systems

MDPI

Editorial

Advancements in AI-Based Information Technologies: Solutions for Quality and Security

Tetiana Hovorushchenko [1,*], Ivan Izonin [2,3] and Hakan Kutucu [4]

[1] Department of Computer Engineering and Information Systems, Khmelnytskyi National University, 29016 Khmelnytskyi, Ukraine
[2] Department of Civil Engineering, School of Engineering, University of Birmingham, Birmingham B15 2FG, UK; i.izonin@bham.ac.uk or ivan.v.izonin@lpnu.ua
[3] Department of Artificial Intelligence, Lviv Polytechnic National University, 79013 Lviv, Ukraine
[4] Department of Software Engineering, Karabuk University, Karabuk 78050, Turkey; hakankutucu@karabuk.edu.tr
* Correspondence: hovorushchenko@khmnu.edu.ua

check for updates

Citation: Hovorushchenko, T.; Izonin, I.; Kutucu, H. Advancements in AI-Based Information Technologies: Solutions for Quality and Security. *Systems* **2024**, *12*, 58. https://doi.org/10.3390/systems12020058

Received: 19 January 2024
Accepted: 8 February 2024
Published: 9 February 2024

At the current stage of development and implementation of information technology in various areas of human activity, decisive changes are taking place, as there are powerful technical resources for the accumulation and processing of large amounts of information [1,2]. However, the application of known methods and tools to process such arrays of information does not meet the expectations of developers and leads to the overuse of resources, the loss of significant information and conflicts between customer expectations and the results [3,4].

At the same time, such areas of the intellectualization of information and data processing as machine learning [5,6], cognitive computing [7,8], big data, deep learning [9,10], semantic WEB [11,12] and others are in active development, which enable us to solve new classes of problems based on the available information resources [13,14].

All of the above are prerequisites for the transition to a new quality level of information processing and, accordingly, for the creation and implementation of a new generation of information technologies. However, the specifics and features of the subject areas for which information technology is developed significantly affect the content and methods of information processing, so the expectation of universal approaches to creating effective information technology for different industries is currently premature [15,16]. Approaches based on the research of characteristics and features of subject branches and the development of new information technologies for concrete branches remain justified [17,18].

Currently, all areas of human activity are related to computer systems and software, so the current problems in the use of computer systems and software are currently reliable for the protection of information from cyber threats and malware and for quality assurance of software and computer systems [19].

The need for quality and safety is based on the fact that errors and failures in software and computer systems and the impact of malware threaten disasters that lead to human casualties, environmental cataclysms, significant time losses and financial damage, or at least reputational damage to a company [20].

Therefore, special attention to the development and implementation of effective information technologies is currently needed in the field of quality and security of software and computer systems. Achieving high-quality software and computer systems, as well as cybersecurity, is a key factor in their effective use and one of the main needs of customers.

This Special Issue aims to disseminate and discuss artificial intelligence-based information technologies that support sophisticated solutions to improve and ensure the quality and security of software and computer systems.

Original, unpublished studies in different application areas on the following topics were sought:

- Intelligent information technologies for the software engineering domain;
- Intelligent information technologies for the cybersecurity domain;
- Intelligent information technologies for software quality assurance;
- Intelligent information technologies for software security assurance;
- Intelligent information technologies for computer systems quality assurance;
- Intelligent information technologies for computer systems security assurance;
- Intelligent information technologies for computer systems reliability;
- Cross-disciplinary intelligent information technologies for various subject areas.

Our Special Issue only considers knowledge-intensive solutions that outline existing quality and safety issues and offer reliable and accurate solutions in the field of artificial intelligence-based information technologies.

Abdulwahab Ali Almazroi et al. (Contribution 1) present a novel six-step framework for detecting new and modified malware. They consider as input eight malware attack datasets and insights from Exploratory Data Analysis. They perform scaling, target variable analysis, One-Hot Encoding, clustering with K-Means and PCA, and feature importance using MDI and XGBoost. The propose the GhostNet ensemble, which, combined with the Gated Recurrent Unit Ensemble and using the Jaya Algorithm, is trained on these datasets to identify and categorize this malware. The proposed model outperforms existing methods by 15% for Accuracy, Recall and AUC metrics and by 10% for time complexity reduction. The obtained results demonstrate the cost-effectiveness of these solutions for detecting eight malware strains.

Keerthi Kethineni et al. (Contribution 2) propose an IoT-based privacy-preserving anomaly detection model for smart agriculture. This detection of anomalies is important due to the large volumes of sensitive and important information from IoT devices, for example, information about crop health, environmental conditions, and resource utilization data and data regarding optimizing resource allocation, preventing crop damage and ensuring sustainable farming practices. The proposed model for intrusion detection and data encryption is based on a privacy-encoding-based enhanced deep learning framework. Data encoding is performed through a new method using a sparse capsule-auto encoder with feature selection, mapping and normalization. Intrusion detection is performed using an attention-based gated recurrent unit neural network model. The metrics Accuracy, Recall, Precision and F1-score have the values 99.9%, 99.7%, 99.9% and 99.8%, respectively.

Elena Zaitseva et al. (Contribution 3) aimed to evaluate the weights of factors and consequences of mobile applications' insecurity. They developed a method of evaluating the weights of factors of mobile applications' insecurity, which provides conclusions about the necessary factors for identifying and accurately evaluating the reliability of forecasting and assessing a mobile application's security, and values for the weights of the factors considering the mutual correlations of consequences from these factors. The authors evaluated the weights of ten OWASP mobile application insecurity factors.

Vinoth Kumar Venkatesan et al. (Contribution 4) present an efficient model, known as RPRSCA, Research Paper Recommendation System Using Effective Collaborative Approach, for the recommendation of quality research papers. The authors use available contextual metadata to gather the hidden relationships between research papers using collaborative filtering. RPRSCA provides personalized recommendations regardless of the research subject and provides better performance. This method and system outperform known methods in overall performance and in the ability to select the most relevant, most valuable and high-quality publications and place them at the top of the list of recommendations.

Kirtee Panwar et al. (Contribution 5) propose a deep learning-based image encryption system for realizing the efficient and secure transfer of medical images with an insecure network. Deep learning provides non-linearity, which secures the encryption system against plaintext attacks, and further improves the recovered image's quality and similarity to the originals using luminance, structure and contrast. The high quality of recovered

images is justified by their PSNR values. The proposed system also provides robust security against differential and statistical attacks.

Chirag Ganguli et al. (Contribution 6) aimed to compare nodes' behavior and fitness during simulated attacks with the purpose of testing the use of adaptive cyber security-based defense mechanisms and achieving the experimental results. The authors proposed a metric for the evaluation of the network performance statistics and the throughput difference of the attacked node before and after the attack. The results of the simulation using the developed metric show the efficiency of the nodes' fitness and differences.

Palash Yuvraj Ingle and Young-Gab Kim (Contribution 7) present a comparative state of the art of video synopsis methods, video synopsis frameworks and their components and classify these methods and systems. The authors investigate single-view-camera-based and multi-view-camera-based methods, their taxonomy on the basis of their characteristics and the most commonly used evaluation metrics and datasets. They then evaluate the different components. The authors immediately distinguish open challenges and new trends and identify the gaps and shortcomings of the different algorithms on the basis of the obtained experimental results.

Author Contributions: Conceptualization, T.H., I.I. and H.K.; methodology: T.H., I.I. and H.K.; state of the art, T.H., I.I. and H.K.; results, T.H., I.I. and H.K.; discussion, T.H., I.I. and H.K.; writing—original draft preparation, T.H., I.I. and H.K.; writing—review and editing, T.H., I.I. and H.K.; visualization, T.H., I.I. and H.K.; supervision, T.H., I.I. and H.K.; project administration, T.H., I.I. and H.K.; funding acquisition, T.H., I.I. and H.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by European Union's Horizon Europe research and innovation programme under grant agreement No. 101138678, project ZEBAI (Innovative methodologies for the design of Zero-Emission and cost-effective Buildings enhanced by Artificial Intelligence).

Data Availability Statement: All data used for analyses and conclusions are presented in this paper.

Acknowledgments: The British Academy's Researchers at Risk Fellowships Programme supported this project. The Editors are sincerely grateful to the entire *Systems* team for the opportunity to organize this Special Issue and for the excellent organization and support of all papers submitted.

Conflicts of Interest: The authors declare no conflicts of interest.

List of Contributions:

1. Almazroi, A.A.; Ayub, N. Enhancing Smart IoT Malware Detection: A GhostNet-based Hybrid Approach. *Systems* **2023**, *11*, 547. https://doi.org/10.3390/systems11110547.
2. Kethineni, K.; Gera, P. Iot-Based Privacy-Preserving Anomaly Detection Model for Smart Agriculture. *Systems* **2023**, *11*, 304. https://doi.org/10.3390/systems11060304.
3. Zaitseva, E.; Hovorushchenko, T.; Pavlova, O.; Voichur, Y. Identifying the Mutual Correlations and Evaluating the Weights of Factors and Consequences of Mobile Application Insecurity. *Systems* **2023**, *11*, 242. https://doi.org/10.3390/systems11050242.
4. Venkatesan, V. K.; Ramakrishna, M. T.; Batyuk, A.; Barna, A.; Havrysh, B. High-Performance Artificial Intelligence Recommendation of Quality Research Papers Using Effective Collaborative Approach. *Systems* **2023**, *11*, 81. https://doi.org/10.3390/systems11020081.
5. Panwar, K.; Singh, A.; Kukreja, S.; Singh, K. K.; Shakhovska, N.; Boichuk, A. Encipher GAN: An End-to-End Color Image Encryption System Using a Deep Generative Model. *Systems* **2023**, *11*, 36. https://doi.org/10.3390/systems11010036.
6. Ganguli, C.; Shandilya, S. K.; Nehrey, M.; Havryliuk, M. Adaptive Artificial Bee Colony Algorithm for Nature-Inspired Cyber Defense. *Systems* **2023**, *11*, 27. https://doi.org/10.3390/systems11010027.
7. Ingle, P. Y.; Kim, Y.-G. Video Synopsis Algorithms and Framework: A Survey and Comparative Evaluation. *Systems* **2023**, *11*, 108. https://doi.org/10.3390/systems11020108.

References

1. Sivarajah, U.; Kamal, M.M.; Irani, Z.; Weerakkody, V. Critical analysis of Big Data challenges and analytical methods. *J. Bus. Res.* **2017**, *70*, 263–286. [CrossRef]
2. Luo, Y.; Bu, J. How valuable is information and communication technology? A study of emerging economy enterprises. *J. World Bus.* **2016**, *51*, 200–211. [CrossRef]
3. Tian, X. Big data and knowledge management: A case of déjà vu or back to the future? *J. Knowl. Manag.* **2017**, *21*, 113–131. [CrossRef]
4. Mauerhoefer, T.; Strese, S.; Brettel, M. The Impact of Information Technology on New Product Development Performance. *J. Prod. Innov. Manag.* **2017**, *34*, 719–738. [CrossRef]
5. Qiu, J.; Wu, Q.; Ding, G.; Xu, Y.; Feng, S. A survey of machine learning for big data processing. *EURASIP J. Adv. Signal Process.* **2016**, *2016*, 67. [CrossRef]
6. Alkhaleel, B.A. Machine learning applications in the resilience of interdependent critical infrastructure systems—A systematic literature review. *Int. J. Crit. Infrastruct. Prot.* **2024**, *44*, 100646. [CrossRef]
7. Navarin, N.; Mulders, D.; Oneto, L. Advances in artificial neural networks, machine learning and computational intelligence. *Neurocomputing* **2023**, *298*, 127098. [CrossRef]
8. Abbasi, A.; Sarker, S.; Chiang, R. Big Data Research in Information Systems: Toward an Inclusive Research Agenda. *J. Assoc. Inf. Syst.* **2016**, *17*, I. [CrossRef]
9. LeCun, Y.; Bengio, Y.; Hinton, G. Deep learning. *Nature* **2015**, *521*, 436–444. [CrossRef] [PubMed]
10. Gheisari, M.; Wang, G.; Bhuiyan, M.Z.A. A Survey on Deep Learning in Big Data. In Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, China, 21–24 July 2017; IEEE: Piscataway, NJ, USA, 2017. [CrossRef]
11. Ristoski, P.; Paulheim, H. Semantic Web in Data Mining and Knowledge Discovery: A Comprehensive Survey. *J. Web Semant.* **2016**, *36*, 1–22. [CrossRef]
12. Karabulut, E.; Pileggi, S.F.; Groth, P.; Degeler, V. Ontologies in digital twins: A systematic literature review. *Future Gener. Comput. Syst.* **2024**, *153*, 442–456. [CrossRef]
13. Ostrowski, D.; Rychtyckyj, N.; MacNeille, P.; Kim, M. Integration of Big Data Using Semantic Web Technologies. In Proceedings of the 2016 IEEE Tenth International Conference on Semantic Computing (ICSC), Laguna Hills, CA, USA, 4–6 February 2016; IEEE: Piscataway, NJ, USA, 2016. [CrossRef]
14. Kazemi, R. Artificial intelligence techniques in advanced concrete technology: A comprehensive survey on 10 years research trend. *Eng. Rep.* **2023**, *5*, e12676. [CrossRef]
15. Golub, K. *Subject Access to Information: An Interdisciplinary Approach*; Libraries Unlimited, An Imprint of Abc-Clio, LLC: Santa Barbara, CA, USA, 2015.
16. Kim, H.; Choi, J. Recommendations for Responding to System Security Incidents Using Knowledge Graph Embedding. *Electronics* **2023**, *13*, 171. [CrossRef]
17. Abulaish, M.; Wasi, N.A.; Sharma, S. The role of lifelong machine learning in bridging the gap between human and machine learning: A scientometric analysis. *WIREs Data Min. Knowl. Discov.* **2024**, e1526. [CrossRef]
18. Liu, C.; Peng, G.; Kong, S.; Lan, C.; Zhu, H. Critical information quality dimensions of conversational agents for healthcare. *Inf. Res. Int. Electron. J.* **2023**, *28*, 18–42. [CrossRef]
19. Hovorushchenko, T.O. Methodology of Evaluating the Sufficiency of Information for Software Quality Assessment according to ISO 25010. *J. Inf. Organ. Sci.* **2018**, *42*, 63–85. [CrossRef]
20. Hovorushchenko, T.; Pomorova, O. Methodology of evaluating the sufficiency of information on quality in the software requirements specifications. In Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 24–27 May 2018; IEEE: Piscataway, NJ, USA, 2018. [CrossRef]