machine learning & knowledge extraction

MDPI

Editorial

Special Issue "Selected Papers from CD-MAKE 2020 and ARES 2020"

Edgar R. Weippl [1,*], Andreas Holzinger [2] and Peter Kieseberg [3]

[1] SBA Research, University of Vienna, 1090 Vienna, Austria
[2] Human-Centered AI Lab, Institute of Forest Engineering, Department of Forest and Soil Sciences, University of Natural Resources and Life Sciences, 1190 Vienna, Austria
[3] Institute of IT Security Research, St. Pölten University of Applied Sciences, 3100 St. Pölten, Austria
* Correspondence: edgar.weippl@univie.ac.at

1. Introduction

In the current era of rapid technological advancement, machine learning (ML) is quickly becoming a dominant force in the development of smart environments. By automating processes, ML can enable the rapid development and deployment of intelligent systems in smart building and smart city applications. However, the knowledge required to create these ML models is often time-consuming and costly to acquire. This has led to a need for new approaches to facilitate the sharing and reuse of these ML models across different environments.

There are many challenges currently facing the field of machine learning and knowledge extraction [1]. Some of these challenges include:

Limited data availability: In many cases, it is difficult to obtain large amounts of high-quality training data, which can limit the performance of machine learning models.

Data bias: Machine learning models can only be as good as the data they are trained on. If the training data are biased, the model is likely to make biased decisions.

Ethical concerns and trust: Machine learning has the potential to perpetuate and amplify societal biases, and there are ongoing debates about the ethical implications of using these models in decision-making processes [2].

Adversarial attacks: Machine learning models can be vulnerable to adversarial attacks, in which an attacker manipulates the input data in a way that causes the model to make incorrect decisions.

Overfitting: It is possible for machine learning models to become too complex, resulting in overfitting to the training data. This can lead to poor generalization performance on new, unseen data.

Hidden threats: For all its benefits, the large-scale adoption of machine learning also holds enormous and unimagined potential for novel, unforeseen threats. Therefore, it is also important to ensure that the traceability, transparency, explainability, validity, and verifiability of AI applications in our everyday lives are guaranteed. It is the responsibility of all stakeholders to ensure the use of trustworthy and ethically reliable AI and to avoid the misuse of AI technologies. Achieving this will require a concerted effort to ensure that AI is always consistent with human values and includes a future that is safe in all respects for all people on this planet [3].

2. Editorial

One such approach, explored in the first paper "Transfer Learning in Smart Environments" [4], is the concept of transfer learning (TL), which enables the transfer of knowledge between different smart environments. The paper explores the potential of communication and transfer learning between smart environments. This can be achieved by allowing for the seamless and automatic transfer of ML models and services between organizations. To support this, a collaboration framework based on knowledge graph principles is needed to describe the machine learning models and their corresponding dependencies.

check for updates

Citation: Weippl, E.R.; Holzinger, A.; Kieseberg, P. Special Issue "Selected Papers from CD-MAKE 2020 and ARES 2020". *Mach. Learn. Knowl. Extr.* **2023**, *5*, 173–174. https://doi.org/10.3390/make5010012

Received: 12 January 2023
Accepted: 18 January 2023
Published: 20 January 2023

In the second paper ("Property Checking with Interpretable Error Characterization for Recurrent Neural Networks" [5]), the development of ML systems also requires the application of techniques for verifying the requirements of recurrent neural networks in the context of sequence classification. This can be achieved through the use of property-checking through learning algorithms such as the probably approximately correct deterministic finite automata (PAC-DFA). This tool is capable of handling nonregular languages and can provide probabilistic guarantees on the correctness of the ML system.

The development of ML systems also requires using unsupervised topic extraction to automatically extract contextual information from large text corpora, as described in the third paper, "Interpretable Topic Extraction and Word Embedding Learning Using Non-Negative Tensor DEDICOM" [6]. This can be achieved through the use of the Decomposition into Directional Components (DEDICOM) algorithm, which provides a matrix factorization for symmetric and asymmetric square matrices and tensors. This can be used to identify latent topic clusters and their relations within the vocabulary and simultaneously learn interpretable word embeddings.

As explored in the fourth paper ("Learning DOM Trees of Web Pages by Subpath Kernel and Detecting Fake e-Commerce Sites" [7]), the development of ML systems also requires the use of the subpath kernel, which is a class of positive definite kernels defined over trees. This kernel can be incorporated into a variety of powerful kernel machines, is invariant to the ordering of input trees, and can be computed in linear time. This kernel has been proven to provide excellent learning performance in intensive experiments.

This Special Issue concludes with the paper "AI System Engineering—Key Challenges and Lessons Learned" [8]; the development of ML systems for smart environments requires using several techniques and tools, including transfer learning, property checking through learning algorithms, unsupervised topic extraction, and the subpath kernel. All of these techniques and tools provide distinct advantages and, when used together, can enable the rapid development and deployment of intelligent systems in smart building and smart city applications.

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

References

1. Holzinger, A.; Kieseberg, P.; Weippl, E.; Tjoa, A.M. Current advances, trends and challenges of machine learning and knowledge extraction: From machine learning to explainable AI. In *Springer Lecture Notes in Computer Science LNCS 11015*; Springer: Cham, Switzerland, 2018; pp. 1–8. [CrossRef]
2. Kieseberg, P.; Weippl, E.; Holzinger, A. Trust for the doctor-in-the-loop. European Research Consortium for Informatics and Mathematics (ERCIM) News: Tackling Big Data in the Life Sciences. *ERCIM News* **2016**, *104*, 32–33.
3. Holzinger, A.; Weippl, E.; Tjoa, A.M.; Kieseberg, P. Digital transformation for sustainable development goals (sdgs)—A security, safety and privacy perspective on AI. In *Springer Lecture Notes in Computer Science, LNCS 12844*; Springer: Cham, Switzerland, 2021; pp. 1–20. [CrossRef]
4. Anjomshoaa, A.; Curry, E. Transfer Learning in Smart Environments. *Mach. Learn. Knowl. Extr.* **2021**, *3*, 318–332. [CrossRef]
5. Mayr, F.; Yovine, S.; Visca, R. Property Checking with Interpretable Error Characterization for Recurrent Neural Networks. *Mach. Learn. Knowl. Extr.* **2021**, *3*, 205–227. [CrossRef]
6. Hillebrand, L.; Biesner, D.; Bauckhage, C.; Sifa, R. Interpretable Topic Extraction and Word Embedding Learning Using Non-Negative Tensor DEDICOM. *Mach. Learn. Knowl. Extr.* **2021**, *3*, 123–167. [CrossRef]
7. Shin, K.; Ishikawa, T.; Liu, Y.-L.; Shepard, D.L. Learning DOM Trees of Web Pages by Subpath Kernel and Detecting Fake e-Commerce Sites. *Mach. Learn. Knowl. Extr.* **2021**, *3*, 95–122. [CrossRef]
8. Fischer, L.; Ehrlinger, L.; Geist, V.; Ramler, R.; Sobiezky, F.; Zellinger, W.; Brunner, D.; Kumar, M.; Moser, B. AI System Engineering—Key Challenges and Lessons Learned. *Mach. Learn. Knowl. Extr.* **2021**, *3*, 56–83. [CrossRef]