybersecurity-assistant/