

Journal of Discrete Mathematical Sciences & Cryptography

Volume 28, Number 5-A, August 2025

Special Issue on

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

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-A, August 2025

Special Issue on

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

CONTENTS

G. L. SAINI, P. D. SINGH, K. D. SINGH AND P. NAROOKA Enhancing data privacy through cryptographic innovations in discrete mathematical systems	1461–1472
A. NOONIA, D. THAKRAL, P. MATHUR, F. SHETH, H. SHAIKH AND A. K. GUPTA A discrete mathematical model and cryptography for secure medical image analysis : Encrypted chest X-ray classification	1473–1486
G. KUMAR, A. SRIVASTAVA V. S. SHARMA AND A. PILLAI Telemedicine formal verification using lightweight cryptography : An efficient, robust, and secure Radix-16 scalar multiplication in application validate	1487–1496
R. K. GODI, V. S. SHARMA, S. K. SHARMA, A. CHAURASIA, A. SRIVASTAVA AND A. PILLAI Secure SVM training using privacy preserving isomorphic encryption algorithm	1497–1504
V. D. GOWDA, N. SUGANTHI, V. N. PRASAD, M. TARAMBALE, P. SVVSR KUMAR AND A. MUTHUSAMY Implementing secure cryptographic protocols in 5G and 6G networks	1505–1515
V. D. GOWDA, V. PRAVEENA, M. NAGABHUSHANAM, P. SVVSR KUMAR, C. R. Q. LEZAMA AND D. PATHAK Homomorphic encryption performance in secure data processing for machine learning	1517–1526
V. D. GOWDA, S. V. CHAKRASALI, P. SVVSR KUMAR, S. A. DHOLE, J. K. PATIL AND S. SINGH A novel cryptographic approach to evaluate the security of federated learning frameworks	1527–1536

T. PANSE, V. V. DESHMUKH, P. D. SHOBHANE, Y. DONGRE, A. MHATRE AND P. MESHRAM Developing efficient crypt analysis techniques for modern cryptographic algorithms	1537–1545
S. KHANDELWAL AND A. CHAUDHARY Cybersecurity meets HR : A decade of trends, challenges, and best practices	1547–1558
S. RAMPAL, M. SHARMA, P. KHURANA, M. KUMAR AND V. BHARDWAJ Crypt analysis of multi-key biometric encryption for business enterprises using cloud storage	1559–1568
D. VAYA AND R. K. SAXENA Security attack classification and performance analysis of machine learning algorithms over CSIC HTTP dataset	1569–1578
S. BUDHAVALLE, L. R. DESAI, S. A. PAITHANE, S. N. AJANI, M. SINGH AND A. R. B. PATIL Elliptic curve-based cryptography solutions for strengthening network security in IoT environments	1579–1588
K. A. WAGHMARE, P. MAHALLE, S. N. AJANI, K. GUPTA, S. S. BADHIYE AND P. SHENDE Integration of blockchain technology with cryptographic solutions for robust healthcare information security	1589–1598
N. GHODKE, R. PHURSULE, R. M. WAHUL, K. BIKRAM, V. NANDGAONKAR AND T. SINGH Implementing secure end-to-end data transmission in wireless sensor networks for healthcare monitoring	1599–1609
P. NAROOKA, S. ARORA, S. SRIVASTAVA, M. TIWARI AND S. YADAV Adaptive machine learning system for cybersecurity threats	1611–1620
D. GOYAL, A. KUMAR, P. MATHUR, F. SHETH AND A. K. GUPTA Robust cybersecurity through discrete and large language models for effective phishing attack detection	1621–1638
B. V. B. RAO, U. RAWAT, S. ROY AND U. UPADHYAY 1-D group cellular automata based image encryption scheme : A lightweight approach for IoT devices	1639–1648
A. K. TIWARI AND S. YADAV Enhancing cloud performance : A framework for connection pooling optimization	1649–1657

N. K. VERMA, N. ARYA, N. K. PANI, J. SWAIN, N. B. TATINI AND A. NOONIA Authentication and authorization models for high-security cloud platforms	1659–1669
Y. GAIDHANI, A. S. BANAIT, P. S. PATIL, K. H. WANJALE, S. CHIWANE AND N. PARATI Implementing elliptic curve cryptography for secure cloud storage solutions	1671–1680
S. DESHMUKH, S. NAMBIAR, P. S. PATIL, M. PHATAK, B. TIPLE AND A. P. MUNSHI Design and implementation of quantum-resistant cryptographic algorithms in blockchain networks	1681–1691
P. S. PATIL, P. CHOUDHARI, R. K. MOJE, K. H. WANJALE, R. WELEKAR AND N. SHELKE Optimizing information security protocols in cloud computing using applied discrete mathematics	1693–1702
M. KALBANDE, M. LOKHANDE, A. MHATRE, A. A. DESHMUKH, P. A. PATIL AND P. MAHESHWARI Real-world applications of quantum computing for cryptographic key generation	1703–1712
S. MALWADE, R. JADHAV, V. JADHAV, A. V. CHITRE, B. NEOLE AND N. SHELKE Blockchain-based secure data sharing and storage system using elliptic curve cryptography	1713–1722
R. KALE, A. S. GAADHE, N. B. POKALE, P. A. PATIL, P. BORKAR AND S. S. UPARKAR Design and implementation of secure cryptographic algorithms for wireless sensor networks in healthcare applications	1723–1731
S. H. KULKARNI, V. V. DESHMUKH, R. K. MOJE, S. H. LAVATE, Y. GANDHI AND N. SHELKE Applied discrete mathematics in developing efficient cryptographic algorithms for enhancing information security in WSN	1733–1742
M. D. KOKATE, A. JULIAN, R. RAMYADEVI, M. RELE, G. I. MARY AND M. VAITHIANATHAN Enhancing network security in wireless sensor networks through real-time intrusion detection systems	1743–1751

J. MOULICK, R. PHURSULE, A. P. KALE, V. S. RANA, S. GOSWAMI AND V. S. KARWANDE Real-time crypt analysis and defense mechanisms in cloud computing services	1753–1761
D. MOUD AND R. K. SAXENA Development of novel signature architecture for signature recognition	1763–1769
D. T. MANE, R. BAKSHI, G. B. SAMBARE, D. R. MORE, S. KEDAR AND R. C. SAMANT Design and implementation of secure communication protocols for enhanced information security in financial transactions	1771–1780
S. BHARDWAJ, S. VAIDYA, N. SHAHARE, S. P. KANADE, U. S. PATIL AND A. P. PRABHAKAR Design and deployment of cryptographic systems for quantum-secure cloud applications	1781–1790
M. KUVESKAR, B. DHARASKAR, S. BHATTACHARJEE, A. DEV, M. M. GAWADE AND M. NAGPAL Efficient cryptographic algorithms for enhancing patient data privacy in medical IoT systems	1791–1801
P. SAHANE, M. GULHANE, N. RAKESH, S. M. M. NAIDU, M. GROVER AND V. MAHAJAN Evaluating lightweight encryption schemes for resource- constrained devices in wireless sensor networks	1803–1812
P. V. BAVISKAR, V. BALPANDE, T. JADHAV, S. M. M. NAIDU, A. SHARMA AND D. MINHAS Analyzing the impact of network topology on cryptographic security and data integrity in IoT applications	1813–1824
V. S. GAIKWAD, K. H. WALSE AND M. ATIQUE Privacy preserving protocols for encrypted data comparison in semi-honest cloud environment	1825–1834
H. GOYAL, S. SINGHAL, M. KHATER, A. MAHANTA AND P. DADHEECH An efficient image steganography using spider monkey optimization	1835–1843