Editorial Preface

Yassine Maleh, National School of Applied Sciences, Khouribga, Morocco

Today everything is digital, and what is not, is soon to be digital. As citizens, we all have access to a computer, a tablet or a telephone for our personal and professional use. These means of communication are increasingly connected, gaining accessibility and simplicity for our daily purposes. We are living in a data-driven age. Data has been located or is going to be located in every point of our life. Most people think that this influence is a consequence of industry 4.0 that makes our life faster than before as all other industrial revolutions.

As cyber-attacks against critical infrastructure increase and evolve, automated systems to complement human analysis are needed. Moreover, chasing the breaches is like looking for a needle in a haystack. Such organizations are so large, with so much information and data to sort through to obtain actionable information that it seems impossible to know where to start. The analysis of the intelligence of an attack is traditionally an iterative, mainly manual process, which involves an unlimited amount of data to try to determine the sophisticated patterns and behaviors of intruders. Besides, most of the detected intrusions provide a limited set of attributes on a single phase of an attack. Accurate and timely knowledge of all stages of an intrusion would allow us to support our cyber-detection and prevention capabilities, enhance our information on cyber-threats and facilitate the immediate sharing of information on threats, as we share several elements.

To tackle the problems, smart security technologies have been researched worldwide, and many useful approaches have been extensively studied and received considerable attention in recent years, as witnessed by the number of related publications. In the context of these trends, the forthcoming issue will address some important topics in the field of smart security technologies. Nowadays, smart security technologies are still a hot research field. While most methods have been improved, the attacks on them also have become smarter and effective. To make the readers of IJSST more aware of the development as well as the existing problems, it is worth dedicating this first issue to the recent results in the field.

This issue has 4 papers that cover the essential areas in the field of smart security. Topics covered include issues of malware detection using deep learning techniques, authentication schemes for Internet of Things, cyber peacekeeping and Bayesian semantic image segmentation.

I hope this first issue would kindle interest of several researchers in the field of smart security technologies.

Yassine Maleh
Interim Editor-in-Chief
IJSST