International Journal of Religion
2024
Volume: 5| Number 9 | pp. 1047 – 1061
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/vy58r270

Application of Innovations in Technical and Technological Updating of Ensuring the Security of Employees Databases of Engineering Enterprises: A Parallel-Vertical Approach to Optimizing Personnel Management

Lesia Danchak[1], Olena Orlova[2], Nila Tiurina[3], Mykola Kuzminov[4] and Tatiana Nazarchuk[5]

Abstract

The main purpose of the article is to present a modern method of parallel-vertical data security, which, thanks to the counting of units in the i-th input bit slice and the parallel formation of the i-th bit slice of a sorted array of numbers, reduces the protection time. The object of the study is the personnel database of an engineering company. The research methodology involves the use of parallel sorting methods for the development of technical and technological means for ensuring the security of data arrays, methods for parallel search for maximum and minimum values for the development of hardware and software tools for searching for maximum and minimum values. The practical aspect of the obtained results lies in the development of technologies for parallel sorting and retrieval of data in real time with high efficiency in the use of equipment. A hardware structure is presented for simultaneous parallel-vertical search for maximum and minimum numbers to increase the speed of ensuring the security of personnel databases. The innovativeness of the results obtained lies in the schematic representation of the proposed approach to application. The diagrams themselves are the author's vision. The structure of a parallel-flow device for ensuring the security of a two-dimensional array of numbers using the displacement method is presented. In our opinion, such a technical-technological update will serve as an innovation in the context of the security of personnel databases of an engineering company.

Keywords: *Security and Safety, Innovations, Optimization Methods, Modeling, Engineering Company, Database, Database Security, Personnel, Technical and Technological Renewal*

INTRODUCTION

In the digital era, databases are central to the operations and strategic decision-making of engineering companies. They contain critical information, ranging from intellectual property and business strategies to employees' personal data. Protecting these databases has become not just a technical and technological renewal but a crucial business imperative. For companies, the personal data of employees—such as social security numbers, addresses, financial information, and health records—represents a vulnerable treasure trove that can be exploited if not adequately secured. The importance of protecting these databases stems from the ethical responsibility to safeguard individuals' privacy, the legal implications of data breaches, and the potential financial and reputational damage to the engineering company (Maceika, Toločka, 2021). Firstly, from an ethical standpoint, companies have a moral obligation to protect the personal information of their employees. This information is shared in confidence, with the expectation that it will be used only for legitimate business purposes and not exposed to unnecessary risk. A breach of this trust can have far-reaching implications for employees, including identity theft, financial loss, and personal distress. Consequently, ensuring the security of databases is fundamental to maintaining trust within the organization, and fostering a culture of respect and responsibility towards personal data (Ramanauskaitė, Slotkienė, 2019).

In today's world, where cyber threats and personnel privacy protection are becoming increasingly important, technology innovation as an innovation plays a key role in ensuring security of personnel databases of an engineering company. This process not only introduces advanced technologies, but also creates new standards

[1] Department of Business Economics and Investment, Lviv Polytechnic National University, Lviv, 79000, Ukraine

[2] Precarpathian Institute named M. Hrushevsky of Interregional Academy of Personnel Management, Lviv, Ukraine; E-mail: bestmaktorn@gmail.com

[3] Department of Management and Administration, Khmelnytskyi National University, Khmelnytskyi, Ukraine
[4] Department of Marketing and Business Management, Pavlo Tychyna Uman State Pedagogical University, Uman, 55000, Ukraine

[5] Department of Management and Administration, Khmelnytskyi National University, Khmelnytskyi, Ukraine

for processing and protecting sensitive information. Updating software and hardware, using modern cryptographic techniques and implementing comprehensive security systems is not just a response to current threats, but a strategic initiative to ensure long-term data stability and reliability. These measures not only strengthen data protection, but maintain the company's reputation as a leading employer and partner (Tseng, et al., 2022).

The need for constant updating of database security is driven by several critical factors that underscore its importance in safeguarding sensitive information and ensuring the ongoing viability of business operations. This necessity is rooted in the evolving landscape of cyber threats, the rapid advancement of technology, and the changing regulatory environment. The nature of cyber threats is dynamic and ever-evolving. Hackers and cybercriminals are continually developing new techniques and tools to exploit vulnerabilities in database systems. As security measures become more sophisticated, so too do the methods used by attackers to breach them. This constant arms race between attackers and defenders makes it imperative for companies to regularly update their database security measures. Failing to do so can leave databases susceptible to emerging threats, which could result in unauthorized access, data theft, or loss. Regular updates ensure that security measures are equipped to defend against the latest cyber threats, thereby protecting sensitive information from being compromised.

The main purpose of the article is to present a modern method of parallel-vertical data security, which, thanks to the counting of units in the i-th input bit slice and the parallel formation of the i-th bit slice of a sorted array of numbers, reduces the protection time. The object of the study is the personnel database of an engineering company (Alazzam, et al., 2023).

Ensuring the security of personnel databases in engineering companies has become a critical concern due to the increasing sophistication of cyber threats and the essential nature of maintaining data integrity and confidentiality. Despite advancements in data protection technologies, there remains a significant gap in efficiently securing these databases while minimizing protection time. Traditional methods often fall short in addressing the high-speed demands and real-time security needs of modern engineering environments. This study introduces a novel parallel-vertical data security method aimed at filling this gap by leveraging parallel sorting and search techniques to enhance data protection efficiency. The primary objective is to develop and present a hardware structure that enables the simultaneous parallel-vertical search for maximum and minimum values, thereby accelerating the security processes of personnel databases. By focusing on the integration of innovative technical and technological updates, this research aims to provide a more effective solution for safeguarding sensitive personnel information within engineering companies.

The structure of the article consists of a literature review, methodology, presentation of results, discussion and conclusions.

LITERATURE REVIEW

The imperative to secure databases, especially in engineering companies with sensitive personnel information, demands a sophisticated blend of technical and technological updates. This literature review explores various approaches and methodologies related to database security, drawing upon a selection of scholarly works that contribute to the foundational understanding and innovative approaches within the field. Kryshtanovych et al. (2023) present a graphical language-based approach for database modeling in higher education information systems, emphasizing the importance of intuitive and accessible database design for enhanced security and usability. This work underscores the relevance of effective database architecture in safeguarding data integrity and facilitating secure information systems. Similarly, Nazarov, Nazarov, & Ţălu (2021) address the information security challenges within the Internet of Things (IoT) ecosystem, highlighting the increasing complexity of database security in interconnected environments. Their findings point to the necessity of innovative security frameworks that can adapt to the expansive nature of IoT networks. The evolution of e-learning and personalized learning paths, as discussed by Jiang et al. (2022)] and Ovtšarenko (2023), provides insight into the potential of data-driven approaches for enhancing learning experiences. These methodologies, while primarily focused on educational outcomes, suggest a broader applicability in terms of data handling and

security within complex systems, illustrating the potential for leveraging data analytics in the development of secure database management systems. Glado et al. (2021) and Maceika & Toločka [4] delve into the specifics of engineering services contracts and the motivation for engineering change in industrial companies, respectively. Their contributions reflect on the broader implications of secure and efficient data management for business operations, emphasizing the importance of technical and technological updates in maintaining competitive advantage and ensuring operational security. Wang & Zhu (2019) explore the application of a quadtree spatial index method for updating landcover databases, offering a perspective on the importance of spatial data integrity. Ellefsen & von Solms (2010) discuss critical infrastructure protection in the developing world, highlighting the global challenges and necessities in securing essential services against cyber threats. These studies collectively underline the critical role of database security across various domains, including geographic information systems and critical infrastructure.

Research by Ying (2016), Putro & Sensuse (2022), and Li et al. (2018) explores the intersections between learning technologies, security principles, and the generation of learning paths. These contributions emphasize the role of technological innovation in both educational and security contexts, suggesting a synergistic approach to developing systems that are both effective in their purpose and secure from potential threats. The economic security of engineering enterprises, as investigated by Sylkin et al. (2018) and Khalina et al. (2019), points to the broader implications of database security on financial stability and organizational resilience. These works contribute to a nuanced understanding of how technical and technological updates in database security can support the overarching goals of economic security and crisis management within engineering firms.

Maček, Magdalenić, and Ređep (2020) provide a comprehensive review of the application of multicriteria decision-making (MCDM) methods for information security risk assessment. Their systematic analysis underscores the utility of MCDM in evaluating and mitigating risks, highlighting the need for robust frameworks that can handle the multifaceted nature of database security in engineering enterprises . This foundational work supports the integration of advanced decision-making processes in developing secure database systems. Goyal, Kumar, and Kumar (2020) extend the discussion on MCDM methods by exploring their application in sustainability. Their review reveals the importance of incorporating sustainability into decision-making, which is pertinent to data security by ensuring long-term effectiveness and resource efficiency. The insights from their work are instrumental in shaping sustainable security strategies for engineering companies . Yamuna Devi (2021) introduces a Parallel Direct-Vertical Map Reduce Programming model for effective frequent pattern mining in dispersed environments, closely aligned with our proposed method. Her research demonstrates the advantages of parallel processing in data analysis and security, showing significant improvements in processing speed and efficiency. This model's principles are applied in our study to enhance the protection of personnel databases through parallel-vertical data security techniques. Kuzmenko, Dotsenko, and Koibichuk (2021) focus on developing database structures for internal economic agents' financial monitoring. Their findings emphasize the importance of well-designed database architectures that support robust security measures. Their work provides valuable structural and architectural insights crucial for securing personnel databases in engineering companies.

The innovative parallel-vertical approach to database security detailed in the article marks a significant advancement in protecting personnel databases in engineering companies. However, as with any pioneering research, there are inherent gaps and areas that warrant further investigation to enhance understanding and application. Here are some of the main gaps (Table 1).

Table 1. The main gaps in Literature

№	Gaps	Characteristics

1	Long-term Sustainability and Maintenance	The long-term sustainability and maintenance of the proposed hardware and software tools are not fully addressed. This includes understanding the lifecycle of the technology, ongoing maintenance requirements, potential obsolescence, and upgrade paths to ensure continuous security enhancements
2	Cost-Benefit Analysis	The financial implications of implementing the proposed security measures are not detailed in the study. A comprehensive cost-benefit analysis, considering the initial investment, operational costs, and potential savings from averting data breaches, would provide valuable insights for decision-makers
3	Impact on Data Processing Speed and System Performance	The study asserts that the proposed method reduces protection time but does not extensively explore its impact on overall data processing speed and system performance. Further research is needed to quantify these effects, particularly in high-volume, time-sensitive environments

In conclusion, the reviewed literature provides a comprehensive backdrop against which our research on implementing a parallel-vertical approach to database security is situated. These studies not only highlight the multifaceted challenges of securing databases in various contexts but also underscore the potential for innovative approaches to enhance security and operational efficiency. Our work builds upon these foundations, proposing a novel methodology that addresses the specific challenges of securing personnel databases in engineering companies.

METHODOLOGY

The methodology of our research hinges on the innovative concept of parallel-vertical data security. This approach is tailored specifically for enhancing the security mechanisms of personnel databases within engineering companies. By focusing on parallel processing techniques, our methodology addresses the critical need for swift and efficient data protection solutions. We employ a combination of parallel sorting algorithms, along with hardware and software tools designed to expedite the search for maximum and minimum values within data arrays. The essence of our methods lies in their ability to significantly reduce protection time without compromising the integrity or confidentiality of the data.

In our article, the sample size in the experiment is intentionally kept small, focusing exclusively on the personnel database of a single engineering enterprise, to maintain a controlled environment that allows for precise measurement and analysis of the proposed parallel-vertical data security method.

At the core of our methodology is the utilization of parallel sorting algorithms. These algorithms are crucial for organizing and managing large datasets efficiently. By implementing a parallel sorting mechanism, we aim to minimize the time required for data processing, thereby reducing the window of vulnerability during which data could potentially be compromised. This is achieved through the parallel formation of the i-th bit slice of a sorted array of numbers, allowing for faster data manipulation and retrieval. The efficiency of parallel sorting not only accelerates the protection process but also enhances the overall performance of the database management system. In conjunction with parallel sorting, our methodology incorporates parallel search techniques for identifying maximum and minimum values within the dataset. This approach is instrumental in developing hardware and software solutions that swiftly pinpoint critical data points. Such capabilities are particularly valuable in scenarios where rapid data assessment is required to enforce security measures. By

leveraging parallel search methods, we facilitate a more dynamic and responsive security framework, capable of adapting to evolving threats and vulnerabilities.

The parallel-vertical data security algorithm introduced in this study is designed to enhance the protection efficiency of personnel databases by leveraging parallel processing techniques. At its core, the algorithm operates by counting units in the i-th input bit slice and concurrently forming the i-th bit slice of a sorted array of numbers. This approach allows for the simultaneous handling of multiple data elements, significantly reducing the overall time required for data protection. The algorithm integrates parallel sorting methods, enabling the rapid organization of data arrays, and employs parallel searches to identify maximum and minimum values within these arrays. By utilizing a hardware structure that supports parallel-vertical operations, the algorithm can perform real-time data sorting and retrieval with high efficiency, ensuring robust security for the personnel databases.

RESULTS AND DISCUSSIONS

The current stage of development of technical and technological updating of database security systems for engineering companies is characterized by the expansion of areas of their application, a significant part of which is associated with the accumulation, sorting and retrieval of data in real time. Such applications include systems for collecting and preprocessing telemetry data, managing complex objects, automated systems for multi-level process control, where large volumes of data are accumulated at the lower levels, requiring preprocessing in real time. When preprocessing data sets, it is often necessary to use data sorting and searching operations, which can take up to 40% of the total time spent working with databases by engineering company personnel. To effectively process data streams, real-time data security technologies are required, based on new and improved methods and models that should be focused on parallel-streaming data flow and adaptation to the intensity of data flow. Real-time data security requires the development of new methods and algorithms focused on modern hardware (graphics processors and programmable logic integrated circuits). That is, a technical and technological update is needed.

To ensure safety and search for maximum and minimum values in real time, it is necessary to create specialized technical and technological means with high efficiency in the use of equipment. It is advisable to implement the hardware implementation of parallel-vertical security of a one-dimensional array of numbers in the form of an ultra-large-scale integrated circuit. The expense of an ultra-large-scale integrated circuit designed for parallel-vertical sorting of a one-dimensional array of numbers is mainly influenced by the chip's area. This area is largely dictated by the number of transistors needed for the implementation and the number of external pins, which are constrained by the die size and the technology level.

Parallel-vertical security of a one-dimensional array of numbers Dk Nk=1 provides for the arrival of a bit slice of N numbers at each clock cycle and its sorting. The structure of an extra-large integrated circuit - a device for parallel-vertical sorting of a one-dimensional array of numbers Dk Nk=1 synthesized on the basis of the developed PE is shown in Fig. 1, where TI is a clock input; PU – initial installation input; Dki – input of the i-th digit of the k-th number; EC – control element; TgD – data trigger; TGU – control trigger; Dki – output of the ith digit of the kth sorted number.

Let's build a network to achieve the key goal of modeling A0, namely improving criminal legislation in Jordan (Fig. 2).

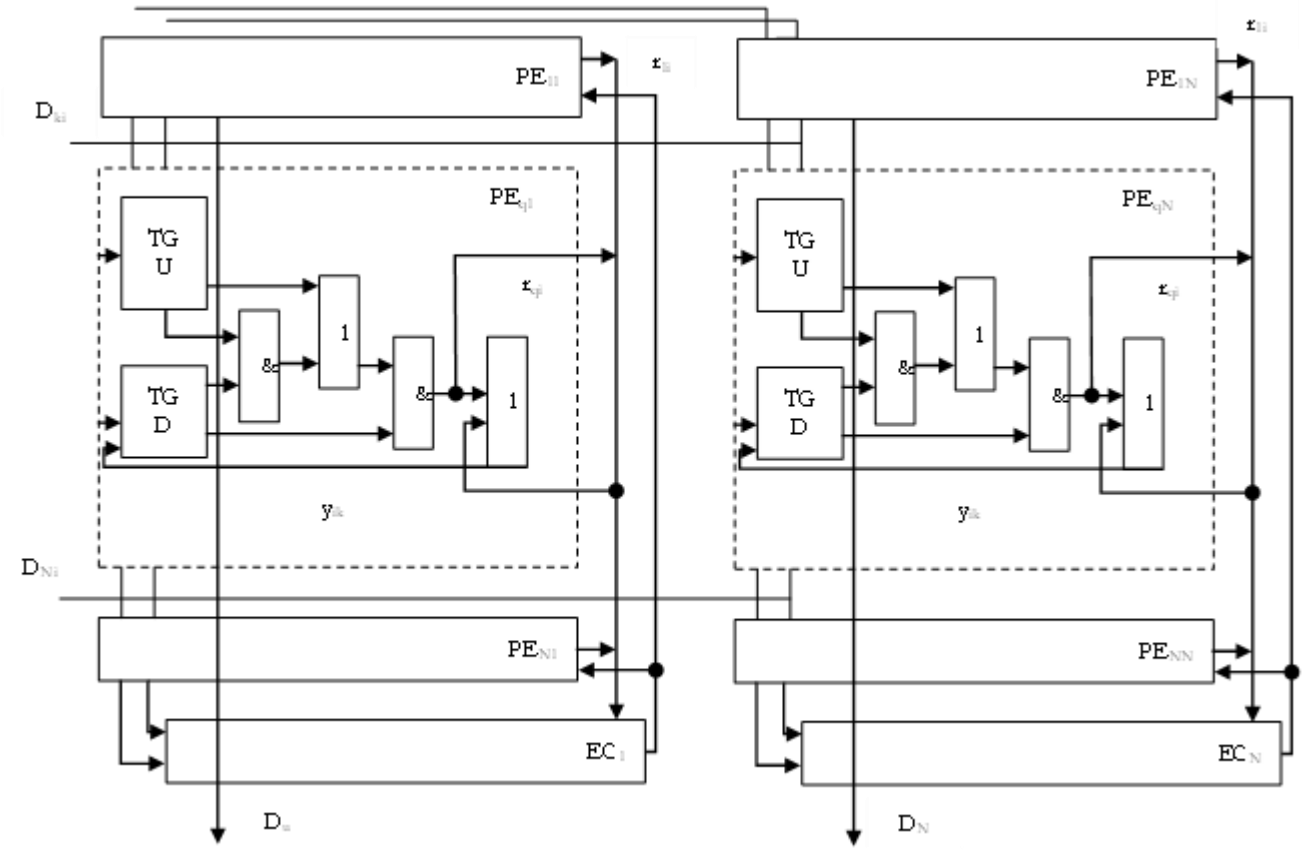

Figure 1. The architecture of a very large integrated circuit device for parallel-vertical security of personnel data through a one-dimensional array of numbers

The structure of a very large integrated circuit (VLSI) device designed for parallel-vertical sorting of personnel data through a one-dimensional array of numbers is matrix-based and consists of N×N processing elements (PE) and N execution units (EU). The formation of the i-th digit of the k-th sorted number is performed by N PEs, which are vertically connected via a common bus to form the p-th column, where p ranges from 1 to N. Each p-th column of PEs is managed by an execution unit (EUp), whose structure is illustrated in Fig. 2. This structure includes a multi-input adder (BCm), a register (Rr), a subtractor (VID), a comparison scheme (SP), and a trigger (TG).

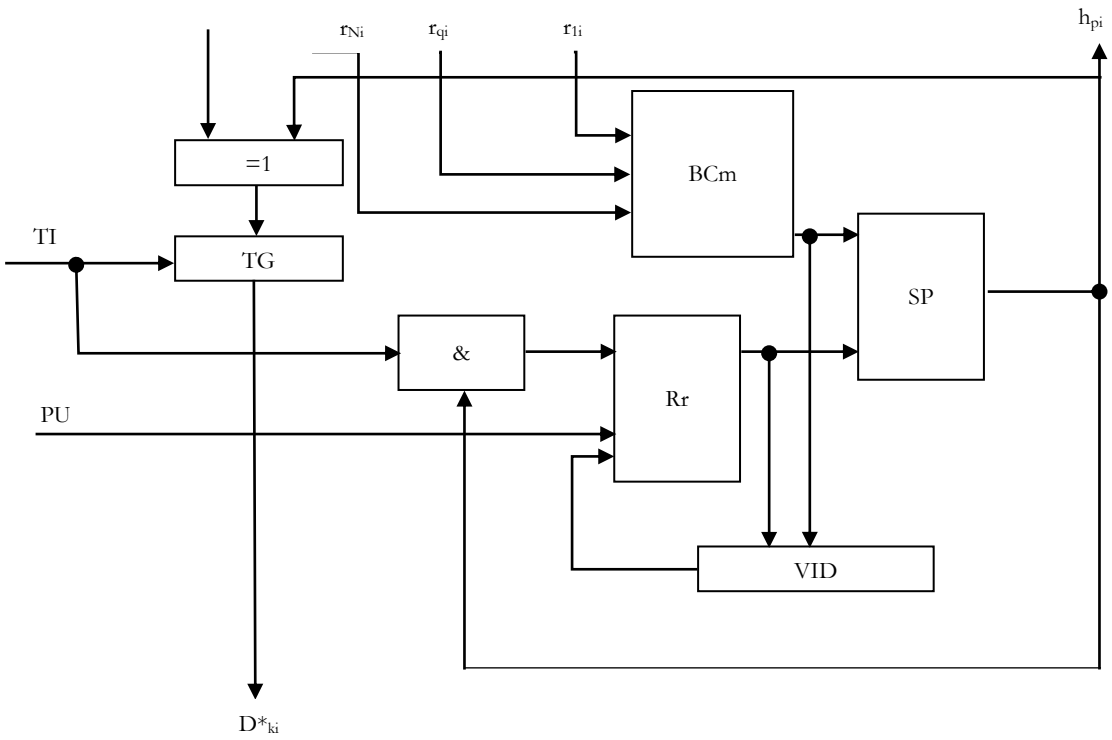

Figure 2. The structure of the k-th database management element

Equipment costs for the implementation of an extra-large integrated circuit device for parallel-vertical sorting of a one-dimensional array of numbers are equal to (1):

$$Wc1=N2(2Wt+4Wi)+N(2Wt+Wp+WVID+WBC+WSP+2Wi) \quad (1)$$

where Wt, WI, Wrr, WBC, WSP та WVID – are hardware costs for the implementation of the flip-flop, type I logic elements, register, N-input one-bit adder, comparison circuit, and subtractor, respectively.

Consider securing a one-dimensional array of M numbers, where M=N×b, using the developed very large integrated circuit device for parallel-vertical sorting of an array of N numbers. The suggested method for this sorting is merge sort. As previously mentioned, the core of security algorithms using the merge method involves the macro operation of merging two ordered subarrays into one ordered array. These first-type macrooperations are executed on three very large integrated circuit devices designed for parallel-vertical sorting of N numbers. These devices are combined into a first-type sorting block, as illustrated in Fig. 3.

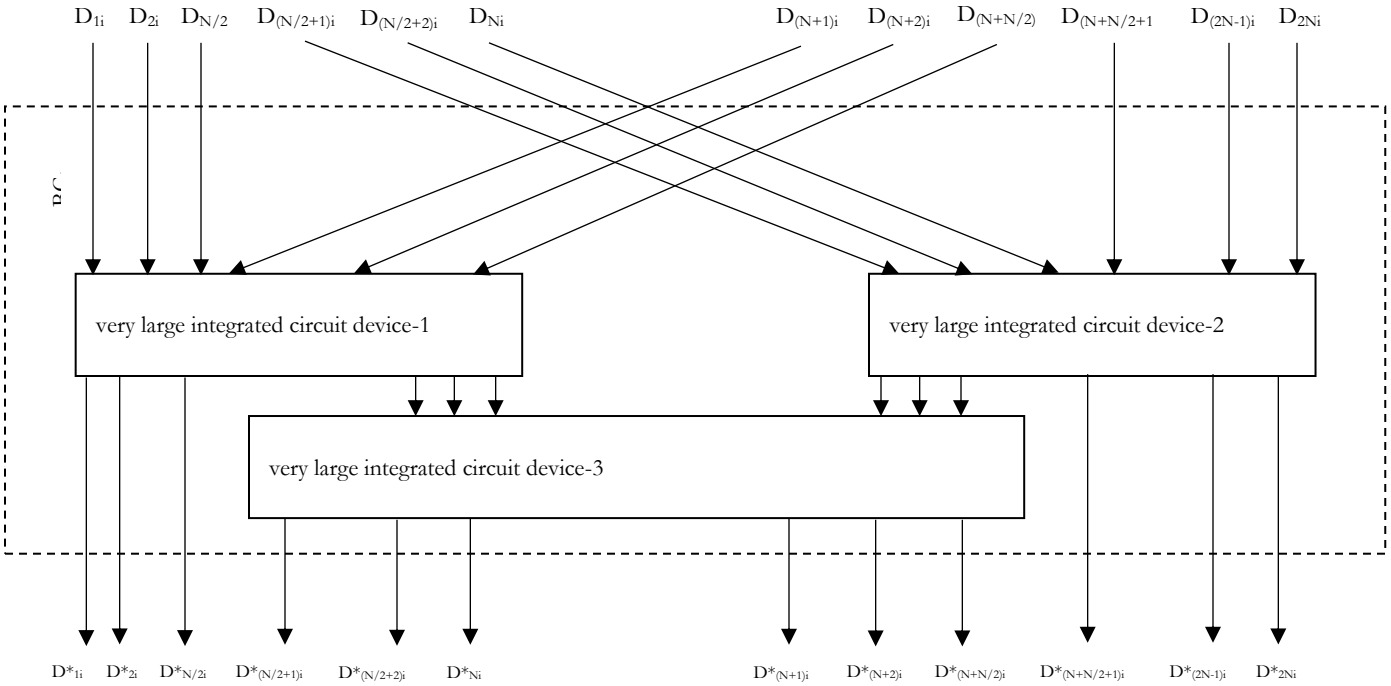

Figure 3. Scheme of the first type of sorting safety block

One approach to increasing the speed of secure sorting for a two-dimensional array of numbers is to boost the number of basic macrooperations performed in parallel by developing parallel-thread structures. The flow security graph for the parallel-flow sorting algorithm of a two-dimensional array of numbers, represented as {Dhj}N/2; Mh=1, by the displacement method is shown in Fig. 4. In this figure, U represents the control input, 1-N/2 are the data inputs, PEk is the jth processor element, FUj1 and FUj2 are the first and second PEj control operators, FKj1 and FKj2 are the first and second switching operators for PEj, FPj1 and FPj2 are the first and second memory operators for PEj, and FS is the operator for sorting N numbers.

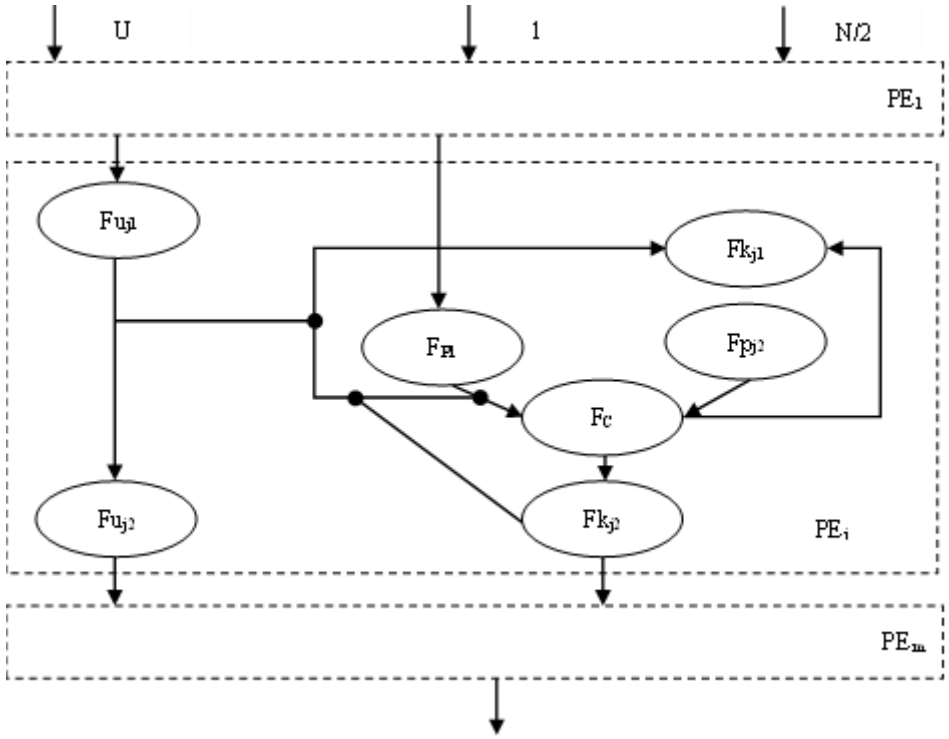

Figure 4. Flowchart of a security algorithm for parallel-stream sorting of a two-dimensional array of numbers using the displacement method

The structure of a parallel-flow device for sorting a two-dimensional array of numbers by the displacement method is shown in Fig. 5, where TI is the input of clock pulses; U – control input; Input1 – InputN/2 data inputs; PE – processor element; Tg – trigger; P - memory; Km - switch; Very large integrated circuit device – very large integrated circuit device sorting N numbers; Output1 – OutputN/2 – outputs of sorted data. landscape.

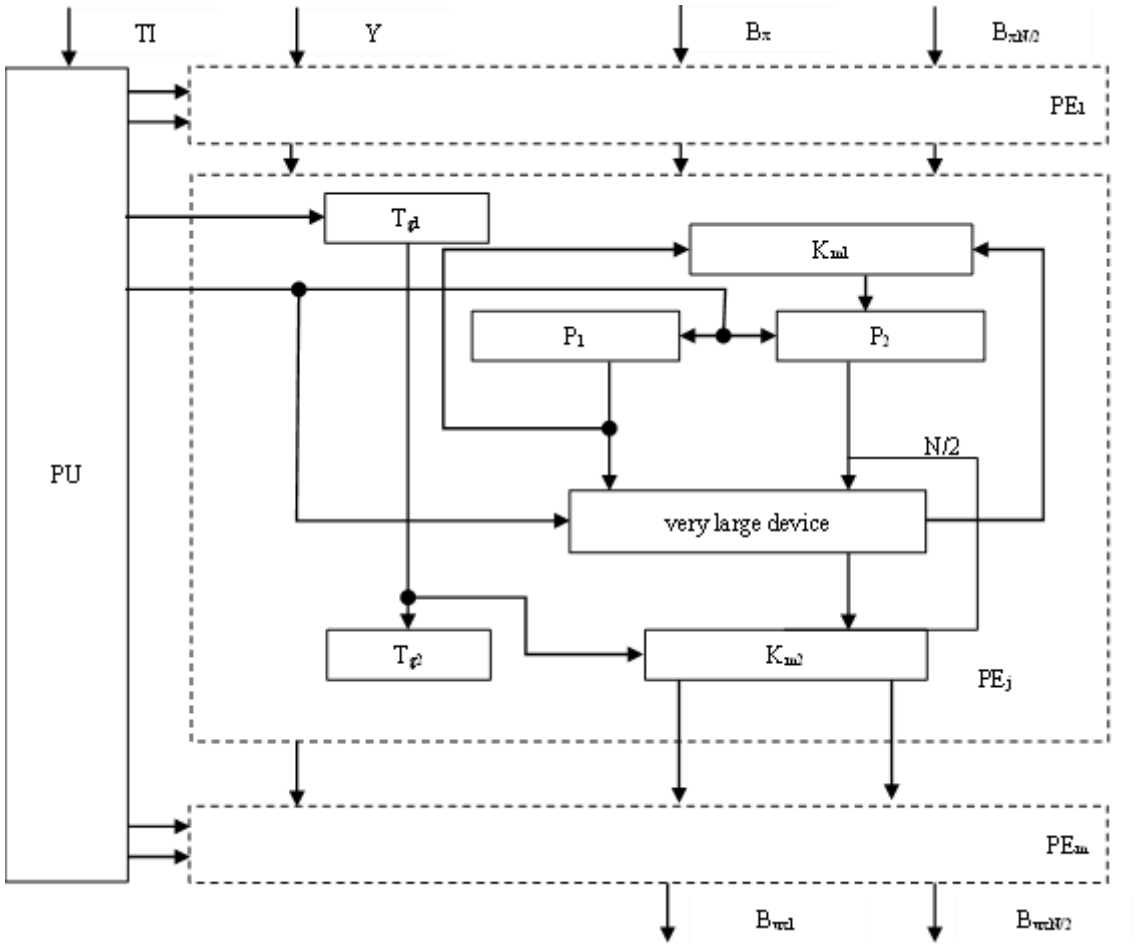

Figure 5. Architecture of a parallel-flow security device for a two-dimensional array of numbers utilizing the displacement method Parallel-vertical security of arrays of large numbers using the developed very large integrated circuit device provides a reduction in sorting time due to the conveyor organization of sorting and the formation of sorted bit pairs in each cycle

The structure of the hardware tool was developed for the simultaneous parallel-vertical secure search of the maximum and minimum numbers in both one-dimensional Dk Nk=1 and two-dimensional Dk N;Mk=1 arrays of data about the engineering personnel of the enterprise, which is shown in Fig. 6.

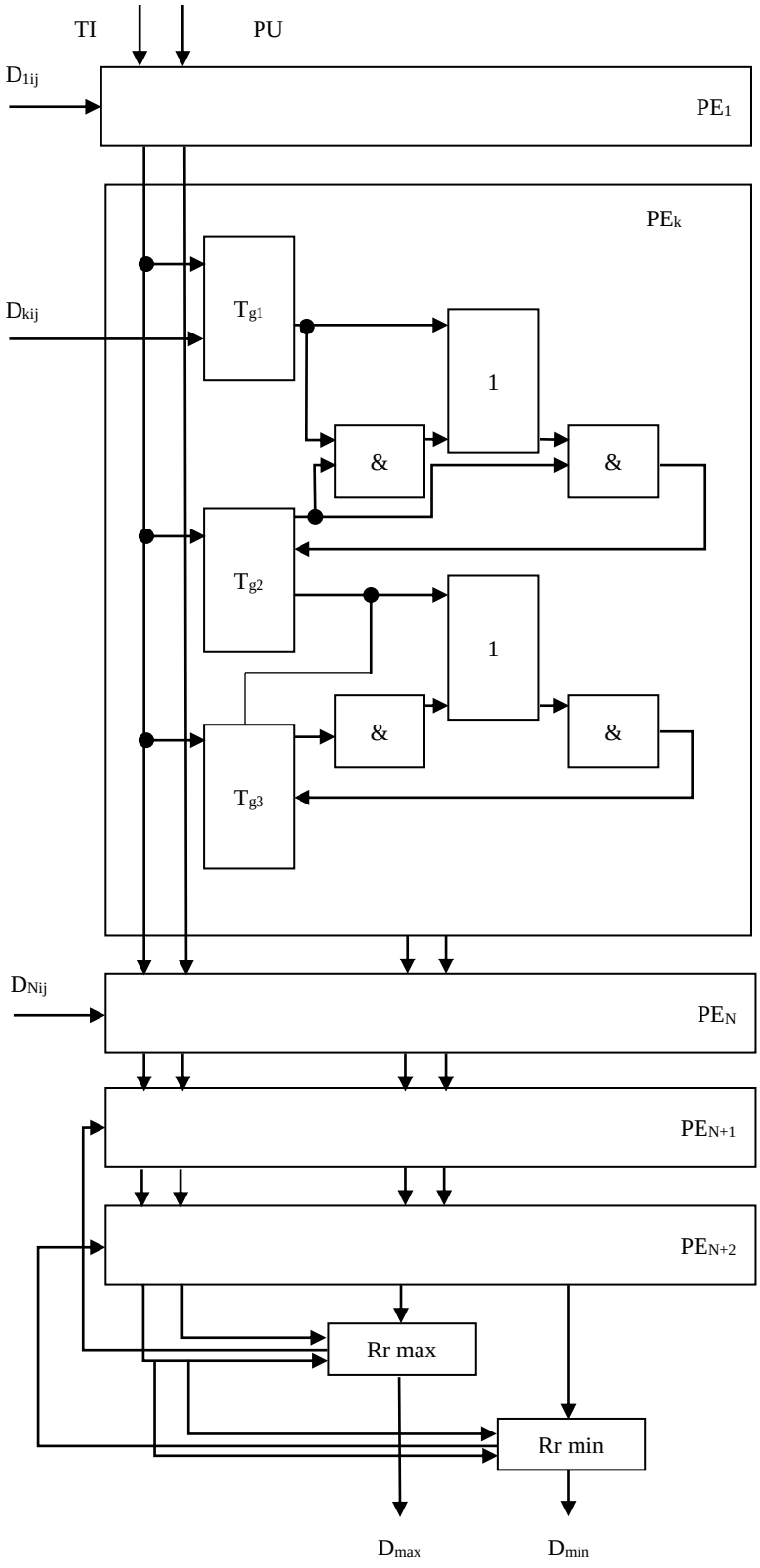

Figure 6. Hardware design for simultaneous parallel-vertical security search of maximum and minimum numbers

The number of PEs connected to the common bus of results, during the simultaneous calculation of the maximum and minimum numbers for a one-dimensional array Dk Nk=1 is determined by the size of the array. The use of a common bus of results ensures parallelization of the process of processing the bit slice, the processing time of which determines the clock of the device.

The use of parallel and vertical data processing methods—such as parallel sorting and searching for maximum and minimum values—significantly speeds up the processing of large datasets. In the context of engineering enterprises, where time and efficiency are critical, these methods can drastically reduce the time needed for data operations, ensuring that personnel data can be managed and secured more quickly. Introducing new methods and technologies for database management, such as the parallel-flow device for securing a two-dimensional array of numbers, represents an innovative step forward. This innovation is key to adapting to the evolving challenges in data security and management faced by modern engineering enterprises.

The proposed parallel-vertical data security method offers significant economic benefits, primarily through enhanced efficiency and reduced operational costs. By leveraging parallel processing techniques, the method significantly decreases the time required for data protection tasks, allowing engineering companies to allocate their resources more effectively. This efficiency translates into lower labor costs as fewer personnel are needed to manage and oversee data security operations. Additionally, the real-time data sorting and retrieval capabilities reduce downtime and increase the productivity of the existing infrastructure, leading to better utilization of hardware and software investments.

Zhou et al. (2023) propose a topological computation model based on Euler numbers for updating land parcel databases. While Zhou and colleagues' work focuses on the spatial data integrity and continuity in geographical information systems, our approach emphasizes the speed and efficiency of data protection in personnel databases. Both methods aim to enhance database security and integrity, but our research extends the applicability of parallel processing techniques to a broader range of data types, beyond the geographical data. Fakiha (208) discusses business organization security strategies against cyber threats. Fakiha's emphasis on comprehensive security strategies resonates with our research's focus on employing both hardware and software tools for database security. However, our approach advances this discussion by detailing a specific, technical method for enhancing security measures, thereby offering a more direct and implementable solution to protecting against cyber threats. Rasheed & Wahid (2019) explore sequence generation for learning transformation, which, although primarily focused on educational technology, shares with our study the underlying theme of utilizing advanced algorithms for data management. Our research diverges by applying parallel processing for security purposes, showcasing the versatility of algorithmic methods across different domains, including the critical area of database security. Minn (2022) investigates AI-assisted knowledge assessment techniques, highlighting the potential of artificial intelligence in analyzing and managing data. This parallels our integration of hardware and software for data security, suggesting a future direction for our research that could incorporate AI and ML algorithms to predict and preempt security threats.

Salim, et al. (2021), Raghu, Sadanandam (2021), Amghar,et al. (2023), and Vainer (2023) present insights into data analytics, schema integration for big data, and password dataset generation, respectively. These studies underscore the importance of data analysis and management in various contexts. Our work complements these efforts by providing a framework for securing databases against unauthorized access, which is paramount for ensuring the integrity and privacy of the data being analyzed and managed. Dallaev et al.(2023) discuss the applications and challenges of the Internet of Things (IoT), highlighting the growing need for robust security measures in the face of expanding IoT networks. Our parallel-vertical approach could be particularly relevant in this context, offering a scalable and efficient method for securing databases that are increasingly interconnected with IoT devices.

Alazzam et al. (2023) explore the formation of innovative models for e-commerce development, focusing on business economic security. Their study highlights the necessity of aligning security measures with legal and regulatory frameworks, ensuring compliance and robust protection. This alignment is critical for engineering companies that must adhere to strict regulatory standards while safeguarding their databases . Tubishat et al.

(2024) discuss the planning required to improve the efficiency of open systems commercial relations, emphasizing the importance of uninterrupted and sustainable development from a regional legal perspective. Their research underlines the significance of strategic planning and legal compliance in maintaining secure and efficient systems, which is directly applicable to the management of personnel databases in engineering companies . Bazyliuk et al. (2019) provide a comparative analysis of the institutional dynamics in regional development publishing and printing activities in Ukraine, offering methodological and practical insights. Although their focus is on a different industry, the methodological approaches and practical considerations discussed are relevant for understanding the broader context of database security and regional development dynamics.

Our research introduces a novel parallel-vertical approach for enhancing database security, particularly focusing on the personnel databases of engineering companies. This method, characterized by its use of parallel sorting and the efficient identification of maximum and minimum values through parallel search algorithms, represents a significant advancement in database security. In comparing our results with those from related works, we gain a broader perspective on our contribution to the field and the uniqueness of our approach. Our comparison with the aforementioned studies not only reaffirms the significance of our contributions but also illuminates potential pathways for future research.

Thus, the innovativeness of our research lies in technical and technological updating as an innovation in the context of security of personnel databases of engineering companies. This approach not only incorporates the latest technologies and methodologies, but also reflects a vision of comprehensively transforming existing data management systems to provide higher levels of security and privacy of personnel. Our research is aimed at developing and implementing integrated solutions to effectively counter modern cyber threats, thereby strengthening database security mechanisms and, accordingly, increasing the overall security of engineering companies.

CONCLUSION

The research presented in this article introduces a groundbreaking parallel-vertical approach to database security, specifically tailored for the protection of personnel databases within engineering firms. The core achievement of our study is the development and implementation of a method that significantly reduces the time required for data protection through the innovative use of parallel processing techniques. By employing parallel sorting methods alongside a novel application of parallel search algorithms for identifying maximum and minimum values, our approach not only enhances the speed but also the efficiency of database security protocols.

The practical effects of our findings are manifold. Firstly, the implementation of parallel sorting algorithms has demonstrated a remarkable improvement in the processing speed of large data sets, thereby reducing the vulnerability window during which data could be exposed to unauthorized access. Secondly, the development of hardware and software tools designed for parallel search operations has facilitated a more robust and dynamic response to security threats, ensuring rapid identification and protection of critical data points. Furthermore, the introduction of a specialized hardware structure for simultaneous parallel-vertical searches represents a significant technological advancement in the realm of database security. This hardware innovation, along with the parallel-flow device for securing two-dimensional data arrays, underscores our approach's potential to revolutionize the efficiency and effectiveness of data protection strategies in real-time scenarios.

Thus, the introduction of technical and technological updating in the context of security of personnel databases of an engineering company. Has enormous practical potential. This approach not only strengthens protective barriers against external attacks and internal information leaks, but significantly increases the speed and accuracy of data processing thanks to modern technologies. These innovations allow engineering companies to not only respond to current challenges, but also adapt to future technological changes, ensuring their sustainability and competitiveness in the market. Looking ahead, the promising results of our current research pave the way for several exciting avenues of future investigation. One key area of focus will be the exploration of advanced algorithms and techniques for further optimizing the parallel-vertical processing framework. This includes the development of more sophisticated parallel sorting and searching algorithms that can adapt to various data

types and structures, thereby broadening the applicability of our approach across different industries and data-intensive applications. Additionally, future research will delve into the integration of artificial intelligence (AI) and machine learning (ML) technologies to enhance the predictive capabilities of our security measures. By incorporating AI and ML algorithms, we aim to develop proactive security systems that can anticipate potential threats and vulnerabilities based on data patterns and trends, thereby offering a more preemptive approach to database protection. Moreover, the scalability and adaptability of the hardware structures introduced in this study will be a focal point of subsequent research efforts. Investigating the potential for modular and scalable hardware designs will ensure that our security solutions can be efficiently implemented in organizations of varying sizes and with diverse data management needs.

REFERENCES

Alazzam, F. A. F., Tubishat, B. M. A.-R., Savchenko, O., Pitel, N., & Diuk, O. (2023). Formation of an innovative model for the development of e-commerce as part of ensuring business economic security. Business: Theory and Practice, 24(2), 594–603. https://doi.org/10.3846/btp.2023.19781

Alazzam, F.A.F., Shakhatreh, H.J.M., Gharaibeh, Z.I.Y., Didiuk, I., Sylkin, O. (2023). Developing an information model for E-Commerce platforms: A study on modern socio-economic systems in the context of global digitalization and legal compliance. Ingénierie des Systèmes d'Information, Vol. 28, No. 4, pp. 969-974. https://doi.org/10.18280/isi.280417

Amghar, S., Cherdal, S., Mouline, S. (2023). A schema integration approach for big data analysis. Ingénierie des Systèmes d'Information, Vol. 28, No. 2, pp. 315-325. https://doi.org/10.18280/isi.280207

Bazyliuk, V., Shtangret, A., Sylkin, O., & Bezpalko, I. (2019). Comparison of institutional dynamics of regional development publishing and printing activities in Ukraine: methodological and practical aspects. Business: Theory and Practice, 20, 116-122. https://doi.org/10.3846/btp.2019.11

Dallaev, R., Pisarenko, T., Ţălu, Ştefan, Sobola, D., Majzner, J., & Papež, N. (2023). Current applications and challenges of the Internet of Things. New Trends in Computer Sciences, 1(1), 51–61. https://doi.org/10.3846/ntcs.2023.17891

Ellefsen, I., von Solms, S. (2010). Critical information infrastructure protection in the developing world. In: Moore, T., Shenoi, S. (eds) Critical Infrastructure Protection IV. ICCIP 2010. IFIP Advances in Information and Communication Technology, vol 342. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-16806-2_3

Fakiha, B. (2021). Business organization security strategies to cyber security threats. International Journal of Safety and Security Engineering, Vol. 11, No. 1, pp. 101-104. https://doi.org/10.18280/ijsse.110111

Glado, Y., Yavorska, O., Tarasenko, L., Tsilmak, O., & Matiienko, T. (2021). Features of the contract for engineering services in civil law of Ukraine: ways to improve the process in the context of improving business. Business: Theory and Practice, 22(2), 462-469. https://doi.org/10.3846/btp.2021.13537

Goyal, P., Kumar, D., & Kumar, V. (2020). Application of multicriteria decision analysis (mcda) in the area of sustainability: a literature review. International Journal of the Analytic Hierarchy Process, 12(3). https://doi.org/10.13033/ijahp.v12i3.720

Jiang, B., Li, X., Yang, S., Kong, Y., Cheng, W., Hao, C., & Lin, Q. (2022). Data-driven personalized learning path planning based on cognitive diagnostic assessments in MOOCs. Applied Sciences, 12(8), 3982. https://doi.org/10.3390/app12083982

Khalina, O., Bazyliuk, V., Chornenka, O., Krasilych, I., & Korzh, M. (2019). Formation of organizational support for the management of the economic security of engineering enterprises: methodical and practical aspects. Business: Theory and Practice, 20, 317-328. https://doi.org/10.3846/btp.2019.30

Kryshtanovych, S., Ivanytska, O., Markova, M., Hliudzyk, Y., Ivanova, A. (2023). A graphical language-based approach for database modeling in higher education information systems. Ingénierie des Systèmes d'Information, Vol. 28, No. 6, pp. 1597-1603. https://doi.org/10.18280/isi.280616

Kuzmenko, O., Dotsenko, T., & Koibichuk, V. (2021). Development of databases structure of internal economic agents financial monitoring. Financial and Credit Activity Problems of Theory and Practice, 3(38), 204–213. https://doi.org/10.18371/fcaptp.v3i38.237448

Li, Y., Shao, Z., Wang, X., Zhao, X., & Guo, Y. (2018). Concept map-based learning paths automatic generation algorithm for adaptive learning systems. IEEE Access, 7, 245–255. https://doi.org/10.1109/ACCESS.2018.2885339

Li, Z., Li, T., & Zhu, F. (2019). An online password guessing method based on big data. In Proceedings of the 2019 3rd International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence (pp. 59–62). https://doi.org/10.1145/3325773.3325779

Maceika, A., & Toločka, E. (2021). The motivation for engineering change in the industrial company. Business: Theory and Practice, 22(1), 98-108. https://doi.org/10.3846/btp.2021.13042

Maček, D., Magdalenić, I., Ređep, N.B. (2020). A systematic literature review on the application of multicriteria decision making methods for information security risk assessment. International Journal of Safety and Security Engineering, Vol. 10, No. 2, pp. 161-174. https://doi.org/10.18280/ijsse.100202

Minn, S. (2022). AI-assisted knowledge assessment techniques for adaptive learning environments. Computers and Education: Artificial Intelligence, 3, 100050. https://doi.org/10.1016/j.caeai.2022.100050

Nazarov, A., Nazarov, D., & Ţălu, Ş. (2021). Information security of the Internet of Things. In Proceedings of the International Scientific and Practical Conference on Computer and Information Security – (INFSEC 2021) (Vol. 1, pp. 136–139). Science and Technology Publications. https://doi.org/10.5220/0010619900003170

Ovtšarenko, O. (2023). Generation of a learning path in e-learning environments: literature review. New Trends in Computer Sciences, 1(1), 32–50. https://doi.org/10.3846/ntcs.2023.18278

Putro, P.A.W., Sensuse, D.I. (2022). Review of security principles and security functions in critical information infrastructure protection. International Journal of Safety and Security Engineering, Vol. 12, No. 4, pp. 459-465. https://doi.org/10.18280/ijsse.120406

Raghu, K., Sadanandam, M. (2021). A perspective study on speech emotion recognition: Databases, features and classification models. Traitement du Signal, Vol. 38, No. 6, pp. 1861-1873. https://doi.org/10.18280/ts.380631

Ramanauskaitė, S., & Slotkienė, A. (2019). Hierarchy-based competency structure and its application in e-evaluation. Applied Sciences, 9(17), 3478. https://doi.org/10.3390/app9173478

Rasheed, F., & Wahid, A. (2019). Sequence generation for learning: a transformation from past to future. International Journal of Information and Learning Technology, 36(5), 434–452. https://doi.org/10.1108/IJILT-01-2019-0014

Salim, S., Turnbull, B., & Moustafa, N. (2022). Data analytics of social media 3.0: Privacy protection perspectives for integrating social media and Internet of Things (SM-IoT) systems. Ad Hoc Networks, 128, 102786. https://doi.org/10.1016/j.adhoc.2022.102786

Sylkin, O., Shtangret, A., Ogirko, O., Melnikov, A. (2018). Assessing the financial security of the engineering enterprises as preconditions of application of anti-crisis management: practical aspect. Business and Economic Horizons, 14(4): 926-940. https://doi.org/10.15208/beh.2018.63

Tseng, F. S. C., Yeh, C.-T., & Chou, A. Y. H. A (2022). Collaborative framework for customized e-learning services by analytic hierarchy processing. Applied Sciences, 12, 1377. https://doi.org/10.3390/app12031377

Tubishat, B.M.A.R., Alazzam, F.A.F., Viunyk, O., Yatsun, V., Horpynchenko, O. (2024). Planning to improve the efficiency of open systems commercial relations to ensure uninterrupted sustainable development: Regional legal aspect. International Journal of Sustainable Development and Planning, Vol. 19, No. 3, pp. 1089-1097. https://doi.org/10.18280/ijsdp.190327

Vainer, M. (2023). Multi-purpose password dataset generation and its application in decision making for password cracking through machine learning. New Trends in Computer Sciences, 1(1), 1–18. https://doi.org/10.3846/ntcs.2023.17639

Wang, H.S., Zhu, J.Y. (2019). A quadtree spatial index method with inclusion relations and its application in landcover database update. Ingénierie des Systèmes d'Information, Vol. 24, No. 3, pp. 241-247. https://doi.org/10.18280/isi.240303

Yamuna Devi N. A (2021) Parallel Direct-Vertical Map Reduce Programming model for an effective frequent pattern mining in a dispersed environment. Concurrency Computat Pract Exper. 33(24):e6470. https://doi.org/10.1002/cpe.6470

Ying F.Q. (2016). Research on blended learning mode based on the micro-lecture in database application, Review of Computer Engineering Studies, Vol. 3, No. 3, pp. 62-66. DOI: 10.18323/rces.030303

Zhou, X.G., Chen, J., Zhan, F.B., Li Z.L., Madden, M., Zhao, R.L., Liu, W.Z. (2013). A Euler-number-based topological computation model for land parcel database updating. International Journal of Geographical Information Science, 27(10): 1983-2005. https://doi.org/10.1080/13658816.2013.780607