Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 5, pp. 4407–4010, DOI 10.12694/scpe.v25i5.4333

INTRODUCTION TO THE SPECIAL ISSUE ON NEXT GENERATION PERVASIVE RECONFIGURABLE COMPUTING FOR HIGH PERFORMANCE REAL TIME APPLICATIONS

C. VENKATESAN*, YU-DONG ZHANG†, CHOW CHEE ONN‡, AND YONG SHI§

The evolution of scientific computing is reshaping the hardware and software requirements, emphasizing the need for high-performance platforms adaptable to real-time applications. Traditional methods with general-purpose processors often lack the agility needed for swift modifications and fast computations during real-time tasks. Reconfigurable computing offers a compelling solution by integrating hardware speed and software flexibility on a unified platform. This technique promises significant acceleration across diverse applications like image processing, encryption, decryption, runtime operations, and intensive computing tasks such as sequence searching and matching in smart environments.

For high-performance applications, software-programmed microprocessors offer versatility. Artificial Intelligence (AI) has proven more robust than traditional methods in noisy environments, relying on reconfigurable designs for efficient operation. Hybrid machine-learning techniques enhance system reliability without compromising performance. Reconfigurable computing systems have recently accelerated intensive algorithms compared to software-optimized versions, leveraging parallel topologies. Deep Neural Architectures with adaptable computation patterns excel in computer vision tasks. Artificial Neural Networks (ANNs) are crucial for pattern recognition, high-performance machine learning, data manipulation, security threats, data mining, signal processing, and other applications, driving ongoing research into reconfigurable hardware and software implementations for ANNs.

It is a privilege for us to introduce the Special Issue on "Next generation pervasive reconfigurable computing for high-performance real-time applications". Among the numerous research papers we received (49 in total), we meticulously selected 22 papers for publication. The overarching objective of this special issue is to investigate the recent advancements and disseminate state-of-the-art research related to reconfigurable computing for high-performance real-time applications and the technologies that make this possible. This special issue represents a showcase of new dimensions of research, offering researchers and industry professionals an illuminating perspective on pervasive reconfigurable computing. We sincerely hope that the contributions in this special issue will not only inform but also inspire future research endeavours, leading to a deeper understanding of the multifaceted world of speed computation during real-time applications.

The paper titled "Vulnerability Detection in Computer Networks Using Virtual Reality Technology" by Songlin Liu, traditional network security challenges are tackled through virtual reality integration. Optimization calculations are employed to extract network security vulnerability attributes, with adjustments made using a web crawler and a detailed analysis of attack characteristics. This approach facilitates automated detection within a virtual reality framework. Empirical results show a significant reduction in detection delay to 75.33 milliseconds, compared to 290.11 milliseconds and 337.30 milliseconds in conventional methods, highlighting the efficiency of the proposed approach.

"Computer Malicious Code Signal Detection Based on Big Data Technology" by Xiaoteng Liu improves

*Department of Electronics and Communication Engineering HKBK College of Engineering, Bangalore, Karnataka, India. (venkatesanc.ec@hkbk.edu.in)
†Chair in Knowledge Discovery and Machine Learning, Department of Informatics, University of Leicester, United Kingdom (yz461@leicester.ac.uk)
‡Department of Electrical Engineering, Faculty of Engineering, University of Malaya, Kuala Lumpur, Malaysia (cochow@um.edu.my)
§Department of Computer Science, Kennesaw State University, Marietta, United States of America. (yshi5@kennesaw.edu)

upon traditional methods by using big data for detecting malicious software behaviour. The approach tackles challenges in mobile malware detection through mean-variance feature selection and advanced techniques like PCA, KLT, and ICA for feature extraction. A decision tree-based multi-level classification model enhances accuracy and addresses data imbalance issues, leading to notable accuracy improvements of 3.36% to 6.41% across different Android detection methods, highlighting the effectiveness of the proposed malware detection technology.

"Network Security with VR-Based Antivirus Protection and Reduced Detection Delays" by Chunna Song et.al., addresses delays in traditional systems by leveraging VR technology. It aims to decrease detection delays, enhance efficiency, and optimize security feature identification. The method includes web crawling for an injection list and virtual protection blocks to mitigate threats, achieving a detection delay of 75.33 milliseconds, surpassing traditional delays of 290.11 ms and 337.30 ms. Empirical evidence supports the efficacy of automatic detection in VR, promising improved network security responsiveness and effectiveness.

Xiaohong Li et.al., in the paper titled "Computer Network Virus Defense with Data Mining-Based Active Protection" presents a novel approach to enhance computer network virus defence beyond traditional technologies. Utilizing Object-Oriented Analysis (OOA) mining, the method analyzes Win API call sequences in PE files to detect deformed and unknown viruses. Experimental results demonstrate the Data Mining-based Antivirus (DMAV) system's superiority with higher accuracy in deformed virus detection, effective defence against unknown viruses (92% recognition rate), improved efficiency, and reduced false alarms for non-virus files. The research introduces an OOA rule generator to optimize feature extraction, bolstering system intelligence and resilience in enhancing computer network security.

"Application of Nonlinear Big Data Analysis Techniques in Computer Software Reliability Prediction" by Li Gao and Hai Wang addresses challenges in using artificial neural networks for software reliability prediction, focusing on improving the PSO-SVM model. Comparative experiments with a Backpropagation (BP) model highlight the PSO-LSSVM model's rapid reduction in training error within 200 generations, compared to BP's 1,733 generations. The optimized PSO-LSSVM model demonstrates superior efficiency with small sample sizes, offering accelerated training and enhanced prediction accuracy for software reliability assessments.

"Enhancing Industrial Control Network Security through Vulnerability Detection and Attack Graph Analysis" by Yan Liao addresses communication attack defence gaps in industrial control networks. The study proposes using attack graphs to improve security and vulnerability assessments, providing detailed construction methodologies. Experimental evaluations using the "earthquake net" virus identify four main attack routes for the "Zhenwang" virus, each with specific loss values and attack success probabilities. This research emphasizes the need for systematic vulnerability analysis to enhance overall industrial control network security.

Chunmei Ji et.al., in the paper titled "Improving Semantic Analysis in Visualization with Meta Network Representation and Parsing Algorithm" introduces the semantic Meta Network (MNet) for advanced semantic analysis in visualization. MNet employs a hierarchical framework to integrate semantic elements, relationships, and attributes, facilitating comprehensive understanding from phrases to complete texts. The study presents a construction algorithm for MNet and parsing methods tailored for natural language interface parsing, validated through empirical experiments. This research enhances semantic analysis capabilities, particularly in interpreting SCADA system instructions, contributing to improved natural language understanding and semantic analysis in visualization contexts.

"Hybrid optimization for high aspect ratio wings with convolutional neural networks and squirrel optimization algorithm" by Pengfei Li presents an efficient approach for optimizing lightweight high-aspect-ratio wings. The study combines a hybrid binary unified coding description, one-dimensional convolutional neural networks for aeroelastic modelling, and the squirrel optimization algorithm for computational efficiency. Experimental results demonstrate a 4.1% reduction in wing weight, showcasing the effectiveness of this hybrid method in optimizing complex wing structures.

"Computer Software Maintenance and Optimization Based on Improved Genetic Algorithm" by Ming Lu aims to enhance software maintenance and network performance using an advanced genetic algorithm. The study refines network architecture through enhanced genetic operations and evaluates satisfaction and fitness index functions with controlled data iterations. Results show network reliability initially improves with iterations but stabilizes due to hardware limitations, highlighting a peak reliability of 0.894 achieved at 100

iterations. This research provides a foundational framework for optimizing computer network reliability with a balanced genetic algorithm approach.

Jing Wang et.al., in the paper titled "Research on Intelligent Transformation Platform of Scientific and Technological Achievements Based on Topic Model Algorithm and Its Application" enhances the conversion of scientific breakthroughs into practical applications using the LDA theme model. The study improves efficiency by extracting pivotal terms and thematic phrases, facilitating information management, retrieval, and recommendations for academic and business sectors. The platform evaluates transformation results and operational efficiency in advancing scientific and technological achievements.

"An Emotional Analysis of Korean Topics Based on Social Media Big Data Clustering" by Yanhong Jin introduces the Online Topic Emotion Recognition Model (OTSRM) to enhance emotional analysis accuracy in Korean social media. Utilizing the Online Latent Dirichlet Allocation (OLDA) model, OTSRM integrates emotion intensity and employs an innovative emotion iteration framework. It introduces an affective evolution channel and distribution matrices for characteristic and affective words, advancing understanding of emotional context. Validation experiments demonstrate OTSRM's effectiveness with emotion recognition accuracy rates of 85.56% and 81.03%, improving precise emotional dynamics assessment in Korean social media.

Xiangying Liu et. al., in the paper titled "Application of Artificial Intelligence Technology in Electromechanical Information Security Situation Awareness System" proposes leveraging AI and big data to enhance predictive capabilities in information security. Using LSTM-RNN and variant GRU models, the study achieves high accuracy with LSTM-RNN showing MAPE of 8.79%, RMSE of 0.1107, and RRMSE of 8.47% on test data. This research highlights AI's potential in developing robust information security situational awareness systems, comparing LSTM and GRU models for effectiveness and efficiency in predictive analysis.

Wenjuan Yang in the paper titled "Analysis and Application of Big Data Feature Extraction Based on Improved K-means Algorithm" addresses challenges in handling large volumes of data by proposing an enhanced K-means algorithm. Focused on mitigating errors, the study applies this algorithm to monitor power equipment, achieving an error rate below one per cent and consistently high accuracy exceeding 95%. The research underscores the algorithm's effectiveness in improving clustering accuracy and efficiency, emphasizing its practical application in big data analysis for energy systems.

"Intelligent Prediction of Network Security Situations Based on Deep Reinforcement Learning Algorithm" by Yan Lu et al. introduces a novel approach using deep learning to enhance network security assessment. The study develops a deep self-encoding model for effective network attack detection and integrates a unique oversampling weighting algorithm to improve pattern detection with limited training data. Experimental results demonstrate significant performance gains over traditional methods like DT, SVM, and LSTM, achieving higher F1 scores by approximately 2.77, 10.5, and 5.2, respectively. This research emphasizes improved accuracy and efficiency in predicting and measuring network security situations.

Min Yan and Hua Zhang in the paper titled "Interface Control and Status Monitoring of Electronic Information Equipment Based on Nonlinear Data Encryption" proposes an advanced system ensuring information fairness, objectivity, and security in traffic accident investigations. The study develops a robust security strategy with PC-based platforms for efficient data acquisition, secure processing, transmission, and storage using nonlinear data encryption methods. Performance tests with files ranging from 3MB to 10MB show a significant 25% average speed improvement over the original platform. This system enhances data integrity during transmission, aids in accurate equipment identification post-accident, and addresses critical security challenges in traffic accident investigations.

Yongqiang Shang in the paper titled "Detection and Prevention of Cyber Defense Attacks Using Machine Learning Algorithms" examines the rise in cyber threats fueled by enhanced computing power, big data utilization, and advanced machine learning techniques. The study explores both defensive and offensive uses of machine learning in cybersecurity, focusing on mitigating attacks targeting machine learning models. It underscores the pivotal role of artificial intelligence in enhancing digital security through tasks like malware analysis, network vulnerability assessment, and threat prediction amidst rapid global digitization.

Zhixiong Xiao in the paper titled "Minimizing Overhead Through Blockchain for Establishing a Secure Smart City with IoT Model" explores the integration of blockchain technology with IoT to enhance security while addressing resource constraints. Traditional blockchain deployments are impractical for IoT due to their

high storage and computational demands. This study proposes an optimized blockchain framework tailored for IoT devices, ensuring essential security measures like authenticity, credibility, confidentiality, availability, and non-repudiation. The approach aims to bolster security without imposing excessive resource burdens, making it suitable for smart city applications.

"Security and Privacy of 6G Wireless Communication Using Fog Computing and Multi-Access Edge Computing" by Ting Xu, Ning Wang, Qian Pang, and Xiqing Zhao addresses data confidentiality challenges in forthcoming 6G networks. The study explores blockchain's potential for enhancing security and incorporates machine learning (ML) to manage vast data volumes. It reviews strategies for protecting automotive communication systems and assesses confidentiality approaches within 6G architecture. The research emphasizes safeguarding private data in the Internet of Everything (IoE) era and proposes ML solutions for data processing challenges, underscoring blockchain's role in securing 6G communications.

"Sustainable Development in Medical Applications Using Neural Network Architecture" by Shuyi Jiang aims to enhance risk management in healthcare through machine learning. The study uses social media data analysis to identify and assess threats, aiding informed decision-making in healthcare management. It employs machine learning algorithms to visualize risk categories and simplifies data processing for efficiency. Empirical analysis of Consumer Value Stores (CVS) reveals operational, financial, and technological risks, categorized by severity. The study highlights the framework's effectiveness in threat identification and mitigation, offering insights for safer healthcare environments.

"Target Image Processing Based on Super-Resolution Reconstruction and Machine Learning Algorithm" by Chunmao Liu proposes a method to enhance the resolution of medical images using super-resolution reconstruction and machine learning. This approach integrates nonlocal autoregressive learning into the reconstruction model, exploiting inherent data similarities in medical images. Additionally, a clustering algorithm refines classification dictionaries to improve efficiency. Experimental results, conducted on CT/MR images, demonstrate significantly improved peak signal-to-noise ratios and structural similarity values compared to other methods, achieving a peak value of 31.49. This study validates the efficacy of combining super-resolution reconstruction and machine learning for enhancing medical image resolution.

"Group Intelligent City Mobile Communication Network's Control Strategy Based on Cellular Internet of Things" by Jiazheng Wei explores enhancing mobile communication networks in urban areas using an improved particle swarm optimization (PSO) algorithm. This study refines PSO to tackle specific network challenges and achieves robust optimization results through simulations. The Grad-PSO algorithm effectively improves network performance with optimized parameters, demonstrating its suitability for enhancing mobile communication efficiency in urban environments.

Shuiquan Zhu presented the paper titled "Performance evaluation of micro automatic pressure measurement sensor for enhanced accuracy" focuses on enhancing the accuracy of micro-automatic pressure measurement sensors through design improvements and rigorous performance testing. The sensor achieved high detection accuracy (0.0452%) and met reliability standards with features such as sensitivity (0.0582%), nonlinearity (0.0741%), hysteresis (0.0266%), and repeatability (0.0625%). It also demonstrated reduced response times compared to traditional sensors, though the study highlights the necessity for additional real-world testing to optimize its performance further.

In summary, this special issue of Scalable Computing: Practice and Experience explores emerging trends in scientific computing that influence hardware and software requirements. It underscores the need for high-performance platforms capable of real-time architectural updates. Traditional computing struggles with adaptability and speed in real-time applications, while reconfigurable computing integrates hardware speed and software flexibility in a unified platform. This approach accelerates applications like image processing, encryption, and machine learning, especially Artificial Neural Networks (ANNs). The issue highlights advancements in reconfigurable computing systems and their impact on enhancing performance in intensive computing domains such as signal processing and computer vision.