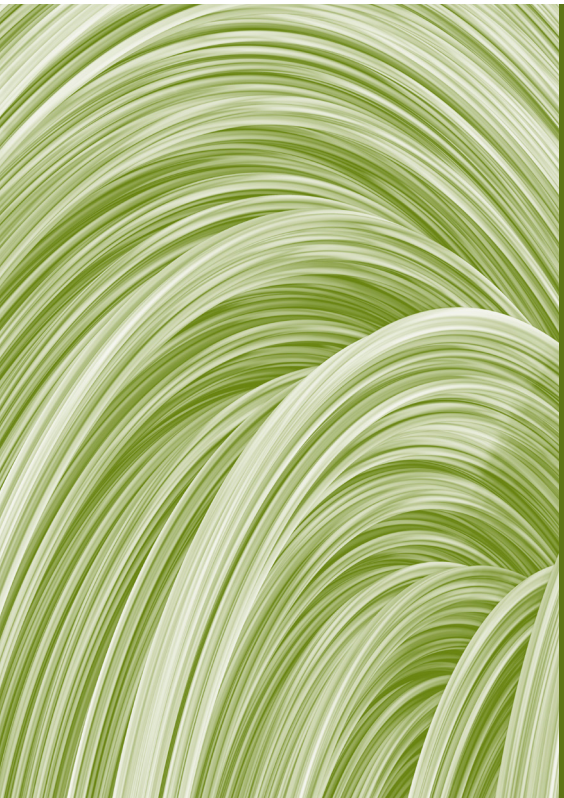
Electronics
an Open Access Journal by MDPI

Impact Factor 2.6
CiteScore 5.3

Section
Computer Science & Engineering



mdpi.com/
journal/
electronics

MDPI

Section Information

The primary focus of the “Computer Science & Engineering” section is the field of advanced computer science and engineering. It presents high-quality papers that address state-of-the-art technology, including Deep Tech, Edge Computing, Fog Computing, Artificial Intelligence, Machine Learning, Deep Learning, Emotional Systems, Fintech, Blockchain, IoT, Industry 4.0, Smart Cities, Smart Grids, Intelligent Textiles, Distributed Computing, as well as other chief technologies in this field.

Author Benefits

Open Access

Unlimited and free access for readers

Open Access

Unlimited and free access for readers

No Copyright Constraints

Retain copyright of your work and free use of your article

Thorough Peer-Review

2023 Impact Factor: 2.6

(*Journal Citation Reports* - Clarivate, 2024)

No Space Constraints, No Extra Space or Color Charges

No restriction on the maximum length of the papers, number of figures or colors

Coverage by Leading Indexing Services

Scopus, SCIE (Web of Science), CAPlus / SciFinder, Inspec, and other databases

Rapid Publication

A first decision is provided to authors approximately 16.8 days after submission; acceptance to publication is undertaken in 2.6 days (median values for papers published in this journal in the first half of 2024)

Selected Papers

Edge HPC Architectures for AI-Based Video Surveillance Applications

Authors: Federico Rossi and Sergio Saponara

Abstract: The introduction of artificial intelligence (AI) in video surveillance systems has significantly transformed security practices, allowing for autonomous monitoring and real-time detection of threats. However, the effectiveness and efficiency of AI-powered surveillance rely heavily on the hardware infrastructure, specifically high-performance computing (HPC) architectures. This article examines the impact of different platforms for HPC edge servers, including x86 and ARM CPU-based systems and Graphics Processing Units (GPUs), on the speed and accuracy of video processing tasks. By using advanced deep learning frameworks, a video surveillance system based on YOLO object detection and DeepSort tracking algorithms is developed and evaluated. This study thoroughly assesses the strengths, limitations, and suitability of different hardware architectures for various AI-based surveillance scenarios.

https://doi.org/10.3390/electronics13091757

Applying Trust Patterns to Model Complex Trustworthiness in the Internet of Things

Authors: Fabrizio Messina, Domenico Rosaci and Giuseppe M. L. Sarnè

Abstract: Key aspects of communities of the Internet of Things (IoT) smart objects presenting social aspects are represented by trust and reputation relationships between the objects. Several trustworthiness models have been presented in the literature in the context of multi-smart object community that could be adopted in the IoT scenario; however, most of these approaches represent the different dimensions of trust using scalar measures, then integrating these measures in a global trustworthiness value. In this paper, we discuss the limitation of this approach in the IoT context, highlighting the necessity of modeling complex trust relationships that cannot be captured by a vector-based model, and we propose a new trust model in which the trust perceived by an object with respect to another object is modeled by a directed, weighted graph whose vertices are trust dimensions and whose arcs represent relationships between trust dimensions. By using this new model, we provide the IoT community with the possibility of representing also situations in which an object does not know a trust dimension, e.g., reliability, but it is able to derive it from another one, e.g., honesty. The introduced model can represent any trust structure of the type illustrated above, in which several trust dimensions are mutually dependent.

https://doi.org/10.3390/electronics13112107

Emulation of Digital Substations Communication for Cyber Security Awareness

Authors: Filip Holik, Sule Yildirim Yayilgan and Guro Bråten Olsborg

Abstract: Increasing power consumption and reliance on non-predictable renewable power generation is pushing the transition from analog to digital power grid substations forward. Grid digitalization helps to reduce substation complexity and therefore costs, and improves observability and management, but introduces new cyber security issues. To make the digital substations secure, cyber security awareness and efficient personnel training is one of the most important research areas as the power grid is a part of critical infrastructure. In our previous work, we have proposed an approach for analyzing cyber security threats and attacks in digital substations based on a case study from Norway. In this article, we present how we developed a tool for emulation of digital substation communication for cyber security awareness based on experiences from the case study. We present technical details of the tool—called the SGSim—so the community can easily replicate the process or only the selected parts. We also freely provide source code on GitHub and distribution in the form of a virtual machine on request. Finally, we validate the tool performance in several scenarios and evaluate its usability on a survey conducted among a wide range of professionals.

https://doi.org/10.3390/electronics13122318

Explaining Misinformation Detection Using Large Language Models

Authors: Vishnu S. Pendyala and Christopher E. Hall

Abstract: Large language models (LLMs) are a compressed repository of a vast corpus of valuable information on which they are trained. Therefore, this work hypothesizes that LLMs such as Llama, Orca, Falcon, and Mistral can be used for misinformation detection by making them cross-check new information with the repository on which they are trained. Accordingly, this paper describes the findings from the investigation of the abilities of LLMs in detecting misinformation on multiple datasets. The results are interpreted using explainable AI techniques such as Local Interpretable Model-Agnostic Explanations (LIME), SHapley Additive exPlanations (SHAP), and Integrated Gradients. The LLMs themselves are also asked to explain their classification. These complementary approaches aid in better understanding the inner workings of misinformation detection using LLMs and lead to conclusions about their effectiveness at the task. The methodology is generic and nothing specific is assumed for any of the LLMs, so the conclusions apply generally. Primarily, when it comes to misinformation detection, the experiments show that the LLMs are limited by the data on which they are trained.

https://doi.org/10.3390/electronics13091673

Invitation to Submit

Modern Computer Vision and Image Analysis

Guest Editors: Prof. Dr. Zhenghao Shi, Prof. Dr. Lifeng He, Dr. Miaohua Zhang, Prof. Dr. Jihua Zhu and Prof. Dr. Feng Zhao
Deadline: 31 August 2024

Advances in Signals and Systems Research

Guest Editors: Dr. Kok Yew Ng, Dr. Adrian Moore, Prof. Dr. Huiru Zheng and Ruth G. Lennon
Deadline: 30 September 2024

Current Trends on Data Management

Guest Editors: Dr. Boni García, Prof. Dr. Mario Munoz-Organero, Dr. Patricia Callejo and Dr. Miguel Ángel Hombrados
Deadline: 15 October 2024

Advanced Natural Language Processing Technology and Applications

Guest Editor: Dr. Michał Marcińczuk
Deadline: 15 November 2024

Applications of Virtual, Augmented and Mixed Reality

Guest Editor: Dr. Joel Weijia Lai
Deadline: 31 December 2024

Special Issue Reprints

Advancement in Blockchain Technology and Applications

Advanced Research and Applications of Deep Learning and Neural Network in Image Recognition

MDPI is a member of

Affiliated Society:

Polish Society of Applied Electromagnetics (PTZE)

Editorial Office
electronics@mdpi.com

MDPI
Grosspeteranlage 5
4052 Basel, Switzerland
Tel: +41 61 683 77 34
mdpi.com