

Journal of Discrete Mathematical Sciences & Cryptography

Volume 26, Number 3, April 2023

Special Issue on

**Current Research Trends in Secure Computer Vision,
IoT and Machine Learning**

Guest Editors

Dinesh Goyal

Anil Kumar

Pankaj Dadheech

Carlos M. Travieso-Gonzalez

Published by:



Guest Editors

Dinesh Goyal

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

Anil Kumar

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

Pankaj Dadheech

Swami Keshvanand Institute of Technology
Management & Gramothan, Jaipur
Jaipur
Rajasthan
India
E-mail: pankajdadheech777@gmail.com

Carlos M. Travieso-Gonzalez

University of Las Palmas de Gran Canaria
Spain
E-mail: carlos.travieso@ulpgc.es

FOREWORD

Security has been the most perpetual domain, with advancements in other domains and applications like Computer vision, IoT and Machine learning, is today's most rapidly growing technical domains to facilitate better human life across the globe and is highly dominated with statistics and data analytics using data science, artificial intelligence, and Machine Learning. All these application areas have developed new security requirements. Recent progress in these fields has been driven both by the development of new learning algorithms and theory by the ongoing explosion in the availability of online data and low-cost computation. With more advancements in technology compelled with need of scaling has provided a challenge to security of system and its architecture. Thus there is a diehard need for secure models or architectures in domains of computer vision, IoT models and Data analytics using Machine Learning.

IoT with an integration of Machine Learning (ML) is introducing new security challenges. The Internet of Things generate massive volumes of data from millions of devices. Machine learning is powered by data and generates insight from it. Machine learning uses past behavior to identify patterns and builds models that help predict future behavior and events. Computer vision is a field of artificial intelligence (AI) that enables computers and systems to derive meaningful information from digital images, videos and other visual inputs, and take actions or make recommendations based on that information. AI and machine learning (ML) can be used by IT security professionals to enforce good cyber security practices.

The objective of this Special Issue is to bring together the research and advancements done in the field of Secure Computer vision, IoT and Machine learning. Researchers can contribute more towards the recent advancement in this field of Mathematical models and algorithms developed in Artificial Intelligence, Computer Vision, IoT and their security frameworks.

With the efforts of editors, the Special Issue received more than 400 papers, which went through peer review process and following the same only 29 papers have been selected for publication in this issue.

The guest editors would like to express their gratitude to authors for sharing their valuable research and the publication partner for their approval regarding the special issue of the esteemed journal. Guest editors especially thank Prof. B. K. Dass, Chief Editor who supported us in bringing out the Special Issue/s on “**Current research trends in secure computer vision, IoT and Machine learning**” of selected peer reviewed, high quality papers in *Journal of Discrete Mathematical Sciences & Cryptography*, published by TARU PUBLICATIONS, New Delhi.

Guest Editors:

Dinesh Goyal

Anil Kumar

Pankaj Dadheech

Carlos M. Travieso-Gonzalez

Journal of Discrete Mathematical Sciences & Cryptography

Volume 26, Number 3, April 2023

Special Issue on

Current Research Trends in Secure Computer Vision, IoT and Machine Learning

CONTENTS

D. DIPALI, T. SUBRAMANIAN AND G. S. KUMARAN A smart oyster mushroom cultivation using automatic fuzzy logic controller	601–615
J. KHANDELWAL AND V. K. SHARMA Extensive dual tree complex wavelet transform-based image steganography using SVD and CNN subspace	617–627
J. T. M. DHAS AND J. MIDHUNCHAKRAVARTHY Modern Metrics (MM): Software size estimation using function points for artificial intelligence and data analytics applications and finding the effort modifiers of the functional units using indian software industry	629–640
R. BHAGAWATI AND T. SUBRAMANIAN Quantum-aided feature selection model – A quantum machine learning approach	641–655
S. SHARMA AND B. SHARMA Performance analysis of trusted security environment in cloud	657–666
V. P. SHARMA, N. S. YADAV, S. S. ADAVI, D. S. D. REDDY AND B. B. GUPTA A two stage hybrid intrusion detection using genetic algorithm in IoT networks	667–676
C. SHARMA, A. KUMAR AND P. K. TIWARI Energy efficient cloud computing using secure virtual machine migration: A taxonomy	677–683
A. KUMAR, H. SHARMA, S. MATHUR, D. SHARMA, G. KHANDELWAL AND G. SHARMA Computer vision, machine learning based monocular biomechanical and security analysis	685–693

V. K. SHARMA, P. KUMAR, S. SINGHAL, B. P. SONI AND P. K. SHUKLA Secret image scrambling and DWT-based image steganography using smoothing operation and convolution neural networks	695–705
S. K. HENGGE, A. UPADHYAY, A. K. SAINI, N. MISHRA, D. SHARMA AND G. SHARMA Analysis and detection of insider attacks using behaviour rule based architecture in enterprise multitenancy	707–718
HANSRAJ, P. K. TIWARI AND A. CHAUDHARY Multi criteria optimize secure VM placement strategy against cross VM attack	719–727
V. KAUR, D. P. BHATT, P. K. TIWARI AND S. THAREWAL Blockchain technology combined with the CNN and Hashing algorithms enabled the secure storage of 3D biometric face and ear data	729–738
N. PUROHIT, S. JOSHI, M. PANDE AND S. LINCKE Pragmatic analysis of ECC based security models from an empirical perspective	739–758
A. JAIMAN, A. KUMAR, H. SHARMA, N. GOUR, N. GOUR AND S. CHAKRAVARTY A mathematical analysis of M-MIMO using ML based signal detection algorithms	759–766
J. STELLA, P. KARTHIKEYAN, S. J. T. SCHWARZ AND S. J. J. ROSE Steganalysis on data embedded medical image	767–777
V. D. GOWDA, P. S. KUMAR, J. LATHA, C. SELVAKUMAR, R. SHEKHAR AND A. CHATURVEDI Securing networked image transmission using public-key cryptography and identity authentication	779–791
M. B. SALUNKE, P. N. MAHALLE AND G. R. SHINDE Embedded security framework for M2M communication using ULBC and Rubik’s Cube encryption algorithm	793–806
D. MOUD AND R. K. SAXENA Development of signature recognition system using VGG16	807–813
B. SHARMA AND D. SAXENA C-QoS-AOMDV: A cluster based QoS aware multipath routing protocol for MANET using hybrid soft computing techniques	815–827

S. KUMAR AND V. SINGH Hash function and DSRC based secure communication protocol for VANET-WAVE architecture	829–839
A. P. SINGH AND M. SINGH Real time malware detection in encrypted network traffic using machine learning with time based features	841–850
P. AJITHA, A. M. S. SUNDARAPANDI, M. SONIYA AND T. TAMILVIZHI An IoT-based integrated health monitoring of bulk milk cooler	851–860
V. DANKAN GOWDA, K.D.V. PRASAD, PRATIK GITE, S. PREMKUMAR, N. HUSSAIN AND V. S. CHINAMUTTEVI A novel RF-SMOTE model to enhance the definite apprehensions for IoT security attacks	861–873
U. GUPTA, V. SINGH AND D. GOYAL Highly secure intelligent computer data detection of anomalies	875–884
P. MANUJA, R. S. SHEKHAWAT AND U. RAWAT Design & analysis of novel IT security framework for overcoming data security & privacy challenges	885–898
A. S. RAO AND K. MAHANTESH Impact of computer vision based secure image enrichment techniques on image classification model	899–911
S. SHARMA AND D. GOYAL Enhanced security using video summarization for surveillance system using deep LSTM model with K-means clustering technique	913–925
R. MANOJ AND S. JOSHI Ensuring wallet application security by resolving reentrancy attacks in blockchain smart contracts	927–937
N. SETHI AND S. B. BAJAJ Neural network based image object detection and tracking for security and surveillance	939–949