

Journal of Discrete Mathematical Sciences & Cryptography

Volume 28, Number 5-B, August 2025

Special Issue on

**Advancements in Intelligent Systems for Information
Optimization in Cyber Security : Challenges and
Innovations (Part-B)**

Guest Editors

Dinesh Goyal

Anil Kumar

Dharm Singh Jat

Published by :



Guest Editors

Dinesh Goyal

Poornima Institute of Engineering & Technology
Jaipur
Rajasthan
India
E-mail: dinesh.goyal@poornima.org

Anil Kumar

Department of Computer Engineering
Poornima Institute of Engineering & Technology
Jaipur
Rajasthan
India
E-mail: anilkumar@poornima.org

Dharm Singh Jat

Department of Computer Science
Namibia University of Science and Technology (NUST)
Namibia
E-mail: dharmsingh63@hotmail.com

FOREWORD

This special issue titled “Advancements in Intelligent Systems for Information Optimization in Cyber Security : Challenges and Innovations” explores the complex intersection of intelligent systems and their effective uses in cybersecurity. This issue addresses a variety of topics, each contributing to the fields of data security, privacy, and cyber security.

The research work discussed here includes the combination of artificial intelligence with optimization techniques and cybersecurity representing a significant step forward in threat detection and analysis in the ever evolving era of artificial intelligence which provides a framework for recognizing patterns and irregularities in data flows, which can help in developing strong security protocols to combat evolving attack methods. On the other hand, optimization offers powerful tools for enhancing performance in threat detection, analysis & prevention, such as lowering false positives and improving resource allocation.

Some of the other research works cover how machine learning models, data-driven analytics, and optimization algorithms can improve security systems and protect data transmission. The research work by authors also examines the use of AI-based systems in real-time adaptive security systems, like threat intelligence platforms and predictive risk assessment. Another important area covered in this issue is network and wireless communication security and its applications.

The research work also addresses the challenges and possible solutions for protecting communication infrastructures. Information system for AI-based cryptography and anti-hacking systems provide helpful insight into current attack surfaces and counter measures. Some of the papers also investigate privacy and security issues on social networks, focusing on protecting user data and maintaining privacy in online communities.

This issue also includes papers on important topics like secure end-to-end transmission in IoT healthcare networks, elliptic curve cryptography for cloud storage, biometric encryption models, threats to federated learning, homomorphic encryption for machine learning, privacy-preserving cryptographic protocols, quantum-resistant

algorithms, and visual cryptography for secure image sharing. The chosen papers also emphasize progress in threat detection using ensemble learning, blockchain-based data sharing, lightweight encryption for devices with limited resources, and AI-supported phishing detection systems.

This special issue is an outcome of the **6th International Conference on Information Management & Machine Intelligence** held at Poornima Institute of Engineering & Technology, Jaipur on 23-24 December 2024, wherein we received more than 280 papers from researchers which went through a rigorous peer review process after which only 71 papers were selected for this special issue, which is being published in two parts : JDMSC 28#5-A and JDMSC 28#5-B, covering a wide range of innovative concepts.

The low rate of acceptance testifies to our dedication to excellence, and we assure that only the most significant contributions appear in this special issue. We are glad to share these selected contributions, which reflect the leading edge of progress in the field.

We express our gratitude to every author for his productive contribution in pushing the knowledge frontier on intelligent systems and cybersecurity. This special issue confirms the relevance of using AI and optimization models to further the security posture of digital environments. We are especially thankful to Professor B. K. Dass, Chief Editor, for his constant motivation and guidance during the publication process of the *Journal of Discrete Mathematical Sciences & Cryptography*, published by Taru Publications, New Delhi.

Guest Editors :

Dinesh Goyal

Anil Kumar

Dharm Singh Jat

Journal of Discrete Mathematical Sciences & Cryptography

Volume 28, Number 5-B, August 2025

Special Issue on

Advancements in Intelligent Systems for Information Optimization in Cyber Security : Challenges and Innovations (Part-B)

CONTENTS

S. K. HENGE, C. K. HINGE, D. KOTHAPETA, S. K. MANDAL, R. SINGH, A. BHAGAT, A. SHARMA, A. VENGALA AND A. UPADHYAY EHC-BGV hybrid homomorphic encryption algorithmic sequences for processing authenticated role based secure keys	1845–1854
A. K. SAINI, M. L. SAINI, D. K. SRIVASTAVA, S. SINGH, P. VATS AND T. K. TAK Secure communication framework using lattice-based encryption and image steganography	1855–1864
S. K. MANDAL, R. SINGH, N. CHANDU, D. MEHTA, S. K. HENGE, D. KOTHAPETA, C. K. HINGE, A. SHARMA AND T. HUSSAIN Evolutionary multi-authentication cryptographic key implications for secure data access control	1865–1874
N. JANU, P. GARG, K. M. BHAGAT, B. THANKACHAN, S. VISHNOI AND P. DADHEECH Graph-theoretic and geometric methods for social network influence analysis	1875–1885
V. P. ARIVANANTHAM, H. M. A. GHANIMI, V. K. SONTI, F. T. AYASRAH, R. M. LENKA, P. HEMALATHA, S. SENGAN AND P. DADHEECH The secured authentication system : Integrated cyber security end-to-end based cyber-physical systems for improved DevOps resilience with authentication	1887–1898
A. GOYAL AND K. LAKHWANI Enhancing network security : A blockchain-based approach for secure data transfer and user authentication	1899–1910

N. KEERTHANA, H. M. A. GHANIMI, P. V. V. S. SRINIVAS, N. R. PENDLI, F. T. AYASRAH, M. A. BENNET, S. SENGAN AND P. DADHEECH Blockchain-based cybersecurity : A predictive privacy and security of cyber-physical systems	1911–1922
R. M. SAIRISE, N. M. PAWAR, S. N. THAKUR, A. SHELKE, B. M. NANCHE AND V. P. TAMTA Elliptic curve-inspired graph neural networks for lightweight cryptographic verification	1923–1934
K. R. PRANEETH, H. M. A. GHANIMI, M. S. NARAYANA, KAFILA, S. NANDURI, R. K. BOMMISSETTI, S. SENGAN AND P. DADHEECH A cyber-physical system with blockchain integrated chaotic secure hash algorithms-256 for secured supply chain management system	1935–1944
R. CHATURVEDI, P. GUPTA, R. C. PANDEY, N. K. RATHORE, A. SHARMA, P. DADHEECH AND R. SHARMA Comparison of cloud and edge computing based face recognition for security enhancement	1945–1955
H. KUMAR, G. SHARMA, N. HEMRAJANI, R. S. SHARMA, S. SHARMA AND G. MAHAJAN Designing error-correcting and combinatorial cryptographic solutions using discrete mathematics	1957–1967
S. VISHNOI, G. SHRIMAL, S. R. DOGIWAL, B. KANWER, M. PAREEK AND T. JAIN Discrete chaos theory for secure key generation in lightweight IoT encryption	1969–1979
S. YADAV, S. RANE, V. PABALKAR, S. SAHU, R. KULKARNI, A. CHITARI AND T. KATTE Advances in fuzzy logic and algebraic structures for industrial applications in control theory	1981–1991
S. RANE, J. CHITRANSHI, A. KAULAGE, A. MISHRA, T. JADHAV AND A. GUPTA Graph theory and network analysis for evolutionary modeling in biological and social systems	1993–2003
S. K. MANDAL, R. SINGH, N. CHANDU, M. PADMAVATHI, S. K. HENGGE, C. K. HINGE, V. SUNKARI AND A. SHARMA Multilayer encryption cipher mitigating salting sequence key approach for securing transit data	2005–2014
N. JANU, S. VISHNOI, S. L. YADAV, T. CHAWLA, P. VATS AND PRIYANKA Elliptic curve-based cryptanalysis techniques : A strategic approach to enhancing information security	2015–2024

KAVITA, N. SHARMA AND G. AGGARWAL Quantum-resistant adaptive RSA (QR-ARSA) for secure networks	2025–2035
S. RAMAGUNDAM, H. KARAMCHANDANI, G. U. PATIL AND P. SUBRAMANIAM Context-aware lightweight and post-quantum cryptographic framework for secure wireless communication	2037–2047
G. KUMAR, S. SHARMA, V. S. SHARMA AND D. S. JAT Dihedral group order 12 noncommutative cryptography primitive generations	2049–2058
M. NAMDEV, K. SHOWKAT, S. VISHNOI AND P. DADHEECH Explainable machine learning frameworks for cryptography protocol design using discrete structures	2059–2069
P. GARG, A. VERMA, S. TANWAR AND P. DADHEECH AI-augmented cryptanalysis using combinatorics and reinforcement learning	2071–2080
V. P. ARIVANANTHAM, H. M. A. GHANIMI, S. R. RANE, V. J. SOWMYA, K. POON, N. MYTHILI, S. SENGAN AND P. DADHEECH Cyber security with blockchain-based cyber-physical system for key generation in medi-cloud computer systems	2081–2092
S. PATHAK, B. KALYANWAT, A. KUMAR AND P. DADHEECH Data-driven, transparent synthesis of lattice-based cryptosystems with hybrid security verification	2093–2102
V. RAMACHANDRAN, H. M. A. GHANIMI, B. MARAPELLI, N. KAUR, M. R. LAXMI, R. K. BOMMISSETTI, S. SENGAN AND P. DADHEECH An enterprise blockchain model : A reliable cryptography-based cyber-physical systems for securing user data	2103–2114
C. ANITHA, A. SAPATNEKAR, A. S. BANAIT, J. L. AMALRAJ, R. A. MULLA AND M. PAWAR Network-based anomaly detection in encrypted data streams : A cryptanalysis perspective	2115–2124
D. B. PATIL, V. G. KALE, S. B. PATIL, A. B. RAJMANE, S. V. JOSHI AND T. N. PAWASE Discrete algebra-based neural models for secure information transmission	2125–2136
A. K. SINGHA, P. K. TIWARI, M. BARI, R. KUMAR AND MANDEEP Securing the cloud : Comparative analysis of NCS, ERSA, and EHS cryptographic methods	2137–2149

S. SHEELA, S. JYOTHI, S. SHALINI AND L. ANUJ Federated learning and deep learning-driven adaptive cryptography for context-aware elliptic curve Diffie-Hellman optimization and anomaly-aware key management in next-generation wireless networks	2151–2161
S. SARDESAI, P. GHORI, U. S. B. K. MAHALAXMI AND Y. K. KIRANGE Secure and intelligent financial data analysis using machine learning, fuzzy logic, and cryptography	2163–2173
A. MALSARIA, V. K. SHARMA, P. DADHEECH, P. K. YADAV, S. R. DOGIWAL AND B. P. SONI Lightweight HECC-DWT-based secure image encryption with integrity verification and access control	2175–2185
M. ALFIRAS, S. GURPUR, S. TIWARI, A. K. AGARWAL, S. DOMMARI AND A. RAINA Implementation of random dynamical systems for data encryption in information security	2187–2195
R. M. LENKA, S. TIWARI, S. DOMMARI, V. K. BHOSALE, P. DASS, N. CHAVAN AND N. TANDON Topological dynamics algorithms for enhanced cybersecurity protocols	2197–2207
V. A. JUJARE, S. DOMMARI, B. M. NANCHE, S. TIWARI, P. DASS, P. P. AHIRE AND R. V. PATIL Utilizing infinite-dimensional Hamiltonian systems for advanced cryptographic methods	2209–2217
M. V. C. RAO, N. SRIMANNARAYANA, K. A. VENKATESH, G. RAMU AND G. RAMESH Minimum absolute deviation covering chromatic energy of graphs	2219–2226
A. K. SINGH AND J. SINGH High-capacity image steganography secured by universal adversarial perturbations	2227–2235