Quality and Security of Critical Infrastructure Systems

Izonin, Ivan; Hovorushchenko, Tetiana; Shandilya, Shishir Kumar

DOI:
10.3390/bdcc8010010

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (Harvard):
Izonin, I, Hovorushchenko, T & Shandilya, SK 2024, 'Quality and Security of Critical Infrastructure Systems', *Big Data and Cognitive Computing*, vol. 8, no. 1, 10. https://doi.org/10.3390/bdcc8010010

big data and cognitive computing

MDPI

Editorial

Quality and Security of Critical Infrastructure Systems

Ivan Izonin [1,2,*], Tetiana Hovorushchenko [3] and Shishir Kumar Shandilya [4]

[1] Department of Civil Engineering, School of Engineering, University of Birmingham, Birmingham B15 2FG, UK
[2] Department of Artificial Intelligence, Lviv Polytechnic National University, 79013 Lviv, Ukraine
[3] Department of Computer Engineering & Information Systems, Khmelnytskyi National University, 29000 Khmelnytskyi, Ukraine; tat_yana@ukr.net
[4] School of Data Science and Forecasting, Devi Ahilya University, Indore 452001, India
* Correspondence: i.izonin@bham.ac.uk or ivan.v.izonin@lpnu.ua

1. Introduction

The amount of information is constantly growing, and thus, the issue of information security is becoming more acute. At the current stage of economic development, when information management becomes a critical business function, malware attacks on critical infrastructure systems and software bugs in such systems pose real threats. Every 12 months, 50% of industrial companies in the world experience one to five cyber incidents. The loss of the world economy as a result of cyber-attacks is USD 445 billion.

Cyber-attacks on and software errors in critical infrastructure systems pose real threats to the security of the human community, leading to human casualties, environmental cataclysms, and significant financial losses. If a company works with the data of individuals, then cyber-attacks and information theft are risk factors that cause reputational and financial damage to the company.

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 the reliable protection of information from cyber threats and malware as well as the quality assurance of software and computer systems. Known methods and tools in the field of cybersecurity and software quality assurance are unable to provide reliable protection from information from malware or the detection and disposal of malware. They also cannot ensure the required software quality of critical infrastructure systems.

Achieving high-quality software and computer systems, as well as their cybersecurity, is a key factor in their effective use and is one of the main needs of customers.

This Special Issue aims to disseminate and discuss models and methods of the quality and security of critical infrastructure systems 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 main topics were welcome:

- Software systems quality;
- Software systems security;
- Software systems reliability;
- Cybersecurity;
- Computer systems quality;
- Computer systems security;
- Computer systems reliability.

2. Accepted Papers Overview

Our Special Issue considers knowledge-intensive solutions that outline existing issues for the quality and security of critical infrastructure systems and propose reliable and

check for updates

Citation: Izonin, I.; Hovorushchenko, T.; Shandilya, S.K. Quality and Security of Critical Infrastructure Systems. *Big Data Cogn. Comput.* **2024**, *8*, 10. https://doi.org/10.3390/bdcc8010010

Received: 22 December 2023
Accepted: 15 January 2024
Published: 22 January 2024

accurate solutions. We obtained 13 submissions, 5 of which, after a careful review process, were accepted for publication in this Special Issue.

The paper [1] is devoted to the development of an effective method for assessing the level of anthropogenic disasters based on information from witnesses of the event. The authors created a conceptual model for assessing the consequences of such disasters, which includes the analysis of collected data, modeling, and the assessment of their consequences. The authors use an intelligent method of classifying the level of anthropogenic disasters that involves data exploration using the EDA method, textual data classification using the SMOTE technique, and data classification using an ensemble of machine learning methods based on the boosting procedure. Data were collected from accident records at 12 different facilities in three different countries.

Experimental results confirmed that for textual data, the best classification is performed at levels V and I with an error of 0.97 and 0.94, respectively, and an average error score of 0.68. For quantitative data, the classification accuracy of the potential level of accidents relative to the industry is 77%, and the F1-score is 0.88, which indicates a fairly high accuracy of the model. Also, a mobile application architecture was developed to classify the level of anthropogenic disasters, which reduces the time needed to assess the consequences of the hazard in the region. The proposed approach provides interaction with dynamic and uncertain environments, which makes it an effective tool for classification.

The authors in [2] underscore the significance of leveraging artificial intelligence for the detection of fraudulent banking transactions. They introduce several classification algorithms applied to discern transaction types based on specific features. The proposed model, centered on an artificial neural network, markedly enhances the precision of fraudulent transaction detection. Furthermore, the paper outlines multiple methodologies aimed at improving detection accuracy, including the management of imbalanced datasets, feature transformation, and feature engineering. The research presents the recognition of banking fraud utilizing artificial intelligence algorithms. Each selected algorithm consistently demonstrated outstanding performance (AUC values consistently exceeding 0.9). This observation is reaffirmed by the ROC curves, which exhibit minimal visual disparity.

This paper also introduces stacked generalization with deformed results of the weak classifier, yielding an AUC of 0.008, surpassing the performance of the best weak classifier. While stacking mitigates bias and variance, it excels at preventing overfitting. The enhancement offered by the linear stacking model over the best individual model was relatively marginal, with instances where no improvement was observed, particularly when the base model was already sophisticated, as exemplified by gradient-boosted trees. The stacked generalization leverages the output deformation of the individual model.

In [3], the authors address the imperative of enhancing the decision-making process for Higher Education Institution (HEI) entrants during the admission procedure. To augment the efficacy of admission outcomes, they explored the prospect of assessing entrants' likelihood of admission to an HEI. A review of the extant literature revealed certain trends in the implementation of Information Technology (IT) systems designed to cater to entrants' requirements. Nevertheless, existing studies exhibit certain limitations, prompting an investigation from [3] into an alternative model aimed at more accurately predicting entrants' success.

A heterogeneous stacking ensemble, comprising a Support Vector Machine (SVM) with an expanded input dataset via a Probabilistic Neural Network (PNN), was employed to scrutinize the prediction of an entrant's likelihood of admission through a binary classification task. The foundational algorithms of the stacking ensemble comprised an SVM with four distinct kernels: linear, sigmoid, polynomial, and Radial Basis Function (RBF). Logistic Regression was chosen as the meta-algorithm. In the initial stage, PNN was utilized to generate two supplementary data features. Subsequently, the extended dataset was processed by a heterogeneous stacking ensemble.

The results of the devised two-stage PNN–SVM ensemble model yielded an accuracy of 0.940, the highest value in comparison to other scrutinized methods. These outcomes sug-

gest the viability of incorporating the proposed model in subsequent stages of developing an information system supporting the decision-making process of HEI entrants.

The paper [4] proposes a universal and computationally efficient algorithm for opening doors of various types by an autonomous mobile robot using machine learning methods. It is based on the use of the YOLOv5 object detection model, an iterative method for estimating the parameters of the RANSAC mathematical model, and the DBSCAN algorithm for solving the clustering task. In addition, alternative methods of clustering are considered, and a comparison of their complexity is given. A study of the developed algorithm and its testing in real-world conditions at the SOMATIC company was also conducted. The percentage of successful door openings out of the total number of attempts was used as a metric of accuracy. As a result, the authors obtained a 95% accuracy based on the proposed solution (with 200 attempts). As for the obtained error, in the simulation, the average error for 10,000 test cases was equal to 1.98 millimeters. So, as a result, the proposed algorithm showed high accuracy and the ability to obtain a solution in real time.

In the paper [5], the authors developed an obstacle detection algorithm based on data obtained from two-dimensional LiDAR with linear complexity. It can work with high-frequency sensors. At the same time, a method of parallelization of the developed algorithm is proposed, which allows for reducing the time of operation of one iteration of the algorithm in proportion to the number of processor cores used. In the application mode, the authors developed a simulator for the performance evaluation of the proposed solution. It helps to test all hypotheses and quickly select hyperparameters for a stated task. In the paper, the clustering quality metrics were used to assess the accuracy of the result of solving obstacles. The two proposed metrics evaluated the accuracy, and both averages are quite high: 86% and 91% for the first and second metrics, respectively.

Author Contributions: Conceptualization, I.I., T.H. and S.K.S.; methodology, I.I., T.H. and S.K.S.; validation, I.I., T.H. and S.K.S.; formal analysis, I.I., T.H. and S.K.S.; resources, I.I., T.H. and S.K.S.; writing—original draft preparation, I.I., T.H. and S.K.S.; writing—review and editing, I.I., T.H. and S.K.S.; supervision, I.I., T.H. and S.K.S.; project administration, I.I., T.H. and S.K.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Horizon Europe (HORIZON) project number 101138678—ZEBAI.

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

Acknowledgments: The editors of this Special Issue are sincerely grateful to the entire *Big Data and Cognitive Computing* Journal team for the opportunity to organize the Special Issue and for the excellent organization and support of all papers submitted. The British Academy's Researchers at Risk Fellowships Programme supports this project.

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

References

1. Lipianina-Honcharenko, K.; Wolff, C.; Sachenko, A.; Kit, I.; Zahorodnia, D. Intelligent Method for Classifying the Level of Anthropogenic Disasters. *BDCC* **2023**, *7*, 157. [CrossRef]
2. Mytnyk, B.; Tkachyk, O.; Shakhovska, N.; Fedushko, S.; Syerov, Y. Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. *BDCC* **2023**, *7*, 93. [CrossRef]
3. Zub, K.; Zhezhnych, P.; Strauss, C. Two-Stage PNN–SVM Ensemble for Higher Education Admission Prediction. *BDCC* **2023**, *7*, 83. [CrossRef]
4. Mochurad, L.; Hladun, Y.; Zasoba, Y.; Gregus, M. An Approach for Opening Doors with a Mobile Robot Using Machine Learning Methods. *BDCC* **2023**, *7*, 69. [CrossRef]
5. Mochurad, L.; Hladun, Y.; Tkachenko, R. An Obstacle-Finding Approach for Autonomous Mobile Robots Using 2D LiDAR Data. *BDCC* **2023**, *7*, 43. [CrossRef]