SCHOLARLY PUBLICATIONS
School of Computer Engineering
KIIT Deemed to be University

Journal Name: IEEE Transactions on Consumer Electronics **IF: 9.9**

Title: AI2-Defense: An Autonomous Counter-AI Framework Against AI-Generated Threats in Consumer Systems

Author: Singh A.; Alzubi J.A.; Hosseinzadeh M.; Salhi A.; Aurangzeb K.

Details: 25th June, 2026

Abstract: The rapid advancement of generative and autonomous artificial intelligence has enabled adaptive cyber threats targeting consumer systems. Traditional security mechanisms struggle against AI-driven attacks such as polymorphic phishing, prompt injection, and autonomous malware. However, existing defenses lack autonomous and adaptive counter-AI capabilities for real-time threat response. This paper introduces AI^2-Defense, an autonomous Counter-AI framework implementing an AI-against-AI security paradigm through generative origin intelligence, adversarial dual-model discrimination, dynamic sandboxing, reinforcement-driven deception, and secure lifecycle governance. Experimental evaluation across CICI-DS2017, Ember, and ISCX URL datasets demonstrates detection accuracy up to 98.3%. Under PGD-based adversarial attacks, evasion rates are reduced from 31.4% to 12.6%. The results demonstrate that the residual attack probability is reduced to below 10% under adaptive reinforcement-based attacks. The framework introduces moderate computational overhead, increasing inference latency by 4–7 ms and GPU utilization by 9–12%, while maintaining real-time feasibility for consumer deployments.

URL: https://ieeexplore.ieee.org/document/11579367

SCHOLARLY PUBLICATIONS
School of Computer Engineering
KIIT Deemed to be University

Journal Name: IEEE Transactions on Consumer Electronics **IF: 9.9**

Title: FedTrust-UNLEARN: Trust-Aware Federated Learning with Auditable Unlearning for Privacy-Preserving Consumer IoMT EEG Intelligence

Author: Rai R.K.; Achar S.; Yambem N.; Pallawi S.; Sharma A.; Aldhyani T.H.; Basheer S.; Kumar M.

Details: 6th July, 2026

Abstract: The growing adoption of EEG-enabled consumer Internet of Medical Things (IoMT) devices and wearable neuro-monitoring systems in healthcare and home-centric environments has raised critical concerns regarding data privacy, trust, and regulatory compliance. Although centralised deep learning approaches achieve strong performance in EEG-based emotion and cognitive state recognition, their reliance on centralised data aggregation limits scalability and applicability in privacy-sensitive consumer healthcare settings. Furthermore, existing federated learning approaches often inadequately address trust heterogeneity, non-IID neurophysiological variability, unreliable client participation, and the emerging requirement of federated unlearning in distributed IoMT environments. This paper proposes FedTrust-UNLEARN, a trust-aware federated learning framework with auditable unlearning for privacy-preserving EEG intelligence across heterogeneous consumer IoMT networks. The proposed framework integrates adaptive spectral representation learning, dynamic trust-aware aggregation, and an auditable federated unlearning mechanism that enables selective attenuation of client influence without requiring complete retraining. Extensive experiments on the SEED, SEED-IV, and DREAMER datasets under subject-dependent and subject-independent settings demonstrate competitive performance relative to centralised learning while improving robustness against unreliable clients, privacy preservation, and practical unlearning behaviour. The results demonstrate stable collaborative optimisation, bounded post-unlearning degradation, and communication-efficient deployment, highlighting the practicality of trustworthy, regulation-aware federated EEG intelligence for real-world consumer IoMT healthcare applications.

URL: https://ieeexplore.ieee.org/document/11595619

SCHOLARLY PUBLICATIONS
School of Computer Engineering
KIIT Deemed to be University

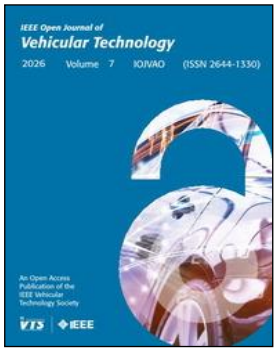
Journal Name: IEEE Open Journal of Vehicular Technology **IF: 6.6**

Title: A Survey on LLM-Enabled UAV Digital Twins for Internet of Vehicles Systems

Author: Bajoria S.; Kanrar S.; Pandey H.; De P.; Akash A.; Hassija V.; Chamola V.

Details: June 2026

Abstract: Vehicular Digital Twins (VDTs) are emerging as a core enabler for real-time monitoring, simulation, and intelligent control in Internet of Vehicles (IoV) systems. While prior research has largely focused on ground vehicles, the integration of Unmanned Aerial Vehicles (UAVs) into vehicular digital twin ecosystems remains underexplored. This paper presents a comprehensive survey on the role of Large Language Models (LLMs) in enabling UAV Digital Twins for autonomous and cooperative operations within IoV environments. By conceptualizing UAVs as cyber-physical entities continuously synchronized with their virtual counterparts, we analyze how LLMs act as cognitive engines for high-level reasoning, multimodal perception grounding, natural-language interaction, and adaptive mission planning. The survey introduces an LLM-enabled UAV Digital Twin architecture incorporating edge-cloud collaboration, real-time state mirroring, and safety-aware control. Communication workflows leveraging vehicular networking paradigms such as V2X are discussed to support low-latency synchronization and fleet-level coordination. Key application domains, including disaster response, infrastructure monitoring, and Drone-as-a-Service within IoV systems, are examined. Finally, open challenges related to real-time synchronization, computational constraints, and scalability are highlighted, along with future research directions involving TinyLLMs, federated learning, and edge-enabled digital twin platforms.



URL: https://ieeexplore.ieee.org/document/11544113

Journal Name: Future Generation Computer Systems **IF: 6.1**

Title: DQVeriChain: Distributed quantum-state-verified and DID-based self-attentive large language model for criminal tracking using blockchain

Author: Shaw, R; Majumder, S

Details: Volume 180, July 2026

Abstract: The increasing complexity of cybercrime and identity manipulation activities demands a secure, verifiable, and quantum-resilient framework for criminal identification. This study introduces 'DQVeriChain', a distributed quantum-state-verified and decentralized identity-based large language model (LLM) designed for criminal tracking using blockchain. The system integrates quantum principal component analysis (QPCA), GHZ state-fidelity validation, and ZZ-feature mapping to ensure high-fidelity quantum entanglement and secure feature encoding. The verification process combines both the Quantum Self-Attention Mechanism (QSAM) and the Quantum Self-Correcting Attention Mechanism (QSCAM) with LLM-driven inference for intelligent anomaly detection. In addition, validation was performed using IBM Qiskit with 10-fold cross-validation and fidelity thresholds (F >= 0.5), achieving prediction accuracy greater than 99% with minimal quantum circuit complexity (5/5 qubits). These experimental results confirm that 'DQVeriChain' offers an efficient, tamper-resistant, and scalable architecture suitable for real-time forensic and cybersecurity applications.

URL:https://www.sciencedirect.com/science/article/pii/S0167739X26000464?pes=vor&utm_source=clarivate&getft_integrator=clarivate

SCHOLARLY PUBLICATIONS
School of Computer Engineering
KIIT Deemed to be University

Journal Name: International Journal of Human-Computer Interaction **IF: 6.1**

Title: Diffusion of Innovation Factors Influencing User Trust and Adoption of AI-Based Cybersecurity Tools

Author: Muhudin, A; Hussein, OD; Osoble, AM; Mondal, J; Mohamud, AA; Omar, AA; Ali, IM

Details: 20th July, 2026

Abstract: The adoption of artificial intelligence (AI)–based cybersecurity tools introduces challenges, positioning user trust as a critical determinant of acceptance. While Diffusion of Innovation (DOI) theory explains adoption, limited empirical work integrates DOI with trust mechanisms. This study examines the mediating role of user trust between DOI attributes and intention to use AI-based cybersecurity tools. Data were collected from 420 participants and analyzed using partial least squares structural equation modeling (PLS-SEM) and artificial neural network (ANN) analysis. Results indicate that Complexity ($\beta = 0.323$, $p < 0.001$) and Observability ($\beta = 0.231$, $p = 0.002$) significantly influence User Trust, whereas Relative Advantage, Compatibility, and Trialability are not significant predictors. User Trust predicts Intention to Use ($\beta = 0.496$, $p < 0.001$) and mediates the effects of Complexity and Observability. ANN results corroborate the dominant predictive roles of Complexity and Trust. Findings support a trust-embedded diffusion framework for AI cybersecurity adoption and identify limitations of classical DOI theory in autonomous, high-risk environments.

URL: https://www.tandfonline.com/doi/full/10.1080/10447318.2026.2702157

SCHOLARLY PUBLICATIONS
School of Computer Engineering
KIIT Deemed to be University

Journal Name: Biomedical Signal Processing and Control **IF: 5.7**

Title: HyMAF-Net: A region-aware multi-agent fusion attention transformer for multiclass brain tumor classification

Author: Swain K.P.; Nayak S.R.; Swain S.K.; Sinha U.

Details: Volume-127, 1st November, 2026

Abstract: Magnetic resonance imaging (MRI) is a primary modality for brain tumor diagnosis; however, manual interpretation is time-consuming and subject to inter-observer variability. Furthermore, the complex spatial heterogeneity of tumor regions and long-range contextual dependencies within MRI scans pose significant challenges for automated analysis. To address these issues, we propose HyMAF-Net, a region-aware multi-agent hybrid framework that synergistically integrates convolutional neural networks (CNNs) for local feature extraction and vision transformers (ViTs) for global contextual modeling as a dual feature module. The framework adopts a cooperative multi-agent regional fusion architecture in which region-specific agents perform adaptive feature fusion via attention-based gating, followed by confidence-aware decision making and inter-agent communication for consensus-based classification. The proposed model is evaluated on a publicly available multi-class brain tumor MRI dataset using standardized data augmentation, and optimized training configurations. Extensive experimental analyses are conducted, including comparisons with CNN backbone networks and transformer-based architectures, evaluation against recent state-of-the-art methods, ablation studies to assess the contribution of individual components, and visualization-based interpretability analysis to enhance clinical transparency. In addition, computational overhead, model complexity, and robustness under noisy imaging conditions are systematically examined for model validation. HyMAF-Net consistently outperforms competing approaches across all evaluations, achieving a classification accuracy of 99.01% and improved sensitivity and robustness across tumor categories. These results demonstrate that region-aware multi-agent reasoning combined with transformer-based global representations yields a reliable, efficient, and interpretable framework suitable for real-time clinical decision support.

URL: https://www.sciencedirect.com/science/article/pii/S1746809426015648?via%3Dihub

SCHOLARLY PUBLICATIONS
School of Computer Engineering
KIIT Deemed to be University

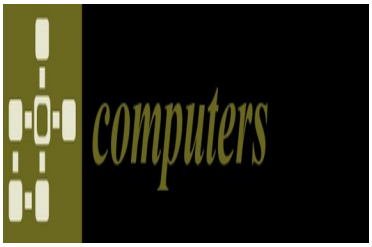
Journal Name: Computers **IF: 5.2**

Title: Dynamic Flow Rule Placement for Real-Time Energy Optimization in SDN

Author: Behera S.; Panda N.; Patra S.S.

Details: Volume-15, Issue-6, June 2026

Abstract: A Software-Defined Network (SDN) renders flexible traffic engineering, but consumes a lot of energy. There is an overhead on the control-plane because flow rule updates are always performed and there is energy consumption by the forwarding hardware. Current energy-aware SDN methods mostly focus on Static or Greedy optimizations. This can cause too many Ternary Content-Addressable Memory (TCAM) updates and unstable rule churn when traffic changes over time. This article introduces a Dynamic Flow Rule Placement (DFRP) framework for real-time energy optimization in SDN. It reduces network energy usage, TCAM update costs, and rule churn all at the same time. The suggested framework uses a convex relaxation method to take decisions on binary switches, links, and rule placement. It also uses a minimum-edit round scheme that only allows small rule changes between time slots. To further reduce instability in the control plane, batch scheduling and receding horizon optimization (RHO) techniques are used. The system uses predicted traffic for future time slots to make decisions, but only the actions for the current time slot are executed. The experiments are carried out on two real-world dynamic SNDlib topologies such as Germany50 and Nobel-Germany, using 288 five-minute traffic matrices over a one-day period. Comparative results against Static and Greedy baselines show that DFRP saves approx. 30% energy while cutting down on TCAM update overhead and rule churn by approx. 20%, consistently across both the networks. Hence DFRP can be applied on dynamic traffic large-scale networks for stable and energy-efficient SDN operations.



URL: https://www.mdpi.com/2073-431X/15/6/349

SCHOLARLY PUBLICATIONS
School of Computer Engineering
KIIT Deemed to be University

Journal Name: Machine Learning with Applications **IF: 4.9**

Title: Emergence of serverless computing in cloud: A state-of-the-art review of challenges and opportunities

Author: Kumari A.; Behera R.K.; Sahoo K.S.; Sahoo B.; Gandomi A.H.

Details: Volume 24, June 2026

Abstract: Serverless computing has emerged as a prominent cloud application development paradigm over the past decade, enabling developers to deploy and execute applications without managing underlying infrastructure. By abstracting resource provisioning, configuration, and auto-scaling, serverless platforms leverage Backend as a Service (BaaS) and Function as a Service (FaaS) models to execute applications as independent, event-driven functions on managed infrastructure. In this paper, a set of well-defined research questions are formulated to systematically analyze the challenges, design trade-offs, and performance implications of serverless computing. A comparative evaluation with traditional cloud models, including Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), is conducted with respect to cost efficiency and response latency. Beyond existing surveys, this work provides a unified and quantitative synthesis of serverless research by jointly examining architectural features, execution workflows, performance metrics (e.g., cold-start overhead, throughput, and cost-effectiveness), and the availability of frameworks and simulators within a single analytical framework. Unlike prior studies that focus on isolated aspects of serverless systems, this review consolidates insights across multiple dimensions, bridges application and system level perspectives, and identifies underexplored research gaps such as stateful serverless execution, benchmarking reproducibility, and simulator-driven evaluation. The paper concludes by outlining emerging research opportunities, offering a comprehensive and up-to-date reference for researchers and practitioners in cloud and serverless computing.

URL: https://www.sciencedirect.com/science/article/pii/S2666827026000277?via%3Dihub

SCHOLARLY PUBLICATIONS
School of Computer Engineering
KIIT Deemed to be University

Journal Name: Scientific Reports **IF: 4.9**

Title: PoinCLIP-VAD: a hyperbolic cross-modal fusion framework for video anomaly detection

Author: Senapati D.P.; Pani S.K.; Baliarsingh S.K.; Dev P.P.; Somula R.

Details: Volume-16, Issue-1, December 2026

Abstract: Weakly supervised video anomaly detection (WSVAD) is fundamentally constrained by the absence of frame-level annotations, which leads to noisy instance selection in Multiple Instance Learning (MIL) and weak correspondence between temporal video segments and semantic descriptions. Vision-language models address this by enabling cross-modal alignment between visual features and textual labels, but when these representations are learned in Euclidean space, they struggle to capture subtle semantic variations and often produce ambiguous instance ranking under weak supervision. To address this limitation, we propose PoinCLIP-VAD, a vision-language framework that performs cross-modal fusion in hyperbolic space. The model embeds visual and textual features into a shared Poincaré ball geometry, where non-linear distance scaling provides a more expressive representation of latent semantic relationships induced by cross-modal interactions, without relying on predefined hierarchical structures. This geometry-consistent formulation enables more reliable similarity estimation and better preserves distinctions between normal and anomalous patterns. The framework adopts a dual-block architecture consisting of a classification block for coarse anomaly scoring and a video-text alignment block for fine-grained correspondence using negative Poincaré distance. Extensive experiments on benchmark datasets demonstrate that PoinCLIP-VAD achieves an AUC of 90.62% on UCF-Crime and an AP of 86.93% on XD-Violence, confirming improved anomaly discrimination and more consistent cross-modal alignment under weak supervision.

URL: https://www.nature.com/articles/s41598-026-56792-z

Journal Name: Information (Switzerland) **IF: 4.3**

Title: RETRACTION: A Tailored Particle Swarm and Egyptian Vulture Optimization-Based Synthetic Minority-Oversampling Technique for Class Imbalance Problem.

Author: Rout S.; Mallick P.K.; V. N. Reddy A.; Kumar S.

Details: Volume-17, Issue-6, June 2026

Abstract: The journal retracts the article titled “A Tailored Particle Swarm and Egyptian Vulture Optimization-Based Synthetic Minority-Oversampling Technique for Class Imbalance Problem” [1], cited above. Following publication, concerns were brought to the attention of the Editorial Office regarding the integrity of the peer-review process for this publication [1]. An internal investigation conducted by the journal identified irregularities in the peer-review process. In particular, the identity and authenticity of at least one reviewer could not be verified, and the peer-review process was therefore found to be compromised. As a result, the journal cannot ensure the integrity of the peer-review process that led to the acceptance of this article. Consequently, the Editorial Board has lost confidence in the reliability of the findings and decided to retract this publication [1], as per MDPI’s retraction policy. This retraction was approved by the Editor-in-Chief of the journal Information. The authors did not agree to this retraction.

URL: https://www.mdpi.com/2078-2489/13/8/386

SCHOLARLY PUBLICATIONS
School of Computer Engineering
KIIT Deemed to be University

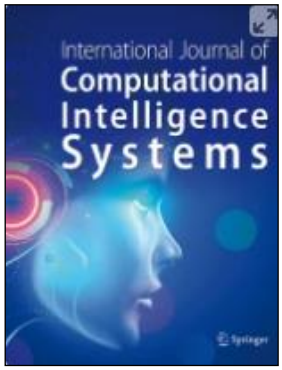
Journal Name: International Journal of Computational Intelligence Systems **IF: 4.0**

Title: Yellow Banded Wasp Algorithm: A Competition-driven Territorial Search Optimizer for Reliable Alignment of Point Cloud Registration

Author: Agrawal U.K.; Panda N.; Aluvalu R.; Tejani G.G.

Details: Volume 19, Issue 1, December 2026

Abstract: This paper presents a fresh swarm-based metaphorical approach termed the Yellow Banded Wasp Algorithm (YBWA) that mimics the adaptive communal dynamics of yellow-banded wasps. The YBWA employs the competition-driven territorial search (CDTS) and the memory-based updating procedure, allowing a balance between exploration and exploitation. The CDTS enables the wasps to adopt a decentralized approach to decision-making, while the memory archive retains the elite solution for future iterations. When utilized together, these aspects simplify the population diversity and the convergence dynamics to the global optimum. The adeptness of YBWA has been meticulously benchmarked on the IEEE-CEC-2017 test functions across dimensions 10 and 30, and the IEEE-CEC-2022 test suite over dimensions 10 and 20. The suggested YBWA outperforms eleven present-day optimization approaches (OAs) in terms of the mean fitness value across all the function types. A chain of non-parametric assessments has been carried out to substantiate the exclusivity of the YBWA. Furthermore, the YBWA has been employed to assess the six rigid transformation components for the Point Cloud Registration (PCR) utilizing the Bildstein Station 1 dataset. The YBWA yields an exact spatial alignment of the point clouds, characterised by low registration error and an optimized set of transformation components. Hence, the YBWA is a viable and reliable approach to be deployed as an optimizer for the registration process and optimistic tasks (OTs).



URL: https://link.springer.com/article/10.1007/s44196-026-01363-3