Call for Participation

We invite you to join us in **International Conference on Computer Science, Information Technology & AI (CSITAI 2023)**

This conference will provide an excellent international forum for sharing knowledge and results in theory, methodology and applications of Computer Science, Information Technology and Artificial Intelligence. The Conference looks for significant contributions to all major fields of the Computer Science, Information Technology and AI in theoretical and practical aspects. The aim of the conference is to provide a platform to the researchers and practitioners from both academia as well as industry to meet and share cutting-edge development in the field.

Highlights of CSITAI 2023 include:

- International Conference on Information Theory and Machine Learning (ITEORY 2023)
- International Conference on Computational Science & Applications (COMSAP 2023)
- International Conference on Information Science and Techniques (ISTECH 2023)
- International Conference on Information Technology, Control and Automation (ITCAU 2023)
- International Conference on Advanced Computational Intelligence (ACINT 2023)

Registration Participants

Non-Author / Co-Author / Simple Participants (no paper)

200 USD (With proceedings)

Here's where you can reach us: **csitai@csitai2023.org** (or) **csitai_conf@yahoo.com**

Accepted Papers

TOMATO DISEASE FUSION AND CLASSIFICATION USING DEEP LEARNING

Patrick Ansah, Sumit Kumar Tetarave, Ezhil Kalaimannan and Caroline John, School of Computer Application, Kalinga Institute of Industrial Technology, India, Department of Cybersecurity, University of West Florida, FL 32514, USA

Abstract
Tomato plants' susceptibility to diseases imperils agricultural yields. About 30% of the total crop loss is attributable to plants with disease. Detecting such illnesses in the plant is crucial to avoid significant output losses. This study introduces "data fusion" to enhance disease classification by amalgamating distinct disease-specific traits from leaf halves. Data fusion generates synthetic samples, fortifying a TensorFlow Keras deep learning model using a diverse tomato leaf image dataset. Results illuminate the augmented model's efficacy, particularly for diseases marked by overlapping traits. Enhanced disease recognition accuracy and insights into disease interactions transpire. Evaluation metrics (accuracy 0.95, precision 0.58, recall 0.50, F1 score 0.51) spotlight balanced performance. While attaining commendable accuracy, the intricate precision-recall interplay beckons further examination. In conclusion, data fusion emerges as a promising avenue for refining disease classification, effectively addressing challenges rooted in trait overlap. The integration of TensorFlow Keras underscores the potential for enhancing agricultural practices. Sustained endeavours toward enhanced recall remain pivotal, charting a trajectory for future advancements.

Keywords
Disease Fusion, Deep Learning Classification, Tomato Leaf Diseases, TensorFlow Keras, Disease Recognition.

Robust Network Anomaly Detection With K-nearest Neighbours (Knn) Enhanced Digital Twins

Peprah Obed Adjei, Sumit Kumar Tetarave, Parthasarathi Pattnayak and Caroline John, School of Computer Applications, Kalinga Institute of Industrial Technology, India, Department of Cybersecurity, University of West Florida, FL 32514, USA

Abstract
This research delves into network anomaly detection by harnessing the power of K-Nearest Neighbours (KNN) within Digital Twins. The study capitalizes on the remarkable performance of the model, characterized by impeccable precision, recall, and F1-score, as indicated by the classification report. The confusion matrix further highlights the model's robustness, showcasing minimal Type-I and Type-II errors. The research aims to amplify the robustness and adaptability of KNN-based Digital Twins dedicated to network anomaly detection. The exploration encompasses dynamic learning mechanisms for real-time adaptation, extension to edge computing environments, multi-modal data fusion for comprehensive insights, and resilience against adversarial attacks. The proposed continuous evaluation framework ensures the model's perpetual relevance, while integrated explainability tools provide transparency in decision-making for network administrators. Cross-domain generalization is scrutinized to assess the model's adaptability to diverse network landscapes. This research underscores the potential of KNN-enhanced Digital Twins as a potent tool in the network security arsenal, paving the way for reliable and agile anomaly detection across various domains and network environments.

Keywords
Network Anomaly Detection, K-Nearest neighbours (KNN), Digital Twins, Robustness and Adaptability.

AI-empowered Learning Models in Economy 5.0: Fostering Meaning Creation Beyond Literacy

Tabea Hirzel, Independent Researcher & Educator, Department of Culture/ Founder & Developer, Learning4Tech, Tomelloso City Council, Ciudad Real, Spain

Abstract
Economy 5.0 signifies a transformative era with profound implications for human development and education. This article examines emerging learning models underpinning Economy 5.0, exploring their impact on politics, personal growth, and global education ecosystems. The paradigm shift in economic evolution prompts a reevaluation of the nexus between politics and personal development, with learning acting as a catalyst for societal and individual transformation. A global perspective on AI in education policies underscores the geopolitical significance of AI-related technologies, reshaping knowledge dissemination through innovative learning platforms and Learning DAOs. Blockchain-based Agile Learning DAOs (BALD) are introduced as a mechanism that revolutionizes content creation with transparency and ethical considerations. Ethical learning, privacy, and addressing information bias emerge as central themes, with AI enhancing personhood. The roles of educators as guides remain pivotal. The future of learning in Economy 5.0 necessitates a balanced partnership between humanity and technology, grounded in ethics and human potential.

Keywords
Economy 5.0, Learning models, Machine learning, Ethical learning, Technology in education.

Securing Llm-integrated Applications: a Novel Evaluation Framework to Measure Prompt Injection Attack Resilience

Daniel Wankit Yip, Aysan Esmradi and Chun Fai Chan, Logistics and Supply Chain MultiTech R&D Centre, Level 11, Cyberport 2, 100 Cyberport Road, Hong Kong

Abstract
Prompt injection attacks exploit vulnerabilities in Large Language Models (LLMs) to manipulate the model into unintended actions or generate malicious content. As LLM-integrated applications gain wider adoption, they face growing susceptibility to such attacks. This study introduces a novel evaluation framework for quantifying the resilience of applications. To ensure the representativeness of simulated attacks on the application, a meticulous selection process was employed, resulting in 115 carefully chosen attacks based on coverage and relevance. For enhanced interpretability, a second LLM was utilized to evaluate the responses generated from these simulated attacks. Unlike conventional malicious content classifiers that provide only a confidence score, this approach produces a score accompanied by an explanation, thereby enhancing interpretability. Subsequently, a resilience score is computed by assigning higher weights to attacks with greater impact, thus providing a robust measurement of resilience. Overall, the framework empowers organizations to make well-informed decisions against potential threats.

Keywords
Large Language Model, Prompt Injection, Cyber Security.

A Comprehensive Survey of Attack Techniques, Implementation, and Mitigation Strategies in Large Language Models

Aysan Esmradi, Daniel Wankit Yip and Chun Fai Chan, Logistic and Supply Chain MultiTech R&D Centre (LSCM)

Abstract
Ensuring the security of large language models (LLMs) is an ongoing challenge despite their widespread popularity. Developers work to enhance LLMs security, but vulnerabilities persist,

even in advanced versions like GPT-4. Attackers exploit these weaknesses, highlighting the need for proactive cybersecurity measure in AI model development. This article explores two attack categories: attacks on models themselves and attacks on model applications. The former requires expertise, access to model data, and significant implementation time, while the latter is more accessible to attackers and has seen increased attention. Our study reviews over 100 recent research works, providing an in-depth analysis of each attack type. We identify the latest attack methods and explore various approaches to carry them out. We thoroughly investigate mitigation techniques, assessing their effectiveness and limitations. Furthermore, we summarize future defences against these attacks. We also examine real-world techniques, including reported and our implemented attacks on LLMs, to consolidate our findings. Our research highlights the urgency of addressing security concerns and aims to enhance the understanding of LLM attacks, contributing to robust defence development in this evolving domain.

Keywords
Large Language Models, Cybersecurity Attacks.

User-centric Privacy Control in Identity Management and Access Control Within Cloud-based Systems

Kelvin Ovabor and Travis Atkison, Department of Computer Science, University of Alabama, USA, Department of Computer Science, University of Alabama, USA

Abstract
The ability to effectively implement user-centric privacy controls in cloud-based identity access management (IAM) systems is crucial in today's age of rapidly rising data and increased privacy concerns. The study tackles the scalability issue inside cloud-based IAM systems, where user-centric privacy controls are paramount. The study aims to guarantee effective system performance despite growing numbers of users and data items by following a carefully crafted approach that uses user- centric privacy algorithms. The findings are expected to increase scalability while maintaining security and user privacy, significantly improving current cloud security and IAM techniques. This study provides significant findings for businesses adapting to the changing environment of cloud-based access and identity management, enhancing the security and privacy aspects of the online environment.

Keywords
Cloud-based System, Identity Management, Access Control, Security, user-centric privacy.

The Impact of Ai on the Future of Tech-entrepreneurship

Heena Sah , Abeba N. Turi, University Canada West, Northeastern University, Canada

Abstract
The boom in Artificial Intelligence has had several impacts on tech businesses globally. Technology-driven startups have catalyzed their future road maps by implementing AI systems that are fair, comprehensible, reliable, and secure to grow business productivity in the next few years. This study examines the effects of AI on the transformation of tech-entrepreneurship careers and on-demand technical skills for achieving career purposes and tasks, providing a competent approach to the tech industry in the rapidly involving digital landscape. It also identifies the role and impact of business intelligence software/applications on tech ecosystems in next-gen tech entrepreneurship. The studyasserts that the rapidly growing AI-driven businesses require revolutionary tech ecosystems and receptive tech-literate entrepreneurs with robot-resistant skills who excel in the opportunities brought by AI technologies beyond the threat.

Keywords
Tech Industry, Tech Entrepreneurship, Artificial Intelligence, Business Intelligence, Next Generation, Education, AI Talent.

Equipping Small and Medium Scale Companies (Smsc) Through Open Innovation- a Refined Proof of Concept and Oi Redesign for Strategic Implementation

Fernando Ferreira Fernandez and Abeba N. Turi, University Canada West, Vancouver, British Columbia, Canada

Abstract
This study presents a novel approach to Open Innovation (OI) as it applies to small and medium companies (SMSCs) suffering from multilayer constraints to benefit from such a collective tech value creation model. Building on the decades-long practice of OI, the chapter looked into the model's evolution, development, and application constraints for the SMSCs and presented a refined concept note that meets the dynamic business and tech environment. Based on this, an OI model that encompasses different stakeholders is designed. The proposed IO model that applies to the SMSCs is built on the Consortium model principles that enable ease of entry and exit for each stakeholder, keeping members' best interest for the common good.

Keywords
Open Innovation, Small and Medium Scale Companies, Collaborative Research, Disruptive Technology, Competitive Differential

Unshuffle Sort and Ideal Merge

Art S. Kagel, ASK Database Management Corp. 222 Dunhams Corner Road East Brunswick, NJ 08816

Abstract
In this paper the author describes a unique data sort algorithm, Unshuffle Sort, and a new algorithm for the merging of multiple sorted sinks, Ideal Merge. Unshuffle is a distribution sort in two phases. Optimizing the second phase resulted in the development of an algorithm for the merge of sorted sinks of which the author has found no previous description and which can be shown to be the best possible. Unshuffle can be shown to a highly efficient sort when applied to real world data sets which are seldom truly random. Unique features of Unshuffle include: Performs no exchanges Can be applied to unusual set sources including arrays, linked lists, and streaming data Can begin to supply sorted output to consumers expecting streaming data immediately upon the arrival of the final input element The Ideal Merge will be shown to be the most efficient algorithm for merging multiple sorted sinks.

Keywords
Sorting, Merging, Distribution Sort

Integrating and Evaluating Initial Computational Thinking Knowledge in an Undergraduate Marine Science Course

Dana Christensen, Department of Natural and Mathematical Sciences, USA

Abstract
Students in undergraduate marine science courses spend time sampling in the field and are expected to draw conclusions from the data they collect. Computational thinking (CT) supports students in navigating these new experiences. Previous CT frameworks were the foundation we

used to develop an intervention for the marine science department at a liberal arts University in the Mid-Atlantic U.S. through the lens of science education research. This intervention incorporates discipline specific content, mathematical principles and computational thinking constructs. Objectives for each of the 6 lessons are supported by unique marine science data sets, topics and skills selected by the faculty at the University. The intervention was distributed to all students enrolled in introductory marine science classes to supplement their lab (N = 67). We developed two assessments to quantitatively assess student progress on: (1) marine science based quantitative skills and (2) CT knowledge. Student artifacts for each lesson are scored with a standard rubric to supplement the pre- and post-test results. Marine science education research is scarce, especially around interventions and assessment focused on CT. Our research has many applications due to the inquiry-based laboratory components that use quantitative skill to understand nature. Our current research addresses initial student scores of (1) marine science quantitative skills as well as (2) CT knowledge. Future implications support how abstraction, emergence, scale levels and interdisciplinarity may be emphasized through CT.

Keywords
Science Education, Computational Thinking, Inquiry Based Learning, Integrated Learning & Marine Science.

Predictive Analytics-based Evaluation of Performance of Public Bus Transportation San Antonio, Texas as a Case Study

Izzat Alsmadi and Mohammad Al-Ramahi, Department of Computing Science, Texas A&M University, San Antonio, USA, Department of Accounting and Finance, Texas A&M University, San Antonio, USA

Abstract
This paper gives complete guidelines for authors submitting papers for the AIRCC Journals. Citizens in large cities utilize public transportation as an alternative to self-driving due to several reasons such as avoiding traffic congestion, parking costs and utilize their time for other things, (e.g. reading a book, or responding to emails). While large cities provide public transportation as services to their citizens, yet they need to consider optimizing their budget and ensure that public transportation is available and reliable. Using our case study, public bus transit system in the city of San Antonio, Texas, in this paper, we used predictive analytics models to evaluate performance of public bus transportation. We used time point stops as the target variable in order to evaluate their impact on the overall performance of the system. We also evaluated methods for the detection of protentional bus-time savings and reported several examples of possible saving.

Keywords
Predictive analytics, GTFS, Transportation intelligence.

Making Artificial Intelligence Talk Business: a Review of Critical Success Factors for Generative Ai Integration in Companies

Simone Malacaria, Michele Grimaldi, Marco Greco and Andrea De Mauro, Department of Enterprise Engineering, University of “Tor Vergata”, Rome, Italy, Department of Civil and Mechanical Engineering, University of Cassino and Southern Lazio, Cassino, Italy, Department of Enterprise Engineering, University of “Tor Vergata”, Rome, Italy

Abstract
Generative AI applications offer transformative potential for business operations, yet their adoption introduces substantial challenges. This paper utilizes the CBDAS data maturity model to pinpoint pivotal success factors for seamless generative AI integration in businesses. Through a

comprehensive analysis of these factors, we underscore the essentials of generative AI deployment: cohesive architecture, robust data governance, and a data-centric corporate ethos. The study also highlights the hurdles and facilitators influencing its implementation. Key findings suggest that fostering a data-friendly culture, combined with structured governance, optimizes generative AI adoption. The paper culminates in presenting the practical implications of these insights, urging further exploration into the real-world efficacy of the proposed recommendations.

Keywords
Artificial Intelligence, Generative AI, Analytics, Maturity Model, Big Data.

Analogical Proportions and Creativity - a Preliminary Study

Stergos Afantenos, Henri Prade and Leonardo Cortez Bernardes, Institut de Recherche en Informatique de Toulouse (IRIT), Université Paul Sabatier,118 route de Narbonne, France

Abstract
Analogical proportions are statements of the form " is to as is to", which expresses that the comparisons of the elements in pair (,) and in pair (,) yield similar results. Analogical proportions are creative in the sense that given 3 distinct items, one can calculate the representation of a fourth item (distinct from the previous items) that forms an analogical proportion with them, provided certain conditions are met. After providing an introduction to analogical proportions and their properties, the paper reports the results of an experiment made with a database of animal descriptions and their class, where we try to "create" new animals from existing ones, retrieving rare animals such as platypus. Descriptions of animals use either Boolean features, or word embeddings.

Keywords
Analogical inference, analogical proportion, creativity.