Annals of Telecommunications (2023) 78:653–654
https://doi.org/10.1007/s12243-023-01003-3

EDITORIAL

Integration of IoT with cloud computing for next generation wireless technology

Mohamed Lahby[1] · **Rachid Saadane**[2] · **Sérgio D. Correia**[3]

Published online: 29 November 2023

The Information and Communication Technology sector's use of IoT, connected devices, and cloud computing has been growing at an unsustainable manner, and its management requirements are already an order of magnitude bigger than that of the network industry before the Covid pandemic. Traffic data demand is still growing, driven not only by end users' usual expectations of ever-higher quality video for conventional video-on-demand and more recent social-networking-driven applications but also by machine-to-machine traffic and operation of expanding cloud services.

The convergence of the Internet of Things (IoT) with cloud computing has ushered in a new era of wireless technology, poised to redefine the landscape of connectivity, data processing, and security across a multitude of sectors. In this context, this special issue serves as a gateway to explore the dynamic junction where IoT and cloud seamlessly coalesce, propelling wireless technology into an era of unparalleled capabilities.

In this special issue, we have selected six high-quality papers. For the first three papers, we invited the authors of the "best" regular papers presented at the 5th International Conference on Cloud and Internet of Things (CIoT 2022) to extend them. The other three papers were selected from the submissions to our call for this special issue. Every paper has been evaluated by three volunteer reviewers after a thorough selection process.

Diverse issues are addressed, including IoT and cloud integration for real-time data processing, security and privacy considerations in next-generation wireless technology, energy-efficient algorithms for IoT devices, machine learning and deep learning applications, and blockchain-based solutions for healthcare and cloud security.

The paper by Moulahi et al. [1] examines malicious attacks, including poison and evasion, and assesses their impact on decision-making processes in the field of e-health. The findings demonstrate that the original model consistently exhibits superior performance compared to the accuracy achieved by the model trained on a combined poisoned dataset. Notably, while the original model outperforms the poisoned model, the observed difference in performance is not especially significant.

The paper by Mekbungwan et al. [2] presents a robust solution for distributed computation in IoT environments with intermittent internet connectivity, utilizing Named Data Network (NDN) and introducing computation functions within NDN routers. The innovation involves treating functions as executable data objects, expressed in NDN interest names, transforming a standard NDN into an ActiveNDN node. Simulation experiments and real-world applications demonstrate the effectiveness of ActiveNDN, particularly in handling complex and time-sensitive scenarios in large-scale wireless IoT networks.

The paper by Bursa et al. [3] explores the challenges of implementing deep learning models for Human Activity Recognition (HAR) on mobile devices with limited resources. The authors evaluate and compare the performance of four deep learning architectures trained on three different datasets from the HAR domain.

The paper by Ayache et al. [4] proposes an enhancement of the existing DASS-CARE 2.0 framework by using a blockchain-based federated learning (FL) framework. The proposed solution provides a secure and reliable distributed learning platform for medical data sharing and analytics in a multi-organizational environment. The blockchain-based federated learning framework offers an innovative solution to overcome the challenges encountered in traditional FL.

The fifth paper by Brahimi et al. [5] is titled "Cloud Services Selection in IoFT-enabled Multi-access Edge Computing:

✉ Mohamed Lahby
MOHAMED.LAHBY@univh2c.ma

[1] Ecole Normale Supérieure, Université Hassan 2 Casablanca, Casablanca, Morocco

[2] Hassania School of Public Works, Casablanca, Morocco

[3] Portalegre Polytechnic University, Portalegre, Portugal

a Game Theoretic approach." In this paper, the authors propose a Game Theory approach for Cloud Services in MEC and UAVs-enabled networks (GTCS) that enables a normal end user to select the most suitable Unmanned Aerial Vehicle (UAV)-Service-Provider based on a set of specific features, limitations, and prices. Simulation results indicate the method's efficiency, achieving low latency, high success rates, and effective energy consumption management with Unmanned Aerial Vehicles (UAVs).

The last paper by Nahid Eddermoug and his colleagues [6] "*klm*-PPSA v. 1.1: machine learning-augmented profiling and preventing security attacks in cloud environments" addresses security challenges in cloud computing by introducing a "klm-based profiling and preventing security attacks (klm-PPSA)" system, designed to detect and prevent both known and unknown security attacks in cloud environments, including cloud-based IoT. The empirical results show that klm-PPSA is the best model compared to other models owing to its high performance and attack prediction capability using Regularized Class Association Rules (RCAR)/Classification Based on Associations (CBA).

Acknowledgements The Guest Editors would like to thank the Annals of Telecommunications for publishing this special issue, particularly the Managing Editor, Laurence Monéger, for her precious help. We also thank all the authors for their valuable contributions on a wide range of topics, the reviewers who helped hone the submitted papers into quality articles, and all the Editors for their work.

References

1. Moulahi T, El Khediri S, Nayab D, Freihat M, Khan RU (2023) Effects of dataset attacks on machine learning models in e-health. Ann Telecommun. https://doi.org/10.1007/s12243-023-00951-0
2. Mekbungwan P, Lertsinsrubtavee A, Kitisin S, Pau G, Kanchanasut K (2023) Towards programmable IoT with ActiveNDN. Ann Telecommun. https://doi.org/10.1007/s12243-023-00954-x
3. Bursa SÖ, Incel ÖD, Alptekin GI (2023) Building lightweight deep learning models with TensorFlow Lite for human activity recognition on mobile devices. Ann Telecommun. https://doi.org/10.1007/s12243-023-00962-x
4. Ayache M, El Asri I, Al-Karaki JN, Bellouch M, Gawanmeh A, Tazzi K (2023) Enhanced DASS-CARE 2.0: a blockchain-based and decentralized FL framework. Ann Telecommun. https://doi.org/10.1007/s12243-023-00965-8
5. Brahimi SY, Mouffak F, Bousbaa FZ, Kerrache CA, Lagraa N, Lakas A (2023) Cloud service selection in IoFT-enabled multi-access edge computing: a game theoretic approach. Ann Telecommun. https://doi.org/10.1007/s12243-023-00950-1
6. Eddermoug N, Mansour A, Sadik M, Sabir E, Azmi M (2023) *klm*-PPSA v. 1.1: machine learning-augmented profiling and preventing security attacks in cloud environments. Ann Telecommun. https://doi.org/10.1007/s12243-023-00971-w