

Editorial

The present issue is the last one of the 2021 volume of *CIT. Journal of Computing and Information Technology* (Vol. 29, No. 4 – December 2021) and consists of papers from the areas of software engineering, security and privacy, and big data.

In the first paper of this issue, Yousef A. Yousef, Abdelrafe Elzamy, Mohamed Doheir and Noor-ayisahbe Mohd Yaacob present a field study investigating the importance of soft skills in software requirement engineering (SRE). In the homonymous paper, titled *Assessing Soft Skills for Software Requirements Engineering Processes*, the authors focus their research on the Gaza Strip, surveying software development experts residing there by using an online questionnaire, and subsequently analyzing the gathered data through descriptive statistics, principal components analysis (PCA) and stepwise regression techniques. The analyzed data determined 31 soft skills associated with SRE, whereas principal components analysis (PCA) extracted six skill factors, namely problem-solving, learning willingness, commitment, pressure resilience, critical thinking, and interpersonal skills. While all soft skills factors were shown to have strong links with SRE, five of them were found to have the strongest associations with SRE (problem-solving, commitment, pressure resistance, critical thinking, and interpersonal skills), and only four (problem-solving, willingness to learn, pressure tolerance, and critical thinking) to positively impact it. Relying on these findings the authors thus infer that the success of software requirements engineering builds on the improvement of soft skills.

The second paper in this issue – *A Cloud-based Mobile Privacy Protection System with Efficient Cache Mechanism* by Wenyun Dai and Longbin Chen – addresses an issue common for mobile devices like smartphones, *i.e.*, the privacy of data stored within them. These data are presently both too freely accessed and over-collected, mainly because of the built-in coarse-grained permission authorizations which are characteristic of mobile operating systems. The authors thus propose a solution to the above problem by introducing a fine-grained access control tuned to accommodate diverse data requests, which is based on organizing data into different directories with different accessing policies based on the respective privacy levels and residing in cloud storage. In order to improve the efficiency of data access, which is a problem existing cloud data storage approaches come across, the authors additionally designed a cache mechanism to retain non-private and highly accessed data within the mobile device, hence optimizing performance and reducing extra communication costs. The approach is evaluated in a simulated environment using a real smartphone. The experiments performed displayed adequate and limited response times for data requests with the possibility to be further improved through the use of the cache mechanism.

The third paper in the issue considers electronic medical records (EMR), specifically their privacy problems, which could arise either locally, as possible malicious tampering to avoid legal responsibilities of medical institutions, or as information leakage when EMRs are shared. The latter approach through sharing EMRs is presently being widely adopted, as it is a convenient and effective technique for improving the quality of medical services as well as for reducing the corresponding storage and management overhead costs. Thus Lu Xu, Mengchen Lin, Yong Feng and Yani Sun introduce a novel approach to accessing EMRs stored on cloud-shared centers from thin clients running on mobile devices, which ensures patients' privacy. In their paper, titled *BPDST: Blockchain-Based Privacy-Preserving Data Sharing on Thin Client for Electronic Medical Records*, they describe a sharing scheme based on blockchain privacy protection that can be ex-

ecuted on thin clients. This scheme combines k -anonymity and cloud storage, allowing patients to manage and safely share their own medical information among doctors, hospitals, companies, and the government. It effectively supports sharing medical information without leaking or tampering with EMRs' privacy, thus achieving privacy protection. The authors performed both a security and a performance analysis of the BPDST approach, confirming its effectiveness.

Improvement of agricultural production and management is of paramount importance for agricultural countries like China. Hence novel development models are currently being researched targeting the modernization of backward production techniques and management models, of which intelligent agriculture is presently the foremost one. However, the underlying technology, which among other things relies on data mining, is currently not yet well suited for this task. This motivated Wei Liu, the author of the last paper of the issue – *Application of Data Visualization and Big Data Analysis in Intelligent Agriculture*, to include data visualization and big data analysis into the application scenarios of intelligent agriculture. In this respect, the author firstly developed an intelligent agriculture data visualization system along with the respective data visualization method named *RadViz* and introduced a novel method of processing intelligent agriculture data using dimensionality reduction through principal component analysis (PCA) and k -means clustering (KMC) optimization. Finally, he devised a crop yield prediction model based on regression algorithms, whose effectiveness he subsequently experimentally proved.

Vlado Glavinić
Editor-in-Chief