KRISTU JAYANTI
(DEEMED TO BE UNIVERSITY)
Under Section 3 of UGC Act 1956
A CMI INSTITUTION | BENGALURU | INDIA

SCHOOL OF COMPUTATIONAL AND PHYSICAL SCIENCES

DEPARTMENT OF COMPUTER SCIENCE
in collaboration with

Carl von Ossietzky
Universität
Oldenburg

&

MURRAY STATE
UNIVERSITY

Proceedings of the
International Conference
on

COMPUTATIONAL INTELLIGENCE [ICCI 2026]

*"Fusion of Computational Mastery and
Intelligence to Explore New Realms for
Real-World Solution"*

29 & 30 JANUARY 2026

PUBLICATION PARTNER:

Journal of Computational and
Cognitive Engineering,

International Research Journal of
Multidisciplinary Technovation
Published by Asian Research Association
(A Non-Profit Educational Trust)

Springer

KRISTU JAYANTI
JOURNAL OF
COMPUTATIONAL
SCIENCES

KRISTU JAYANTI
(DEEMED TO BE UNIVERSITY)
Under Section 3 of UGC Act 1956
A CMI INSTITUTION | BENGALURU | INDIA

SCHOOL OF COMPUTATIONAL AND PHYSICAL SCIENCES

Department of Computer Science
in collaboration with

**University of Oldenburg
Haarentor Campus**

**Murray State
University**

COMPUTATIONAL INTELLIGENCE [ICCI 2026]

Proceedings of the
International Conference
on
Computational Intelligence (ICCI 2026)

*"Fusion of Computational Mastery and Intelligence to Explore New
Realms for Real-World Solution"*

DISCLAIMER
The authors are solely responsible for the contents of the papers compiled in this volume. The publishers or editors do not take any responsibility for the same in any manner. Errors, if any, are purely unintentional, and readers are requested to communicate such errors to the editors or publishers to avoid discrepancies in future

FOREWORD

Fr. Dr. Augustine George CMI
Vice Chancellor,
Kristu Jayanti (Deemed to be University)

In an era characterised by rapid technological advancements and evolving societal demands, the field of computational intelligence stands as a beacon of innovation and insight. This conference serves as a testament to our collective commitment to explore, discuss and harness the transformative potential of computational intelligence across diverse domains. The theme of this conference, "Fusion of Computational Mastery and Intelligence to Explore New Realms for Real-World Solution," encapsulates the essence of our shared journey towards understanding and leveraging computational intelligence in an ever-changing landscape. As we navigate through the complexities of artificial intelligence, machine learning, data analytics and related disciplines, it becomes imperative for us to remain adaptive, resilient and forward-thinking. This platform provides an opportunity to engage in meaningful dialogues, exchange cutting-edge research findings and foster collaborations that transcend geographical boundaries and disciplinary silos. The conference proceedings present a diverse range of concepts, approaches and applications that reflect the inventiveness and vitality of the computational intelligence field.

As we embark on this intellectual journey, let's embrace the spirit of curiosity, collaboration and amazement that defines our pursuit of knowledge. I hope these proceedings will provide us with the inspiration and tools we need to face the challenges of the digital age with compassion, creativity, and an unwavering commitment to quality. On behalf of the organising committee, I extend my deepest gratitude to all contributors, reviewers and collaborating partners, whose dedication and support have made this conference possible. I am confident that the insights gained and connections forged during this gathering will propel us toward new frontiers of discovery and innovation.

I wish you all a stimulating and rewarding experience at the International Conference on Computational Intelligence - Fusion of Computational Mastery and Intelligence to Explore New Realms for Real-World Solution.

Fr. Dr. Augustine George CMI
Kristu Jayanti (Deemed to be University)

ABOUT THE CONFERENCE

Computational Intelligence stands as a transformative paradigm in evolutionary computation, mirroring the intricate reasoning processes of human intelligence through pillars such as neural networks and fuzzy logic. This paradigm empowers computers to navigate and solve complex real-life problems, drawing insights from experimental data and observations. Across diverse sectors, including healthcare, business, education, travel, gaming, and entertainment, Computational Intelligence, bolstered by advanced computing technologies, emerges as a rapidly evolving approach, facilitating autonomous information processing and applications. In the realm of intelligent and sustainable engineering solutions, Computational Intelligence plays a pivotal role, fostering continuous innovation, research, and development to tackle social and global challenges and enhance computational performance across various domains.

ICCI-2026 brings together scholars, researchers, engineers, and scientists from across the nation to delve into state-of-the-art developments, key methodologies, research trajectories, challenges, and unresolved issues within the field of Computational Intelligence. By providing a platform for presenting new advancements and research outcomes, this conference fosters collaboration and knowledge exchange, bridging the gap between academic research and the practical needs of IT practitioners. Beyond academic pursuits, ICCI-2026 also explores the societal and commercial implications of Computational Intelligence, addressing the social, economic, and environmental facets of our nation with these innovative technologies.

Within these proceedings lie the insights, discussions, and contributions of our esteemed participants, encapsulating a wealth of knowledge, ideas, and solutions aimed at advancing the frontiers of Computational Intelligence and its impact on society. I extend my sincere appreciation to all attendees, speakers, and contributors for their invaluable contributions to ICCI-2026, and I trust that these proceedings will serve as a source of inspiration and guidance for researchers, practitioners, and stakeholders alike in the ongoing journey of Computational Intelligence.

[Conference Convenors - ICCI 2026]
Dr. Divya K.S
Dr. Gopinath D
Dr. Sherin Rappai

Editorial - ICCI 2026

It is with an immense sense of satisfaction and happiness that we welcome you to the conference proceedings of the International Conference on Computational Intelligence - Fusion of Computational Mastery and Intelligence to Explore New Realms for Real-World Solution. As the editors, we are honored to present the culmination of your research, insights, and innovations in the field of computational intelligence. This compilation stands as a testament to the collective wisdom and scholarly endeavors encapsulated within the diverse array of contributions, exploring the transformative potential of computational intelligence presented during the conference.

In an era defined by rapid technological advancements and evolving societal needs, your work serves as a testimony to the vital role of computational intelligence in shaping our understanding and utilization of emerging technologies. The theme of this conference, "Fusion of Computational Mastery and Intelligence to Explore New Realms for Real-World Solution," encapsulates the imperative for continuous adaptation and innovation in the face of evolving technological landscapes. As we navigate the complexities of artificial intelligence, machine learning, data analytics, and related disciplines, your research findings and insights serve as guiding beacons, illuminating pathways toward discoveries and applications. Your collective efforts have enriched the discourse surrounding computational intelligence and have the potential to drive meaningful change across various domains.

We extend our heartfelt appreciation to all authors for their scholarly contributions and to the organizing committee for their dedication to orchestrating this conference. We also extend our gratitude to the reviewers, whose expertise and insights have ensured the quality and rigor of the contributions presented within these proceedings. May these conference proceedings serve as a source of inspiration and knowledge exchange, fostering continued dialogue and collaboration in the exciting field of computational intelligence. We are confident that your contributions will pave the way for further advancements and innovations, propelling us toward a future where technology and intelligence converge to address complex challenges and opportunities.

 Wishing you all a fruitful and enriching experience as you engage with the insights and discoveries presented within these proceedings.

[Editorial Team]
Faculty: **Dr. Haripriya M P, Dr. Mary Jacob**
Student: **Sam Benjamin Blessen (23BCAA51), Akshay Sudheesh (24DTSA07)**

ABOUT THE UNIVERSITY

Kristu Jayanti (Deemed to be University) is a beacon of learning and innovation since its inception in 1999 as an affiliated institution under Bangalore University. The Institution is managed by St. Joseph Province Kottayam, Kerala of Carmelites of Mary Immaculate (CMI), the first indigenous catholic religious congregation in India. Marking a significant milestone in its journey, Kristu Jayanti attained the 'autonomous' status in the year 2013. As per the notification dated July 08, 2025, vide letter No. 9-13/2025 U.3(A), Kristu Jayanti has been conferred the status of Deemed to be University under section 3 of UGC Act, 1956, by the Department of Higher Education, Ministry of Education, Government of India under General Category.

 Kristu Jayanti Deemed to be University offers undergraduate and postgraduate programmes in Arts, Science, Management and Commerce, and integrated Law programmes. The institution was reaccredited with the highest grade 'A++' by the National Assessment and Accreditation Council (NAAC) in the Third Cycle of Accreditation in 2021. In the National Institutions Ranking Framework 2025, the institution has been ranked 34th place in the colleges category and is one of the top 100 colleges in the country. Moreover, the programmes of the Institute of Management are internationally accredited by the Accreditation Council for Business Schools and Programs [ACBSP], USA. The Institution was accorded 'DBT Star College' status under the strengthening component by the Department of Biotechnology, Ministry of Science & Technology, Government of India during the year 2020. Kristu Jayanti has consistently featured as one of the top institutions in rankings and surveys conducted by various agencies.

Kristu Jayanti Deemed to be University stands as a dynamic centre of excellence, committed to fostering scholarship, leadership and societal impact. The institution strives to fulfil its mission to provide educational opportunities for all aspiring youth to excel in life by developing academic excellence, fostering values, creating civic responsibility, inculcating environmental concern and building global competencies in a dynamic environment.

ABOUT THE DEPARTMENT

With a rich legacy spanning over two decades, the Department of Computer Science takes pride in offering one of the nation's most distinguished BCA programmes, ranked 4th at the national level and 2nd at the state level. The department offers a diverse portfolio of academic programmes, including BCA, BCA Analytics, BCA Cloud Computing, BCA Cyber Security, B.Sc Data Science, B.Sc Internet of Things (IoT), B.Sc Artificial Intelligence & Machine Learning, B.Sc Blockchain Technology, B.Sc Animation and Game Design, B.Sc Quantum Computing, and offering PhD programmes in Computer Science, Computer Applications, and Data Science. These programmes are meticulously designed to integrate strong theoretical foundations with extensive practical exposure, equipping students with industry-relevant competencies. The department further enhances academic rigor through the integration of NPTEL and other MOOC-based courses, enabling students to access high-quality learning resources from premier institutions and earn globally recognized certifications.

A distinctive strength of the department is its Skill Studio fosters hands-on learning through experiential and project-based activities, strengthening students' practical skills.The Computer Academy, a vibrant student-led club of the department with over 2500 members, serves as a vital bridge between academia and industry. Through guest lectures, workshops, seminars, industrial visits, hackathons, ideathons, and datathons, students gain continuous exposure to emerging technologies and innovative practices. The department further promotes a strong culture of innovation through the Student Research Forum, which encourages students to undertake research projects, publish papers, and present their work at conferences in National and International Level.

The department maintains strong collaborations with reputed industry and academic partners such as UiPath, Salesforce, Oracle Academy, Qlik, NASSCOM and other leading organizations. These partnerships support the delivery of certification courses, value-added programmes, and industry-aligned training, helping to bridge skill gaps in emerging domains.

The department has earned recognition for its consistent academic excellence, strong industry connect, impactful student outcomes, and impressive placement record, with a significant percentage of students securing placements in reputed organizations each year. Our graduates continue to make meaningful contributions across corporate sectors, research institutions, and national quality forums.

Dr. R. Kumar

Message from Dean, School of Computational and Physical Sciences

It is with great pleasure that I present the proceedings of the International Conference on Computational Intelligence organized by the Department of Computer Science, School of Computational and Physical Sciences.

The scholarly contributions compiled in this volume reflect the intellectual rigor, creativity, and research commitment of academicians, researchers, and practitioners who continue to expand the frontiers of knowledge in this rapidly evolving domain.

The papers included in this proceeding showcase contemporary advancements across key areas such as Artificial Intelligence, Machine Learning, Data Science, Cybersecurity, Internet of Things, Cloud and Edge Computing, Quantum Technologies, and Intelligent Systems. Each contribution represents thoughtful inquiry and meaningful progress toward addressing complex, scientific and societal challenges through computational innovation.

I encourage readers to engage deeply with the research presented, to reflect critically on the ideas proposed, and to draw inspiration for future exploration. The true strength of computational intelligence lies in its interdisciplinary nature and its potential to foster collaboration across domains, enabling solutions that are both innovative and impactful.

I extend my sincere appreciation to the authors for their valuable contributions, to the reviewers for upholding academic quality through their meticulous evaluations, and to the organizing and editorial teams for their dedication in bringing this proceedings volume to fruition. It is hoped that this collection will serve as a useful reference for the researchers and contribute meaningfully to ongoing research and innovation in computational intelligence.

Dr. R. Kumar

Dean, School of Computational and Physical Sciences

Dr. Sevuga Pandian A
Message from the Head, Department of Computer Science

As the Head of the Department of Computer Science, I am inspired by the dedication and passion that each of you brings to this conference. Your commitment to advancing the boundaries of computational intelligence is not only commendable but also essential in shaping the future of our discipline. The abstracts presented within this book encapsulate the diverse perspectives, novel ideas, and ground breaking research that characterise computational intelligence today. From machine learning algorithms to neural networks, from data mining techniques to evolutionary computation, each abstract represents a step forward in our collective quest to unravel the mysteries of intelligence and cognition.

As you peruse these abstracts, I encourage you to engage with the ideas presented, to question assumptions, and to explore new avenues of inquiry. The beauty of computational intelligence lies in its ability to transcend disciplinary boundaries and inspire interdisciplinary collaboration. Let us seize this opportunity to foster dialogue, share insights, and forge connections that will propel our field into uncharted territories.

I extend my deepest gratitude to the authors for their contributions, to the reviewers for their invaluable feedback, and to the organisers for their tireless efforts in bringing this conference to fruition. May the abstracts contained within these pages serve as a source of inspiration and insight, guiding us toward a future where computational intelligence continues to redefine the possibilities of human achievement.

On behalf of the Department of Computer Science, I wish you all a stimulating and enriching experience at the International Conference on Computational Intelligence.

Dr. Sevuga Pandian A
Head, Department of Computer Science

CONTENTS

ICCI2026001: Subsidy Access and Household Food Acquisition Patterns in India: Urban vs Rural Comparison

Aaddya Shukla[1], Azarudeen S[2], Vyshali Gogi[3]
Department of Statistics and Data Science
CHRIST(Deemed to be University)
Bengaluru,India

ABSTRACT

Using HCES 2024 microdata, this study looks at whether household consumption patterns in India differ between those who receive government subsidies and those who do not. Ration access, LPG subsidies, PMGKY, Ayushman, and free electricity are all linked with consumption indicators for online food purchases and ration item uptake in a combined household dataset (N = 28,000). Both parametric and non-parametric tests reject the null hypothesis of no difference. Recipients have significantly higher ration categories, with an average of 1.275 ± 1.149 compared to 0.000 ± 0.000, and the p-value is less than 0.001. Non-recipients have higher online food categories, averaging 0.478 ± 1.237, compared to recipients, who average 0.211 ± 0.862; the p-value is less than 10^{-24}.. A strong dose-response relationship exists between higher ration uptake and lower online consumption when subsidies are more intense. The findings indicate that market-based and subsidized food acquisition replace each other, which has implications for welfare design, digital commerce, and targeting.

Keywords - Household consumption, public distribution system, subsidies, welfare targeting, online retail, ration, India

ICCI2026002: A Comprehensive Survey on Deep Learning Models for CCTV-Based Smart City Surveillance: Trends, Challenges, and Future Directions

P. Karthik[1], Dr. Karthikeyan. P[2]

Research Scholar

Department of Computer Science and Engineering

RV University

Bengaluru, India

ABSTRACT

With the rapid growth of urbanization and the increasing need for public safety, smart city surveillance systems have gained significant attention in recent years. Proceeds from Closed-Circuit Television (CCTV) cameras now function as basic data sources because deep learning technologies enable simultaneous monitoring and face recognition in addition to event detection and crowd population control. The survey provides an extensive evaluation of modern deep learning approaches used for CCTV-based surveillance operations in smart cities. Research categorizes existing models for their usage purposes which include detecting objects while analyzing behaviors and recognizing activities. The document presents different datasets alongside system architecture specifications and necessary computational frameworks for real-world CCTV surveillance implementation. The analysis assesses four essential challenges which consist of data privacy as well as model interpretability alongside scalability and noisy/imbalanced data handling. The study examines current trends involving autonomous intelligence at network borders as well as distributed network processing along with multiple input data integration. Recommendations for future studies aim to resolve current shortcomings by improving the strength and performance together with ethical oversight of AI-based surveillance methods for smart cities.

Keywords: YOLO, UAV, DLM

ICCI202603: Sectoral Carbon Emission Trends in India: Insights from Hybrid Time Series Modeling of GHG Data (2005–2018)

Diya Shah[1], 2 Hemlata Joshi[2], and Vijayalakshmi A[3]

ABSTRACT

This study analyzes greenhouse gas emissions in India's Energy, Industry, and Waste sectors between 2005 and 2018, extending forecasts till 2025. To address this complexity we applied a hybrid time-series framework that combines ARIMA models with LSTM neural networks. The study used data from the Greenhouse Gas Platform India to track historical patterns, estimate sectoral contributions, and project emissions. Compared to ARIMA model, the ARIMA–LSTM hybrid delivered stronger results, particularly in capturing nonlinear growth in India's emissions. Model performance was validated through indicators such as Mean Absolute Percentage Error (MAPE), Root Mean Square Error (RMSE), and the Ljung–Box test. By 2018, Energy accounted for nearly 69% of total emissions, Industry for 27%, and Waste for 4%, with the latter expected to increase alongside urban growth. These findings emphasize the need for targeted interventions while demonstrating the value of hybrid modelling tools in producing reliable forecasts to guide long-term climate policy.

Keywords: Greenhouse Gas Emissions , ARIMA Hybrid Times Series , LSTM Neural Networks , Forecasting , India

ICCI202604: StyleEval: Programmatically Evaluating Style of Student Produced Code

Justin L. Holder[1], Matthew F. Tennyson[2]

Department of Computer Science & Information Systems, Murray State University, Murray, KY, U.S.A.

ABSTRACT

The process of grading programming style is long and tedious, which might contribute to its underutilization in the academic sphere. Despite this, the ability to program well-styled and readable code is highly sought after in the professional atmosphere. This leads many facilitators to endure a long, inconsistent process of manually evaluating code based on style and, in some cases, completely ignoring code style. The current implementations aiming to tackle this evaluation process programmatically are language-dependent, require syntactically correct source code, and often are not user-friendly or configurable. This research develops and presents a grading tool called StyleEval, which aims to tackle these problems and promote style considerations in the academic field. Instead of following previous implementations, which rely on linters and stripped-down compilers, we will focus on a different approach that relies on formatters, which are efficient, extensible, and, most importantly, readily available and often open-source. StyleEval was then analyzed using controlled source code–or, more accurately, correctly styled source code with artificially introduced style violations–and real-world student-produced code. From this analysis, StyleEval is shown to be considerably more accurate than the manual alternative. Notably, this accuracy did not diminish when the volume of code increased. Furthermore, StyleEval was shown to detect violations far more consistently and thus provide far more accurate grades.

Keywords: Programming style, CS education, Automated code grading, Code formatting

ICCI202605: Bridging Cattle Farming and Technology: The Development of MooManager

Matthew Hayes[1], Jason T Owen, DBA[2], Issac Reynolds[3]

Computer Science Department Student

Arthur J. Bauernfeind College of Business

Murray State University

102 Curris Center

Murray, KY 42054, USA

ABSTRACT

Small-scale cattle producers face persistent challenges in adopting digital tools for herd management, often due to barriers such as limited digital literacy, software complexity, and poor alignment with practical workflows. Existing literature highlights the potential benefits of mobile applications in agricultural contexts, yet adoption rates remain low among smaller operations. This thesis investigates how a streamlined, mobile-first application can address these adoption barriers while supporting essential farm management tasks. The study details the design and development of MooManager, a mobile application built with React Native and Supabase and structured around core features such as cattle tracking, beef sales logging, and role-based user access. Methods included iterative interface design, unit and integration testing, and preliminary usability evaluation with a representative end user. The implementation of the application indicates that simplifying feature sets and prioritizing accessibility can meaningfully reduce the entry threshold for digital adoption in livestock settings. MooManager serves as both a functional tool for small-scale producers and a design case study for user-centered agricultural technology.

Keywords: Mobile-first application,Small-scale cattle farming,Digital adoption,User-centered design,Herd management system

ICCI202606: Investigating students' proficiency across statistical software and preferences of statistical software design

Ashen White[1], Jason T Owen, DBA[2], Maria Dodson[3]

[1,3]Computer Science Department Student

Arthur J. Bauernfeind College of Business

Murray State University

102 Curris Center

Murray, KY 42054, USA

[2]Computer Science and Information Systems Department

Arthur J. Bauernfeind College of Business

Murray State University

102 Curris Center

Murray, KY 42054, USA

ABSTRACT

This paper investigated students' perceptions of their proficiency with statistical software applications and their preferences regarding software features. Results indicated that students' statistical and coding experience, as well as the specific application used, did not significantly influence their self-perceived proficiency. This suggests that it may be more effective to focus on building student skills within a chosen application, rather than tailoring the application to match existing student capabilities. While students showed clear preferences for certain features, favoring clarity over depth, flexibility over safeguards, and built-in checks over unrestricted freedom, these preferences generally leaned toward balanced design rather than extremes. This paper also covers development of a statistical software application that takes a balanced approach to its design.

Keywords: Statistical software proficiency; Student preferences; Software usability; Data analysis tools; User interface design.

ICCI202607: Empowering Educators in the Age of Generative AI

Jason T. Owen, DBA[1], Hassan Mistareehi, PhD[2]
Computer Science and Information Systems Department
Arthur J. Bauernfeind College of Business
Murray State University
102 Curris Center
Murray, KY 42054, USA

ABSTRACT

The rapid advancement of Generative AI (GenAI) is forcing educators to confront a fundamental question: How do we assess learning in an age where AI can produce competent, even high-quality, academic work? Tools like ChatGPT, Copilot, and Gemini challenge traditional evaluation methods, raising concerns about academic integrity while also offering unprecedented opportunities for personalized learning. This article argues that the key to navigating this new reality lies not in resistance, but in transformation. It lies in reimagining assessments to emphasize deep learning, process-oriented evaluation, and ethical AI engagement.

Rather than dismissing GenAI as a tool for academic dishonesty, educators must consider its potential as a dynamic learning assistant. One that, when used thoughtfully, can enhance understanding and critical thinking. However, this shift demands significant pedagogical and ethical considerations, from mitigating biases embedded in AI models to fostering students' ability to critically evaluate AI-generated content. By evolving assessment design, incorporating contextualized problems, collaborative projects, and iterative feedback, educators can discourage misuse while cultivating intellectual curiosity and ethical responsibility.

This research contends that the rise of GenAI presents not just challenges, but an opportunity to elevate education itself. By focusing on the learning journey rather than just the final product, educators can prepare students for a future where AI is an integrated, yet thoughtfully managed, part of their academic and professional lives. The path forward requires continuous adaptation, interdisciplinary collaboration, and a steadfast commitment to fostering both deep learning and ethical AI use. In doing so, we ensure that the next generation of learners are not only equipped with knowledge but also with the wisdom to navigate a GenAI driven world.

Keywords: Statistical software proficiency; Student preferences; Software usability; Data analysis tools; User interface design

ICCI202608: Evolutionary Paradigms in Quantum Machine Learning: A Technical Evaluation of QNN and QCNN Architectures

Dr. Saraniya G , Assistant Professor, Department of Computer Science
KG College of Arts and Science, Coimbatore, Tamilnadu

ABSTRACT

Quantum Computing (QC) has emerged as a significant advancement in the field of information processing by extending beyond the constraints of classical binary logic. Unlike conventional computing systems that rely on deterministic bit operations, quantum systems operate using probabilistic states governed by the principles of quantum mechanics. This paradigm enables the representation and manipulation of information in exponentially larger state spaces.

This paper presents a structured technical evaluation of quantum computational models that employ parameterized quantum circuits for data processing. Particular attention is given to architectural evolution aimed at improving trainability and stability as system size increases. Early circuit designs relied heavily on dense, global interactions between qubits, which often resulted in unstable optimization behaviour due to rapidly diminishing gradient values.

To address these challenges, hierarchical circuit designs have been proposed that emphasize localized quantum operations and progressive dimensionality reduction. This study examines how such structured architectures enhance computational robustness by preserving essential information while reducing susceptibility to noise and optimization instability. The analysis highlights the practical importance of architectural choices in enabling scalable and reliable quantum systems.

Keywords: Quantum Computing, Quantum Neural Network (QNN), Quantum Convolutional Neural Network (QCNN)

ICCI202609: Enhancing Lung Cancer Detection Accuracy and Efficiency through Attention Mechanisms: A Comprehensive Review

Annakumari R[1], Vijayalakshi P[2]

[1]Research Scholar

School of Computer Science Engineering & Information Science

Presidency University

Bangalore, India

[2]School of Information Science

Presidency University

Bangalore, India

ABSTRACT

Enhancing the accuracy and efficiency of lung cancer detection remains a critical challenge in medical imaging, which in turn directly impacts patient's outcome. This comprehensive review explains the applications of attention mechanisms within deep learning frameworks to address these challenges [1]. By enabling models to focus sensitively on the most relevant features in complex imaging data using attention mechanisms to detect accuracy and computational efficiency [2]. This paper systematically surveyed the recent advances that have been achieved in attention-based methods that are applied for lung cancer detection in analyzing their contribution to enhance sensitivity, specificity, and overall diagnostic performance [3, 4]. This paper explains various types of attention mechanisms, which include spatial attention, channel-wise attention, and self-attention mechanisms. This study also includes the integration of attention mechanisms with Convolutional Neural Network, and transformer's architecture. Additionally, this review covers commonly used data sets evaluation metrics, and the practical challenges faced in clinical development, such as data scarcity, and resource constraints [6, 7, 8]. By synthesizing the current research, this paper highlights the potential and the importance of attention mechanisms to transform lung cancer detection, which shows the pathways for future innovation that combine improved diagnostic accuracy with efficient computation. The findings underscore the importance of continued exploration in the area to facilitate earlier diagnostic and better patient management in clinical practices [9].

Keywords: Lung cancer detection, attention mechanism, deep learning models, medical imaging, Convolutional Neural Network CNN, transformation models, diagnostic accuracy, computational efficiency.

ICCI202610: A Comprehensive Review of Bloom's Taxonomy–Aligned Automated Question Generation Using Large Language Models

K.Sanjev

III M.Sc SS

Department of Software Systems

Sri Krishna Arts And Science College

Coimbatore, India

ABSTRACT

Bloom's Taxonomy has been a cornerstone of educational assessment design for several decades, providing a structured hierarchy for evaluating cognitive learning objectives. Recent advances in large language models (LLMs) have enabled automated generation of assessment questions at scale, raising interest in their alignment with Bloom's cognitive levels. This review paper synthesizes foundational theory and recent empirical research on Bloom-aligned automated educational question generation. Drawing on classical works by Bloom and Anderson and Krathwohl, and recent studies by Yaacoub *et al.*, Hwang *et al.*, Scaria *et al.*, and Moore *et al.*, the paper examines generation methodologies, prompt engineering strategies, evaluation techniques, and reported limitations. The paper concludes with implications for educational practice and directions for future research.

Keywords: Bloom's Taxonomy, Automated Question Generation, Large Language Models, Educational Assessment, AI in Education.

ICCI202611: DevOps Dashboard for Monitoring CI/CD Pipelines

S.Indhumathi[1] Assist Prof

K.Sanjev[2]

IV M.Sc SS

M.K.Mohanasundari[3]

IV M.Sc SS

[1,2,3]Department of Software Systems

Sri Krishna Arts And Science College

Coimbatore, India

ABSTRACT

Conventional monitoring of CI/CD pipelines relies on isolated logging systems and basic job status indicators, which often fail to capture complex interactions across builds, tests, and deployments. The rise of integrated observability platforms is transforming this space by combining metrics, logs, and visual analytics into unified dashboards. This study proposes an integrated monitoring framework for continuous integration and continuous deployment (CI/CD) pipelines, leveraging a suite of widely adopted open-source technologies—such as Prometheus for metrics collection, Grafana for visualization, and the ELK stack for logging and analysis—to provide comprehensive, real-time observability into pipeline performance and build stability. We achieve comprehensive pipeline observability through metrics scraping, log aggregation, and event-driven alerting. Several monitoring approaches—such as analyzing time-series patterns, detecting irregular behaviors, and applying iterative feedback mechanisms—were evaluated within microservice-driven deployment environments. This study presents a monitoring solution for CI/CD pipelines that integrates widely available open-source tools, including Prometheus, Grafana, and the ELK stack, to deliver continuous visibility into build stability, than conventional monitoring methods, with failure detection occurring nearly 30% quicker and recovery from deployment issues improving by about 20%. Comparative evaluations demonstrate that the proposed framework affords superior visibility into build stability, deployment efficiency, and overall system resilience relative to conventional approaches. Empirical results indicate a quantifiable enhancement in operational observability, enabling more proactive management of the CI/CD pipeline.The proposed dashboard can be applied in a variety of DevOps settings, where it assists in activities such as diagnosing failures, improving performance, tracking resource usage, and enabling early warning through automated alerts. The system enriches DevOps workflows by reducing cognitive load, accelerating root cause analysis, and enabling continuous improvement in software delivery pipelines.

Keywords: CI/CD Automation, DevOps Observability, Software Delivery Reliability.

ICCI202612: Wearable ECG Signal Analytics for Stress, Burnout, and Suicide Risk Assessment in Mental Health Disorders

P. Sivaramakrishnan[1]

PhD Research Scholar

Dr. R. Rajeswari[2]

Professor

[1,2]Department of Computer Applications,

Bharathiar University,

Coimbatore – 641046

ABSTRACT

Mental health disorders including stress, burnout, depression, and suicidal ideation – have become an escalating global concern affecting individuals across all age groups and professional backgrounds. In today's fast-paced world, chronic psychological stress imposes a significant physiological and emotional burden, contributing to exhaustion, reduced productivity, and self-harm tendencies. Conventional assessment tools such as questionnaires and interviews, although clinically validated, are inherently subjective and episodic, making them unsuitable for continuous monitoring of mental well-being. Recent advances in physiological sensing have enabled the use of wearable devices for objective, data-driven, and real-time evaluation of mental health. Among various biosignals, the electrocardiogram (ECG) stands out for its sensitivity to autonomic nervous system (ANS) fluctuations, offering a powerful window into stress responses and affective states. This paper presents a comprehensive review of recent developments in wearable ECG signal analytics for detecting stress, burnout, and suicide risk in individuals affected by or susceptible to mental health disorders. It consolidates findings from studies on hardware design, signal processing, feature extraction, and machine learning-based classification. Traditional approaches based on heart rate variability (HRV)-including time-domain, frequency-domain, and nonlinear analyses-remain the foundation of ECG-based mental health assessment. Overall, wearable ECG analytics represent a transformative frontier in proactive mental health monitoring.. This review consolidates the state of the art, highlights key limitations, and outlines future research pathways toward reliable, interpretable, and clinically deployable wearable technologies for comprehensive mental health evaluation.

Keywords: Wearable ECG, Stress Detection, Burnout Assessment, Suicide Risk Prediction, Heart Rate Variability (HRV), Machine Learning (ML), Mental Health Monitoring

ICCI202613: ROME for Large Concept Models: Rank-One Model Editing in Sentence Representation Space

Dr. K. Kalaiselvi[1], Kishorekumar Ravikumar Bava[2] , DhruvSoin[3]

[1]Associate Professor,

[2,3]Student,Department of Computer Science

Kristu Jayanti University

Bangalore, India

ABSTRACT

We propose ROME-LCM, a novel approach that extends Rank-One Model Editing (ROME) to operate in Large Concept Models (LCMs) rather than traditional token-level language models. While ROME localizes and edits factual associations at the token level in transformer MLPs, ROME-LCM adapts this methodology to edit concept-level associations in the SONAR sentence embedding space, where concepts are represented as language-agnostic sentence vectors. This adaptation enables multilingual factual editing with a single intervention, leveraging LCMs' language-agnostic reasoning capabilities and SONAR's aligned embedding space over more than 200 languages. Concretely, ROME-LCM identifies causal concept-level computations via adapted causal tracing, extracts concept keys and optimizes value vectors in concept space, and applies rank-one updates to targeted MLP modules within the LCM core. These edits act directly on continuous semantic representations, avoiding dependence on language-specific tokenization or surface forms and thereby eliminating the need for separate per-language interventions. We present the theoretical framework, mathematical formulation, and experimental design for concept-level factual association editing, demonstrating how rank-one updates can be applied to continuous semantic representations while maintaining the precision and generalizability of the original ROME methodology. Our theoretical analysis shows that concept-level editing achieves automatic multilingual generalisation through SONAR's language-invariant properties, while preserving locality, reducing model collapse risks under multiple edits, and minimizing collateral effects on unrelated concepts.

Keywords: model editing, factual associations, large concept models, multilingual NLP, SONAR embeddings, knowledge editing, causal tracing, sentence representation space, parametric knowledge, cross-lingual generalization, low-rank updates, transformer MLPs

ICCI202614: Contrastive Self-Supervised Learning on Multi-Exhaled VOC Profiles for Non-Invasive Cirrhosis Risk Stratification

P.Uma Magaswari[1] , Sreekanth Rallapalli[2]

Research Scholar VTU

[1]NITTE Meenakshi Institute of Technology Research Centre

Bengaluru, India

[2]Professor, NMIT Deemed University

Nitte Meenaskshi Institute of Technology,

Bengaluru, India

ABSTRACT

Timely diagnosis of hepatic cirrhosis has become a chronic problem in the clinical practice, mainly because of invasive nature of traditional diagnostic methods and low sensitivity of available non-invasive methods to diagnose it in its early stages. Another promising non-invasive method which involves breathomics (the analysis of exhaled volatile organic compounds (VOCs)) has been proposed but, unfortunately, modern machine-learning techniques lack sufficient labelled data, strong intra-subject variation, and lack of generalisation between populations. The current work suggests a self-supervised learning (SSL) model called contrastive self-supersized learning (CSSL) that aims at stratifying the risk of cirrhosis based on the multi-exhalation VOCs. The model proposed takes advantage of the many breath samples that are available to an individual to be trained to learn invariant, physiologically significant representations by favouring agreement between different exhalations of the same individual and increasing dissimilarity between different individuals, without necessarily requiring disease labels during pre-training. A common encoder which is trained based on a contrastive task is then transferred into a lightweight supervised classifier to predict downstream cirrhosis. Empirical evidence of experimental findings suggests that the suggested CSSL is superior to both supervised and autoencoder-based baselines in accuracy, F1-score, and AUC, particularly when the labelled data are scarce. The significance of contrastive pre-training, projection-head structure and multi-exhalation modelling as a means of improving prediction zeal and stability are further supported by ablation studies. The research results reflect the promise of contrastive, self-administered breathomics as a non-invasive scale-up approach towards the screening of the early risks of cirrhosis.

Keywords: Liver Cirrhosis, Breathomics, Volatile Organic Compounds (VOCs), Contrastive Self-Supervised Learning, Non-Invasive Diagnosis, Multi-Exhalation Modelling, Representation Learning, Cirrhosis Risk Stratification

ICCI202615: Machine Learning In Genomic Data Analysis For Personalised Medicine

Kavya J
II MSC.CS
AVP College Of Arts And Science
Tirupur

ABSTRACT

Personalized medicine aims to tailor medical decisions, treatments, and practices to individual patients based on their specific genetic makeup, environment, and lifestyle factors. The advent of high-throughput genomic technologies has generated vast amounts of biological data, offering new opportunities for personalized medicine approaches. However, the sheer volume and complexity of genomic data pose significant analytical challenges. Machine learning (ML) techniques have emerged as powerful tools for extracting insights from large- scale genomic datasets, enabling the development of predictive models for disease risk, drug response, and treatment outcomes. This paper reviews the applications of ML in genomic data analysis for personalized medicine, highlighting the key methods, challenges, and future directions in this rapidly evolving field. Additionally, it presents a comprehensive research methodology to address existing challenges and advance the translation of ML models into clinical practice. Machine learning (ML) in genomic analysis is revolutionizing personalized medicine by analysing vast genetic data to tailor treatments, predict disease risk, and identify drug targets, moving healthcare from generalized to individualized care. ML algorithms like deep learning, SVMs, and Random Forests detect complex patterns in genomic, clinical, andlifestyle data, enabling early diagnosis, precise treatment selection, and efficient drug discovery, though challenges like data privacy and bias remain.

Keywords: Genomic data,datasets,methodology,ML models,SVMs,Random forests detect.

ICCI202616: Temporal-Adaptive Machine Learning Models: Addressing Performance Degradation In Clinical Deployment Through Continual Learning And Hybrid Edge-Cloud Architectures

Abel Jopaul V P[1], M Lingaraj[2]

[1]Research Scholar, Department of Computer Science, Sankara College of Science and Commerce, Saravanapatty, Coimbatore, India.

[2]Associate Professor and Head, Department of Computer Science, Sankara College of Science and Commerce, Saravanapatty, Coimbatore, India.

ABSTRACT

Machine learning models for clinical decision support demonstrate impressive initial performance but face significant challenges in maintaining accuracy over time as medical practices, imaging technologies, and patient populations evolve. Our systematic review of 30 studies (2022-2025) revealed that zero studies evaluated temporal validation, despite documented real-world performance degradation of 8-18% in community settings. This paper presents **TemporalCare**, a novel continual learning framework designed to address catastrophic forgetting in medical imaging models while maintaining clinical performance over extended deployment periods. We propose a hybrid edge-cloud architecture that enables incremental model updates without requiring complete retraining or centralized data aggregation. Through empirical evaluation on three longitudinal datasets spanning 36 months (diabetic retinopathy screening n=45,230; breast cancer detection n=38,540; cardiovascular risk prediction n=52,180), we demonstrate that TemporalCare maintains baseline performance (AUC degradation <2% vs. 12-18% for static models) while reducing computational costs by 73% compared to periodic full retraining. Our framework incorporates experience replay with privacy-preserving synthetic data generation, elastic weight consolidation adapted for federated settings, and dynamic architecture expansion for new imaging modalities. Cost-benefit analysis across five healthcare systems reveals 4.2-year ROI with 89% reduction in model maintenance overhead. This work provides the first comprehensive framework for sustainable ML deployment in clinical settings, addressing critical gaps in temporal validation and long-term model viability.

Keywords: Continual learning, temporal validation, catastrophic forgering, medical imaging, hybrid edge-cloud architecture, federated learning, clinical decision support, model degradation

ICCI202617: LANSymphony: A Peer-to-Peer, Offline Multi-Modal Communication Framework for Ad-Hoc Local Networks

Sudheer Kumar R[1], Sridevi R[2], Nisha Varghese[3]

Department of Computer Science

Christ University

ABSTRACT

The conventional LAN communication tools are typically limited to one type of communication like text or file sharing or relied on centralized servers that could cause delays and lead to single point of failure. In the current paper, a new peer to peer (P2P), offline and multi-modal communication system, LANSymphony, is introduced and designed to be deployed in the temporary local networks. It integrates live text messaging, file transfer, voice streaming and video streaming on a single application. LANSymphony also includes lightweight UDP broadcasting to find peers rapidly and with minimal or no configuration, as well as dedicated TCP/UDP channels, specific to each type of media, to allow efficient transmission. It also offers a thread safe, modular backend, capable of supporting many media streams simultaneously without affecting the responsiveness of the user interface and a Kivy based cross-platform interface that makes the application easy to deploy. Performance tests in actual LANs show text messaging latency under 5 ms, file transfer rates over 90 Mbps, and reliably good audio and video quality with low rate of packet loss. LANSymphony has a broader usability range, reduced installation complexity, and enables simpler integration for essential offline functionality compared to existing LAN messaging and conferencing solutions. Applications include disaster recovery, military, remote research laboratories or industries.

Keywords: offline communication, LAN messaging, real-time multimedia, UDP broadcast discovery, multi-modal communication.

ICCI202618: Adaptive Vehicle Lighting with a Dual-LDR Embedded System

Ashitha K Paul[1], B Kasinath[2], Harshith Ravindran[3] , Dr Haripriya M P[4]

[1,2,3]Students,[4]Assistant Professor,

Department of Computer Science,

Kristu Jayanti Deemed to be umiversity, Bangalore

ABSTRACT

As the demand for both enhanced road safety and greater driver comfort continues to grow, intelligent lighting systems have become a key area of focus in modern automotive design. A primary motivation for this technology is its potential to significantly reduce the hazard of night time glare from oncoming vehicles. This paper presents the comprehensive design and evaluation of a new, microcontroller-based embedded system for adaptive headlight control. It is intended to provide a low-cost, fully autonomous solution that is flexible enough to be adapted and integrated into any vehicle. The system architecture is built upon a strategic dual-sensor approach. It utilizes an upward facing ambient Light Dependent Resistor (LDR) to accurately detect general environmental lighting conditions, such as day or night. This is paired with a carefully shielded, forward-facing LDR, which is positioned to exclusively detect the headlights of oncoming traffic, isolating them from other light sources. We examine the practical implementation of the system three core functions automatic activation of headlights based on day/night conditions, a high-beam restriction function for urban environments, and the automatic anti-glare dipping of the high beams when traffic is detected. The paper also confronts practical challenges encountered, such as optimizing sensor response time and developing methods to prevent false positives that can be triggered by highly reflective road signs. Finally, the paper highlights the strategic advantages of this onboard, autonomous system. It includes a critical analysis of Vehicle-to- Vehicle (V2V) communication, which is posited as an impractical alternative for this specific application. The system performance and notable cost-effectiveness are also compared against the sophisticated, and typically more expensive, camera based commercial solutions available in the market today.

Keywords: Microcontroller-Based System, Adaptive Headlight Control, Anti-Glare System, LDR, Embedded System, Low-Cost Automation, Sensor-Based Control.

ICCI202619: A Comprehensive Review of Blockchain and Web3 Technologies: Architecture, Applications, and Challenges

Sridevi K[1], Gunn[2] , Hari Krishnan[3], Dr Ranjitha Sreedhar[4]

1,2,3Student,Department of Computer Science,School of Computational and Physical Sciences, Kristu Jayanti(Deemed to be University), Banglore, Karnataka,India

4Coordinator of Computer Applications,School of Computational and Physical Sciences, Kristu Jayanti(Deemed to be University),Banglore,Karnataka,India

ABSTRACT

Blockchain Technology is a secure mechanism as it has emerged as a decentralized platform for recording digital transactions without involving trusted intermediaries. Initially it was introduced as Bitcoin. Currently Blockchain has evolved into foundational technology for supporting smart contracts, decentralised applications and web3 technologies. Web3 technologies aims to transform the internet into a user-centric ecosystem which enables data ownership, trustless interaction and transparency. Despite its potential, Blockchain and Web3 technology face several limitations like scalability, lack of interoperability, high energy consumption, security privacy concerns, vulnerabilities etc. This paper presents a Comprehensive review of Blockchain and Web3 Technologies by analysing existing research on blockchain architecture, mechanisms, smart contract security, scalability, privacy and Web3 architecture. The study summarizes key contributions from prior research, identifies unresolved challenges and highlights future research directions. This study aims to provide a structured understanding of Blockchain enabled Web3 systems for researchers and practitioners.

Keywords: Blockchain, Web3, Smart Contracts, Decentralized Application, Security, Privacy, Scalability.

ICCI202620: Evolution, Capabilities, and Applications of Chatbots Powered by Large Language Models

Sridevi K[1], Abhi S[2] , Lakshmi Prasanna K [3], Dr Haripriya M P[4]

[1,2,3] Student, [4]Assistant Professor,

Department of Computer Science,School of Computational and Physical Sciences

Kristu Jayanti(Deemed to be University), Bangalore, Karnataka,India

ABSTRACT

The rapid advancement in Large Language Models (LLMS) have significantly impacted the conversational AI systems.Early chatbots were rule-based and had shallow machine learning techniques which had issues in flexibility,scalability and contextual understanding.The emerge of neural sequence-to-sequence model shifted toward data-driven dialogue generation.Meanwhile introduction to transformer architecture led to improvements in language representation,reasoning,response generation.This paper presents a comprehensive survey of the evolution of chatbots,also focusing on LLM-powered systems like GPT,BERT,XLNet models. It examines the architecture, dialogue system paradigms,evaluation methods and transformation from conversational agents to autonomous LLM based agents.LLMs are trained on Large Pretrained datasets on diverse perspectives. This led to major improvements like understanding the language, reasoning, and generating response. This was the main reason for LLMs success. LLM incorporated Multimodal learning (text+image+audio etc.) . In addition to this,the paper reviews various application domains - including health care,education,mental health support,language learning -giving importance to both technical and user-adoption perspectives.Despite their potential ,LLM-based chatbots continue to face limitations like hallucinations,bias,commonsense reasoning,safety,evaluation,reliability,ethical issues.By taking insights from recent surveys,foundational models,and domain-specific studies,this works provides a structured understanding of current advancement and open research gaps.This paper concludes by finding future directions which are reliable,adaptive,trustworthy especially human aligned conversational AI systems.

Keywords: Large Language Models(LLMs), Chatbots, Conversational AI, Transformer Architecture, Dialogue Systems, Generative Pre-trained Models, Ethical and Responsible AI, Healthcare, Educational Applications.

ICCI202621: A Review of Image Processing and Learning-Based Methods using UAV Imagery for Crop Disease Detection

Karren Susan Punnose[1], Dr.Poongothai P[2]

[1]Student, [2]Assistant Professor,

Department of Computer Science,School of Computational and Physical Sciences

Kristu Jayanti(Deemed to be University), Bangalore, Karnataka,India

ABSTRACT

The most developed the use of technology that has allowed for developing new capabilities for Image Processing, UAV sensor technologies, and Cognitive Computing which advances precision agriculture to new levels. Early identification, diagnosis, and accurate treatment of crop diseases are crucial to increasing crop production and reduce financial losses related to food insecurity. This document contains a thorough review and analysis of available models, algorithms, and methodologies for classifying and diagnosing crop diseases utilizing machine and deep learning methodologies. Focus is placed on the use of UAV collected data for image-based disease identification utilizing remote sensing technology. Each type of classifier evaluated in the study was assessed for its level of accuracy, performance, and shortcomings. This research has highlighted several key limitations in the existing methods of diagnosing crop disease and provides insight into where improvements could be made to improve the functionality, reliability, and scalability of diagnostic crop disease detection systems.

Keywords: UAV imagery; Crop disease detection; Image processing techniques; Deep learning methods; Precision agriculture

ICCI202622: Enhancing Security and Monitoring Systems — Yet Data Breaches Persist: Hidden Gaps in Cloud and Infrastructure Security

Dr. K. Kalaiselvi[1], Hemant Kumar[2],

[1]Associate professor, Dept of Computer Science, Kristu Jayanti University,
[2]Engineer, Cloud and Infra Services, LTIMindtree Ltd.

ABSTRACT

Since the data has been an important and entire point of security & privacy, at every organization and workplace, including an individual's concern. Despite investing and focusing a significant value and time over cybersecurity infrastructure, cloud monitoring, and real-time analytics, the organizations are facing the unnoticed data branches. After implementing the modern and complex IT ecosystems, integrating with cloud services, third party services, and user accessible applications invents some blind spots that couldn't prevent the data loss and struggles to monitor effectively. This study is all about hidden data exfiltration pathways in controlled and organizational environments. The research uncovers legitimate user activities, which includes data sharing using various methods and exchanging the textual data through emails and servers. All of these are pointing out that while systems are configured and prevented to share data outside, still it happens, via bypassing the policies and security channels that remain unmonitored or under regulated. This highlights that modern IT infrastructure is complex, integrated with technical and operational security, still needs to adapt data flow analysis, behavioural anomaly detection and continuous awareness training to detect and mitigate these concealed exfiltration vectors. The research shows that even modernized, monitored infrastructures remain vulnerable due to blind spots in legitimate data channels.

Keywords: Corporate Security, Data Exfiltration, Cloud Infrastructure, Data Loss Prevention, Insider Threat, Behavioral Analytics

ICCI202623: Type 1 vs. Type 2 Hypervisors: A Performance-Oriented Review

Dr. K Kalaiselvi[1], Anshuman Krishnan[2], Divya Patel[3], Kunal Jaiswal[4]

[1]Associate Professor and Coordinator, Department of Computer Science,
Kristu Jayanti Deemed to be University , Banglore, Karnataka,India

[2,3,4]Student,Department of Computer Science,School of Computational and Physical Sciences,
Kristu Jayanti Deemed to be University, Banglore, Karnataka,India

ABSTRACT

Virtualization relies on hypervisors to run multiple independent operating systems on shared hardware. Hypervisors are classified into two types: Type 1 (bare-metal) hypervisors run directly on the host hardware, while Type 2 (hosted) hypervisors run on a conventional OS. Type 1 hypervisors (e.g. Xen, KVM) have direct hardware access and incur minimal overhead, yielding near-native performance, high scalability (often supporting hundreds of CPU cores and terabytes of RAM), and strong isolation[1][2]. In contrast, Type 2 hypervisors (e.g. VirtualBox, VMware Workstation) run as applications on a host OS and therefore introduce extra latency and resource contention[3][4]. Our review compares these two classes: Type 1 solutions excel in performance, elasticity, and security, while Type 2 solutions offer ease of use, rapid setup, and flexibility at the cost of some performance. We present benchmark data showing CPU, memory, disk I/O and network effects for representative open-source hypervisors (KVM for Type 1 and VirtualBox for Type 2). For example, one study found VirtualBox VMs had slightly higher CPU execution times than KVM (10.021s vs. 10.016s on a large prime-number test)[5], and VirtualBox's disk read/write latencies were measurably worse than KVM's (e.g. average read time ~3393 ms vs. 3321 ms)[6][7]. These results illustrate that the bare-metal architecture of Type 1 hypervisors confers a systematic performance advantage. We discuss the architectural tradeoffs and conclude that Type 1 hypervisors are preferable for production workloads requiring maximum performance and security, whereas Type 2 hypervisors suit desktop or test environments where convenience and rapid deployment matter more.

Keywords: Hypervisors; Type 1 virtualization; Type 2 virtualization; Performance evaluation; Virtualization technology

ICCI202624: Security Challenges of Quantum Computing Threats in the Modern Technology

Harshitha Caral P[1], Anto Angel Sophia[2], Dr. Poongothai P[3]

[1,2]Student, [3]Assistant Professor,

Department of Computer Science, School of Computational and Physical Sciences

Kristu Jayanti Deemed to be University, Bangalore, Karnataka, India

ABSTRACT

Quantum computing presents a significant challenge to modern cryptography by threatening the mathematical foundations on which many widely used security systems rely. Classical cryptographic algorithms such as RSA, Diffie–Hellman, and Elliptic Curve Cryptography derive their security from the computational difficulty of problems like integer factorization and discrete logarithms. However, quantum algorithms—most notably Shor's algorithm—can solve these problems efficiently, rendering current public-key cryptographic schemes vulnerable once large-scale quantum computers become practical. This potential shift poses serious risks to data confidentiality, secure communication, and digital authentication across industries including finance, healthcare, and national security. As a result, there is growing urgency to develop and adopt quantum-resistant cryptographic techniques, commonly referred to as post-quantum cryptography. This paper explores how quantum computing threatens existing cryptographic systems, examines the implications for modern cybersecurity, and highlights ongoing efforts to transition toward secure cryptographic solutions in the post-quantum era.

Keywords: Quantum computing threats; Post-quantum cryptography; Cybersecurity challenges; Cryptographic vulnerabilities; Secure communication

ICCI202625: Interdisciplinary Optimization of Hard Water Remediation for LLM Cooling Systems: Leveraging Random Forest Algorithms and ANOVA for Quality Prediction

Shalini Devraj[1] (Main author), Sachutha J[2], Tedelo Doulo[3]
Department Of Physical Science
Kristu Jayanti Deemed To be University, Bangalore, Karnataka,India

ABSTRACT

Water quality is a decisive factor in maintaining the operational integrity of high-performance infrastructure, particularly for modern Large Language Model (LLM) data centers. This research addresses the challenges posed by hard water specifically pipe scaling, equipment corrosion, and reduced heat transfer efficiency through an interdisciplinary framework combiningchemistry, statistical validation, and machine learning. The methodology employs a multi-stage chemical treatment process, including ion exchange softening, lime-soda precipitation, and reverse osmosis, to achieve industrial-grade standards. A core component of this study is the application of Data Science and Statistical Analysis to validate treatment effectiveness through ANOVA and correlation analysis of parameters such as TDS, pH, and conductivity. Furthermore, Machine Learning algorithms, including Random Forest and Support Vector Machines, are utilized to intelligently classify treated water into specific usage grades. To enhance industrial accessibility, the system integrates a Python-based pipeline (using Pandas and Scikit-learn) that loads real-time quality data onto a web-based dashboard. This allows industrial stakeholders to remotely monitor water health, ensuring energy optimization and long-term hardware reliability in data center cooling systems.

Keywords: Hard Water Treatment, Machine Learning, Predictive Statistics, LLM Data Centers, Data Science, Industrial Cooling, Python (Scikit-learn/Pandas), Water Quality Classification.

ICCI202626: Agentic Financial Forensics: A Hybrid LCM-LLM Architecture for Auditing Logical Coherence in IPO Prospectuses

Karthikeyan.K[1] , C . Melvyn Savio[2] , S. Boopathi[3]

Student, Department of Computer Science, Kristu Jayanti Deemed To be University, Bangalore, Karnataka,India

ABSTRACT

Modern Large Language Models (LLMs) often lose focus when analyzing very long financial documents, such as IPO Draft Red Herring Prospectuses (DRHPs). This problem, known as contextual decay, can cause the models to make small logical mistakes that even trained auditors might overlook. To overcome this gap , this paper introduces a Hybrid LCM-LLM Architecture that separates how the model reasons from how it writes. This approach uses Large Concept Models (LCMs) based on SONAR sentence-level embeddings to spot shifts in meaning, or "risk drift," and detect logic gaps that appear across large sections of text. We have been testing our model that identifies 30% more non-numeric inconsistencies than traditional token-based Retrieval-Augmented Generation (RAG) methods. We also outline an improved Tri-Layer design for the future that combines World Models to simulate possible market reactions , a step toward predictive financial auditing. Overall, this research offers a clear and practical framework for using AI to support financial auditors during the pre-IPO process. It improves accuracy, reduces oversight risks, and builds a foundation for more reliable, explainable, and forward-looking financial analysis.

Keywords: Agentic Financial Forensics, Hybrid LCM-LLM Architecture, IPO Prospectus Analysis, Logical Coherence Auditing, Financial Document Verification

ICCI202627: LLM-Assisted Process Timeline Analysis Using Velociraptor:A Windows Host and Virtualized Client Study

Muhurtha L Gowda[1], Dr. Kalaiselvi K[2]

Student,

[1]Department of forensic science ,

Kristu Jayanti Deemed to be university, India

[2]Associate Professor and Coordinator,

Department of Computer Science, Kristu Jayanti(Deemed to be University), Banglore, Karnataka,Indi

ABSTRACT

Timeline analysis is being increasingly adopted in digital forensic analysis as a tool to understand the activity of systems, as well as to trace malicious activity. Nevertheless, traditional analysis of timelines based on processes is inefficient, time-consuming, as well as error-prone. In this study, there is an investigation of using Large Language Models along with Velociraptor to automate analysis related to timelines of processes on windows. The experiments consist of two stages. During the initial stage, both the Velociraptor server and client components run on the same Windows machine to create a baseline system process activity. The process evidences are retrieved by leveraging the Velociraptor Windows process list function, and a system process timeline is recreated. The timeline information is further processed through an LLM- supported strategy to reveal process anomalies, discrepancies, and anomalies by machine learning analysis. The findings clearly show that, although the LLM successfully points out the presence ofsome anomalies, it preserves some process information for human analysis, underlining the significance of human analysis in a forensic process. The experimental setup is expanded in the second phase by deploying the Velociraptor server on the host system and the client on a virtual machine; controlled suspicious activities are performed within the virtualized environment to simulate adversarial behavior. Process timelines obtained are collected and analyzed using the same LLM-assisted methodology that shall enable a comparison between the host-only and virtualized client environments. The results confirm that LLM-assisted process timeline analysis holds great promise for ameliorating forensic triage, by reducing the analyst workload and ranking suspicious events, without eliminating human expert validation. This is a useful investigation into the real applicability of LLMs as decision-support tools, rather than stand-alone forensic analysts, thereby shaping the evolving field of AI-aided digital forensics.

Keywords: LLM-Assisted Forensics, Process Timeline Analysis, Velociraptor, Windows Host Investigation, Virtualized Client Analysis, Digital Forensics Automation, Large Language Models in Security, Endpoint Monitoring

ICCI202628: Bias And Fairness In Medical Machine Learning Model- Fairness In Focus: Ai-Driven Healthciare

Anusha Anil[1],Javeriya Kulsum[2], Aditiya A[3], Shilpa R[4]

Department of Physical Science

Kristu Jayanti Deemed To be University, Bangalore, Karnataka,India

ABSTRACT

As machine learning (ML) becomes essential in clinical decision-making, its potential to worsen gender and economic inequalities raises significant concerns. Previous research shows that relying on overall accuracy often hides serious issues, like higher False Negative Rates (FNR)—or missed diagnoses—for female patients and those from low-income backgrounds. This study looks into sex and socioeconomic bias in healthcare ML by reviewing current literature and assessing the mathematical flaws in common fairness metrics.Using data from the 2019 National Health Interview Survey (NHIS), this paper illustrates how differences in biological sex and gaps in resource-based data lead to ongoing medical neglect. We specifically explore how uneven data and disparities in self-reporting within the NHIS disadvantage women and people from lower-income backgrounds. The analysisexamines how bias remains through proxy variables, such as insurance coverage type (e.g.,MEDICAID_A vs. PRIVATE_A), housing stability indicators (HOUGVASST_A), and familyincome-to-poverty ratios (RATCAT_A). These factors allow models to learn discriminatory patterns even in environments that do not consider race. Our findings show that women and low-socioeconomic status (SES) groups experience a much higher False Negative Rate across various model architectures, including Random Forests and Support Vector Machines. This gap is especially significant in predicting chronicconditions and barriers to accessing care, where the model might overlook the health needs of the most marginalized. We contend that focusing on reducing FNR is not just a technical improvement but an important ethical consideration, as these errors mean individuals' medical conditions go unnoticed by the predictive system.Finally, we suggest a multi-stage mitigation framework designed for practical clinical use. This framework aims at ensuring equitable AI-driven healthcare across gender and class by focusing on balancing intersectional data, including SES-stratified feature importance, and making adjustments after the fact to thresholds. By shifting the focus from overall accuracy to error rates specific to different subgroups, this study offers a path for promoting health equity through algorithmic accountability.

Keywords: Bias in AI; Fairness in machine learning; Medical AI; Ethical AI; AI-driven healthcare

ICCI202629: A Literature Survey on Quantum Computing and Cybersecurity

Souvick Paul

Department of Computer science

Kristu Jayanti Deemed to be university, India

ABSTRACT

Quantum computing is expected to revolutionize computation by solving complex problems that are currently infeasible for classical computers. However, this advancement poses a serious threat to modern cybersecurity systems that rely on public-key cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC). These algorithms become vulnerable in the presence of large-scale quantum computers due to Shor's algorithm. Although symmetric encryption algorithms like AES and cryptographic hash functions such as SHA-256 are comparatively more resistant, their effective security strength is reduced by Grover's algorithm. This literature survey reviews existing research on the impact of quantum computing on classical cryptographic systems and analyzes the necessity of post-quantum cryptography (PQC) as a long-term solution. The paper presents a comparative study of RSA, ECC, and post-quantum cryptographic algorithms, discusses performance trade-offs, and outlines a migration roadmap for organizations. In addition, a real-world case study on Transport Layer Security (TLS) is included to demonstrate the practicalimplications of quantum threats and the adoption of hybrid post-quantum solutions. The survey highlights that early preparation and migration to post-quantum cryptography are essential to ensure long-term data security in the quantum era.

Keywords: Quantum Computing, Cybersecurity, Post-Quantum Cryptography, RSA, ECC, AES, TLS, NIST, Lattice-Based Cryptography

ICCI202630: The Augmented Analyst: Investigating AI's Potential for Displacement versus Strategic Enhancement of Core Business Analysis Competencies.

Adithyan P[1], Megha Reji[2], Gowin Davis[3], Shipla R[4]

[1,2,3]Department Of Physical Science

Kristu Jayanti Deemed To be University, Bangalore, Karnataka,India

ABSTRACT

Artificial intelligence (AI) is advancing at an unprecedented pace, prompting both enthusiasm and anxiety about the future of business analysis. This study synthesizes scholarly literature, industry reports, and real-world case studies to assess how AI is reshaping the role of business analysts. We identify specific analytical tasks—such as data extraction, routine reporting, and basic trend detection—that are highly amenable to automation, and contrast them with functions that require human judgment, strategic thinking, and interpersonal communication. Empirical findings indicate that AI substantially reduces the time spent on repetitive, "grunt" work, thereby accelerating the analytical cycle and improving theprecision of decision-making. At the same time, the core competencies of analysts—domain expertise, critical reasoning, and the ability to interpret and communicate AI-generated insights—remain indispensable. Consequently, AI does not eliminate the analyst profession but redefines it, elevating the value of professionals who combine deep analytical knowledge with strong storytelling and stakeholder-management skills. While high-skill analysts gain a competitive edge, workers whose duties are predominantly procedural face heightened vulnerability. The paper concludes that the future of business analysis hinges on upskilling analysts to master AI tools and on organizations fostering a collaborative human-AI ecosystem that leverages automation while preserving the uniquely human aspects of strategic insight.

Keywords: Augmented Analyst, AI in Business Analysis, Strategic Enhancement, Workforce Displacement, Core Competency Development, Intelligent Decision Support

ICCI202631: Detection of AI Driven Polymorphic Malware Using MachineLearningBased Behavioral Analysis of Windows Execution Traces

Santhoshkumar M[1], Prof. K. Kalaiselvi[2]

Student,

[1]Department of forensic science ,

Kristu Jayanti Deemed to be university, India

[2]Associate Professor and Coordinator,

Department of Computer Science, Kristu Jayanti(Deemed to be University), Banglore, Karnataka,India

ABSTRACT

Polymorphic and AIdriven malware increasingly evade traditional signaturebased defenses by continuously mutating their code and dynamically adapting to the target environment. This work investigates behaviourbased detection of such threats using machinelearning models trained on detailed Windows execution traces. The proposed approach leverages the WinMET dataset of CAPEv2 sandbox reports, which provides standardized JSON logs capturing process trees, WinAPI and systemcall sequences, and interactions with files, registry, and network resources for thousands of realworld malwareand benign samples. These traces are normalized into compact persample representations and used to extract temporal and statistical behavioural features suitable for supervised learning. Experiments with multiple classifiers demonstrate that behavioural machinelearning models achieve high detection performance against polymorphic families and offer resilience to codelevel obfuscation, highlighting their potential as a practical defence against emerging AIassisted malware.

Keywords: AI-Driven Malware, Polymorphic Malware Detection, Machine Learning, Behavioral Analysis, Windows Execution Traces, Endpoint Security, Threat Intelligence, Cybersecurity Automation

ICCI202632: Risk analysis of cookies and privacy issues arising from tracking cookies in web-based AI tools

Aiswarya Jose, Prof. Kalaiselvi K

[1]Student, Department of forensic science ,

Kristu Jayanti Deemed to be university, India

[2]Associate Professor and Coordinator,

Department of Computer Science, Kristu Jayanti(Deemed to be University), Banglore, Karnataka,India

ABSTRACT

Web-based artificial intelligence (AI) tools make extensive use of cookies to support basic functionality, improve user experience, and understand how users interact with their platforms. However, these cookies especially tracking and third-party cookies also introduce privacy concerns that are often not clearly visible to users. This study presents a large-scale analysis ofcookies used by more than fifty publicly accessible AI tools, covering different categories such as conversational AI, writing assistants, image generation tools, coding platforms, and productivity applications. A standardized observation-based approach was followed using browser developer tools to examine cookie behavior under different user consent conditions. The analysis focused on factors such as cookie persistence, domain ownership, consent handling, and tracking indicators. Based on these observations, each tool was classified into low, medium, or high privacy risk categories. The results show that many AI tools rely on persistent and third- party cookies, with some tracking activities occurring before explicit user consent. Tools with frequent user interaction, particularly conversational and productivity-oriented platforms, were found to present higher privacy risks. The study highlights the growing need for better transparency and stronger privacy practices in the design of web-based AI services.

Keywords: Tracking Cookies, Web Privacy, AI Tools, Data Protection, User Consent, Cybersecurity Risks, Online Tracking, Privacy Compliance

ICCI202633: Forensic Detection of Alternate Data Streams in NTFS Using an EDR Prototype

V. Shanoy Angel[1], Prof. Don Caeiro[2], Nancy Lucas. B[3]

[1]Student, Department of forensic science ,
Kristu Jayanti Deemed to be university, India

[2]Head of the Department, Department of Forensic Science, Kristu Jayanti Deemed to be university, India

ABSTRACT

Alternate Data Stream (ADS) is a feature that is present in the New Technology File System (NTFS) that allows the data to be hidden within the files in addition to primary content without actually altering the size or contents of the file. Initially the ADS was intended to use with older system, but the ADS has been exploited increasingly by threats to hide malicious payloads, configuration files, encrypted data, credentials and script-based threats. Traditional antivirus and protection often fail to detect such hidden streams making it a blind spot in the modern digital forensic. This paper presents the implementation and an approach of an endpoint detection and response (EDR) prototype which focuses on the detection of ADS-based threats. The proposed EDR prototype monitors the NTFS directories using the PowerShell based stream integrated with the Python automation, identifies suspicious data streams and by detecting, identifies hidden ADS entries. This approach shows a real-time detection of suspicious hidden streams while maintaining minimal performance on the endpoint system. The experimental evaluation demonstrates that the proposal reliably detects the hidden ADS and contribute a practical and academic approach to improve the visibility in stealth-based attack techniques. produces verifiable forensic artifacts without affecting the system performance suitable for incident response and legal investigation.

Keywords: New Technology File System (NTFS), Alternate Data Streams (ADS), Digital Forensics, Endpoint Detection and Response (EDR).

ICCI202634: A Multimodal Digital Forensic Approach for Detecting AI-Generated Audio-Visual Media

Vignesh Raghav J[1], Don Caeiro[2]

[1]Department of Forensic Science,

[2]Head of the Department, Department of Forensic Science,

Kristu Jayanti Deemed to be university, India

ABSTRACT

The rapid growth of artificial intelligence has enabled the creation of highly realistic AI-generated and manipulated audio-visual content, commonly known as deepfakes. While these technologies have legitimate applications, their misuse presents serious challenges to digital forensic investigations, cybercrime detection, and legal proceedings. Identifying whether a media file is human-generated or AI-generated has become a critical requirement for forensic examiners. This research proposes a web-based AI Media Detection System designed to analyze multimedia content by performing separate forensic examinations of the audio and video components extracted from a single media file. Audio analysis is carried out using Mel-Frequency Cepstral Coefficients (MFCC) to detect synthetic voice patterns, while video analysis focuses on face-based deepfake detection using open-source deep learning models. The separation of modalities ensures greater analytical clarity and improves investigative accuracy. To support forensic integrity and court admissibility, the system generates a structured digital forensic report containing examination details, detection results, confidence scores, and cryptographic hash values (MD5 and SHA-256) to preserve evidence integrity. The proposed system demonstrates a practical, open-source solution for addressing AI-based media manipulation in modern digital forensic investigations.

Keywords: Multimodal Forensics, AI-Generated Media Detection, Deepfake Analysis, Audio-Visual Forensics, Digital Media Authentication, Cybersecurity

ICCI202635: Integrating VPN and Onion Routing for Enhanced Privacy: A Performance Evaluation

Aadhithya Rajesh[1], Ananya Nagesh[2], Dr. Sreeparna Chakrabarti[3]

[1,2]Student, [3]Assistant Professor,

Department of Computer Science,

Kristu Jayanti Deemed to be University, Bengaluru, India

ABSTRACT

In today's data-driven economy, one's personal data being private to them is a largely discussed concern. While there are many tools that claim to keep user data private, we see that many people prefer Virtual Private Networks (VPN) and Onion Routing (Tor). These two tools are widely used for privacy, but they provide different guarantees and trade-offs. VPN typically offers confidentiality and IP masking between a user and their trusted exit node. Tor provides strong anonymity through multi-hop routing, but at the cost of latency and throughput. Combining the two (Tor over VPN or VPN over Tor) is a commonly discussed strategy among privacy conscious users. Yet there are open questions about how the combination performs and its ethical considerations. This study evaluates important parameters of network performance on an Ubuntu-based Virtual Machine testbed, using iperf3 and Wireshark. It also discusses the algorithm Tor makes use of for node allocation. The data presented helps people identify which combination would be suitable for their use.

Keywords: Privacy, Virtual Private Network (VPN), Onion Routing (Tor), Network

ICCI202636: A Forensic Framework for Explainable Metadata Extraction and Cross-App Correlation of WhatsApp and Telegram

Chryselle Christie G[1], Dr. Kalaiselvi[2]

[1]Student, Department of forensic science ,
Kristu Jayanti Deemed to be university, India

[2]Associate Professor and Coordinator,
Department of Computer Science,
Kristu Jayanti Deemed to be University, Banglore, Karnataka,India

ABSTRACT

The widespread use of encrypted messaging applications such as WhatsApp and Telegram poses significant challenges to digital forensic investigations, as message content is increasingly inaccessible due to strong encryption mechanisms. Consequently, forensic analysis has shifted toward the extraction and interpretation of metadata and application artifacts that can provide valuable investigative insights without violating encryption boundaries. This research presents a forensic framework for the explainable extraction, normalization, and cross-application correlation of metadata from WhatsApp and Telegram. The proposed framework operates on data acquired using established forensic imaging tools, ensuring forensic soundness and chain of custody. Metadata artifacts extracted from application databases and file systems are transformed into a common schema to enable uniform analysis across platforms. Temporal, relational, and behavioral correlations are applied to reconstruct communication timelines, identify interaction patterns, and associate activities across multiple messaging applications. To enhance transparency and forensic reliability, explainable analysis techniques are incorporated to clearly justify correlations and inferred relationships, allowing investigators and legal stakeholders to understand how conclusions are derived. The framework aims to complement existing forensic tools by providing cross-app visibility and explainable analytical outputs, supporting investigations involving victims or suspects where multiple communication platforms may be used. The outcome of this research contributes a practical, ethical, and court-admissible approach to metadata-driven mobile forensic analysis, strengthening digital evidence interpretation in modern investigations.

Keywords: Digital Forensics, Metadata Extraction, Cross-App Analysis, WhatsApp Forensics, Telegram Forensics, Explainable AI

ICCI202637: QR Code–Based Cyber Attacks and Prevention

Divya Drishty R[1], Amrutha PM[2], Dr.Poongothai[3]

[1,2]Student, Department of Computer Science, Kristu Jayanti Deemed to be University, Bengaluru, India

[3]Teacher, Department of Computer Science, Kristu Jayanti Deemed to be University, Bengaluru, India

ABSTRACT

Due to rapid growth of digital payments, QR code usage has now become common in daily life. They are used to access websites, pay bills, download apps, and share information. However, this increased usage of QR code technology has led to the development of new threats in the form of cyber attacks. Cyber attacks using QR code technology occur when hackers change and substitute the legitimate usage of the QR code with their own.When the user scans the fake QR code, the attackers create fake websites and steal passwords and bank information. The major reason for this attack is the difficulty in reading the code. To raise awareness of cybersecurity and how it should be practiced to prevent QR code-related cyber threats by simple precautions. In real-life implementation, QR Code Risk Assessment Algorithm operates as an intermediate security layer between QR code scanning and user interaction. Once a QR code is scanned, the algorithm extracts the encoded content and performs real-time analysis without immediately redirecting the user. The system evaluates domain authenticity, redirection behavior, encryption status, and payment consistency to calculate a risk score. Based on this score, the user is alerted with appropriate warnings or the action is blocked. This approach ensures practical deployment on mobile devices while providing effective protection against QR code–based cyber attacks. By implementing the above mentioned method , users can safely benefit from QR code technology while protecting themselves from potential cyber threats.

Keywords: QR Code Security, Cyber Attacks, Phishing, Malware Distribution, Threat Prevention, Mobile Security, Cybersecurity Awareness, Risk Mitigation

ICCI202638: Anti-Forensic Tools Used In Moblie Phones: A Comparative Study

Jenoleena.G[1], Ms. Nivya George[2]

[1]Student, Department of forensic science ,
Kristu Jayanti Deemed to be university, India
[2]Assistant professor, Department of forensic science,
Kristu Jayanti Deemed to be University

ABSTRACT

Android smartphones have become vital sources of digital evidence, but antiforensic methods such as encryption, steganography, and rapid data deletion increasingly threaten the completeness and reliability of mobile investigations. This work presents an opensource, ethically controlled approach for examining Android antiforensic behaviour on a nonrooted Android 11 device, using only synthetic (nonpersonal) test data. The experimental setup creates a dedicated test environment on an Oppo smartphone, performs an initial logical acquisition using Android Debug Bridge (ADB), and then applies harmless antiforensic actions including encrypted containers, steganography within images, and scripted file deletion. The resulting "before" and "after" datasets are acquired using the same ADBbased procedure and analysed in Autopsy together with additional opensource tools such as ExifTool for filelevel metadata extraction, Plaso/log2timeline for basic timeline reconstruction, and utilities like bulk extractor and Binwalk for entropybased anomaly detection. The analysis highlights clear indicators of antiforensic activity, such as unexplained changes in timestamps, unusual filesystem metadata (for example unexpected file sizes, locations or extensions), highentropy artefacts that suggest encrypted or deliberately hidden content, and mismatches between the logical view of the data and the file system state that should be present. The primary contribution is a reproducible workflow that relies only on freely available tools—using ADB for acquisition and Autopsy plus the above opensource utilities for automated metadata and entropy analysis—allowing researchers and practitioners to systematically simulate and detect Android antiforensic behaviours without exposing real user data, and providing a practical basis for future automation and machine learning-based anomaly detection in mobile forensics.

Keywords: Mobile Forensics, Anti-Forensic Tools, Smartphone Security, Data Concealment Techniques, Digital Evidence Analysis, Cybersecurity, Forensic Investigation

ICCI20239: A Systematic Literature Review on Explainable AI for Heart Disease Prediction using SHAP and LIME

Nadiya Tabassum[1], Nadiya Tabassum[2], Saheba Rizwan[3], Jishnu MS[4],Revathy VR[5]

[1,2,3]Student Department of Computer Science

Kristu Jayanti Deemed to be University, Bengaluru, India

[4,5]Assistant Professor Department of Computer Science

Kristu Jayanti Deemed to be University, Bengaluru, India

ABSTRACT

This paper presents a systematic review of explainable artificial intelligence (XAI) methods for heart disease prediction, focusing on Shapley Additive Explanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME). Thirty peer-reviewed studies published during 2025 were analysed to identify commonly used machine learning and deep learning models, datasets, evaluation metrics, and interpretability methods. The review shows that ensemble models, especially Random Forest and XGBoost, are widely used because they perform well on structured clinical data. SHAP is mainly used to explain overall feature importance and also provide patient-level insights, while LIME is mostly used to explain individual predictions. The findings suggest that adding XAI improves transparency, interpretability, and clinician trust without reducing prediction performance. The review also highlights key limitations, including limited clinical validation and weak evaluation of explanation usefulness. Future research should focus on larger clinical studies, integration with electronic health records, and user-based testing to support real-world use of explainable heart disease prediction systems.

Keywords: Heart disease prediction, Explainable Artificial Intelligence (XAI), Machine Learning, Systematic literature review (SLR), SHAP (SHapley Additive Explanations), LIME (Local Interpretable Model-Agnostic Explanations), Random Forest, XGBoost, Clinical decision support.

ICCI202640: Optimizing Data Centre Energy Efficiency Through Business Analytics: A Predictive Energy Management Approach

Arshitha R[1], Dr Revathy V R[2]

[1]Student Department of Computer Science

Kristu Jayanti Deemed to be University, Bengaluru, India

[2]Assistant Professor,Department of computer science

Kristu Jayanti Deemed to be University, Bengaluru, India

ABSTRACT

The rapid escalation of global digitalization and AI workloads has positioned data center energy consumption as a critical bottleneck for sustainable development. With global footprints projected to surpass 1,000 TWh by 2026, a shift toward intelligent, data-driven frameworks is essential. This research introduces the Predictive Energy Management (PEM) framework, which utilizes Business Analytics to treat energy as a dynamic strategic variable. Using a Python-based simulation of a 24-hour operational cycle, the study employs an LSTM model to forecast demand spikes and execute "Cap-and-Shift" commands. The results demonstrate three significant outcomes: first, a 26.4% reduction in peak power demand through temporal load shifting to early morning "energy valleys"; second, a strong inverse correlation where 95% predictive accuracy stabilized the Power Usage Effectiveness (PUE) at an optimized 1.25; and third, a 30% reduction in carbon emissions achieved via geospatial heatmapping and workload migration to renewable-heavy regions. These findings provide an evidence-based roadmap for integrating predictive analytics into infrastructure management. By adopting this framework, organizations can achieve the dual objectives of operational cost reduction and environmental stewardship, aligning with the "Triple Bottom Line" of modern sustainable business practices.

Keywords: Data Centre Energy Efficiency, Predictive Analytics, Energy Management, Business Analytics, Sustainable Computing, Resource Optimization

ICCI202641: Business Impact Analysis of Neuro-Symbolic AI in Healthcare: Optimizing Patient Diagnosis, Treatment Recommendations, and Drug Discovery

Jokim Prathap A[1], Jokim Prathap A[2], Revathy V R[3], Jishnu M S[4]

[1,2]Student ,School of computational and physical sciences,
Kristu Jayanti Deemed to be University

[3,4]Assistant Professor
School of computational and physical sciences,
Kristu Jayanti Deemed to be University, Bengaluru, India

ABSTRACT

Healthcare systems face increasing challenges in clinical decision-making due to diagnostic inaccuracies, inefficient treatment planning, and lengthy drug discovery processes, leading to higher costs and suboptimal patient outcomes. This study examines the application of Neuro-Symbolic Artificial Intelligence, a hybrid approach that integrates neural learning with symbolic reasoning, to enhance decision support in healthcareoperations. The research focuses on three critical areas: patient diagnosis support, treatment recommendation systems, and drug discovery workflows. Simulated and structured datasets representing real-world healthcare scenarios are used to evaluate system performance and business impact. Scenario modelling and return-on-investment analysis are conducted using Microsoft Excel, while Power BI dashboards are employed tovisualize operational insights. The findings indicate that the proposed approach improves diagnostic accuracy by approximately 15 percent, reduces clinical decision-making time by nearly 20 minutes per patient, lowers treatment-related costs by 12 percent, and enhancespatient outcome indicators by 8 percent. Additionally, drug discovery timelines are reduced by about 30 percent, with a 10 percent improvement in success rates.

Keywords: Neuro-Symbolic Artificial Intelligence, Healthcare Decision Support Systems, Clinical Diagnosis Support, Treatment Recommendation Systems, Drug Discovery Optimization, Explainable AI, Data-Driven Healthcare.

ICCI202642: Beyond Noise:Algorithms That Listen to Silence

Neelufur.N[1], Ms Amudha Madhu[2], Samantha Judi Dyall[3]

[1,3]Student

[2]Assistant professor,Department of physical science,

Kristu Jayanti Deemed to be University

ABSTRACT

Most digital systems panic when nothing happens. No clicks, no taps, no signals—just silence. This paper argues that silence is not laziness, but information waiting to be understood. We introduce algorithms that listen to silence, detecting periods of inactivity and treating them as meaningful system signals rather than errors or timeouts. By carefully observing when users, signals, or networks go quiet, the proposed approach helps systems respond more intelligently, save resources, and avoid unnecessary "Are you still there?" moments. Through algorithmic modeling and practical examples, this study shows that sometimes the smartest systems are the ones that know when to stop talking.

Keywords: Audio signal processing; Silence detection; Noise reduction algorithms; Machine listening; Acoustic analysis

ICCI202643: Green ai

Dr K Kalaiselvi[1], Indhu K P[2], Malvin Samuel Ashok[3], Joanna Shalom[4]

[2,3,4]Student,Department of computer science,

Kristu Jayanti Deemed to be University

[1]Associate Professor and Coordinator,

Department of Computer Science,

Kristu Jayanti Deemed to be University

ABSTRACT

As Artificial Intelligence (AI) models grow exponentially in complexity, the environmental cost of training and deploying these systems has become critical concern. This   paper aims to explore how Green AI can contribute to innovation across various fields, specifically focusing on major sectors like technology, health care, environmental science and AI itself. It also explores the transition from "AI – characterized by massive energy consumption for marginal accuracy gains to Green AI", which prioritizes efficiency and sustainability and cost reduction.

Keywords: Green AI, Sustainable Artificial Intelligence, Energy-Efficient AI, Eco-Friendly Machine Learning, Carbon-Aware Computing, AI Model Optimization

ICCI202644: AI - driven Breast Carcinoma Detection for Early Diagnosis using Medical Image Analysis

Dr. Revathy V R[1], Anjumol Aby[2]

[1]Assistant Professor,School of computational and physical sciences,
Kristu Jayanti Deemed to be University, Bengaluru, India
[2]Student, Department of Computer Science,
Kristu Jayanti Deemed to be University, Bengaluru, India

ABSTRACT

Breast Cancer has shown a significant increase in incidence in recent years and remains as one of the leading causes of cancer related mortality among women across the world, emphasising the growing burden of disease and the immediate need for effective early detection strategies for cancer. However, as the traditional diagnostic approaches rely heavily on manual interpretation of medical images, which is time consuming and subject to inter observer variability, leads to diagnostic delays and further problems.The recent advancements in the domain of Artificial Intelligence (AI) and medical analysis have brought up the development of effective computer aided diagnosis systems for early cancer detection. This Research paper presents an AI driven early detection of breast carcinoma using Image Analysis. The methodologies include Image Preprocessing, Deep Learning based Feature Extraction, and Classification of breast lesions into benign (non-cancerous) and malignant (cancerous) spectrum. This experimental evaluation shows that the developed AI –driven model achieves high accuracy, sensitivity and reliability in detecting breast abnormalities. The outputs demonstrate the capability of AI assisted technologies to support radiologists in clinical decision making, reducing diagnostic errors and to facilitate timely intervention.

Keywords: AI in Healthcare, Breast Carcinoma Detection, Medical Image Analysis, Early Diagnosis, Deep Learning, Computer-Aided Diagnosis, Cancer Detection

ICCI202645: A Comparative Study of Free Forensic Tools for Detecting AI-Synthesized Deepfake Images

Petchiammal M[1], Ms Nivya George[2]

[1]Student,Department of forensic science,
Kristu Jayanti Deemed to be University

[2]Assistant professor, Department of forensic science,
Kristu Jayanti Deemed to be University

ABSTRACT

The rapid advancement of artificial intelligence has significantly improved the realism of synthesized images, giving rise to deepfake content that poses serious challenges to digital authenticity, forensic investigations, and legal proceedings. Detecting AI-generated images has therefore become a critical task in the field of digital image forensics. This study presents a comparative analysis of selected free and open-source forensic tools used to identify AI-synthesized deepfake images. The evaluation focuses on metadata examination, error level analysis (ELA), noise pattern analysis, and clone detection techniques to assess their effectiveness in differentiating authentic images from manipulated or AI-generated content. A diverse dataset comprising original camera images, software-edited images, and AI-generated images was analyzed using tools such as Exif Tool, Forensically Beta, Foto Forensics, Metadata Analyzer, and AI detector freely available forensic utilities. The findings indicate that while metadata-based analysis is effective in identifying software-generated and edited images, it is insufficient as a standalone method for detecting advanced AI-synthesized content. Pixel-level forensic techniques, including noise and compression artifact analysis, provide additional indicators of manipulation but vary in reliability depending on image format and processing history. This study highlights the strengths and limitations of free forensic tools and emphasizes the need for a multi-layered forensic approach when examining suspected deepfake images. Camera details, metadata, editing evidence these are the features are played crucial role in result. The results contribute to a better understanding of the practical applicability of cost-effective forensic solutions in combating the growing threat of AI-generated visual misinformation.

Keywords: Deepfake Detection, AI-Synthesized Media, Digital Forensics, Forensic Tools Comparison, Image Authentication, Cybersecurity

ICCI202646: Beyond Exif Metadata: A Comparative Study Of Metadata In Ai-Generated Images And Smartphone Captured Photographs

R V Ishitha Reddy[1], Nivya George[2]
[1]Student,Department of forensic science,
Kristu Jayanti Deemed to be University
[2]Assistant professor, Department of forensic science,
Kristu Jayanti Deemed to be University

ABSTRACT

There has been a remarkable surge in the field of generative AI, leading to the development of innumerable image creation tools. They pose significant forensic challenges during image authentication and digital media verification in law enforcement. The aspect of metadata examination has not been explored much in existing literature. Though there are standards, like IPTC and C2PA, that declare AI generated content, their consistency across platforms has not been documented. This study examined the metadata of 100 AI generated images from 20 different tools and compared that to the metadata profile of smartphone captured images using both Apple and Android. The metadata profiles were examined using Exiftool, MediaInfo and other forensic analysis tools. Most prominent metadata fields that conclusively indicate that an image is AI generated, such as Software Tag, C2PA and Digital Source Type, were identified and checked if they are consistently present in all the tools. The study establishes IPTC DigitalSource Type as a reliable primary indicator. Findings support the development of standardised forensic protocols for AI image authentication, cross-platform standardisation efforts, and support the implementation of metadata-based detection in forensics.

Keywords: Digital forensics, metadata analysis, AI-generated images, IPTC standards, C2PA provenance

ICCI202647: Employing AI for combating Deep fakes in Criminal Investigations

Vishal Vinod Naik[1], Swetha Thomas[2]

[1]Student,Department of forensic science,
Kristu Jayanti Deemed to be University

[2]Assistant professor, Department of forensic science,
Kristu Jayanti Deemed to be University

ABSTRACT

The rapid rise of generative artificial intelligence has made deepfakes—highly realistic synthetic or manipulated audio-visual content—an increasingly serious threat to theintegrity of criminal justice processes, raising concerns about evidence reliability and the erosion of institutional trust. Recent systematic research underscores that deepfakes pose significant risks to courts and investigations, highlighting the urgent need for advanced detection methods and stronger safeguards. This study examines how AI-driven tools can be effectively employed to combat deepfakes in criminal investigations, and the current AI-based detection tools available, then evaluating their real-world applicability, strengths, and limitations for forensic and law-enforcement settings. Drawing on this analysis, the research proposes practical, AI-centered strategies to enhance detection accuracy, procedural readiness, and policy responses—aiming to bridge technological developments with investigative needs and contribute to more resilient criminal justice mechanisms in an era of sophisticated synthetic media.

Keywords: AI-based deepfake detection; Criminal investigations; Digital forensics; Fake media mitigation; Machine learning

ICCI202648: Emotion Analysis from Text Using a Hybrid Deep Learning Model

Kalleshwari[1],Divya Shree M[2]

[1]Teacher,Department of physical science,
Kristu Jayanti Deemed to be University
[2]Student,Department of physical science,
Kristu Jayanti Deemed to be University

ABSTRACT

Emotion analysis from text is a key research area in Natural Language Processing (NLP) that focuses on identifying human emotions expressed through written language. It is widely used in applications such as customer feedback analysis, social media monitoring, mental health support systems, and chatbots. Traditional approaches for emotion detection include lexicon-based methods and machine learning algorithms such as Naïve Bayes and Support Vector Machine (SVM). Although these methods are simple and easy to implement, they suffer from several limitations, including poor handling of context, inability to understand complex sentence structures, and low performance on noisy and informal text commonly found on social media.To overcome these limitations, proper dataset cleaning and preprocessing are essential steps. This includes removing noise, stop-word elimination, tokenization, and converting text into numerical representations. Based on the disadvantages of traditional methods, this project proposes a hybrid deep learning model that combines Convolutional Neural Networks (CNN)and Recurrent Neural Networks (RNN) or Long Short-Term Memory (LSTM). CNN is used to extract important local features from text, while RNN/LSTM captures sequential and contextual information. The hybridized model improves emotion classification accuracy by effectively learning both feature patterns and contextual dependencies, making it more suitable for real-world emotion analysis tasks.

Keywords: Emotion analysis; Text mining; Hybrid deep learning; Natural language processing; Sentiment detection

ICCI202649: A comparative study of cyber hygiene practices and cyber crime awareness between generations.

Amitesh Ashok Das[1], Dr. Swetha Thomas[2]

[1]Student, Department of forensic science,
Kristu Jayanti Deemed to be University

[2]Assistant professor, Department of forensic science,
Kristu Jayanti Deemed to be University

ABSTRACT

The rapid expansion of digital technologies has reshaped communication, commerce, and daily life, creating both unprecedented opportunities and heightened vulnerabilities to cyber threats. As cybercrimes grow in complexity, understanding how different generations perceive and practice cyber hygiene has become increasingly important. This study conducts a comparative analysis of Generation X (born 1965–1980) and Generation Z (born 1997–2012) to examine variations in cyber hygiene behaviors, awareness of cybercrime, preventive attitudes, and susceptibility to online risks. Using a mixed-methods approach combining quantitative survey data and qualitative insights, the research evaluates key parameters such as password management, phishing identification, privacy settings, social media practices, device security, and responsiveness to cyber threats. Preliminary findings indicate that while Gen Z demonstrates higher digital exposure and familiarity with technological tools, they also engage in riskier online behaviors due to frequent internet use and a tendency to overlook security protocols. Conversely, Gen X exhibits comparatively cautious online practices but has limited technical knowledge, which may reduce their ability to recognize newer forms of cybercrime. The study highlights generational differences that contribute to varying levels of vulnerability, emphasizing the need for targeted awareness programs, inclusive cybersecurity education, and policy interventions tailored to diverse digital literacy levels. Overall, the research underscores the importance of bridging generational gaps in cyber hygiene to enhance collective resilience against cybercrime.

Keywords: Cyber hygiene, Cybercrime awareness, Digital security practices, Generational differences, Generation X, Generation Z, Online risk behavior, Cybersecurity education, Digital literacy, Phishing and privacy protection

ICCI202650: Digital Forgetting Algorithms

Dr Amutha Madhu[1], Avanthika Manoj[2], Ranjna[3]

[1]Assistant professor, Department of physical science,
Kristu Jayanti Deemed to be university

[2,3]Student,Department of physical science,
Kristu Jayanti Deemed to be University

ABSTRACT

Modern software systems are designed to store data indefinitely, which can lead to privacy risks, outdated information usage, and regulatory challenges. Unlike human memory, which naturally forgets irrelevant information over time, digital systems lack mechanisms for intentional forgetting. This paper introduces the concept of Digital Forgetting, a novel computational approach in which software systems intelligently discard data based on relevance, risk, and time. A conceptual framework is proposed that models forgetting as a continuous process using relevance decay and data half-life, rather than static deletion policies. The study outlines a high-level algorithm and architecture for integrating digital forgetting into existing systems. By treating forgetting as a deliberate design feature, this work presents a creative and ethical perspective on future data management and privacy-aware computing

Keywords: Digital forgetting, Data lifecycle management, Privacy-aware computing, Relevance decay, Data half-life, Ethical data management, Intelligent data deletion, Software system design, Data minimization

ICCI202651: How Agentic AI and Block-Chain can transform modern banking

Ishan sutwala[1], Dr. Gopinath D[2]

[2]Assistant Professor, Department of computer science,
Kristu Jayanti Deemed to be University
[1]Student,Department of physical science,
Kristu Jayanti Deemed to be University

ABSTRACT

The rapid evolution of financial technologies is reshaping the global banking landscape, with blockchain and agentic artificial intelligence (AI)emerging as two of the most transformative forces. Blockchain technology introduces decentralized, tamper-resistant ledgers that enhance transparency, security, and trust in financial transactions, while reducing reliance on intermediaries. Concurrently, agentic AI—characterized by autonomous decision-making, goal- oriented behavior, and adaptive learning—enables intelligent automation across banking operations, including fraud detection, risk assessment, personalized financial services, and regulatory compliance. This paper explores the synergistic integration of blockchain and agentic AI in modern banking systems, examining how their combined capabilities can improve operational efficiency, strengthen security frameworks, and foster innovation in digital financial services. Through analysis of existing banking models and emerging use cases, the study highlights key applications such as smart contract automation, decentralized finance (DeFi), real-time auditing, and autonomous financial agents. Additionally, the paper discusses challenges related to scalability, governance, ethical considerations, and regulatory alignment. The findings suggest that the convergence of blockchain and agentic AI has the potential to redefine banking infrastructures, enabling more resilient, transparent, and customer-centric financial ecosystems.

Keywords: Agentic AI, Blockchain technology, Modern banking systems, Financial technology (FinTech), Smart contracts, Decentralized finance (DeFi), Autonomous financial agents, Fraud detection, Digital banking transformation, Regulatory compliance

ICCI202652: Scalable and Interoperable Decentralized Identity (DID)

Asfiya Shaikh[1], Dr. Gopinath D[2]

[2]Assistant Professor, Department of computer science,
Kristu Jayanti Deemed to be University

[1]Student,Department of physical science,
Kristu Jayanti Deemed to be University

ABSTRACT

Decentralized Identity (DID) systems represent a transformative approach to digital identity management, granting users sovereignty and enhanced privacy control beyond traditional centralized models. However, current DID platforms face critical challenges including limited interoperability across heterogeneous blockchains, scalability constraints impacting real-time performance, and usability barriers hindering widespread adoption. This research addresses these multifaceted gaps by proposing an integrated architecture that synergizes five key algorithmic innovations: a cross-chain interoperability protocol enabling seamless communication across diverse blockchain networks; Layer-2 scalability optimizations tailored for credential management; a user-centric key recovery algorithm enhancing usability and security; privacy-preserving selective disclosure mechanisms; and an adaptive trust scoring framework to enforce decentralized governance. The proposed system is rigorously evaluated through blockchain testnet experiments, performance benchmarking, user studies emphasizing usability, cross-domain validation scenarios, and regulatory compliance analysis. Demonstrated within practical contexts including Internet of Things (IoT), e-Health, and e-Voting, the architecture exhibits significant improvements in interoperability, transaction throughput, user experience, and trustworthiness. This comprehensive framework advances the practical adoption of scalable, secure, and user- friendly decentralized digital identity systems, positioning them as viable alternatives for cross-domain applications.

Keywords: Decentralized Identity (DID), Blockchain interoperability, Scalable identity systems, Layer-2 solutions, Self-sovereign identity, Privacy-preserving authentication, Selective disclosure, Cross-chain protocols, Decentralized governance, Digital identity management

ICCI202653: A Transfer Learning–Enabled Framework for Intelligent Anomaly Detection in Smart City Systems

Varshasree Suresh Bandaru[1], Vajramol K M[2], Ms Shilpa R[3]

[1,2]Student, [3]Teacher,

Department of Physical Sciences

Kristu Jayanti Deemed to be University

ABSTRACT

As smart cities transition toward fully integrated digital infrastructures, the systems leading urban data become increasingly vulnerable to cyber-threats and operational failures. Detecting these anomalies is critical for maintaining public safety; however, newly established urban environments often suffer from data scarcity, lacking the historical records needed to train robust Artificial Intelligence models. Furthermore, traditional deep learning approaches are computationally expensive, presenting an obstacle for cities with limited high-performance computing resources. This paper proposes a conceptual framework centered on Transfer Learning to overcome these limitations. Our methodology involves a two-stage approach: first, utilizing a high- capacity model pre-trained on large-scale network datasets, and second, applying Domain Adaptation to align that knowledge with specific urban data patterns. By "fine-tuning" the model's parameters, we hypothesize that the framework will identify security breaches and system irregularities with high precision using minimal local data. This proposed approach aims to provide a scalable, resource-efficient strategy for safeguarding the digital integrity of evolving smart city ecosystems without the need for massive data collection or from-scratch model training.

Keywords: Transfer Learning, Anomaly Detection, Domain Adaptation, Urban Data Security, Knowledge Transfer, Computational Efficiency.

ICCI202654: Artificial intelligence in healthcare

MS Ankitha P[1], Arjundev A[2],Minto P james[2]

[2,3]Student, [1]Teacher,

Department physical science

Kristu Jayanti Deemed to be University

ABSTRACT

Artificial Intelligence (AI) is transforming healthcare by improving clinical decision-making, efficiency, and patient-centred care. This paper reviews recent advancements in AI-based healthcare applications and their role in addressing challenges such as rising costs, workforce shortages, and unequal access to services. The integration of multi-modal health data with technologies such as the Internet of Things and cloud computing enables the development of intelligent and connected healthcare systems. The study also highlights key requirements for trustworthy AI, including ethical compliance, transparency, and continuous evaluation. The findings demonstrate that AI can effectively augment clinicalexpertise, supporting precision medicine, personalized treatment, and improved population health outcomes.

Keywords: Artificial Intelligence, Healthcare, Clinical Decision-Making, Precision Medicine, Personalized Treatment, Intelligent Healthcare Systems, Internet of Things (IoT), Cloud Computing, Multi-modal Health Data, Ethical AI, Patient-Centred Care, Population Health Outcomes.

ICCI202655: Fault-Tolerant URL Shortener for Unstable Network

Dharshini K[1], Amutha mam[2]

[1]Student, [2]Teacher,

Department of physical science, Kristu Jayanti Deemed to be University

ABSTRACT

Abstract In many regions across the world, internet connectivity is unreliable due to poor infrastructure, frequent power outages, and limited network coverage. Traditional URL shortening services rely on constant internet availability and centralized cloud systems, which makes them ineffective in such environments. This paper proposes the design of a fault-tolerant URL shortener specifically intended for use in countries with unstable internet connectivity. The proposed system focuses onreliability, availability, and resilience by using decentralized architecture, local caching, and asynchronous data synchronization. Even during network failures, the system ensures that shortened URLs continue to function through fallback mechanisms and locally stored mappings. By supporting offline-first access and graceful recovery, this solution improves accessibility to digital resources and enables dependable information sharing in connectivity-challenged regions. The proposed design contributes toward digital inclusion and reliable web access in underserved areas.

Keywords: Fault-tolerant systems, URL shortener, Unstable network environments, Offline-first architecture, Decentralized systems, Local caching, Asynchronous synchronization, Network resilience, Digital inclusion, Reliable web access

ICCI202656: Blockchain Security

Smeeta Das[1], Thanushree V[2] ,Amutha M[3]

[1,2]Student, [3]Teacher,

Department of physical science, Kristu Jayanti Deemed to be University

ABSTRACT

Blockchain security focuses on protecting decentralized systems that store and transfer data through distributed ledgers. By using cryptographic techniques, consensus mechanisms, and immutability, blockchain reduces risks related to data tampering, fraud,and unauthorized access. However, despite its strong security foundations, blockchain systems still face challenges such as smart contract vulnerabilities, 51% attacks, and scalability-related risks. This research project examines key security features of blockchain technology, identifies potential threats, and analyzes existing defense mechanisms.Understanding blockchain security is essential for ensuring trust, transparency, and reliability in applications across finance, healthcare, and digital governance systems.

Keywords: Blockchain security, Distributed ledger technology, Cryptography, Consensus mechanisms, Smart contract vulnerabilities, 51% attacks, Decentralized systems, Data integrity, Cybersecurity threats

ICCI202657: ExplainX

Dinesh S[1], Iqra Nafia[2], Anto Jinola[3], Preethi S[4] , Amutha[5]

[1,2,3,4]Student, [5]Teacher,

Department of physical science, Kristu Jayanti Deemed to be University

ABSTRACT

Today, many intelligent systems provide results without clearly explaining how those results are obtained, making them difficult tounderstand and trust. ExplainX is designed to solve this problem by focusing on logic and rule discovery rather than prediction. The system analyzes input and output data to identify the exact mathematical or logical relationships behind a pattern. Instead of using learning models or probability-based methods, ExplainX applies symbolic reasoning to derive simple and verifiable expressions. Every generated rule can be checked and understood step by step, ensuring complete transparency. By prioritizing explanation over approximation, ExplainX supports reliable and interpretable problem-solving for realworld applications.

Keywords: Explainable systems, Symbolic reasoning, Rule discovery, Interpretable artificial intelligence, Transparent computation, Logic-based models, Mathematical expression discovery, Trustworthy AI, Explainability

ICCI202658: Balancing the Plate: Understanding the Interaction of Domestic Agriculture and International Trade Implications for Global Food Security

C Anisha joy[1], Sumalatha A[2]

[1]Student,

[2]Assistant Professor, Department of computer science, Kristu Jayanti Deemed to be University

ABSTRACT

Climate change and unstable markets are the new zeros in the struggle for global food security. National agriculture may be critical for food supply, but access and stability crucially rely on international trade. We do this by analyzing the complex relationship between regional food production, global trade networks, and national food security outcomes. Our findings indicate that, although a strong TRI significantly enhances the stability of food security, especially for importer countries, the current trade regime holds significant risks. Protectionist policies, such as export restrictions in major producing countries, hike global prices and reduce access by poor groups. We conclude that the optimisation of domestic productivity and building more diverse, transparent, and resilient international trade mechanisms go hand in hand for sustainable global food security. Policy efforts should focus on preventing protectionism and promoting regional trade integration to improve shock management**.**

Keywords: Global food security, Domestic agriculture, International trade, Trade resilience index (TRI), Agricultural productivity, Trade policy, Protectionism, Food supply stability, Climate change impacts, Sustainable food systems

ICCI202659: Categorization of Defensive Cybersecurity Tools Using Functional Security Domains with a Web-Based Prototype

Dhanush R[1] , Dr. Kalaiselvi K[2]

[1]Student ,Department of Forensic Science ,

[2]Assistant professor,Department of Computer Science

Kristu Jayanti Deemed to be University

ABSTRACT

It is a challenge to cybersecurity practitioners to use the security tools in the market due to the large number of over 100 solutions at any given moment when an incident has occurred that should be managed within a limited period. The current paper addresses this issue with a critical literature review, in particular, and systematic mapping of the wide range of tools to fight cybercrime open-source and proprietary ones, to the phases of the attack life cycles by offenders. According to the sound mixed method design science methodology, the research paper is based on the systematic analysis with the design of the fully operational no code web prototype, basingon HTML, CSS, and JavaScript. The system has an easy user interface, which is sorted alphabetically, and the threat-tools correlations validated, which allows the informed and fast decisions on the tool to be used. The deployable artifact is to serve the requirements of students, academic researchers, and security professionals, help reduce cognitive load, accelerate the process of incident response, and enhance decision-making efficiency when it comes to SecurityOperations Center and the digital forensics context. This work is a useful practical tool that can help with education, threat inquiry and operational defense by bridging the disconnect betweenideas of cybersecurity and practical applications of those ideas in tools. This shall produce an authenticated prototype, an official taxonomy of tool-threat alignment, and applicable recommendations that will together address the extant voids in tool recommendation systems, and consequently make a contribution to the art of cybersecurity training and research.

Keywords: Cybersecurity tools, Defensive security domains, Tool categorization, Attack lifecycle mapping, Incident response, Security Operations Center (SOC), Digital forensics, Tool–threat alignment, Web-based prototype, Cybercrime mitigation

ICCI202660: Analyzing The Impact of Data Poisoning In Lora And Qlora Fine-Tuned Models

Dr. Divya K S [1], Kavya B Raj[2]

[1]Associate Professor,

[2]Student, Department of Computer Science, Kristu Jayanti Deemed to be University, Bangalore, India

ABSTRACT

LoRa and QLoRa are efficient parameter tuning techniques widely used for Natural Language Processing (NLP), as they are capable of leveraging large pre-trained models while reducing memory overhead and compute requirements. Under limited computational resources available, adapting LoRA and QLoRA allows large language models to work efficiently, ensuring optimal performance even in the presence of data poisoning. Although both LoRA and QLoRA has shown effective performance, the effects of poisoning attacks on both these models remain largely unexplored. This research paper explores how data poisoning can render the behaviour of the models that have been trained with LoRa and QLoRa methodologies. This experiment shows label flipping attacks varying data poisoning levels from 10% to 100% and assessed model performance through accuracy and F1 scores. Both LoRa and QLoRa demonstrate degradation in performance with increasing intensity of data posioning, thus highlighting the need for reliable clean data. While QLoRa reveals a slight improvement in accuracy at different levels of data poisoning, both techniques show vulnerability to substantial data corruption. As a result, the ability to perform efficient fine-tuning of models is dependent on the validation of data used to train the models and to ensure that the training of the models takes place in a secure environment. Our findings of this studyreveal that resource efficient fine-tuning techniques are still susceptible to adversarial attacks.

Keywords: Low-Rank Adaptation (LoRA), Quantized Low-Rank Adaptation (QLoRA), Data Poisoning Attacks, Label Flipping Attack, Robustness of Fine-Tuned Models, Large Language Models (LLMs)

ICCI202661: Students' Perceptions of the Impact of Generative AI Tools on Learning and Creativity

Dr. Divya K S[1] , Nandini V[2] , Navya D[3] , Raksha B H[3] , Aiman Baig4
[1]Associate Professor
[2,3,4]Student, Department of Computer Science[UG],
Kristu Jayanti Deemed To be University,Bangalore ,India

ABSTRACT

As Generative AI tools such as ChatGPT, Gemini, and Copilot have become increasingly integrated into higher education, empirical evidence regarding students' perceptions of their impact on academic development and creative thinking in the Indian context remains limited.To address this gap, the present study employed a primary quantitative survey of 100 undergraduate and postgraduate students. AI usage patterns were conceptualized as the independent variable, while perceived effects on Cognitive Engagement, Deep Learning, andcreative output were treated as dependent variables. Additionally, drawing on the framework of Effort-Efficiency Tension, the study examined how disciplinary backgrounds and ethical attitudes shape students' actual academic behaviour. Results indicated strong overall student support for Generative AI, particularly for its role in improving task efficiency and facilitating comprehension of complex academic concepts. However, perceptions of creativity were mixed; although many participants reported using AI for brainstorming and idea generation, a substantial proportion expressed concerns aboutreduced originality and intellectual dependency. The findings also revealed a clear Disciplinary Gap, with technical and non-technical students using AI for distinct academic purposes. Furthermore, a significant Awareness-Behaviour Gap emerged: although 90% of respondents were knowledgeable about academic integrity policies, approximately one-third admitted to a pragmatic reliance on AI that diminished personal effort. This illustrates a Pragmatic Paradox in which efficiency often takes precedence over ethical commitment.Collectively, these findings highlight the need for discipline-specific guidelines to ensure that Generative AI supports, rather than replaces, independent learning.

Keywords: Generative AI in education, Student perceptions, Learning outcomes, Creativity, Cognitive engagement, Deep learning, Academic integrity, Effort–efficiency tension, Disciplinary differences, Higher education in India

ICCI202662: Ransomware

Habel Jacob[1], Kesia Ann Wilson[2], Anagha R[3], Anousha Sam Samuel[4], Navya Francis[5]

[1,2,3,4]Student,

[5]Assistant Professor,

Department of Computer Science, Kristu Jayanti College, Bangalore

ABSTRACT

Ransomware has become one of the most serious cybersecurity threats in today's digital world, affecting individuals, organizations and even critical infrastructure. This study explores how ransomware attacks have evolved over time, focusing on common attack vectors, methods of spread and the level of awareness users have about ransomware threats and prevention. The research combines an analysis of real ransomware incidents with an evaluation of users' technical knowledge and cybersecurity readiness. Participants were assessed based on their understanding of how ransomware works and how they would respond to simulated attack scenarios. The data collected helped identify patterns in security awareness, risk perception and response behavior. The study further examines how emerging technologies such as automation and artificial intelligence are being misused by attackers to develop more efficient and sophisticated ransomware campaigns. By analyzing various attack models and exploitation techniques,the research identifies key vulnerabilities that enable ransomware infiltration and lateral movement within systems. The findings highlight a growing gap between rapid technological advancement and user preparedness, emphasizing the need for stronger cybersecurity awareness, improved defensive strategies and proactive risk mitigation. This study also provides a foundation for future research on ransomware resilience across different sectors and user demographics.

 Keywords: Ransomware, Cybersecurity, Malware Analysis, Attack Vectors, Data Protection, User Awareness, Threat Intelligence, Network Vulnerabilities, Risk Mitigation, Digital Security

ICCI202663: Computational characterization of proportional counters and plastic scintillators used in the GRAPES-3 Experiment

Vaishnavi K[1], B. Hariharan b[2] , V. Vadhana Sharon[3], Shivaraj R. Maidur[3]

[1,2,3]Department of Physics, School of Computational and Physical Sciences, Kristu Jayanti Deemed to be University, Bengaluru 560077, Karnataka,

[2]India Cosmic Ray Laboratory, Tata Institute of Fundamental Research, Raj Bhavan, Ooty 643001, TamilNadu, India.

ABSTRACT

Experimental cosmic ray detectors generate large volumes of raw data that require computational processing for accurate interpretation. This work presents a computational analysis of data from two detector systems: a plastic scintillator coupled to a photomultiplier tube and a proportional counter. The detector outputs were systematically processed and visualized to study gain, signal stability, and response characteristics. Pulse height distributions, amplitude variations, and count-rate trends were extracted using structured analysis workflows. This enabled direct comparison of detector behavior under identical experimental conditions. Careful plotting and noise-aware visualization ensured reliable interpretation of signals. Reproducible computational practices supported consistent and trustworthy results. The study highlights the role of data visualization and parameterextraction in detector characterization. The workflow provides a foundation for scalable andautomated analysis of cosmic ray measurements.

Keywords: Cosmic rays, detector characterization, data analysis, data visualization, signal processing;

ICCI202664: A Visual Analytics–Based Reporting System for Multi-Branch Retail Performance Analysis

Alakananda M[1], Revathy V R[2], Navya Francis[3]

[1]Student,[2,3]Assistant professor ,

Department of Computer Science School of Computational and Physical Sciences Kristu Jayanti University Bengaluru,India

ABSTRACT

A Visual Analytics–Based Reporting System for Multi-Branch Retail Performance Analysis provides top-level management with real-time, interactive dashboards to monitor key operational metrics across distributed retail locations. Modern retail environments face persistent challenges including fragmented data across inventory, finance, CRM, and sales functions; manual reconciliation processes prone to errors; and limited visibility into branch-level performance. These issues often result in stockouts, overstocking, financial discrepancies, suboptimal customer retention, and delayed strategic responses to market dynamics. Such a reporting system integrates diverse enterprise datasets into a cohesive visualization platform, transforming raw transactional data into actionable insights through intuitive charts, KPIs, and drill-down interfaces that support rapid decision-making. The methodology begins with comprehensive requirement analysis from cross-functional stakeholders to identify priority metrics—such as stock turnover ratios, reorder thresholds, ledger balance accuracy, customer lifetime value, and branch-wise revenue trends. Data preparation involves extraction from relational databases, cleansing to address common real-world issues like duplicates, missing values, and inconsistent formats, followed by aggregation into multidimensional models suitable for dynamic querying. Visualization design emphasizes user-centric layouts featuring bar charts for performance comparisons, heatmaps for anomaly detection, trend lines for temporal analysis, and scatter plots for behavioral segmentation, all enabled by conditional filtering, hierarchical drill-downs, and comparative analysis capabilities. Implementation outcomes include accelerated inventory optimization through fast-moving SKU identification, streamlined financial audits via automated discrepancy flagging, enhanced CRM targeting based on purchase pattern analysis, and overall reduction in reporting cycle times from days to minutes. This approach establishes a scalable foundation for descriptive analytics in multi-branch retail operations, with clear extensibility toward predictive modeling, real-time streaming integration, and enterprise-wide deployment to drive competitive advantage through data-driven operational excellence.

Keywords:

Visual analytics, Retail performance analysis, Business intelligence dashboards, Multi-branch retail systems, Data visualization,KPIs, Inventory optimization, Customer relationship management, Decision support systems, Data-driven management.

ICCI202665: A Comparative Study of Machine Learning Algorithms for Email Spam Detection

Diya Surendran[1] , Siddharth S[2] , Dr. Poongothai P[3]

[1,2]Student,

[3]Assistant Professor, Department of Computer Science, Kristu Jayanti Deemed to be University Bengaluru – 560077

ABSTRACT

Email continues to be one of the most widely used forms of communication, but spam remains a major issue faced by users every day. Spammers often target individuals through unsolicited emails containing harmful links, phishing attempts, or fraudulent schemes, making inbox security extremely important. Over time, traditional filtering methods based on fixed rules and keyword matching have become less reliable, since spammers constantly change their strategies to avoid detection. As a result, machine learning hasemerged as a smarter and more adaptable approach for identifying spam emails. This paper explores how patterns in email text can be analyzed to train supervised learning models to distinguish spam from genuine messages. Techniques such as Bag-of-Words and TF-IDF arecommonly used to represent email content in a format that machines can process efficiently. Several classifiers, including Naïve Bayes, Support Vector Machines, Logistic Regression, Decision Trees, and Random Forest, have shown strong performance in real-world evaluations. Benchmark studies also suggest that ensemble-based methods often achieve the highest accuracy, sometimes exceeding 99%. Looking ahead, deep learning can further enhance spam detection by capturing deeper semantic meaning in emails through advanced models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and transformer-based architectures like BERT. Overall, intelligent learning-based techniques offer a promising and scalable solution for improving email filtering and ensuring safer communication.

Keywords: Email spam detection, Machine learning algorithms, Supervised learning, Text classification, TF-IDF, Bag-of-Words, Ensemble methods, Deep learning models, Phishing detection, Email security

ICCI202666: Smart Ambulance Monitoring System Using Iot.

P Preethika[1], Dinesh C[2], Aishwarya Pramod Mahadevan[3], Aanchal Verma[4] ,

Ms. Mohana Priya[5]

[1,2,3,4]Student, [5]teacher

Department of computer science,

Kristu Jayanti Deemed to be university Bengaluru – 560077

ABSTRACT

Severe traffic congestion in urban regions poses a major challenge to emergency medical transportation, often delaying ambulance services and increasing the risk of fatal outcomes. To mitigate this problem, this paper introduces a Smart Ambulance Monitoring System leveraging Internet of Things (IoT) and Artificial Intelligence (AI) technologies to enable intelligent traffic management for emergency vehicles. The proposed system utilizes real-time video streams captured by IoT-enabled cameras at road intersections, where an AI-driven vision model detects ambulances by analyzing distinctive visual characteristics such as flashing emergency lights and vehicle markings. Once an ambulance is detected, control commands are transmitted to traffic signal units to temporarily modify signal phases and provide priority passage. The system architecture incorporates edge-level processing to achieve low-latency detection, along with cloud-based storage for operational monitoring and performance analysis. By automating ambulance recognition and traffic signal control, the proposed solution aims to minimize response time, reduce dependence on manual intervention, and enhance the effectiveness of emergency healthcare delivery. The design methodology and potential deployment in highly congested metropolitan environments are also discussed.

Keywords: Smart ambulance system, Internet of Things (IoT), Intelligent traffic management, Emergency vehicle prioritization, Artificial intelligence, Computer vision, Real-time monitoring, Edge computing, Smart city applications, Emergency healthcare systems

ICCI202667: An Analytical Study of Cyberforensic Processes and Tools in Advanced Digital Environments

Emy Elizebath Oommen[1], Dr. Haripriya M P[2] , Ms. Vishnu Priya P M[3]

[1]Student, [2,3]Assistant Professor

Department of Computer Science

Kristu Jayanti Deemed to be University,Bengaluru,Karnataka.

ABSTRACT

Cyberforensics, also referred to as digital forensics, is a crucial discipline within cybersecurity that focuses on the identification, preservation, analysis, and presentation of digital evidence related to cyber incidents. The increasing prevalence of cloud computing, mobile technologies, Internet of Things (IoT) devices, and advanced persistent threats has significantly complicated cyberforensic investigations. This paper examines current cyberforensic techniques, tools, and investigative frameworks used to analyze cybercrimes across networks, operating systems, and digital storage environments. Key stages of the cyberforensic process including evidence acquisition, validation, chain of custody, analysis, and reporting are discussed, along with challenges such as data volatility, encryption, anti-forensic methods, and legal and jurisdictional constraints. Furthermore, the paper reviews emerging trends in cyberforensics, including the application of artificial intelligence, automation, and cloud-based forensic solutions. The study highlights the need for standardized methodologies and adaptive forensic models to ensure the integrity and reliability of digital evidence in an evolving threat landscape.

Keywords: Cyberforensics, Digital Forensics, Cybercrime Investigation, Network Forensics, Cloud Forensics, Digital Evidence

ICCI202668: On-Chain Auto-Adaptive Clinical Pathways: A Blockchain-Native Orchestration Layer for Real-Time Medical Automation and Analytics

P Maria Sharon[1], Regan P[2], Syeda Zahra[3], Prof.Stephen A[4] ,

[1,2,3]Student,[4]Assistant professor

Department of computer science,

Kristu Jayanti Deemed to be University

ABSTRACT

Imagine we're building a system for healthcare that basically runs itself. We want to use blockchain to create a core layer that can manage and adapt clinical pathways in real-time. This means we can automate medical processes and get instant insights from the data."Yeah, I get the gist of it."Right now, the old-school, one-size-fits-all clinical paths for managing long-term health problems are a real drag on healthcare. They're actually a big reason why people end up back in the hospital when they shouldn't, and why doctors sometimes miss important patient issues until it's too late.This paper talks about a new system. It proposes a way to manage clinical stuff using blockchain from the ground up, right from the core.Think of these "pathways" like smart contracts that can change over time. They get updated by information from things like smart devices or your medical records, and then they automatically do stuff in the clinic. All the while, they collect information for analysis in a way that keeps your privacy, so we can make these pathways even better through updates approved by the right people.We're basically combining a few cool ideas here: We use something called zero-knowledge proofs to keep patient info totally private, then we add homomorphic encryption to securely pull all that data together without actually seeing it, and finally, federated learning helps us train a model across different hospitals without them ever sharing their raw data.A simulation was designed for five thousand virtual people using made-up diabetes management data.We want to see how much we can cut down on hospital stays, speed up response times, and make things easier to check, especially when looking at the old ways of doing things with electronic health records.The architecture is quite something; it's a complicated setup that brings together lots of different elements. You might think it is a simple solution from the outside, but trust me, it's not. It certainly goes to show what you can achieve with a bit of clever design. The whole idea is to have a flexible system that can really adapt to various needs, rather than being stuck with one rigid way of doing things.This whole thing was designed to help thousands of patients, and it's built on a Layer 2 blockchain to keep costs low.it costs money to move stuff around.

Keywords: Blockchain healthcare, Smart contracts, Clinical pathway automation, Privacy-preserving analytics, Digital health systems

ICCI202669: Beyond the Boundary: A Data-Driven Exploration of Virat Kohli's Cricketing Mastery in Batting

Akel Varghese[1], Gobi Ramasamy[2], Nisha Varghese[3], Deepthi Das[4]

[1,4]Statistics and Data Science, [2,3]Computer Science

CHRIST University

Bangalore, India

ABSTRACT

Cricket, a globally cherished bat-and-ball sport with origins in England, has deeply resonated in India, evolving into a cultural cornerstone and a source of immense pride. The Indian cricket team's illustrious history, enriched by legendary players, includes five major ICC tournament triumphs. Among India's cricketing legends, Virat Kohli stands out as a beacon of excellence, celebrated for his record-breaking 80 international centuries and his transformative leadership. This manuscript delves into cricket analytics, focusing on the development of an interactive Power BI dashboard that visualizes Kohli's batting achievements and career milestones. The primary objective of this work is to employ data visualization and statistical analysis to highlight Kohli's performance across formats, locations, and time periods, offering fans and analysts a deeper understanding of his contributions to cricket. By incorporating line charts, bar charts, histograms, scatter plots, and interactive filters, the dashboard provides dynamic insights into key aspects of Kohli's career. Users can explore top-ground performances, monthly and quarterly trends, opposition-specific records, and match participation summaries. The novelty of this research lies in its ability to merge the fields of cricket and data analytics, offering an engaging tool that celebrates individual achievements while demonstrating the broader applications of data-driven insights in sports. The dashboard serves as a testament to the role of analytics in enhancing the spectator experience, enabling a nuanced appreciation of player performance, and supporting strategic decision-making. This manuscript underscores the value of cricket analytics as a growing field and positions the Virat Kohli century analysis dashboard as a model for celebrating cricket's legends through data.

Keywords— Data Analysis, Data Visualization, Cricketing Mastery, Key Performance Index

ICCI202670: AI-driven optimization revolutionizing CCTV storage efficiency with unprecedented efficacy

Nisha Varghese[1], Gobi Ramasamy[2], Elangovan Sivalingam[3], Elangovan Sivalingam[4]

[1,2]Computer Science

Christ University Bangalore, India

[3]eBay, US

[4]University of Oxford, UK

ABSTRACT

Abstract—In contemporary monitoring systems, CCTV footage management and analysis of CCTV scenes are raising substantial challenges. This is disabled by focusing on efficient storage optimization and analytical techniques, especially in removing these challenges, which is aimed at fighting these challenges. The unnecessary frames inside the OpenCV library are identified and removed from the CCTV views, which reduces storage requirements without compromising the integration of critical motion events. These advantages of the OpenCV library of the Python's OpenCV library, complemented by Janko, SQLite, and Bootstrap, ensure effective data visualization, strength, scalability, and user-friendliness. The proposed solution offers practical gains, including the proposed solution, improved analysis and improved analysis. Moreover, by providing a valuable and industry-based approach, this method substantially contributes to the progress of technology storage optimization in the CCTV monitoring domain. In addition, the acceptance of this innovative solution is also likely to inspire the evolution of more intelligent and efficient observation systems to encourage further development in the region. This approach improves security and monitoring capacity by leading the upgrade, convenience, and observations in various areas and apps.

Keywords- video capturing, storage optimization, motion detection, machine learning, MSE

ICCI202671: SPAM SHIELD: Leveraging Large Language Models for Phishing and Spam Detection

Gobi Ramasamy[1], Nisha Varghese[2], Elangovan SivalingaM[3], Selvakumar Ramachandran[4]

[1,2]Computer Science

Christ University Bangalore, India

[3]eBay, USA

[4]University of Oxford, UK

ABSTRACT

Cyber Attacks on digital communication platforms in professional settings have become a significant concern. Phishing attacks and spam mail are persistent challenges, and manual mail evaluation is time-consuming and prone to error. With advanced cybercrime tools available, cyber-attacks can happen without a trace. The study aim is to develop a Smart email Classifier that can automatically classify emails as Phishing and spam, provide a sentiment tone, and generate a summary of the mail by leveraging the power of Large Language Models without having the need to read the mail manually and prevent keylogger or Cyber Attacks. Leveraging Large Language Models (Llama 3.1) for comprehensive mail analysis offers detailed feedback to the user, including links to the attachments. Emails are extracted from the user mail account via Imap, and the extracted content is fed to the model for analysis. The mail is classified based on the sender's address, subject body content, and attachments. LangChain implements sequential execution of processing tasks, incorporating prompt template, llama 3.1 model, and parser. The output Response is formatted to structured content for user experience. The Llama 3.1 model is accessed using Groq API for the best computing speed and capacity. The model demonstrated its ability as promising and highly influential in classifying phishing and spam mail during manual testing.

Keywords— Cyber-crime shield, spam & phishing classifier, large language models, groq, miniumum latency

ICCI202672: SaptaRaaga : Emotion Classification of Kannada Songs using FastText Embeddings and Machine Learning Models

Sulekha K R[1], Nisha Varghese[2], Sridevi R[3]

Department of Computer Science

Christ University

ABSTRACT

To classify Kannada songs into seven emotional categories—Devotional, Fear, Folk, Happy, Love, Patriotic, and Sad—this study proposes a supervised machine learning-based approach. The methodol- ogy involves lyric preprocessing, class balancing using ADASYN, feature extraction with FastText embed- dings, and classification using Support Vector Ma- chines (SVM). These steps are tailored to address the mor- phological richness and linguistic complexity of the Kannada language. A comparative analysis was also performed using Random Forest, Logistic Regression, Naïve Bayes, and Decision Trees. Among these models, the SVM clas- sifier combined with FastText features achieved the highest accuracy of 89.2 This method has real-world uses in cultural study, content moderation, and mood based music recommendation. By tackling the difficulties of emotion categorization in a low-resource, morphologically complicated language like Kannada, it also advances regional NLP and provides a promising avenue for further study and use.

Keywords: Emotion classification, Kannada song lyrics, FastText embeddings, Machine learning, Support Vector Machines

ICCI202673: Next Word Prediction in Kannada using NLP Techniques

Dixitha V, Nisha Varghese, Sridevi

Department of Computer Science

Christ University

ABSTRACT

Next word prediction is an important natural language processing (NLP) task that improves text input systems by suggesting continuations for incomplete sentences. Even though high-resource language have seen great progress, morphologically rich and underrepresented languages like Kannada still face difficulties because of their large lexical diversity and limited datasets. This work presents an optimized Kannada next word prediction system for a medium-sized dataset of approximately 5,000 sentences. The framework employs a hybrid modelling method that combines a neural architecture build on long short-term memory (LSTM) and attentional mechanisms with advanced preprocessing and tokenization approaches. The architecture allows for strong performance even on limited training data by maintaining a balance between the flexibility of neural networks and the accuracy of statistical methods. The outcomes show that the hybrid model produces inclusive, contextual, meaningful, and varied prediction, consistently outperforming individual strategies. This contribution indicates the potential of hybrid NLP systems in under-resourced languages and advances the related endeavor to create inclusive language technologies at large.

Keywords: Next-word prediction, Kannada, Natural Language Processing (NLP), Hybrid model, LSTM, Attention system, Statistical patterns, Low-resource languages.

ICCI202674: Evaluating Mathematical Reasoning Capabilities of Large Language Models in Malayalam: A Study on Low-Resource Indic Language Performance

Elwin Roy[1], Nisha Varghese[2], Sridevi R[3], Vikram Vincent[4], Ashok Immanuel[5]

[1,2,3,5]Department of Computer Science

[1,2,3,5]Christ University,

[4]Freethought Labs Pvt Ltd

Bangalore, India

ABSTRACT

Abstract— Large Language Models (LLMs) have demonstrated remarkable abilities in mathematical reasoning tasks, especially in high-resource languages such as English. However, their performance in under-resourced Indian languages remains largely unexplored. This paper comprehensively assesses mathematical and logical abilities in Malayalam, a morphologically rich Dravidian language spoken by more than 35 million people. Translated from English sources, we created a curriculum-adjusted dataset of mathematical problems spanning grades 6-9, and evaluated the performance of the Mistral-7B-Instruct model. The overall accuracy of our model is only 35%, which is a significant drop from average English benchmarks. We find, through fine-grained error analysis, that the most common sources of failure are 18% due to translation ambiguity, 28% due to logical breakdown, and 25% due to illusory reasoning. The results suggest that more native datasets and a particular approach to mathematical logic will be required, especially for educational purposes in local languages and low-resourced languages.

Keywords: Large Language Models, Chain-of-Thought, Multilingual NLP, Educational AI, and Mistral-7B

ICCI202675: HAPCA: A Hybrid Adaptive PCA Framework for Structure-Aware Dimensionality Reduction in Vision Transformer Embeddings

Jesvin K Justin[1], Nisha Varghese[2], Sridevi R[3]

Department of Computer Science

Christ University

Bangalore, Karnataka – 560029

ABSTRACT

Abstract—Vision Transformer (DeiT) embeddings have strong inter-feature correlation, rendering global linear reduction schemes like PCA non-ideal. This paper presents Hybrid Adaptive PCA (HAPCA), a novel structure-informed dimensionality reduction system combining spectral clustering and adaptive local PCA. HAPCA identifies correlated feature clusters automatically through Laplacian eigengap analysis and applies variance-preserving PCA on each cluster. Evaluated on a garbage image dataset with DeiT features and XGBoost, HAPCA reduced reconstruction error by approximately 50% and raised classification F1-score to 0.9103 from 0.9006, a statistically significant gain (95% CI [0.0061, 0.0231]). The Laplacian spectrum also indicated the presence of two intrinsic correlation groups, which indicate the flexibility of the approach. Even though global PCA is still optimal under the least-squares sense, HAPCA generated more discriminative downstream task representations, which suggests it can be used as a scalable, transformer-aware dimension-reduction method.

Keywords: Hybrid Adaptive PCA (HAPCA), Vision Transformer (DeiT), PCA, Dimensionality Reduction, Spectral Clustering, XGBoost, Feature Correlation, Transformer Embeddings, Structure-Aware Learning, Machine Learning, Image Classification.

ICCI202676: Evaluating Mathematical Reasoning in Regional-Language LLMs: An Analysis of Class 10 to 12 Problem-Solving in Malayalam

Ashik Antoo[1], Nisha Varghese[2], Sridevi R[3], Vikram Vincent[4], Ashok Immanuel[5]

[1,2,3,5]Department of Computer Science

[1,2,3,5]Christ University,

[4]Freethought Labs Pvt Ltd

Bangalore, India

ABSTRACT

The study discusses the reasoning of a Malayalam Large Language Model (LLM) on higher secondary (Classes 10, 11 and 12) mathematics problems. Although the performance in earlier testing was only partially at the elementary level in arithmetic, more advanced subjects like algebra, trigonometry, calculus, and coordinate geometry present a symbolic load and require more problematic demands on regional-language LLMs than multi-step reasoning. We test the outputs of the Malayalam textbook-aligned model on a battery of tasks. The findings indicate that they had genuine gaps in reasoning (permanent), lack of comprehension of the symbolic phrases, and failure to sustain the reasoning process in the derivation stages. Considering these results in the light of the current state-of-the-art prompting systems, we highlight the structural weakness of the current Malayalam LLMs and indicate the way towards multilingual fine-tuning and combining symbolic and neural approaches.

Keyword: Mathematical Reasoning, Regional-Language LLMs, MathPrompter, Hint-based prompting, Symbolic Reasoning.

ICCI202677: Collision Prediction Using Small Language Models on Edge Devices for Autonomous Vehicles

Pratham Jain, Nisha Varghese, Sridevi R
Dept. of Computer Science
CHRIST (Deemed to be University)
Bengaluru, Karnataka

ABSTRACT

Autonomous vehicle safety depends on collision prediction, but conventional rule-based and computer vision methods suffer from limited generalization and a lack of data. In this work, the use of Small Language Models (SLMs) for scenario-based collision risk prediction is examined. We propose a novel approach that represents multi-modal sensor data as structured natural language and fine-tune Microsoft's Phi-3.5- mini-instruct model (3.8B parameters) using parameter-efficient LoRA on 200 synthetic traffic scenarios. Evaluated across 600 varied test cases, our model hits 96% accuracy overall – spotting high-risk situations flawlessly, hitting full precision and recall - beating baseline approaches by 15.5 times. Running on just 0.55 GB RAM, it works right on edge devices.This work establishes SLMs as a data-efficient, interpretable alternative to conventional collision prediction systems, even though the current latency (824.58 ms) needs to be optimized for real-time use. To enable reproducible research in LLM-based autonomous systems, all models and code are made publicly available as open-source.

Keywords: Autonomous Vehicles, Collision Prediction, Small Language Models, Fine-Tuning, Phi-3.5-mini-instruct, Risk Assessment, Safety-Critical Systems, Low-Rank Adaptation (LoRA), Transfer Learning, Edge Computing

ICCI202678: A Systematic Mapping of Cybersecurity Tools To Adversary Attack Phases with a Web Based Prototype

Dhanush R
Student, Department of forensic science ,
Kristu Jayanti Deemed to be university, India

ABSTRACT

It is a challenge to cybersecurity practitioners to use the security tools in the market due to the large number of over 100 solutions at any given moment when an incident has occurred that should be managed within a limited period. The current paper addresses this issue with a critical literature review, in particular, and systematic mapping of the wide range of tools to fight cybercrime open-source and proprietary ones, to the phases of the attack life cycles by offenders. According to the sound mixed method design science methodology, the research paper is based on the systematic analysis with the design of the fully operational no code web prototype, basing on HTML, CSS, and JavaScript. The system has an easy user interface, which is sorted alphabetically, and the threat-tools correlations validated, which allows the informed and fast decisions on the tool to be used. The deployable artifact is to serve the requirements of students, academic researchers, and security professionals, help reduce cognitive load, accelerate the process of incident response, and enhance decision-making efficiency when it comes to Security Operations Center and the digital forensics context. This work is a useful practical tool that can help with education, threat inquiry and operational defense by bridging the disconnect between ideas of cybersecurity and practical applications of those ideas in tools. This shall produce an authenticated prototype, an official taxonomy of tool-threat alignment, and applicable recommendations that will together address the extant voids in tool recommendation systems, and consequently make a contribution to the art of cybersecurity training and research.

Keywords: Cybersecurity tools, Attack lifecycle mapping, Incident response, Web-based prototype, Digital forensics

ICCI202679: Autonomous AI Agents: Scaling Secure Enterprise Systems

Dinesh G,
Student, Department of physical science,
Kristu Jayanti Deemed to be University, Bengaluru, Karnataka.

ABSTRACT

The rise of autonomous Artificial Intelligence (AI) agents is transforming the management and operation of enterprise AI infrastructures by enabling systems that can independentlyperceive, reason, and act across distributed environments with minimal human oversight. This research integrates recent advances in modular agent frameworks, multi-agent coordination, and agentic business automation to propose a unified, scalable, and resilient approach to enterprise AI. Key capabilities such as dynamic resource allocation, real-time fault recovery, adaptive decision-making, and enhanced cybersecurity position autonomous agents as foundational components of next-generation systems. Multi-agent architectures, through task partitioning and collaboration, enhance performance and reliability in complex workflows, effectively addressing diverse enterprise demands. To ensure trust, privacy, and regulatory compliance, this work explores security frameworks tailored for distributed agent ecosystems. Lifelong learning and decentralized coordination promote adaptability and robustness, while dynamic role discovery supports flexible task management in evolving operational contexts. Additionally, foundational protocols for agent infrastructure enable coherent context sharing and governance, ensuring transparency and accountability. This comprehensive framework offers actionable strategies for leveraging autonomous agents to drive operational efficiency, innovation, and sustainability. It bridges theoretical developments with practical applications and presents a forward-looking roadmap for enterprises pursuing AI-driven transformation.

Keywords: Artificial Intelligence, Multi-agent Systems, Decision-making, Reinforcement Learning

ICCI202680: Smart Traffic Signal System For Ambulance Prioritization Using Iot And Ai

P Preethika[1], Aishwarya Pramod Mahadevan[2], Dinesh C[3], Aanchal Verma[4]

Student,Department of computer science,

Kristu Jayanti Deemed to be University

ABSTRACT

Traffic in the major Indian cities has become a menace for emergency medical services, particularly ambulances. Late arrival of ambulances frequently amount to a critical loss of life, since in medical emergency like road trafficaccident, trauma and cardiac arrest immediate attention is mandatory. Here in this study, we propose smart traffic signal prioritization-based system that employs the IoT and AI technologies for automatic ambulance detection and offer priority clearance at road junctions.

The solution is built on the AI-based computer vision model that analyses real-time video feeds from IOT-enabled cameras mounted at traffic junctions. The model recognizes ambulances based on different visual cues, such as patterns of emergency lights, the vehicle body and medical inscriptions. When an ambulance is identified, IoT controller sends a communication to the traffic signal controller and takes control over normal cycle and provides a green corridor for smooth flow.

The proposed architecture comprises edge processing for near real-timedetection, cloud based data logging capabilities for monitoring and analysis, as well as reliable communication protocols to cater the dense traffic conditions inIndia. The system is intended to shorten ambulance response time, eliminate manual traffic control and improve efficiency of emergency healthcare. The paper presents the design of the system, flows of methodology, and validation through survey limitations and anticipated impacts with introduction to Indian metro cities where scope for application is immense.

Keywords: Smart traffic signals, Ambulance prioritization, Internet of Things (IoT), Artificial intelligence, Computer vision

ICCI202681: Ghost Data: Representational Inertia and the Quest for Verifiable Forgetting in Modern Artificial Intelligence

Dr Divya K S[1],Tejashree S[2]

[2]Student, Department of computer science,
Kristu Jayanti Deemed to be University

[1]Assistant Professor, Department of computer science,
Kristu Jayanti Deemed to be University

ABSTRACT

Machine learning models increasingly underpin critical decision-making systems and are often trained on large datasets containing sensitive or regulated information. In response to data protection frameworks such as the General Data Protection Regulation (GDPR) and its "right to be forgotten," organizations commonly assume that deleting specific data from training sets and retraining models is sufficient to erase its influence. This study critically examines that assumption by investigating whether deleted data can continue to exert residual influence on trained models, a phenomenon referred to as ghost data. Using a controlled experimental setup with a neural network trained on the MNIST dataset, selected data segments were removed and the model retrained via fine-tuning. Itsbehavior was then compared with a model trained entirely from scratch on a sanitized dataset. The analysis focused on behavioral divergence, output bias, and internal activation patterns. The results indicate that fine-tuned models retain subtle yet measurable traces of deleteddata, visible through persistent internal representations and biased decision tendencies. These findings demonstrate that forgetting in machine learning is not necessarily absolute. This work highlights a critical gap in current data deletion practices and underscores the need for robust, verifiable machine unlearning mechanisms to ensure ethical, secure, and regulation-compliant AI systems.

Keywords: Machine unlearning, Ghost data, Verifiable forgetting, Neural networks, Data protection regulations

ICCI202682: Autonomous Delivery Robot for Smart Urban Mobility - Routbotix

Abdur Raheem N[1], Amjad Hassan Khan MK[2] , Aswin Herbert Sathish R[3],Joel Shibu Daniel[4]

[1,2,4]Department of Physical sciences, Kristu Jayanti Deemed to be University

[3]Department of Computer science (UG), Kristu Jayanti Deemed to be University

ABSTRACT

Routbotix is an autonomous ground delivery robot developed to address short- distance last-mile logistics challenges commonly seen in Indian cities and organizational environments. Many delivery operations take place within restricted areas such as apartments, campuses, tech parks, and corporate facilities, where using two-wheelers is inefficient, expensive, and environmentally unsustainable. To tackle this, Routbotix integrates a Raspberry Pi as the primary controller and an ESP32 microcontroller for real-time motor and sensor operations. The robot employs LiDAR, GPS, IMU, ultrasonic sensors, and onboard imaging toachieve reliable navigation, mapping, and obstacle avoidance in unstructured Indian terrains. A connected mobile/web application enables users to place delivery requests, while an admin dashboard manages robot assignment, status monitoring, and fleet coordination. The robot validates handovers through an OTP/QR-secured cargo bay and autonomously returns to base upon task completion. By replacing short-radius bike-based deliveries, Routbotix reduces traffic congestion, fuel consumption, emissions, and operational inefficiencies. The system demonstrates a scalable, cost-effective approach to autonomous local logistics tailored to Indian infrastructure and suitable for both urban and organizational use, contributing to cleaner, safer, and more efficient mobility ecosystems.

Keywords: Routbotix, Raspberry Pi, LiDAR, GPS, IMU

ICCI202683: AI scam detection system

Varunesh H N[1], Prof. Don caeiro[2]

[1]Student,Department of forensic science

Head, Department of forensic science,

Kristu Jayanti Deemed to be University

ABSTRACT

The widespread use of digital communication platforms has resulted in a growing number of scam messages, including deceitful job offers, online payment scams, impersonation messages, and account-related threats. Traditional spam detection techniques mainly depend on fixed keyword matching, which often fails to identify advanced scams that use subtle wording, psychological manipulation, and constantly changing patterns. This projectproposes a multi-layer scam message detection system that integrates rule-based logic with Large Language Model (LLM) analysis to enhance detection effectiveness. In the first stage, predefined rules and regular expressions are used to detect well-known scam categories such as OTP misuse, UPI fraud, job-related scams, unsafe links, and impersonation attempts. Messages that are not clearly identified are then processed by an LLM, which analyzes the context, intent, urgency, and linguistic behavior of the message. A risk scoring mechanism combines signals from both layers to decide whether a message should be classified as spam. This hybrid design improves accuracy, minimizes false negatives, adapts to emerging scam strategies, and is suitable for practical real-world deployment.

Keywords: AI scam detection, Fraud message analysis, Large language models, Cyber fraud prevention, Risk scoring systems

ICCI202684: Students' Perceptions of the Impact of Generative AI Tools on Learning and Creativity

Dr.Divya K S[1], Navya D[2], Raksha B H[3], Aiman Baig[4]

[1]Assistant Professor, Department of computer science,
Kristu Jayanti Deemed to be University
[2,3,4]Student,Department of physical science,
Kristu Jayanti Deemed to be University

ABSTRACT

As Generative AI tools such as ChatGPT, Gemini, and Copilot have become increasingly integrated into higher education, empirical evidence regarding students' perceptions of their impact on academic development and creative thinking in the Indian context remains limited. To address this gap, the present study employed a primary quantitative survey of 100 undergraduate and postgraduate students. AI usage patterns were conceptualized as the independent variable, while perceived effects on Cognitive Engagement, Deep Learning, and creative output were treated as dependent variables. Additionally, drawing on the framework of Effort-Efficiency Tension, the study examined how disciplinary backgrounds and ethical attitudes shape students' actual academic behaviour. Results indicated strong overall student support for Generative AI, particularly for its role in improving task efficiency and facilitating comprehension of complex academic concepts. However, perceptions of creativity were mixed; although many participants reported using AI for brainstorming and idea generation, a substantial proportion expressed concerns about reduced originality and intellectual dependency. The findings also revealed a clear Disciplinary Gap, with technical and non-technical students using AI for distinct academic purposes. Furthermore, a significant Awareness-Behaviour Gap emerged: although 90% ofrespondents were knowledgeable about academic integrity policies, approximately one-third admitted to a pragmatic reliance on AI that diminished personal effort. This illustrates a Pragmatic Paradox in which efficiency often takes precedence over ethical commitment. Collectively, these findings highlight the need for discipline-specific guidelines to ensure that Generative AI supports, rather than replaces, independent learning.

Keywords: Generative AI, Student perceptions, Learning outcomes, Creativity, Academic integrity

ICCI202685: E-Chimp-Vanet: A Predictive, Stability-Aware Chimp Optimization Framework Foremergency Message Dissemination In Next-Generation Vanets

Mr. S. Balasubramani[1], Dr. Shiva Prasad M S[2], Dr. R Karthik[3]

[1,2]Assistant Professor, Kristu Jayanti University, Bengaluru.

[3]Assistant Professor, Sri Krishna Adithya College of arts and Science Coimbatore.

ABSTRACT

The upcoming transport system is dependent upon fast vehicle message systems capable of predicting dangers in an instant. Rather than waiting, cars alert each other in an instant. The older VANET scheme does not work when traffic is dense or in disarray. Due to network dynamics, paths change very frequently. For self- driving vehicles, smarter connections are required during abrupt changes in traffic flow. To address these challenges, this work introduces the CHIMP-VANET model a clustering model using an optimized CHIMP strategy to predict changes while giving priority to stability. Unlike strategies limited to using present network information without predicting changes or giving sufficient priority to path stability through network edges in connection reliability evaluation, this strategy combines predicted locations information with network edges support regarding network connections reliability evaluation coupled with weight changes based on vehicle density - therefore facilitating smarter CH Heads election suitable for stable performance even during high-speed traffic changes. A hybrid dataset - combining true SUMO movement traces collected from traffic simulations with predicted paths using an AI strategy - is used in this work using an optimized version of an NS- 3 network simulator realizing an integrated 5G NR side link; in this scenario, the performance of E-CHIMP- VANET surpasses existing schemes using strategies driven by Particle Swarm Optimization as well as traditional schemes. Performance analysis demonstrates nearly 24% improvement in message delivery ratios, an average of 43% increase in end-to-end delays reduced in urgency message transmissions, sustaining clusters nearly 59% longer, besides relevant improvement in network data communication through an increase of about 32% in network communication speed while broadcasting urgent messages. The outcome positively validates this model's effectiveness in self-autonomous transport systems and compatibility within emerging 5G or 6G vehicle networks integrating urgent connectivity within an appropriate communication interval.

Keywords: VANET, E-CHIMP Optimization, Predictive Mobility, Autonomous Traffic, Link Stability Forecasting, 5G-V2X, Edge Intelligence, Emergency Message Dissemination, Metaheuristic Clustering.

ICCI202686: Smart home-remote patient monitoring system using IoT for healthcare

Amjad Hassan Khan MK[1] , Aswin Herbert Sathish R[2] , Abdur Raheem N[3] , Nathan Sam Joseph[4]

[1,3,4]Department of Physical sciences, Kristu Jayanti Deemed to be University
[2]Department of Computer science (UG), Kristu Jayanti Deemed to be University

ABSTRACT

The Internet of Things (IoT) technology connects everything, and it has been dubbed the coming technological revolution.The advancement of technology has enabled the development of Smart Healthcare systems, which can provide remote patient monitoring and healthcare services in Smart Homes .This paper presents a remote patient monitoring system based on the Internet of Things (IoT) for smart healthcare in a smart home. The system consists of a set of sensors, a gateway, and a cloud-based server. The sensors measure vital signs such as heart rate, blood pressure, temperature, and respiration rate, and transmit the data to the gateway. The gateway processes the data and sends it to the cloud-based server. The server stores the data and provides real-time monitoring of the patient's health status. The system also provides an alert system that can notify the doctor or family members in case of an emergency. The system is designed to provide a cost-effective and convenient way to monitor the health of elderlyor chronically ill patients in their homes. The system can also be used to monitor the health of healthy individuals to detect any health issues in the early stages. The proposed system can be used to provide remote patient monitoring and healthcare services in Smart Homes.

Keywords: cloud-based server, gateway, IoT, Patient care, Patient monitoring, sensors, smart healthcare

ICCI202687: Self Supervised Learning for CodeGeneration Models: Mitigating Hallucination and Ensuring Functional Correctness

Dr Prakesh VS[1] , Vigneshwaran Vijayan[2]

[1]Associate Professor, Department of Computer Science, Kristu Jayanti College, Bengaluru

[2]Student, Brunel University of London, United Kingdom

ABSTRACT

Large language models trained on source code are increasingly used for automatic code generation and software assistance. Although these models achieve strong results on standard benchmarks, they often generate code that is syntactically plausible but functionally incorrect, or that conflicts with task requirements and project context. Such hallucinations remain a major obstacle to their reliable use in practice. In this work, we examine this problem from the perspective of self-supervised learning for code models and recent empirical findings on error patterns in LLM-generated code. We review representative code representation models and large code generation models and summarise common hallucination types and bug categories reported in prior studies. Based on these observations, we introduce a lightweight retrieval-augmented, test-driven generation pipeline that grounds model outputs in relevant reference code and filters candidate solutions throughexecution-based verification using unit tests. The proposed framework operates entirely at inference time and does not require additional model training. We evaluate the approach using a structured experimental dataset of Python programming tasks spanning arithmetic, string processing, and data-structure manipulation, and compare a broad set of inference-time strategies. Experimental results show that retrieval improves grounding and reduces incorrect API usage, while execution-based selection further increases functional correctness and mitigates failure modes through selective abstention.

Keywords: Code generation · Large language models · Self-supervised learning · Hallucination mitigation · Functional correctness · Retrieval-augmented generation

ICCI202688: A Hybrid Machine Learning Framework for Multi-Class Anemia Severity Classification

Bal Kiran R[1], Salve Margaret Joseph[2]
Department of Science
Christ Deemed to be University
Pune, India

ABSTRACT

Anemia is a widespread hematologic disorder with varying levels of severity that requires different levels of clinical attention. Although prior machine learning studies have focused primarily on binary anemia detection, severity-aware classification remains underexplored. This study proposes a hybrid machine learning framework for multi-class anemia severity classification using Complete Blood Count (CBC) data. The framework integrates clinically validated rule-based severity labeling with supervised machine learning models to classify anemia into mild, moderate, and severe categories. Hemoglobin is used exclusively for severity labeling and is excluded from the model features to prevent target leakage. Experiments conducted on an extended CBC dataset demonstrate realistic predictive performance, with ensemble-based models achieving superior accuracy while maintaining interpretability. The proposed approach provides clinically significant severity stratification and supports anemia screening in resource-constrained healthcare settings.

Keywords: Anemia Severity, CBC, Hybrid Machine Learning, Multi-Class Classification, Clinical Decision Support

ICCI202689: Deep Feature Engineering for AI-generated Image Classification: A Robust Approach to Detecting Fake Faces

Dr. Gopika S[1] , Ms. Gayathri S[2],Dr. Mary Jacob[3], Dr. K. Kalaiselvi[4]

[1,3,4] Kristu Jayanti Deemed to be University, Bengaluru, India

[2]CDAC , Trivandrum

ABSTRACT

Generative Adversarial Networks have become well-known primarily because of their capability to generate realistic images of human faces. The impressive clarity and detail of images produced in recent years have surpassed humans' capacity to tell the difference between these artificial images and genuine ones. Such images have been recognized for their ability to successfully mislead face recognition systems to some extent. Current developments in forensic systems consider adversarial attacks to establish more thorough detection methods. Various GAN algorithms, including StackGAN and StyleGAN, employ distinct architectures to generate images. Because the methods used differ from each other, it is challenging for any single detection algorithm that is trained on one type of GAN to identify fake images produced by a different type of GAN. In this study, we employ a robust set of features derived from the image that is compatible with a deep learning model to distinguish between fake and real images within a GAN or CASIA V2. 0 dataset. Comprehensive tests have been carried out on the Siamese model to evaluate the efficiency of the suggested method. The findings indicate that the suggested method substantially outperforms current techniques, achieving an accuracy of over 94% in the majority of tests.

Keywords: Digital forensics, deepfake images, image forgery, Siamese triplet loss, AI generated images

ICCI202690: Behaviour-Aware Explainable Artificial Intelligence Framework for Criminal Offender Profiling

Dr.K.Dheenathayalan

Assistant Professor, Department of Computer Science

NIFT-TEA College of Knitwear Fashion, Tirupur

ABSTRACT

In recent years the use of artificial intelligence for criminal offender profiling has grown which at the same time has seen the2 issue of transparency in most predictive models which has not gone away still we have issues with belief in these models, with who is responsible when something goes wrong, and also the ethical play out of these in the criminal justice field. We don\'t see it as sufficient that a model is accurate in criminal justice settings; what we also require is that the model's decisions are also made clear to human stakeholders. That is what this paper sets out to do which is present an Explainable AI based framework in which we look at the behavioural patterns of the offender at risk instead of the dense stats. Also, we put forth a set of behaviour-based features which we get from past offense reports. Recidivism risk is estimated using ensemble-based machine learning models, and explainability techniques are then used to interpret the predictions. These explanations offer both localised explanations for specific offender predictions and global perceptions of important behavioural factors. According to the experimental results, the suggested framework significantly improves model interpretability while achieving competitive predictive performance.

Keywords: Explainable Artificial Intelligence, Criminal Offender Profiling, Recidivism Prediction, Behavioural Analytics, SHAP and LIME.

ICCI202691: Explainable Chronic Kidney Disease Classification Using Hybrid Feature Selection and Machine Learning

K.Varshini[1], K.T.Thomas[2]

Department of Science

Christ Deemed to be University

Pune, India

ABSTRACT

Early identification of Chronic Kidney Disease (CKD) is essential for reducing disease progression and improving patient outcomes. This paper presents a machine learning framework for CKD classification based on hybrid feature selection and explainable predictive modeling. A two-stage feature selection process combining Boruta and Recursive Feature Elimination (RFE) is employed to identify a compact subset of clinically relevant attributes. The selected features are used to train Logistic Regression, Support Vector Machine, Random Forest, and Multi-Layer Perceptron classifiers. Experimental results on the UCI CKD dataset indicate that the Random Forest model achieves an accuracy of 98.72% and a recall of 100%. Model interpretability is enhanced using SHAP-based explainable artificial intelligence, which highlights key biomarkers influencing CKD prediction. Robustness of the proposed framework is further validated through comparative evaluation using baseline and MICE-based imputation strategies. The proposed approach demonstrates that accurate and interpretable CKD diagnosis can be achieved without relying on complex deep learning architectures.

Keywords: Chronic Kidney Disease, Hybrid Feature Selection, Boruta, RFE, Random Forest, Explainable AI, SHAP

ICCI202692: Sectoral Volatility Analysis of the Indian Stock Market During Indo-Pak Conflicts Using GARCH Model

Kiran Kumar[1], Dr. Avichal Sharma[2]

School of Sciences

CHRIST (Deemed to be University)

Pune - Lavasa, India

ABSTRACT

Geopolitical events introduce sudden uncertainty into financial markets, often resulting in abrupt changes in investor behavior and heightened market volatility. This study ex- amines the event-wise sectoral response of the Indian stock market to major geopolitical incidents, including the Mumbai attack, Uri attack, Pulwama attack, and the Pahalgam incident. Sectoral indices representing the FMCG, Oil and Gas, and Defence sectors are analyzed using an event study framework with a symmetric trading window around each event. Exploratory analysis based on price trends, return dynamics, and volatility proxies is conducted to identify heterogeneous sectoral reactions. To formally capture time-varying volatility and volatility persistence, the Generalized Autoregressive Conditional Heteroskedasticity (GARCH) model is employed. The study constructs event-aligned datasets suitable for GARCH-based volatility modeling, providing insights into sectoral resilience and sensitivity under conditions of geopolitical stress.

Keywords: Event study, sectoral indices, geopolitical events, stock market volatility, Indian financial markets

ICCI202693: Energy-aware and trust-based secure routing in manets using Qos & Load Aware techniques

Mrs.Manju V[1], Dr.P.Sumathi[2]

[1]Research Scholar, [2]Associate Professor

PG and Research Department of Information Technology Governments Arts College, Coimbatore, India

ABSTRACT

This paper introduces a novel cross-layer federated learning (FL)-based clustering protocol, termed designed to support multicast routing in IoT-enabled mobile ad hoc networks (MANETs) integrated with Adaptive Energy-QoS Optimization Framework (AEQOF) systems. The proposed AEQOF algorithm combines cross-layer optimization with federated learning to improve network stability and connectivity through efficient cluster head (CH) selection and cluster formation. The cross-layer framework exploits physical-layer parameter including node mobility (speed and direction), location, channel capacity, and residual energy together with network-layer connectivity information to maximize a unified cost function for clustering decisions. Federated learning is employed to enhance clustering intelligence while meeting the demands of future mobile networks. During the CH selection phase, FL performs a classification task to determine suitable nodes for CH or cluster member (CM) roles. In the cluster formation phase, FL addresses a regression problem by dynamically optimizing the cost-function weights associated with mobility similarity, link quality, residual energy, and channel capacity, enabling each node to select the most appropriate CH. Simulation results demonstrate that the CFLC protocol outperforms existing benchmark schemes in terms of connectivity, scalability, and control overhead. Furthermore, the results reveal superior performance under the reference point group mobility (RPGM) model compared to the random waypoint (RWP) model, underscoring the effectiveness of CFLC in maintaining stable and well-connected MANET topologies. To improve all the performance metrics a new algorithm is introduced AEQOF. To overcome this Adaptive Energy-QoS Optimization Framework (AEQOF) is used.

Keywords: Energy, Load Aware, FL

ICCI202694: An AI-Native Linux Distribution with Integrated Local LLM Assistance for System Interaction and Debugging

George Shaiju[1] , Rishi Naman Singh[2] ,Dr. Sherin Rappai[3]

[1]Student, Kristu Jayanti Deemed to be University, Bangalore

[2]Software Engineer, Caze Labs Pvt. Ltd.

[3]Asst. Prof., Kristu Jayanti Deemed to be University, Bangalore

ABSTRACT

Recent advancements in lightweight large language models have enabled an efficient on-device AI inference, creating opportunities for intelligent system-level assistance without reliance on cloud services. However, current desktop operating systems are lacking native integration of local AI models for real-time user support, system debugging, and task automation. This paper ArchAI, an AI-native Linux distribution built upon Arch Linux and the Hyprland compositor, it is designed to provide a seamless AI-assisted desktop experience. The proposed system integrates a persistent floating AI iconaccessible through a shortcut or on-screen icon, enabling natural language interaction with the operating environment. Users can execute system tasks, receive debugging guidance from real-time log monitoring, and switch or deploy custom local language models according to hardware capability. The architecture emphasizes on modularity, privacy- preserving offline operation, and full user customizability inherent to Linux ecosystems. Experimental evaluation demonstrates reduced troubleshooting time, improved user interaction efficiency, and minimal system overhead. The proposed approach establishes a foundation for next-generation intelligent operating environments that combine open-source flexibility with embedded local AI assistance.

Keywords: On-device AI, Lightweight Large Language Models, AI-assisted Desktop Environment, Arch Linux, Hyprland Compositor, Local AI Inference, System Automation, Privacy-Preserving Computing, Intelligent Operating Systems, Offline AI Assistance

ICCI202695: SIM Centric Analysis of Multi-SIM Android Devices for Mobile Forensic Investigations

Chryselle Christie Gomes[1] , Dr Kalaiselvi K[2]

[1]Student, Department of forensic science ,

Kristu Jayanti Deemed to be university, India

[2]Associate Professor and Coordinator,

Department of Computer Science, Kristu Jayanti(Deemed to be University), Banglore, Karnataka,India

ABSTRACT

As Android smartphones with dual-SIM and multi-SIM features become more common, mobile forensic investigations face new challenges. SIM cards hold important identifiers and telephony data that reveal user behaviour, network ties, and device use. Yet, most forensic methods focus on extracting data instead of analyzing it, and often depend on user-interface indicators that are not reliable as evidence. This research introduces a SIM-focused forensic analysis framework that organizes, standardizes, and connects telephony data from Android devices using non-intrusive methods. The framework works with both single-SIM and multi-SIM devices, allowing slot-specific analysis to avoid confusion about which SIM was used. By using clear, rule-based logic, the approach helps identify forensic signs like inactive or missing SIM slots, multi-SIM use, and possible SIM removal or carrier changes. A snapshot-based temporal analysis mechanism further provides defensible documentation of SIM state at the time of acquisition, while an explainability layer translates technical findings into human-readable forensic interpretations suitable for investigative reporting and legal scrutiny. Initial validation through controlled test scenarios demonstrates the framework's ability to reliably infer SIM configurations and behaviours without reliance on user-modifiable settings. This ongoing research contributes toward bridging the gap between raw SIM artefact extraction and higher-level forensic interpretation in modern mobile investigations.

Keywords: Android forensics, SIM analysis, multi-SIM, telephony data, mobile investigations

ICCI202696: Invasive Brain–Computer Interfaces: Advancements, Challenges, and Societal Considerations

Rathore[1],Jitraj Esh[2],Dr. kalaiselvi[2]

[1,2]Student, Department of Computer Science

[3]Associate Professor and Coordinator,

Department of Computer Science, Kristu Jayanti(Deemed to be University), Banglore, Karnataka,India

ABSTRACT

Invasive brain–computer interfaces (BCIs) record neural signals directly from the cortex,offering high-resolution control signals for digital devices. Neuralink's "Telepathy" N1system exemplifies this approach, using thousands of fine electrode threads implantedwith a robotic inserter. Since its FDA approval for human trials, Neuralink has reportedinitial success in enabling a paralyzed patient to control a computer by thought. This reportexamines Neuralink's technology custom ASICs, flexible polymer threads, and surgicalrobot alongside other invasive BCI platforms such as Blackrock's Utah array, Synchron'sStentrode, and Paradromics' Connexus. Key challenges include neural tissue reactions(gliosis) that degrade signal quality over time, device durability, and safe chronicimplantation. We review the system's current clinical status, potential medicalapplications such as restoring communication and motor function, and advantages overnon-invasive EEG, notably higher signal fidelity. Ethical, regulatory, and societal issues arealso considered, including public sentiment, privacy, and safety standards for neural data.

Keywords: Invasive BCI, Neuralink, neural implants, brain–computer interface, neural recording, neurotechnology

ICCI202697: Users Detection Of Ai Errors And Trust In Ai Outputs

Hiba[1],Shahin[2],A stephen[3]

[1,2]Student,[3]Assistant professor

Department of computer science,

Kristu Jayanti Deemed to be University

ABSTRACT

There is a heavy defiance on Artificial intelligence amongst the modern youth. While AI systems offer efficiency and convenience, they are not immune to errors, users often place high levels of trust in Al-genersted information, raising concerns about over-reliance and reduced critical evaluation. This study examines users'trust in AI outputs and their ability to detect incorrect Al-generated information, with particular attention lo the role of automation bias, familiarity, and user behavior. A quantitative survey-based research design was employed, collecting data from 5D participants with varying levels of AI experience. The questionnaire measured AI usage patterns, trust in AI outputs, error detection ability, verification behavior, and caution in high- risk tasks. The flndlngs reveal that most users Interact with AI systems frequently and exhibit moderate to high trust in Al outputs. However, users do not consistently detect incorrect or misleading AI outputs, with many reporting that they only sometimes notice errors. Subtle and confidently presented errors were especially difficult to identify. The results support existing literature on automation bias nnd the Technology Acceptance t•\odel, demonstrating that increased familiary and perceived usefulness enhance trust whim *imultannounty reducing critical evaluation. Usnr* with highnr Al familiarity nhow'nd 9tightty better error detection abilities, but were not immune to over-reliance. The stucly highlights the need for improved Al transparency, user education, and design strategies that encourage verification rather than blind trust. These findings contribute to research on human—AI interaction and provide practical implications for safer and more responsible AI use.

Keywords: Artificial Intelligence, Automation Bias, User Trust, Error Detection, Human–AI Interaction, Technology Acceptance Model, Over-reliance on AI, Critical Evaluation

Kristu Jayanti (Deemed to be University)

K.Narayanapura, Kothanur, Bengaluru, Karnataka 560077
Tel:080-68737777 | Fax: 080-68737799
E-mail: info@kristujayanti.com
Website: www.kristujayanti.edu.in

[Editorial Team]
Faculty: Dr. Haripriya M P, Dr. Mary Jacob
Student: Sam Benjamin Blessen (23BCAA51), Akshay Sudheesh (24DTSA07)