Call for Participation

We invite you to join us in **2nd International Conference on Computer Science, Engineering and Information Technology Trends (CSEITT 2024)**

This conference will provide an excellent international forum for sharing knowledge and results in theory, methodology and applications of Computer Science, Computer Engineering and Information Technology Trends. 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 fields.

Highlights of CSEITT 2024 include:

- 5th International Conference on Electrical Engineering (ELEG 2024)
- 2nd International Conference on Blockchain and Applications (BLKCA 2024)
- 2nd International Conference on Machine Learning and IoT (MLIoT 2024)
- 2nd International Conference on Computer Graphics, Animation & Signal Processing (CGASP 2024)
- 2nd International Conference on Vision and Computational Intelligence (VCOI 2024)
- 2nd International Conferences in Clinical Research and Pharmaceutical Sciences (CRPS 2024)
- 5th International Conference on Applied Control, Electrical and Electronics Engineering (CEEE 2024)
- 5th International Conference on Mechanical Engineering (MECN 2024)

Registration Participants

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

100 USD (With proceedings)

Here's where you can reach us: **cseitt@cseitt2024.org (or) cseittconf@yahoo.com**

Accepted Papers

THE NEEDED BRIDGE CONNECTING SYMBOLIC AND SUB-SYMBOLIC AI

Maikel Leon, Department of Business Technology, Miami Herbert Business School, University of Miami, Florida, USA

ABSTRACT

Innovations that combine the interpretability of symbolic AI with the learning capabilities of sub-symbolic AI can flourish in the nexus of symbolic and sub-symbolic AI. This research presents Fuzzy Cognitive Maps (FCMs). This hybrid model combines the best features of both paradigms as a workable answer to the problems of interpretability and explainability in artificial intelligence (AI) systems. FCMs have become a robust framework for logically and intuitively supporting decision-making processes and expressing causal information. A more organic and adaptable problem-solving approach is made possible by FCMs' ability to manage the inherent ambiguity and uncertainty present in real-world situations. Because of their innate flexibility and ability to learn and adapt from sub-symbolic AI, FCMs are an excellent fit for applications requiring high interpretability and explainability.

KEYWORDS

Fuzzy Cognitive Maps, Symbolic AI, and Sub-symbolic AI.

BIG DATA, BIG TECH AND PERSONAL INFORMATION. HOW SECURE ARE WE?

KLODIAN LIPA

ABSTRACT

Protecting personal information privacy has become a controversial issue among online social network providers and users. Most social network providers have developed several techniques to decrease threats and risks to the users' privacy. These risks include the misuse of personal information which may lead to illegal acts such as identity theft. This study aims to measure the awareness of users on protecting their personal information privacy, as well as the suitability of the privacy systems which they use to modify privacy settings. Survey results show high percentage of the use of smart phones for web services but the current privacy settings for online social networks need to be improved to support different type of mobile phones screens. Because most users use their mobile phones for Internet services, privacy settings that are compatible with mobile phones need to be developed. The method of selecting privacy settings should also be simplified to provide users with a clear picture of the data that will be shared with others.

KEYWORDS

Smart Mobile Phone, Social Networks, Mobile Network, Privacy, Personal Information.

ENHANCED DETECTION TECHNIQUES FOR CYBERSECURITY THREATS

Naga Satya Praveen Kumar Yadati

ABSTRACT

The dynamic field of cybersecurity has seen a surge in sophisticated cyber threats, necessitating advanced detection and mitigation strategies. This paper explores various advanced threat detection methodologies, including machine learning algorithms, behavioral analytics, threat intelligence feeds, and deception technologies. By adopting these cutting-edge techniques, organizations can significantly enhance their ability to detect and respond to complex cyber threats, thereby securing their digital assets more effectively.

KEYWORDS

cybersecurity, threat detection, machine learning, artificial intelligence, behavioral analytics, threat intelligence, deception technologies, endpoint detection, network traffic analysis, continuous monitoring.

THE EU ARTIFICIAL INTELLIGENCE ACT WILL REGULATE THE WORST PROBLEMS WITH POWERFUL AI MODELS, BUT IT WILL INEVITABLY FAIL TO SOLVE THE OVERALL DILEMMA OF RESPONSIBLE AI USAGE

Anvita Datla, The Dickson Poon School of Law, King's College London

ABSTRACT

The EU AI Act is the much-awaited document for regulating AI technologies. The risk-based approach of the act curtails the major problems that are predictable with technology. However, despite the seemingly robust measures taken by the EU AI act, it falls short of ensuring that AI is used responsibly. Responsible AI usage goes beyond the mitigation of immediate risks and requires comprehensive inclusion of ethical deliberation in the design and deployment of AI by ensuring transparency, privacy, non-discrimination, and the safety of society.

KEYWORDS

AI and Law, Biometric Systems, Healthcare Sector, Migration, Asylum and Border Control Management, Deepfakes.

ENHANCING IOT SECURITY BASED ON ARTIFICIAL INTELLIGENCE

Wissal Lazraq[1] and Soufiane Lahlali[2], [1]Department of Computer Science and Mathematics, ENSAK, Ibn Tofail University, Kenitra, Morocco, [2]Department of Computer Science and Mathematics, ENSAK, Ibn Tofail University, Kenitra, Morocco

ABSTRACT

The intersection of the Internet of Things (IoT) and Artificial Intelligence (AI) represents a transformative advancement in technology, unlocking new capabilities and efficiencies across various sectors. This article explores the integration of Artificial Intelligence (AI) with the Internet of Things (IoT) and its pivotal role

in enhancing IoT security. It highlights how AI-driven solutions such as anomaly detection, malware detection, secure data transmission through authentication, and access control which significantly bolster the security of IoT systems. By employing machine learning, deep learning, and advanced analytics, AI can detect and mitigate threats in real-time, ensure data integrity, and adapt to evolving security challenges. The article concludes that AI is essential for creating robust, resilient IoT ecosystems capable of withstanding sophisticated cyber threats.

KEYWORDS

Internet of Things, Artificial intelligence, Machine learning, Deep learning, Security.

INNOVATIVE AI SOLUTIONS FOR IOT SECURITY: INTRUSION DETECTION WITH MACHINE LEARNING

LAHLALI Soufiane and LAGRAT Ismail, National School of Applied Sciences Ibn Tofail University, Kenitra, Morocco

ABSTRACT

This article addresses the multifaceted security challenges inherent in the rapidly expanding Internet of Things (IoT) and proposes advanced solutions based on machine learning for effective intrusion detection. The discussion begins with a thorough review of common threats and vulnerabilities affecting IoT devices, such as botnets, which can exploit numerous devices for malicious activities, and Distributed Denial of Service (DDoS) attacks, which can severely disrupt network functionality. The article then explores various IoT architectures and technologies, including wireless sensor communication protocols like ZigBee and Bluetooth Low Energy (BLE), and application protocols such as the Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT). These technological frameworks are essential for the seamless operation and integration of diverse IoT devices. The study's core methodology involves a detailed intrusion detection approach utilizing machine learning algorithms, specifically K-Nearest Neighbors (KNN), Decision Tree, and Random Forest. The authors emphasize advanced data preprocessing techniques, such as dataset balancing and numerical feature normalization, to enhance model performance. Experimental results indicate that AI-based models, particularly Decision Tree and Random Forest, can significantly improve the accuracy of intrusion detection by effectively identifying abnormal behaviors and reducing false positives, thereby bolstering IoT network security. The article concludes by highlighting the critical necessity of robust security measures in IoT deployments and the promising potential of machine learning-based intrusion detection systems to mitigate these challenges. Future work is proposed to refine these models further and integrate them with real-time simulation tools like Node-RED, enabling dynamic, continuous monitoring and proactive threat mitigation in IoT environments.

KEYWORDS

IoT, Machine Learning, Intrusion Detection, IoT Vulnerabilities & Threats.

AI Teachers using A VR/MR Environment for Greater Student Interaction and Immersion

L.M. Escobedo F, School of Engineering, InterNaciones University, Guatemala City, Guatemala, June 2024

Abstract

The transmission of knowledge has been a fundamental tool throughout the history of hu-mankind, where each generation imparted and improved the knowledge and skills of the previous one.However, at certain times in history, some individuals attempted to monopolize this knowledge to gain ad-vantages over their peers, thus restricting access to knowledge. As societies grew and diversified, it became evident that collaboration between individuals from different backgrounds and cultures accelerated and enhanced the expansion of knowledge. This process was further enhanced with the arrival of technological revolutions, such as the internet. Currently, artificial intelligence represents a new technological revolution that, if used properly, can produce better prepared individuals equipped with the best tools in history of humanity to expand and improve the knowledge acquired.

Keywords

Education, artificial intelligence, virtual reality, mixed reality.

Electroculture, Radionics Biophotonic Transmission: A Synergistic Approach to Enhancing Plant Growth And Health

Thomas Imlauer, Vorticesdynamics, Strada Intrarea Ghioceilor 14, Petrești, 077067 Ilfov, Romania

Abstract

This study examines the effects of stimulating electrical, radionic, and biophotonic fields and radiation on plant growth. The findings indicate significantly greater performance improvements in terms of plant growth, yield, and resilience compared to traditional planting and growing methods. Consequently, there is great potential to integrate this synergistic approach of electroculture and radionics into sustainable agriculture, where plants can be nurtured in a controlled environment without the detrimental impact of external influences during the critical initial growth phase, as is common in greenhouse cultivation. This could lead to more efficient and environmentally friendly agricultural practices that harness the unseen energies of the natural world to enhance plant productivity and health.

Keywords

Electroculture, radionics, rife, electrical field, magnetic field, electrostatic field, Biophotonic.

ANALYSIS OF THE THERAPEUTIC POTENTIAL OF ABRUS PRECATORIUS AND TABERNAEMONTANA ELEGANS IN THE TREATMENT OF BILHARZIOSIS IN THE VILLAGE OF MASSAMBE-MASSINGA DISTRICT

Osvaldo Bernardo Muchanga ,St Tomas University,Mozambique

ABSTRACT

The present research was carried out in the Massambe Village and it was aimed at analyzing the Therapeutic Potential of Abrus precatorius and Tabernaemontana elegans, medicinal plants used in the Treatment of Bilharziosis in this Village. The research was mixed and developed in two phases. In the first one, a semi-structured interview was applied to the participants, which consisted in gathering information from the parts of the plants used, as well as the preparation and administration. At this stage participated 21 interviewees, including 1 Secretary, 7 Herbalists, 10 Traditional Medicine Practitioners and 3 Elderly people who were intentionally selected. The second phase was held in the Natural Products research laboratory of the Biology Department of the Pedagogical University Headquarters. It consisted in the identification of active principles present in the roots and leafs of the two plants under study related to the cure of bilharziosis. For the identification of active principles cold extraction (maceration) and chemical reactions were applied. The results of the interviews showed that the population uses roots, leaves, flowers and blends of roots and leaves. For the preparation of the drug, the same uses decoction, infusion and burning and for administration uses ingestion at varying dosages. The active principles identified in plant organs under study and implicated in the treatment of Bilharziosis are tannins, alkaloids, flavonoids and saponins. These active principles relate to the anthelmintic potential because they inhibit the normal development of S. mansoni.

KEYWORDS

Abrus precatorius; Tabernaemontana elegans; Traditional Medicine; Bilharziosis treatment; Shistosoma mansoni; Actives principles.

PHARMACOKINETIC EVALUATION OF AMLODIPINE TABLET COMPARED WITH NORVASK® TABLET IN HEALTHY INDONESIAN ADULT

Priyanto[1,2], Yunica NT[1], Widiastuti E[1], Wahyono BH[1], Susilo MJ[1], Siregar P[3], Mutiawati Y[3], and Kancanawatie DG[3], [1]Equitrust Lab, Jakarta, Indonesia, [2]University of Muhammadiyah Prof. Dr. HAMKA, Post Graduate Faculty of Pharmacy, Jakarta, Indonesia, [3]PT Tropica Mas Pharmaceuticals, Cianjur, Indonesia

ABSTRACT

This study objective to evaluate the pharmacokinetics of Amlodipine 10 mg Produced by PT. Tropica Mas Pharmaceuticals compared to Norvask® 10 mg Tablet Produced by PT. Pfizer Indonesia, in healthy Indonesian Adults through bioequivalence study. This study is utilized by randomized, single-dose, open-label, two-way cross-over design with a washout period 14 days and fasting. This study involved 17 of 18 subjects as included in the statistical analysis. Plasma samples were collected 17 times for 72-hour per period. Amlodipine concentrations were measured using LCMS/MS. Bioequivalence was determined by value of 90% confidence interval (CI) with $\alpha = 5.00\%$ within the range of 80.00–125.00% for AUC and Cmax. The geometric mean ratios (90% CI) of the test drug vs. the innovator drug were 101.67% (97.16 –

106.39) for AUC0-t and 100.46% (95.00 – 106.23) for Cmax. Based on the result, the test drug is bioequivalent to the comparator drug.

KEYWORDS

Pharmacokinetic, Bioequivalence, Amlodipine, AUC, and Two-Way Crossover.

BIOEQUIVALENCE AND PHARMACOKINETIC EVALUATION OF ETHAMBUTOL 400 MG FILM-COATED TABLET: A SINGLE-DOSE, OPEN-LABEL, RANDOMIZED, TWO-WAY CROSSOVER DESIGN STUDY

Priyanto[1,2], Yunica NT[1], Widiastuti E[1], Wahyono BH[1], Susilo MJ[1], Siregar P[3], Mutiawati Y[3], and Kancanawatie DG[3], [1]Equitrust Lab, Jakarta, Indonesia, [2]University of Muhammadiyah Prof. Dr. HAMKA, Post Graduate Faculty of Pharmacy, Jakarta, Indonesia, [3]PT Tropica Mas Pharmaceuticals, Cianjur, Indonesia

ABSTRACT

This study objective was to determine the bioequivalence of Ethambutol 400 mg Film-Coated Tablet produced by PT Kimia Farma Tbk compared to its recommended comparator product by WHO, Myambutol 400 mg Film-Coated Tablet produced by Pantheon Inc, Ontario, Canada for STI Pharma LLC, in healthy subjects. The study was conducted in a randomized, single-dose, open-label, two-way crossover design, in a fasting state. The number of subjects who completed the study was 29 of 32. Blood samples were collected 18 times. Ethambutol concentrations were determined by LC-MS/MS method. Bioequivalence was determined by value of 90% confidence interval (CI) with $\alpha = 5.00\%$ within the range of 80.00–125.00% for AUC and Cmax. The geometric mean ratios (90% CI) of the test drug vs. the innovator drug were 103.67% (97.23-110.52%) for AUC0-t and 91.53 % (84.80-98.79%) for Cmax. Based on the result, the test drug is bioequivalent to the comparator drug.

KEYWORDS

Ethambutol, AUC, Bioequivalence, Comparator, and Crossover.