SCHOLARLY PUBLICATIONS
School of Computer Application
KIIT Deemed to be University

Journal Name: Information Fusion **IF: 14.8**

Title: A clinical diabetes prediction based support system based on the multi-objective metaheuristic inspired fine tuning deep network

Author: Dhal P.; Pradhan B.; Fiore U.; Francis S.A.J.; Roy D.S.

Details: Volume 122, October 2025

Abstract: Diabetes Mellitus (DM), a condition that requires early detection and prompt treatment to prevent life-threatening complications, is a critical focus in intelligent healthcare. Accurate diagnosis and prediction of DM are hindered by challenges such as the lack of comprehensive annotated data and an incomplete understanding of the complex interplay between the disease and various physiological factors. To address these challenges, this research introduces MOODM-Net, a Multi-Objective Optimization (MOO)-based deep network for DM prediction. A novel hybrid Feature Selection (FS) approach, combining multi-objective Harris Hawk Optimization (HHO) with Gray Wolf Optimization (GWO), is used to identify the most informative features from different data sources. This FS step, a critical aspect of data fusion in smart healthcare, aims to extract meaningful insights from potentially noisy and redundant information collected from diverse sources such as wearable sensors, Electronic Health Records (EHRs), and genetic data. Using these carefully selected features, the proposed deep network is fine-tuned with a hybrid exploration–exploitation strategy to optimize its performance for accurate DM prediction. Experimental validation on two widely used DM datasets demonstrates that MOODM-Net outperforms existing approaches, achieving superior prediction accuracy. This highlights the potential of this data fusion-driven approach for improving DM management and advancing personalized healthcare solutions within smart healthcare systems.

URL: https://www.sciencedirect.com/science/article/pii/S1566253525002611?via%3Dihub

SCHOLARLY PUBLICATIONS
School of Computer Applications
KIIT Deemed to be University

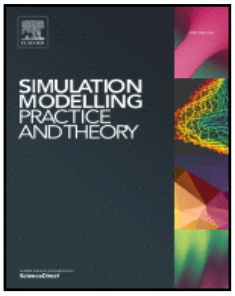
Journal Name: Simulation Modelling Practice and Theory **IF: 4.6**

Title: JaGW: A hybrid meta-heuristic algorithm for IoT workflow placement in fog computing environment

Author: Apat H.K.; Sahoo B.

Details: Vol. 144, November 2025, Article no. 103163

Abstract: In recent years, applications of the Internet of Things (IoT) have experienced rapid growth, driven by the widespread adoption of IoT devices in various sectors. However, these devices are typically resource-constrained in terms of computing power and storage capacity. As a result, they often offload the generated data and tasks to nearby edge devices or fog computing layers for further processing and execution. The fog computing layer is located in close vicinity of the IoT devices and comprises a set of heterogeneous fog computing nodes to supplement the capacities of resource-constrained IoT devices. The fog computing nodes often pose computational challenges for various computation-intensive tasks such as image processing application, comprises various machine learning and artificial intelligence enabled tasks. In such a scenario, finding the effective task placement for dynamic and heterogeneous applications is computationally hard. In this work, we formulate the IoT application workflow placement problem as a multi-objective optimization problem formulated as Integer Linear Programming (ILP) model with the objective of minimizing the makespan, cost of execution, and energy consumption. A hybrid metaheuristic approach is proposed that combines the strengths of the Jaya algorithm (JA) and Grey Wolf Optimization (GWO) named as JaGW to derive a sub-optimal solution. The proposed JaGW is compared with conventional GWO and other state of the art algorithms such as Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO) using the Montage scientific workflow dataset. The simulation results demonstrate that the proposed algorithm achieves an average reduction in energy consumption of 24.84% compared to JAYA, 14.67% compared to ACO, 14.65% compared to PSO, and 8.78% compared to GWO, thereby exemplifying its superior performance over other metaheuristic algorithms.



URL: https://www.sciencedirect.com/science/article/pii/S1569190X2500098X?via%3Dihub

SCHOLARLY PUBLICATIONS
School of Computer Applications
KIIT Deemed to be University

Journal Name: Scientific Reports **IF: 3.9**

Title: Integration of metaheuristic based feature selection with ensemble representation learning models for privacy aware cyberattack detection in IoT environments

Author: Karthikeyan M.; Brindha R.; Vianny M.M.; Vaitheeshwaran V.; Bachute M.; Mishra S.; Dash B.B.

Details: Vol. 15, Issue 1, December 2025, Article no. 22887

Abstract: The Internet of Things (IoT) connects virtual and physical objects inserted with software, devices, and other technology that interchange data utilizing the Internet. It enables diverse devices and individuals to exchange data, interconnect, and personalize services to ease usage. Despite IoT's merits, rising cyberthreats and the rapid growth of smart devices increase the risk of data breaches and security attacks. The increasing complexity of cyberattacks demands advanced intrusion detection systems (IDS) to defend crucial assets and data. AI techniques such as machine learning (ML) and deep learning (DL) have shown robust potential in improving IDS performance by accurately detecting and classifying malicious network behavior in IoT environments. The data normalization stage initially applies Z-score normalization to convert input data into a beneficial format. The AMFS-ELPPCD model utilizes the adaptive Harris hawk optimization (AHHO) model for the feature process selection of the subset. Furthermore, ensemble models such as bidirectional gated recurrent unit (BiGRU), Wasserstein autoencoder (WAE), and deep belief network (DBN) are used for the classification process. Finally, social group optimization (SGO) optimally adjusts the ensemble classifiers' hyperparameter values, resulting in better classification performance. A set of simulations is performed to exhibit the promising results of the AMFS-ELPPCD under dual datasets. The experimental validation of the AMFS-ELPPCD technique portrayed a superior accuracy value of 99.44% and 98.85% under the CICIDS-2017 and NSLKDD datasets over existing models.

URL: https://www.nature.com/articles/s41598-025-05545-5

SCHOLARLY PUBLICATIONS
School of Computer Applications
KIIT Deemed to be University

Journal Name: Scientific Reports **IF: 3.9**

Title: A deep dive into artificial intelligence with enhanced optimization-based security breach detection in internet of health things enabled smart city environment

Author: Jayanthi S.; Suhasini S.; Sharmili N.; Laxmi Lydia E.; Shwetha V.; Dash B.B.; Bachute M.

Details: Vol. 15, Issue 1, December 2025, Article no. 22909

Abstract: Internet of Health Things (IoHT) plays a vital role in everyday routine by giving electronic healthcare services and the ability to improve patient care quality. IoHT applications and devices become widely susceptible to cyber-attacks as the tools are smaller and varied. Additionally, it is of dual significance once IoHT contains tools applied in the healthcare field. In the context of smart cities, IoHT enables proactive health management, remote diagnostics, and continuous patient monitoring. Therefore, it is essential to advance a strong cyber-attack detection method in the IoHT environments to mitigate security risks and prevent devices from being vulnerable to cyber-attacks. So, improving an intrusion detection system (IDS) for attack identification and detection using the IoHT method is fundamentally necessary. Deep learning (DL) has recently been applied in attack detection because it can remove and learn deeper features of known attacks and identify unknown attacks by analyzing network traffic for anomalous patterns. This study presents a Securing Attack Detection through Deep Belief Networks and an Advanced Metaheuristic Optimization Algorithm (SADDBN-AMOA) model in smart city-based IoHT networks. The main aim of the SADDBN-AMOA technique is to provide a resilient attack detection method in the IoHT environment of smart cities to mitigate security threats. The effectiveness of the SADDBN-AMOA method is investigated under the IoT healthcare security dataset. The experimental validation of the SADDBN-AMOA method illustrated a superior accuracy value of 98.71% over existing models.

URL: https://www.nature.com/articles/s41598-025-05850-z

SCHOLARLY PUBLICATIONS
School of Computer Applications
KIIT Deemed to be University

Journal Name: Sustainable Computing: Informatics and Systems **IF: 3.8**

Title: LESP:A fault-aware internet of things service placement in fog computing

Author: Apat H.K.; Sahoo B.

Details: Volume 32, Issue 2, 2025

Abstract: The rapid advancement of 5G networks enables increase adoption of Industrial Internet of Things (IIoT) devices which introduces variety of time-sensitive applications requires low-latency, fault-tolerant, and energy-efficient computing environments. Fog computing infrastructure that extends cloud computing capabilities at the network edge to provide computation, communication, and storage resources. Due to the limited computing capacity of the Fog node, it restricts the number of tasks executed. The other key challenges are the risk of hardware and software failure during task execution. These failures tend to disrupt the configuration of fog computing nodes, affecting the reliability and availability of services. As a result, this can negatively impact the overall performance and service level objectives. The fault-tolerant-based IoT service placement problem in the fog computing environment primarily focuses on optimal placement of IoT services on fog and cloud resources with the objective of maximizing fault tolerance while satisfying network and storage capacity constraints. In this study, we compared different community-based techniques Girvan-Newman and Louvain with Integer Linear Programming (ILP) for fault tolerance in fog computing using the Albert-Barabási network model. In addition, it proposed a novel Louvian based on eigenvector centrality service placement (LESP) to improve conventional Louvian methods. The proposed algorithm is simulated in iFogSim2 simulator under three different scenario such as under 100, 200 and 300 nodes. The simulation results exemplify that LESP improves fault tolerance and energy efficiency, with an average improvement of approximately 20% over Girvan-Newman, 25% over ILP, and 12.33% over Louvain. These improvements underscore LESP's strong efficiency and capability in improving service availability across a wide range of network configurations.

URL: https://www.sciencedirect.com/science/article/pii/S2210537925000174?via%3Dihub

SCHOLARLY PUBLICATIONS
School of Computer Applications
KIIT Deemed to be University

Journal Name: Bioengineering **IF: 3.7**

Title: Medical LLMs: Fine-Tuning vs. Retrieval-Augmented Generation

Author: Pingua B.; Sahoo A.; Kandpal M.; Murmu D.; Rautaray J.; Barik R.K.; Saikia M.J.

Details: Volume 12, Issue 7, July 2025

Abstract: Large language models (LLMs) are trained on huge datasets, which allow them to answer questions from various domains. However, their expertise is confined to the data that they were trained on. In order to specialize LLMs in niche domains like healthcare, various training methods can be employed. Two of these commonly known approaches are retrieval-augmented Generation and model fine-tuning. Five models—Llama-3.1-8B, Gemma-2-9B, Mistral-7B-Instruct, Qwen2.5-7B, and Phi-3.5-Mini-Instruct—were fine-tuned on healthcare data. These models were trained using three distinct approaches: retrieval-augmented generation (RAG) alone, fine-tuning (FT) alone, and a combination of both (FT+RAG) on the MedQuAD dataset, which covers a wide range of medical topics including disease symptoms, treatments, medications, and more. Our findings revealed that RAG and FT+RAG consistently outperformed FT alone across most models, particularly LLAMA and PHI. LLAMA and PHI excelled across multiple metrics, with LLAMA showing superior overall performance and PHI demonstrating strong RAG/FT+RAG capabilities. QWEN lagged behind in most metrics, while GEMMA and MISTRAL showed mixed results.

URL: https://www.mdpi.com/2306-5354/12/7/687

SCHOLARLY PUBLICATIONS
School of Computer Application
KIIT Deemed to be University

Journal Name: IEEE Access **IF: 3.4**

Title: GANCE: Generative Adversarial Network Assisted Channel Estimation for Unmanned Aerial Vehicles Empowered 5G and Beyond Wireless Networks

Author: Gupta, C; Das, RK; Barik, RK; Qurashi, SN; Roy, DS; Yadav, SS

Details: Vol. 13, 2025

Abstract: Unmanned aerial vehicles (UAVs) have discovered a plethora of societal applications such as remote sensing, disaster management, medical emergency, security and surveillance, etc. UAVs require fast and reliable communication lines, and selecting the appropriate channel estimation (CE) technique is pivotal in reliable communication. Orthogonal time frequency space (OTFS) is an innovative modulation technique designed to support reliable communication in rapid mobility environments for 5G and beyond applications, effectively addressing challenges posed by Doppler shifts and multipath propagation. Current OTFS receivers utilize threshold methods such as least squares (LS) and minimum mean square error estimators for CE. To further enhance the accuracy and robustness of the CE process, this paper proposes a generative adversarial network (GAN) for learning channel parameters and performing CE in OTFS-based communication systems for high-speed UAVs (100-500 km/h). Firstly, a system model considering the Doppler effect has been modeled mathematically, and then the solution to the CE problem is presented for UAVs-assisted networks using GAN. The proposed GAN architectures comprise a U-Net-based generator and a PatchGAN discriminator for adversarial training of the model. The proposed model is compared with the baseline approaches in terms of bit error rate (BER), outage probability (OP), and normalized mean squared error (NMSE) for different velocities and modulation schemes. The proposed model has given an improvement of 70%, 55%, 45% in BER performance and 40%, 30%, 20% in OP compared to the conventional LS estimator, machine learning-based estimator, and deep learning-based estimator, respectively.

URL: https://ieeexplore.ieee.org/document/10815946

SCHOLARLY PUBLICATIONS
School of Computer Application
KIIT Deemed to be University

Journal Name: IEEE Access **IF: 3.4**

Title: A Novel Pairing Free Revocable Certificateless Encryption with Ciphertext Evolution for Healthcare System

Author: Singh M.R.; Barik R.K.; Qurashi S.N.; Thokchom S.; Roy D.S.

Details: Volume 13, 2025

Abstract: With the advancement of modern healthcare systems, patients now utilize medical sensor nodes to generate health data. These data are then transmitted to healthcare providers for analysis and diagnosis of the patient. These data are sensitive in nature and, therefore, need to preserve their privacy, security, and confidentiality. Another crucial aspect of a healthcare system is the effective revocation of malicious users. Revocable encryption schemes, particularly those with ciphertext evolution, have emerged as promising solutions. However, all the existing revocable schemes with ciphertext evolution have expensive bilinear pairing, map-to-point hash, modular exponentiation operations, rendering them unsuitable for resource constrained medical sensor nodes. In this paper, we propose a novel pairing free revocable certificateless encryption scheme with ciphertext evolution. Also, we prove that our scheme is secure against adaptive chosen ciphertext attacks. Our comparative analysis demonstrates that our scheme achieves substantial reductions in total computational cost by 74.9% to 86.4% and reduces ciphertext communication cost by 45.9% to 72.9%, making it the most effective among related schemes.

URL: https://ieeexplore.ieee.org/document/10851271

SCHOLARLY PUBLICATIONS
School of Computer Application
KIIT Deemed to be University

Journal Name: IEEE Access **IF: 3.4**

Title: A Faster, Integrated and Trusted Certificate Authentication and Issuer Validation System based on Blockchain

Author: Priyadarshini R.; Pandey R.; Ankit K.C.; Bhandari D.; Khadka B.; Barik R.K.; Saikia M.J.

Details: Volume 13, 2025

Abstract: Verifying the legitimacy of original documents such as educational degree certificates is crucial. If these are found to be fraudulent, it can cause significant disruptions in the hiring process, resulting in substantial productivity losses. The researchers suggested several proposals to preserve these certificates. However, the challenge is still to have an integrated, tamper-proof and low-cost solution where the certificate issuer and the certificate itself are validated in a single platform. This paper proposes an integrated solution that uses a decentralized blockchain-based certificate verification and issuer validation system. In addition to this, it will protect the certificates from being tampered with. To search faster, hash function mapping has been employed. The proposed solution is experimentally validated by creating a blockchain network using Ethereum where each peer node represents an entity of a certificate verification system such as a validator, certificate issuer, certificate holder and the end-user of the client. The performance of the designed solution is measured by the execution and transaction cost in terms of gas consumption. A comparative analysis has been performed on similar types of tasks reported in the existing work performed on the same platform. It has been observed that the cost incurred for adding a certificate is minimal for the proposed approach. Furthermore, the searching time for the certificates is minimized by using a hash-based searching methodology. The results show that the search time has drastically gone down when certificates are not available.

URL: https://ieeexplore.ieee.org/document/10872957