Editorial

As digital infrastructures, intelligent algorithms, and cyber–physical systems continue to expand across sectors, new challenges emerge around security, efficiency, reliability, learning, and system observability. The eight research papers featured in this editorial collectively reflect how contemporary scholarship is responding to these challenges through innovative architectures, adaptive models, data-driven assessment frameworks, and practical tools. Spanning topics from Zero Trust security and private 5G systems to neural network design, learning analytics, reliability engineering, healthcare AI, network visualization, and drone detection, these works highlight the growing convergence of theory, technology, and real-world applicability.

The first paper addresses a foundational concern in modern cybersecurity: securing resource-constrained Internet of Things devices under a Zero Trust Architecture. By treating every device as untrusted and enforcing continuous verification, Zero Trust presents particular challenges for IoT environments. The proposed Time-based Identity Management and Flow Rule Control Engine (TIMeFoRCE) introduces a lightweight, time-based authentication mechanism that aligns with Zero Trust principles while remaining feasible for constrained devices. By providing concrete metrics and a viable implementation pathway, this work advances the practical adoption of Zero Trust in IoT ecosystems where prior studies largely identified problems without offering implementable solutions [1].

The second contribution explores private 5G as an alternative to traditional wired cable TV services, particularly in multi-dwelling and rural contexts. Recognizing spectrum limitations in the sub-6 GHz band, the paper proposes a hybrid Multiple-Input Multiple-Output (MIMO) approach that simultaneously supports reliable broadcasting and efficient data communication. By combining diversity MIMO and multi-stream MIMO within a single framework, the study addresses frequency efficiency challenges and strengthens the case for private 5G as a flexible and scalable broadcasting infrastructure [2].

Automating the design of deep neural networks is the focus of the third paper, which introduces structurally adaptive DNNs, termed StradNet models. Rather than relying on manual trial-and-error or post hoc pruning, this approach integrates structural adaptation directly into the training process. By progressively pruning weak connections and refining network structure during learning, StradNet produces efficient, partially connected architectures that perform well in dynamic and high-dimensional environments. Experimental validation demonstrates superior scalability and performance compared to conventional pruning strategies, underscoring the potential of adaptive architectures in real-world machine learning applications [3].

The fourth study shifts attention to education, proposing a method to assess learners' conceptual understanding of data science through open-ended responses. By combining natural language processing techniques, such as Word2vec embeddings, with machine learning models including random forests, Naive Bayes, and logistic regression, the framework identifies both understood and misunderstood concepts. The integration of teacher–learner interaction data and electrodermal activity further enriches the analysis. Despite a limited sample size, the results show strong performance, highlighting the promise of linguistic and behavioral analysis in diagnosing learning difficulties and providing targeted instructional support [4].

Reliability engineering is addressed in the fifth paper, which investigates the persistent gap between laboratory reliability predictions and real-world field performance. By introducing a closed-loop reliability correlation framework, the study significantly improves alignment between lab-tested and field-observed failure modes. The integration of traditional DFMEA with system-level tools such as Function Block Diagrams, Interface Matrices, and usage-context analysis enables a more holistic, user-centered understanding of product behavior. This approach enhances predictive accuracy and supports proactive mitigation strategies that better reflect operational realities [5].

The sixth paper reviews privacy-preserving artificial intelligence in the context of the Internet of Medical Things, focusing on Federated Learning enhanced by Differential Privacy and Blockchain technologies. Through a comprehensive comparison of FL-DP and FL-BC frameworks, the study highlights trade-offs in privacy guarantees, trust, scalability, and energy efficiency. The analysis reveals that while differential privacy offers strong mathematical protection, blockchain-based approaches ensure transparency and traceability. Emerging hybrid architectures are identified as a promising direction for secure, trustworthy, and regulation-compliant healthcare AI systems [6].

Observability and analysis of complex networked systems are the subject of the seventh contribution, which extends the PerfVis tool into a comprehensive timestamp data analyzer. By integrating statistical outputs, customizable traffic patterns, and external data sources, the enhanced tool supports deeper insights into system and protocol behavior. Case studies involving real 5G networks and established measurement protocols demonstrate the value of flexible visualization and analysis in uncovering temporal patterns, performance anomalies, and protocol dynamics [7].

The final paper responds to growing concerns around drone proliferation by presenting a comprehensive dataset of drone acoustic signatures and an interactive web-based exploration tool. Covering 32 drone categories, the dataset includes raw audio, spectrograms, and MFCC representations, supporting research in acoustic-based drone detection and classification. The accompanying web application enhances accessibility and educational value, enabling users to explore and analyze drone sounds interactively. This contribution fills a critical gap in publicly available resources for acoustic drone detection research [8].

Collectively, these eight papers illustrate how modern research is tackling complexity across technological, educational, and operational domains. From securing IoT devices and optimizing wireless spectrum usage to automating neural network design, assessing learning comprehension, improving product reliability, safeguarding medical data, visualizing network behavior, and enabling drone detection, each study emphasizes practical relevance grounded in rigorous methodology. Together, they underscore a broader shift toward adaptive, data-driven, and user-aware systems that are better aligned with real-world constraints and evolving societal needs, offering valuable foundations for future research and deployment.

References:

[1] V. Morris, K. Kornegay, J. Falaye, S. Richardson, M. Tienteu, L.J.D. Tchuenkou, “TIMeFoRCE: An Identity and Access Management Framework for IoT Devices in A Zero Trust Architecture,” Advances in Science, Technology and Engineering Systems Journal, 10(6), 1–22, 2025, doi:10.25046/aj100601.

[2] H. Ito, H. Ohno, H. Kitano, S. Matsumoto, “Private 5G MIMO for Cable TV IP Broadcasting,” Advances in Science, Technology and Engineering Systems Journal, 10(6), 23–28, 2025, doi:10.25046/aj100602.

[3] D. Degbor, H. Xu, P. Singh, S. Gibbs, D. Yan, “StradNet: Automated Structural Adaptation for Efficient Deep Neural Network Design,” Advances in Science, Technology and Engineering Systems Journal, 10(6), 29–41, 2025, doi:10.25046/aj100603.

[4] K. Yasuda, H. Shimakawa, F. Harada, “Identifying Comprehension Faults Through Word Embedding and Multimodal Analysis,” Advances in Science, Technology and Engineering Systems Journal, 10(6), 42–54, 2025, doi:10.25046/aj100604.

[5] R. Lawrance, N.K.R. Gorla, “System-Level Test Case Design for Field Reliability Alignment in Complex Products,” Advances in Science, Technology and Engineering Systems Journal, 10(6), 55–64, 2025, doi:10.25046/aj100605.

[6] S.A. Farooqi, A.A.R. Rahman, A. Saad, “Federated Learning with Differential Privacy and Blockchain for Security and Privacy in IoMT A Theoretical Comparison and Review,” Advances in Science, Technology and Engineering Systems Journal, 10(6), 65–76, 2025, doi:10.25046/aj100606.

[7] M. B¨ohmer, T. Herfet, “PerfVis+: From Timestamps to Insight through Integration of Visual and Statistical Analysis,” Advances in Science, Technology and Engineering Systems Journal, 10(6), 77–87, 2025, doi:10.25046/aj100607.

[8] M.Y. Wang, M. Linn, A.P. Berg, Q. Zhang, “A Multi-class Acoustic Dataset and Interactive Tool for Analyzing Drone Signatures in Real-World Environments,” Advances in Science, Technology and Engineering Systems Journal, 10(6), 88–96, 2025, doi:10.25046/aj100608.

Editor-in-chief

Prof. Hamid Mattiello