Key trends in applied ICT technologies for 2024

Pal Varga

WE arrived at a many-ways turbulent era at the end of 2023. Focusing on the science and technology, the evolution of Generative AI (GenAI) is at the forefront of the changes. Previously a subject of theoretical discourse, GenAI is now real and practical. This shift is not just about technological advancement but has become strategically important in various areas, from science to education and business to company operations. Enterprises are expected to implement GenAI in real-world applications, moving from a heavy emphasis on training and infrastructure costs to a more nuanced consideration of inference and operational expenses.

Another significant development is the collaboration between hyperscalers and AI models in data analytics. This partnership is destined to revolutionize how data is processed and used, with a shift toward real-time fine-tuning and the ability to adapt to current data. In current applied scientific results, we already see that such solutions drive advancements in AI applications across various industries, leading to improvements in speed, accuracy, and cost. The creation of a powerful, responsive ecosystem through this collaboration will enable the development of large-scale, complex models to address an array of industry-specific use cases.

In the cybersecurity domain, a notable trend is the convergence of IT and security teams. As the boundaries between these two traditionally separate areas blur, a more unified approach to managing digital threats is emerging. This integration is driven by the rapid advancement of technology and the evolving landscape of security risks.

Quantum computing is also set to make notable strides, particularly in the realm of quantum communications. This includes the adoption of post-quantum cryptography (PQC) to protect data against future quantum attacks and the emergence of quantum networking. Although RSA is expected to remain a robust encryption method for a while, it faces increased scrutiny and potential vulnerability from quantum computing advancements. Researchers are actively exploring strategies to leverage quantum computing to break RSA and ECC, including the possibility of hybrid attacks combining quantum and traditional computing methods. The advancements in the quantum field will be crucial for data security and processing, attracting significant research and investment, particularly from sectors with high data security demands.

Still, in the middle of these advancements, human skills remain indispensable, especially in the uptake of AI. There is a growing focus on closing skills gaps through reskilling and upskilling initiatives. The interplay between human expertise and advanced technologies will be a defining feature of the upcoming period, as the Industry 5.0 initiative also seeks to balance the benefits of automation with the special understanding that only human professionals can provide.

Having these in mind, let's briefly see the December 2023 issue of Infocommunications Journal.

In her paper, Eszter Udvary focuses on integrating Quantum Key Distribution (QKD) with high-speed optical data transmission using Dense Wavelength Division Multiplexing (DWDM) in optical fibers. This integration aims to enhance network security in a cost-effective manner. The paper explores different scenarios for optimal channel allocation and the necessary bandwidth separation between classical and quantum channels.

The paper by Ammar Al-Adhami, Yasir Al-Adhami, and Taha A. Elwi explores the integration of a 3D antenna array with solar cells for self-powered applications in modern wireless communication networks. It focuses on a cubical antenna array geometry integrated with a solar panel to achieve a selfpowered node. The design aims to enhance the performance of Multi-Input Multi-Output (MIMO) systems while considering energy efficiency.

In their current paper, Beatrix Koltai, András Gazdag, and Gergely Ács proposes a novel anomaly detection mechanism for the CAN-bus in vehicles. This mechanism integrates timeseries forecasting and signal correlation analysis to enhance detection accuracy in onboard Intrusion Detection Systems (IDS). The approach predicts sets of correlated signals collectively and identifies anomalies when the combined prediction error exceeds a predefined threshold. The paper demonstrates that this method significantly outperforms existing solutions, offering more accurate detection of a broader range of attacks with minimal delay, making it highly effective for vehicular network security.

Péter Orosz, Balázs Nagy, and Pál Varga discuss the changes in DDoS attack profiles observed in real data center infrastructures in their paper, and provide a comprehensive survey of state-of-the-art detection methods tailored to these recent attacks. The authors emphasize the significance of novel attack methods and tools, the increasing frequency, extent, and complexity of attacks, and the emergence of multi-vector attacks combining L3-L7 profiles.

But this is just the briefing – let's see the papers themselves.

Pal Varga is the Head of Department of Telecommunications and Media Informatics at the Budapest University of Technology and Economics. His main research interests include communication systems, Cyber-Physical Systems and Industrial Internet of Things, network traffic analysis, end-to-end QoS and SLA issues – for which he is keen to apply hardware acceleration and artificial intelligence, machine learning techniques as well. Besides being a member of HTE, he is a senior member of IEEE, where he is active both in the IEEE ComSoc (Communication Society) and IEEE IES (Industrial Electronics Society) communities. He is Editorial Board member in many journals, and the Editor-in-Chief of the Infocommunications Journal.