

Journal of Information & Optimization Sciences

Volume 47, Number 8, August 2026

Special Issue on

**Intelligent Computational Frameworks for Secure
Cyber-Physical Systems, Blockchain, Artificial
Intelligence, and Next-Generation Communication
Networks**

Guest Editors

Priya Mathur

Amit Kumar Gupta

Carlos M. Travieso-Gonzalez

Published by :



Guest Editors

Priya Mathur

Department of Mathematics
Poornima Institute of Engineering & Technology
Jaipur 302022
Rajasthan
India
E-mail: priya.mathur@poornima.org

Amit Kumar Gupta

Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India.
E-mail: dramitkumargupta1983@gmail.com

Carlos M. Travieso-Gonzalez

Department of IDeTIC. Signals and Communication
University of Las Palmas de Gran Canaria
Spain 35017
E-mail: carlos.travieso@ulpgc.es

FOREWORD

This special issue titled “Intelligent Computational Frameworks for Secure Cyber-Physical Systems, Blockchain, Artificial Intelligence, and Next-Generation Communication Networks” brings together cutting-edge research at the intersection of mathematics and allied areas. The issue reflects the rapidly growing demand for mathematically grounded and computationally intelligent solutions capable of addressing complex challenges related to security, privacy, scalability, and reliability in modern digital ecosystems.

The exceptional response to this special issue reflects the increasing global interest in the integration of mathematical modeling, optimization, artificial intelligence, cybersecurity, blockchain technologies, and intelligent communication systems for addressing complex real-world challenges. The call for papers attracted more than 200 manuscript submissions from researchers, academicians, and industry experts across the world, representing a broad spectrum of theoretical and applied research. To ensure the publication of high-quality and impactful contributions, each manuscript underwent a rigorous multi-stage peer-review process conducted by internationally recognized subject experts. The evaluation criteria emphasized originality, mathematical rigor, optimization efficiency, methodological soundness, technical innovation, and practical applicability. Following a thorough editorial assessment and reviewers’ recommendations, 26 outstanding research articles were selected for publication. The accepted papers collectively present significant advances in optimization-driven computational frameworks, mathematical modeling, artificial intelligence, blockchain

security, privacy-preserving machine learning, intelligent communication networks, cyber-physical systems, and secure digital infrastructures, thereby contributing to the continued advancement of information sciences and optimization research.

We express our sincere gratitude to all authors for their valuable contributions and dedication to advancing knowledge in these rapidly evolving research areas. We are particularly thankful to Professor B. K. Dass, Chief Editor, for his constant support and encouragement during the publication process in the *Journal of Information & Optimization Sciences*, published by Taru Publications, New Delhi.

Guest Editors :

Priya Mathur

Amit Kumar Gupta

Carlos M. Travieso-Gonzalez

Journal of Information & Optimization Sciences

Volume 47, Number 8, August 2026

Special Issue on

Intelligent Computational Frameworks for Secure Cyber-Physical Systems, Blockchain, Artificial Intelligence, and Next-Generation Communication Networks

CONTENTS

K. KASU AND Y. R. RAO HATS : Hybrid adaptive transform selection for wavelet-enhanced OTFS in sparse IoT communications	2847–2855
B. VISHWANATH AND P. C. REDDY AI-driven framework for adaptive resource allocation and channel selection in V2X communication	2857–2865
N. KULKARNI, M. ANEES, M. JYOTHIRMAI, A. PRATIMA, K. A. SWAMY AND T. S. D. MURTHY Adaptive multi-resource covert communication framework for embedded and distributed learning systems	2867–2876
G. DHONGADE, O. CHANDRAKAR AND R. KHANDE Malware detection using machine learning	2877–2889
P. SHARMA AND B. KESWANI An optimization-driven reinforcement learning with vision transformer generative adversarial network for medical image reconstruction	2891–2902
Y. M. MANJUNATH, H. L. PARASHIVAMURTHY, S. G. BABU AND G. MANJUNATH Optimizing network security response through graph-based detection of suspicious activities and recovery strategies	2903–2916
P. SHARMA AND B. KESWANI Secure and optimized ViT–Trans GAN architecture : A mathematical modeling approach for encrypted MRI brain image reconstruction	2917–2929
SUSHAMA, S. VAIDYA, S. SHARMA, P. VATS AND A. ARORA Hybrid-IDPS for IoT networks : A feature-augmented approach to anomaly detection	2931–2938

V. D. GOWDA, S. K. GUPTA, K. D. V. PRASAD AND P. SARMA Real-time sensor fusion and signal processing for enhanced collision avoidance in autonomous vehicles	2939–2953
S. SHARMA AND S. SHARMA Hybrid CNN–transformer model for real-time drowsiness detection using eye aspect ratio & facial landmarks	2955–2968
S. S. KUSHWAHA, S. GUPTA, L. GOEL, A. K. AGARWAL AND P. HEMRAJANI A discrete mathematical framework for security and cryptographic analysis of Ethereum smart contracts	2969–2976
G. H. KUMAR, D. K. J. B. SAINI, P. V. B. REDDY, C. R. MURTHY, Y. RAUT AND T. GOPIKRISHNA SHADE : Privacy-preserving multivariate anomaly detection in industrial IoT using CKKS homomorphic encryption	2977–2986
S. S. KUSHWAHA, P. GUPTA, L. GOEL, Y. L. PRASANNA AND S. GUPTA A security aware discrete mathematics framework for Nash-equilibrium based incentive design against selfish mining and validator collusion	2987–2995
D. KUMAR, S. R. THAKARE AND A. KULKARNI Evaluating deep learning–based computer vision techniques for robust object detection in video surveillance applications	2997–3006
D. VAYA AND R. K. SAXENA Lightweight multi-modal malware intelligence : A unified framework for efficient graph, temporal, causal, and federated detections	3007–3015
B. K. KAVYA, S. ANNAMALAI AND A. S. KUMAR Integrating AI models for code analysis and enhancing interpretability with explainable AI for human-readable bug detection	3017–3031
S. SHANKER, A. K. PHOGAT, A. MISRA, S. BHUSHAN, P. VATS AND M. MANDOT A secure and scalable SDN architecture for dynamic traffic management and cryptography-based tenant isolation	3033–3041
A. KHAN, S. S. BISWAS, B. ALANKAR, H. KAUR AND S. ZAFAR End-to-end encryption architecture for enhancing confidentiality and integrity in secure online examination system	3043–3052
VISHAL, R. BHAKHAR, P. PANDEY, A. GOYAL AND M. MANDOT A feature-augmented hybrid intrusion detection and prevention system for secure IoT networks	3053–3062

S. KUMAR, D. AWASTHI, R. K. PANDEY, A. K. UTTAM AND S. K. GUPTA	
A multi-level trusted security framework for high-fidelity GAN video deepfake detection in real-time systems	3063–3072
G. H. KUMAR, D. K. J. B. SAINI, V. NAMALA, N. GIREESH, K. A. SWAMY AND G. S. KUMAR	
Federated learning assisted power control for covert and secure UAV-enabled IoT communications	3073–3081
Y. V. SINGH AND P. VATS	
A mathematical framework for fake news detection in digital media using an intelligent fuzzy neural network model	3083–3092
S. S. KUSHWAHA, P. HEMRAJANI AND V. HIMTHANI	
Secure and dynamic Sharding : Advancing blockchain scalability and security through partitioned consensus and coordinated cross-shard protocols	3093–3102
M. KAUR	
Security-enhanced machine learning-based predictive control for automated emergency braking using multi-sensor data fusion	3103–3114
G. H. KUMAR, A. V. SURANA, P. V. B. REDDY, N. GIREESH, D. K. J. B. SAINI AND U. P. KUMAR	
CAKE : Energy-aware crypto-agile key management for energy-harvesting IoT with runtime switching between ASCON-128 and ML-KEM	3115–3125
P. MATHUR AND A. K. GUPTA	
A discrete mathematical approach for cryptanalysis using the normalized cipher randomness index	3127–3142