SPECIAL ISSUE CISIS 2020-IGPL

The 12 papers included in this special issue represent a selection of extended contributions presented at 13th International Computational Intelligence in Security for Information Systems (CISIS 2020) held in Gijón, Spain, 11–13 September 2020, and organized by the BISITE group and the University of Oviedo.

CISIS 2020 aims to offer a meeting opportunity for academic and industry-related researchers belonging to the various, vast communities of computational intelligence, information security and data mining. The need for intelligent, flexible behaviour by large, complex systems, especially in mission critical domains, is intended to be the catalyst and the aggregation stimulus for the overall event.

The contributions are organized as follows.

The first contribution, by Dutta *et al.*, presents an intrusion detection mechanism that leverages Deep AutoEncoder and several deep decoders for unsupervised classification. This work incorporates multiple network topology setups for comparative studies. The efficiency of the proposed topologies is validated on two established benchmark datasets: UNSW-NB15 and NetML-2020. The results of their analysis are discussed in terms of classification accuracy, detection rate, false-positive rate, negative predictive value, Matthews correlation coefficient and F1-score. Furthermore, comparing against the state-of-the-art methods used for network intrusion detection is also disclosed.

The main objective in the next contribution, by Caballero-Gil *et al.*, is to present the design and an initial implementation of a decentralized rental system that takes advantage of smart contracts developed on a public blockchain, combined with the potential of the internet of things and its intimate relationship with cyber-physical systems. The logic to be implemented in the blockchain is applied in this paper by using the Ethereum programming language, so that the developed application covers the entire car rental process offered in traditional web applications, but adding more autonomy, functionalities and ease of use for both lessees and lessors. Following Ethereum application development guidelines, all business logic is located in the smart contracts implemented in the network, where they can be used to control the car rental system. While this is a work in progress, the results obtained in the first proof of concept have been very promising.

The goal of the following paper, by Alemany *et al.*, is to provide information about the sensitivity of the content of a publication when a user is going to share it in OSN. For this purpose, the authors developed a privacy-assistant agent that detects sensitive information. Based on this information, the agent provides a message through a nudge mechanism warning about the possible risks of sharing the message. To avoid being annoying, the agent also considers the user's previous behaviour and adapts the messages it sends to give more relevance to those categories that are more important to the user from the point of view of the privacy risk. This agent was integrated into the social network Pesedia, and the performance of different models to detect a set of sensitive categories were analysed, in a dataset of tweets in Spanish.

Following, in paper four, Carriegos *et al.* deal with time series of cybersecurity aggregates, which means time series obtained from cybersecurity databases of time-stamped raw reports formatted using some reporting standard. The goal of this paper is to show how it is possible to forecast some time series of such type. In order to achieve that goal, the authors briefly review a method to integrate time series from aggregable databases, they recall some non-standard theoretical results motivating their approach and, finally, present some concrete experiments performed on real public databases of cybersecurity threats.

https://doi.org/10.1093/jigpal/jzac001

The next contribution, by Aubin *et al.*, the use of small segments of the handwritten stroke for writer verification is proposed. A grapheme is defined as the concatenation of smaller segments or fragments. Average of gray level of the perpendicular line to the skeleton and local binary pattern is adopted as descriptor. A database of 3000 images of 50 writers, with 6 types of segments, 10 samples per segment has been developed and a binary output support vector machine was applied as classifier. Thus, 50 classifiers were trained using 100 balanced data sets generated using subsampling of the majority class. Experiments are carried out with the proposed models, with an identity verification hit rate of 97% on average.

The sixth paper, by Gwang-Myong, Seok-Jun and Sung-Bae, proposes a deep metric neural network with strategic sampling algorithm that properly extracts salient features and directly learns a quantitative measure of similarity. A strategic sampling method of heuristically generating and learning training pairs through Monte Carlo search is proposed to select a training pair that can represent the entire dataset. With the TPC-E-based benchmark data trained with 11,000 queries for 11 roles, the proposed model produces the classification accuracy of 95.41%, which is the highest compared with the previous models. The results are verified through comparison of quantitative and qualitative evaluation, and the feature space modelled in the neural network is analysed by t-distributed stochastic neighbour embedding algorithm.

The subsequent contribution, Cardell *et al.* perform a deep study of the randomness of the GSS-concatenated sequences, generated from the family of generalized self-shrunken sequences. The authors apply the most important batteries of statistical and graphical tests providing powerful results and a new method to construct sequences with good cryptographic properties.

The next work, by Kozik *et al.*, faces the proposition of an innovative distributed architecture to tackle the above-mentioned problems. The architecture uses state-of-the-art technologies with a focus on efficiency, scalability and also openness, so that community-created components and digital content analyzers could be added. Moreover, the authors prove the usability of the prototype on Kaggle fake news dataset. In particular, different configurations of the proposed deep neural network are considered, and the presented results reflect the effectiveness, scalability and transferability of the proposed solution.

The ninth paper, by Mezquita *et al.*, points out the main problems associated with conventional models and makes a survey of the new ones which are based on blockchain technology. This type of model is already being developed as a proof of concept by different countries. With the use of this technology in land registry systems, it is possible to improve the transparency of the processes as well as optimize costs and execution time. To show the theoretical results of this study, the Spanish land registry has been taken as an example of a use case scenario.

In the next contribution, by Gayoso Martínez, Hernández Encinas and Martín Muñoz, presents equivalent schemes in one, two and three dimensions, which allow anyone to make the transition to the four-dimension NewHope algorithm easier to undertake. In addition to that, the effect of modifying some of the parameters associated with NewHope's reconciliation mechanism is studied, which has allowed us to propose different sets of parameters that could increase the security of NewHope implementations.

The following contribution, by Khalid Alabdulsalam *et al.*, first propose an IoT network architecture for the forensic purpose that uses machine learning algorithms to autonomously detect IoT devices. Then authors posit the importance of focusing on the links between different IoT devices and design an approach to do so. Specifically, the authors' approach adopts a graph for modelling IoT communications' message owes to facilitate the identification of correlated network traffic based on the direction of the network and the associated attributes. To demonstrate how such an approach can be deployed in practice, the authors provide a proof of concept using two IoT controllers to

generate 480 commands for controlling two IoT devices in a smart home environment and achieve an accuracy rate of 98.3% for detecting the links between devices.

The final contribution, by Quintián *et al.*, proposes the application of a novel projection method (Beta Hebbian Learning) under Intrusion Detection in flows from a visualizations perspective. With the aim to validate this method, 8 traffic segments, containing many flows, have been analysed by means of this projection method. The promising results obtained for these segments, extracted from the University of Twente dataset, validate the proposed application.

The guest editors wish to thank Professor Dov Gabbay, (Founding Editor-in-Chief of Logic Journal of the IGPL) for providing the opportunity to edit this special issue. We would also like to thank the referees who have critically evaluated the papers within the short time. Finally, we hope the reader will share our joy and find this special issue very useful.

Enrique Antonio de la Cal
Computer Science Department, Faculty of Geology
University of Oviedo, Oviedo, Spain
E-mail: delacal@uniovi.es

José Ramón Villar Flecha
Computer Science Department, Faculty of Geology
University of Oviedo, Oviedo, Spain
E-mail: villarjoseg@uniovi.es

Héctor Quintián
Department of Industrial Engineering, CTC
University of A Coruña, A Coruña, Spain
E-mail: hector.quintian@udc.es

Emilio Corchado
Department of Computer Science and Automatic
University of Salamanca, Salamanca, Spain
E-mail: escorchado@usal.es