

PREFACE TO THE EDITION

It is a pleasure to present the forthcoming issue of the **Eduschool Journal of Computer Science Research Studies (EJCSRS)**, which brings together a timely collection of scholarly works addressing some of the most significant challenges and emerging directions in contemporary computer science. The contributions in this issue reflect the rapidly evolving nature of intelligent computing, with particular emphasis on security, robustness, privacy, trustworthy artificial intelligence, and scalable distributed technologies.

The issue opens with a comprehensive review of adversarial attacks and certified defences for deep image classifiers, examining the vulnerability of deep learning systems to carefully crafted perturbations and the distinction between empirical robustness and formally certified guarantees. The article compares major certification approaches and highlights the continuing gap between clean and robust accuracy, while emphasizing the importance of adaptive attack evaluation in assessing the reliability of defensive mechanisms.

The second contribution explores diffusion models for image restoration and super resolution, reflecting the growing role of generative models in reconstructing degraded visual information. The study examines conditional models and prior-based approaches across problems such as blur, noise, downsampling, and missing pixels. It also draws attention to the important relationship between distortion-based and perceptual evaluation, as well as unresolved challenges including blind degradation and the generation of hallucinated details.

The issue further extends the application of artificial intelligence to cybersecurity and financial security through graph neural networks for malware and financial fraud detection. By treating malicious software and fraudulent activity as graph-structured phenomena, the contribution demonstrates how structural relationships among program components, accounts, devices, and attributes can be exploited for detection. At the same time, it identifies persistent challenges involving class imbalance, adaptive adversaries, camouflage, and inappropriate temporal evaluation protocols.

Privacy and intellectual-property concerns in deployed artificial intelligence systems are examined in the article on model extraction and membership inference attacks. The contribution distinguishes attacks targeting the reconstruction of proprietary models from those seeking to determine whether particular records were used during model training. It also discusses defensive approaches and highlights the limitations of commonly used evaluation practices and watermarking strategies, reinforcing the need for stronger approaches to protecting both models and the individuals whose data contribute to them.

The issue concludes with an exploration of zero-knowledge proofs in distributed systems, with particular attention to zk-SNARKs and zk-STARKs and their applications in privacy-preserving and scalable blockchain systems. The article presents the fundamental principles behind zero-knowledge proofs and examines the practical trade-offs between proof size, verification efficiency, trusted setup requirements, and security. Its discussion of confidential transactions and validity rollups demonstrates the continuing convergence of cryptography, distributed systems, privacy, and blockchain technology.

Taken together, the contributions in this issue demonstrate an important shift in computer science research: technological advancement must increasingly be accompanied by security, verifiability, privacy, robustness, and responsible evaluation. Whether the subject is an intelligent image classifier, a generative restoration model, a graph-based security system, a deployed machine-learning service, or a decentralized blockchain application, questions of trust and reliability remain central.

We hope that this issue of EJCSRS will provide researchers, academics, practitioners, and students with useful perspectives on current developments and stimulate further investigation into the challenges identified across these rapidly developing fields. We gratefully acknowledge the contributions of the authors and the scholarly efforts involved in bringing this issue together.

Dr. Sr. Mini T V
Chief editor

CONTENTS

SL. NO	TITLE	AUTHOR	PAGE NO
1	Adversarial Attacks and Certified Defences for Deep Image Classifiers	Rasmi M	1-6
2	Diffusion Models for Image Restoration and Super Resolution: Methods and Evaluation	Rejina P V	7-11
3	Graph Neural Networks for Malware and Financial Fraud Detection	T Ramaprabha	12-16
4	Model Extraction and Membership Inference Attacks on Deployed Models	Juby George	17-21
5	Zero-Knowledge Proofs in Distributed Systems: zk-Snarks and zk-Starks For Privacy-Preserving and Scalable Blockchain Applications	Tintu George	22-27