Editorial: Sustainable Information Security and Forensic Computing

Paul D. Yoo, *Senior Member, IEEE* and Zahir Tari, *Senior Member, IEEE*

Modern societies are becoming increasingly reliance on inter-connected digital systems where commercial activities and government services are delivered. Despite the benefits, it is impossible to overstate the importance of information security and forensics in a highly inter-connected system. To address security threats to network infrastructure devices and sensitive data, many different solutions capable of providing a suitable degree of security and forensic capability have been developed. However, such solutions have not been properly designed to address important aspects such as computational costs, scalability, energy efficiency and resource usage. This special issue thus focuses on practical aspects of information security and forensics in sustainable computing. We solicited original contributions on recent challenges, including threats, defence and security, information, tools, and digital forensics applications in sustainable computing. We also sought contributions that focused on real-world security and forensic problems as well as theoretical work that has practical application.

This special issue is dedicated to the identification of techniques/methods designed for sustainable information security and forensic systems. We received a total of 31 submissions for this special issue, of which only 11 papers have been accepted. Each paper went through a rigorous peer review process, in addition to multiple follow-up rounds with the authors. A summary of the selected papers is provided below.

- In "WARDOG: Awareness detection watchdog for Botnet infection on the host device", a team of researchers from Switzerland, United Kingdom and Greece proposed a sustainable end-user awareness system for botnet mitigation on the infected machine's side. Once a botnet attack is detected by a legitimate and trusted network entity, the involved infected machines are alerted.
- In "The Status of Quantum-Key-Distribution-Based Long-Term Secure Internet Communication", the authors from Technische Universität Darmstadt, Germany and University of California, San Diego, USA presented an analysis of the performance and security of existing point-to-point Quantum Key Distribution (QKD) technology followed by discussions on approaches to enabling QKD in large-scale multi-user networks. Finally, important challenges that need to be addressed in order to make QKD-based long-term secure communication on the Internet practical is identified.
- In "A Secure and Sustainable Framework to Mitigate Hazardous Activities in Online Social Networks", researchers from United Kingdom and Malaysia studied a design of automatic two-phase (pre- and post-filtering) approach with the objective of mitigating the cyber threats in online social network (OSN) platforms in order to address the lack of functionalities of the current OSN platforms for automatic users protection in initiating online friendship and online users interaction within their circle.
- In "Solving Coupling Security Problem for Sustainable Sensor-Cloud Systems based on Fog Computing", the team from United States of America, United Kingdom and China presented an extended the Kuhn-Munkres algorithm based on fog computing to achieve sustainability. They designed a buffer queue in fog computing layer which will return the result to the cloud layer directly to increase the resource utilization. They then extended the Kuhn-Munkres algorithm to get the initial assignments of resources. To determine whether the initial assigned resources can be further scheduled, which means that they need to further improve the resource utilization to realize sustainable resource management.

Despite the significant amount of efforts devoted to addressing sustainable information security and forensic computing, there are still a number of challenges that remain to be addressed in the near future. Potential topics for future research would include:

- Sustainability of AI-based security software – the computational and environmental costs of training of an AI model grew proportionally to model size and then exploded when additional tuning steps were used to increase the model's final accuracy.
- For security and forensic computing to be truly sustainable, all phases of the system life-cycle, from manufacturing to disposal, must be considered.

- *Paul D. Yoo is with the Department of Computer Science and Information Systems, Birkbeck College, University of London Malet Street WC1E 7HX London, U.K. E-mail: paul.d.yoo@ieee.org.*
- *Zahir Tari is with the School of Science, Royal Melbourne Institute of Technology, Melbourne 3001, Australia. E-mail: zahir.tari@rmit.edu.au.*

Digital Object Identifier no. 10.1109/TSUSC.2020.3039652

Paul D Yoo (Senior Member, IEEE) is currently with the CSIS, Birkbeck College, University of London and leading BIDA Data-Driven Cyber Security Laboratory. Prior to this, he held academic/research posts in Cranfield (Defence Academy of the UK), Sydney (USyd) and South Korea (KAIST). In his career, he has amassed more than 80 prestigious journal and conference publications, has been awarded more than US$ 2.3 million in project funding, and a number of prestigious international and national awards for his work in advanced data analytics, machine learning and secure systems research, notably IEEE Outstanding Leadership Award, Capital Markets CRC Award, Emirates Foundation Research Award, and the ICT Fund Award. Most recently, he won the prestigious Samsung award for research to protect IoT devices using machine-learning approach and Research England's Global Challenge Research Fund (GCRF) for research to protect global environment (e.g., marine resources) using edge intelligence techniques. He currently serves as an associate editor for *IEEE Transactions on Sustainable Computing*, *IEEE Access* and *Journal of Big Data Research (Elsevier)*. He had served as an editor for IEEE COMML (big data and machine learning areas) from 2014 to 2019. He is also affiliated with the University of Sydney and Korea Advanced Institute of Science and Technology (KAIST) as a visiting professor. He is also a fellow of the HEA.

Zahir Tari (Senior Member, IEEE) received the bachelor's degree in mathematics from the University of Algiers, USTHB, Algeria, in 1984, the MSc degree in operational research from the University of Grenoble, France, in 1985, and the PhD degree in computer science from the University of Grenoble, France, in 1989. He is currently a full professor of distributed systems with RMIT University (Australia). From 1990-1992, he joined the Database Laboratory at EPFL (Swiss Federal Institute of Technology) as a senior researcher, where he worked on various aspects of distributed database systems. In 1993, he was appointed as a lecturer at QUT (Queensland University of Technology), and later joined the Royal Melbourne Institute of Technology(RMIT), in 1996 as a senior lecturer and is currently a professor, where he led the DSN (Distributed Systems and Networking) discipline at the School of Computer Science and IT. His research interests include system performance (e.g., P2P, Cloud, IoT) and system security (e.g., SCADA systems, Cloud). He regularly publishes in prestigious journals (e.g., *IEEE Transactions on Parallel and Distributed Systems*, *IEEE Transactions on Computers*, *JSAC*) and major international conferences (e.g., INFOCOM, ICDCS, ICDE, WWW). He has been PC (Program Committee) chair of more than 12 International conferences and GC (general chair) of more than 25 international conferences. He is a recipient of more than 11M$ in funding from ARC (Australian Research Council), industries (e.g., Siemens/Germany), and more lately part of a successful seventh Framework AU2EU (Australia to European) bid on Authorisation and Authentication for Entrusted Unions. He is also an associate editor of the *ACM Transactions on Computing Surveys*, *IEEE Transactions on Computers (TC)*, *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, and *IEEE Cloud Computing*.