

Advancing ICT Frontiers through Artificial Intelligence, Intelligent Systems, and Cybersecurity

Eva Tuba* 

Department of Computer Science, Trinity University, Texas, 78212, USA

*Corresponding Author

Eva Tuba

✉ eic.ictasa@gr-journals.com

Published Online: 30 September 2026

Citation

Eva Tuba, Advancing ICT frontiers through artificial Intelligence, intelligent systems, and cybersecurity, *Journal of Information and Communications Technology: Algorithms, Systems and Applications*, 2026, **2**, 26318, <https://doi.org/10.64189/ict.26318>.

Open Access

This article is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/), which permits the non-commercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as appropriate credit to the original author(s) and the source is given by providing a link to the Creative Commons License and changes need to be indicated if there are any. The images or other third-party material in this article are included in the article's Creative Commons License, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons License and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this License, visit: <https://creativecommons.org/licenses/by-nc/4.0/>

© The Author(s) 2026

It is our pleasure to present Volume 2, Issue 3 (September 2026) of the *Journal of Information and Communications Technology: Algorithms, Systems and Applications*. This issue brings together eight scholarly contributions that reflect the rapidly evolving landscape of information and communications technology, with particular emphasis on artificial intelligence, intelligent computing, cybersecurity, wireless communication, digital transformation, and computational methods. The continued convergence of artificial intelligence with communication networks, cybersecurity, financial systems, industrial infrastructure, and environmental sustainability is creating new opportunities while simultaneously introducing complex technical and societal challenges. The contributions in this issue address several of these emerging challenges through theoretical investigations, computational approaches, methodological frameworks, and applied research.

Oni *et al.* reported a systematic assessment of AI-driven approaches to industrial control system cybersecurity, analyzing 147 studies published between 2018 and 2024. It highlights the strong performance of graph-based and hybrid methods while identifying persistent challenges in benchmarking, adversarial robustness, safety–security integration, and real-world validation, and proposes future directions including safe reinforcement learning, federated learning, explainable GNNs, and digital twins. Overall, the synthesis suggests that graph-based and hybrid methods yield the best detection accuracy (reported from 92% to 99.5% with less than 3% false-positive rates), whereas classical methods still seem to be the most suitable for resource-constrained applications.^[1] Shaikh *et al.* present Finistral-7B-LoRA, a parameter-efficient financial sentiment classifier developed by applying Low-Rank Adaptation (LoRA) to the 7-billion-parameter Mistral-7B-v0.1 model, updating only 0.58% (≈ 41.9 million) of its parameters. Following rigorous decontamination, the model achieves 98.9% accuracy on the Financial Phrase Bank, 87.7% accuracy (0.883 F1) on FiQA-SA, and 78.9% accuracy (0.796 F1) on Twitter Financial News Sentiment, while identifying a substantial 75.2% training–test overlap, highlighting the importance of contamination-aware, rigorous, and reproducible benchmarking in financial NLP.^[2] Ar-Reyouchi *et al.* proposes Delay-Aware Reinforcement Coding (DARC), a Markov decision process-based reinforcement learning controller

that jointly optimizes relaying strategy, random linear network coding parameters, and packet redundancy across 81 network contexts and 12 control actions. Evaluated over 120,000 transitions and 10 independent learning seeds, DARC achieves a normalized cost of 0.3364, outperforming store-and-forward by 2.2% and remaining within 0.29% of the exact MDP oracle, demonstrating its potential for adaptive optimization of latency, reliability, coding overhead, and goodput in multi-hop wireless networks. [3] Iqbal *et al.* proposes an integrated digital twin-based predictive maintenance (PdM) framework for complex industrial machinery, particularly wind turbines, combining IoT-enabled real-time monitoring, failure prediction, proactive maintenance scheduling, and blockchain-based secure data sharing. As a conceptual and theoretical framework, the study highlights the potential of digital twins to reduce downtime and maintenance costs and support more reliable Industry 4.0 operations, while noting that the projected benefits require empirical validation using physical equipment and real-world operational data. [4]

Nagalpara *et al.* introduces the AI Environmental Impact Framework (AI-EIF), a mathematically formalized four-pillar framework addressing energy consumption, carbon emissions, resource depletion, and standardized environmental measurement. Validated on 3,847 AI-class workloads from the Google Cluster Trace v3 dataset, AI-EIF-Eval achieves 94.3% measurement accuracy, outperforming existing approaches, while demonstrating potential reductions of 38.4% in energy consumption, 41.2% in carbon emissions, and 22.7% in water usage, alongside a 47.3% improvement in the GreenFLOPS Index. [5] Ansari *et al.* addresses the challenge of fragmented investment decision-making in India by proposing an AI-supported unified investment guidance platform covering stocks, metals, real estate, mutual funds, and cryptocurrencies. By integrating real-time and historical data with Random Forest, Long Short-Term Memory (LSTM), sentiment analysis, and AI-based advisory mechanisms, the platform achieves strong predictive performance, with R^2 values of 0.92 for gold, 0.88 for real estate, 0.78 for stocks, 0.80 for cryptocurrency, and 0.99 for mutual funds. [6] Hammad *et al.* introduces CNS-STGU Defense, a trust-conditioned spatiotemporal framework for IoT intrusion detection that integrates CNN, BiLSTM, and additive attention with calibrated confidence, uncertainty, prototype distance, and distribution monitoring for reliable decision-making. Evaluated on a 187,360-window reference matrix, the framework achieves 99.495% accuracy, 99.505% macro-F1, 0.9939 MCC, and 0.603% false-alarm rate, while demonstrating 94.207% and 94.707% macro-F1 in balanced transfer reconstruction, highlighting its potential for auditable and adaptive IoT cybersecurity. [7] Praveen Kumar Gundaram formulates key recovery for

the International Data Encryption Algorithm (IDEA) as a quantifier-free bit-vector satisfiability problem and employs the Z3 SMT solver to analyze reduced-round instances of the 64-bit block cipher with a 128-bit key. Using a single plaintext-ciphertext pair and 112 disclosed key bits, the approach successfully recovers the planted key in reduced-round settings, providing reproducible measurements of SMT-based cryptanalysis while emphasizing that the results do not constitute a practical attack on full-round IDEA. [8]

In conclusion, *Volume 2, Issue 3* reflects the increasingly interdisciplinary and rapidly evolving nature of artificial intelligence, intelligent computing, communication systems, and cybersecurity research. From parameter-efficient financial language models and adaptive wireless networking to digital twin-based predictive maintenance, sustainable AI infrastructure, intelligent investment platforms, IoT intrusion detection, and solver-based cryptanalysis, the contributions demonstrate diverse applications of computational intelligence across modern technological domains. Collectively, these studies highlight the importance of developing efficient, reliable, secure, sustainable, and data-driven intelligent systems capable of addressing emerging challenges in industrial, financial, communication, and cyber-physical environments.

Conflict of Interest

There is no conflict of interest.

Artificial Intelligence (AI) Use Disclosure

The author declare that artificial intelligence (AI)-assisted tools were used only for language refinement, grammar improvement. All technical content, experimental implementation, results, and interpretations were independently developed and verified by the author.

References

- [1] O. M. Oni, J. E. Efiog, A. Akinwale, O. A. Amoo, A. Afolabi, O. E. Balogun, E. A. Olajubu, AI approaches for industrial control system cybersecurity: A comprehensive review of methodological contexts, *Journal of Information and Communications Technology: Algorithms, Systems and Applications*, 2026, **2**, 26318, doi: 10.64189/ict.26318.
- [2] A. J. Shaikh, F. J. Parkar, A. Q. A. Rahim Khan, Z. Mirza, Finistral AI: an efficient financial-sentiment LoRA adapter and a train/test contamination case study, *Journal of Information and Communications Technology: Algorithms, Systems and Applications*, 2026, **2**, 26314, doi: 10.64189/ict.26314.
- [3] El M. Ar-Reyouchi, A. A. Douiri, Delay-aware reinforcement coding for multi-hop narrowband wireless mesh networks: joint RTT, redundancy, and forwarding optimization, *Journal of*

- Information and Communications Technology: Algorithms, Systems and Applications*, 2026, **2**, 26315, doi: 10.64189/ict.26315.
- [4] K. Iqbal, S. Elahi, M. Nawaz, M. Rafey, N. Mir, Z. Kurd, AI-powered predictive maintenance framework using digital twin technology enhancing industrial efficiency and reducing downtime, *Journal of Information and Communications Technology: Algorithms, Systems and Applications*, 2026, **2**, 26313, doi: 10.64189/ict.26313.
- [5] S. Nagalpara, A. Dadavala, Green Computing and Artificial Intelligence Infrastructure: Design, Mathematical Modeling, and Experimental Evaluation of the AI Environmental Impact Framework (AI-EIF), *Journal of Information and Communications Technology: Algorithms, Systems and Applications*, 2026, **2**, 26311, doi: 10.64189/ict.26311.
- [6] M. A. Ansari, H. Z. H. Shah, T. Ansari, A. V. Kamble, A. Ansari, AI-driven unified investment guidance platform for diverse asset classes, *Journal of Information and Communications Technology: Algorithms, Systems and Applications*, 2026, **2**, 26312, doi: 10.64189/ict.26312.
- [7] A. A. Hammad, K. S. Oza, K. G. Kharade, CNS-STGU defense: Trust-conditioned cross-dataset IoT intrusion detection with unknown-family rejection and drift-aware response control, *Journal of Information and Communications Technology: Algorithms, Systems and Applications*, 2026, **2**, 26317, doi: 10.64189/ict.26317.
- [8] P. K. Gundaram, Cryptanalysis of a reduced-round IDEA cipher using Z3 Solver, *Journal of Information and Communications Technology: Algorithms, Systems and Applications*, 2026, **2**, 26316, doi: 10.64189/ict.26316.

Publisher Note: The views, statements, and data in all publications solely belong to the authors and contributors. GR Scholastic is not responsible for any injury resulting from the ideas, methods, or products mentioned. GR Scholastic remains neutral regarding jurisdictional claims in published maps and institutional affiliations.