CIT. Journal of Computing and Information Technology, Vol. 27, No. 4, December 2019, i–ii
doi: 10.20532/cit.2019.1005033

Editorial

This year's last issue (December 2019; Vol. 27, No. 4) of *CIT. Journal of Computing and Information Technology* includes four papers from the areas of network security, Semantic Web, computer graphics and mobile services.

In the first paper of the issue, Meenal Jain and Gagandeep Kaur research network intrusion detection techniques involving both supervised and unsupervised machine learning algorithms. As such an approach entails handling data with a large number of attributes, feature reduction is required. In their paper, titled *A Study of Feature Reduction Techniques and Classification for Network Anomaly Detection*, the authors strive to refine known reduction techniques in order to meet newly found attacks. They consider three reduction techniques, along with four machine learning classifiers, and additionally introduce four novel performance measurement metrics to be applied on the actual and reduced datasets. The presented results show that, with respect to accuracy of detection and false positive rates, Nonlinear Principal Component Analysis (NLPCA) and Neural Network (NN) are better suited for the reduction of dimension space in network intrusion detection system (NIDS) datasets than traditional Principal Component Analysis (PCA). Additionally, among the various classifiers studied, the Decision Tree (DT) has been shown to be the best one.

Resource Description Framework (RDF) is a well-known W3C metadata specification used in modeling information implemented in Web resources, primarily intended to support the Semantic Web. Although it has been increasingly used since, the authors of the next paper Li Yan, Zheqing Zhang and Dan Yang claim that traditional centralized RDF storage models cannot meet the needs of large-scale, massive RDF data management, especially in the case of temporal RDF data. Hence, in their paper, properly titled *Temporal RDF(S) Data Storage and Query with HBase*, they propose a new storage model for temporal RDF data, which is based on the open-source non-relational distributed Apache HBase database system, hypothesizing both the feasibility of storing large temporal RDF data with the proposed model, as well as improved query efficiency. The authors experimentally evaluated their approach using the standard Lehigh University Benchmark (LUBM) dataset with temporal information added, eventually confirming the initial hypothesis.

The paper *Using Poisson Disk Sampling to Render Oil Particles at Sea* by Vancuong Do and Hongxiang Ren addresses simulation of oil spills spreading at sea, which are the result of accidents, along with the appropriate rendering methods. Such three-dimensional simulations are quite demanding as the oil film constantly interacts with and is influenced by the environment, thus making its composition and properties highly changeable with time. In their oil spill physical model, the authors use both Lehr's spreading model and Hoult's drifting model, applying the Poisson Disk algorithm in three-dimensional space to divide the oil film into particles. This differs from previous studies where the algorithm was applied to static and solid objects only, and not to fluids. Two cases were considered: moving oil particles, eventually reaching an island and oil particles continuously spreading and drifting under the influence of environmental factors. The developed model is limited to oil shapes consisting of a cluster of a few thousand particles, which the authors claim to be appropriate for real-time simulations, when quick reaction from emergency rescue parties is to be ensured. A comparison with other 3D oil spill models is provided, which demonstrates improvements being brought by the proposed model.

In the last paper of this issue, Adebukola Onashoga, Adesina Sodiya and Idowu Osinuga tackle the issue of ensuring confidentiality and integrity in user–provider communication within Loca-

tion-Based Mobile Services (LBMS), a group of innovative mobile services which is increasingly becoming the integral part of the ever-growing number of mobile applications. Accordingly, their paper, titled *Privacy Preserving Location-Based Client-Server Service Using Standard Cryptosystem*, deals with a combined concept of location privacy, message authentication and a novel integrity checking of server response messages. In this respect, the authors propose a practical system, named Location-Based Service for enhancing Privacy and Integrity (LBS_PI), which is based on a cryptographic scheme with no trusted intermediary that guarantees users' privacy as well as integrity of servers' response. The scheme uses both symmetric and asymmetric encryption algorithms, while AES-256 is used to encrypt the message and user location in order to overcome the related computational complexity. LBS_PI was tested within a group of 8 Points-Of-Interest (POIs) spanning an area of 5 km around the users' position, showing performance improvements with respect to comparable systems.

Vlado Glavinić
Editor-in-Chief