IT Professional Special Issue on Security and Data Protection During the COVID-19 Pandemic and Beyond

José L. Hernández-Ramos, *University of Murcia, 30100, Murcia, Spain*
Paolo Bellavista, *University of Bologna, 40136, Bologna, Italy*
Georgios Kambourakis, *University of the Aegean, 83200, Karlovasi, Greece*
Jason R.C. Nurse, *University of Kent, CT2 7NF, Kent, U.K.*
J. Morris Chang, *University of South Florida, FL, 33620, USA*

The global landscape has been reshaped by the COVID-19 pandemic, causing unprecedented health, economic, and societal disruptions. In this transformative period, technology emerged as a vital lifeline, serving as both a shield against the virus and a catalyst for adapting to new challenges. Digital contact tracing frameworks rapidly emerged and became popular worldwide, thus enabling swift identification of potential exposure and containment of infections. In addition, the subsequent development of digital COVID certificates for vaccinations, immunity, and testing facilitated the safe resumption of daily activities and cross-border travel.

In fact, in recent years, technological advancements stemming from AI as well as the use of technologies like the Internet of Things (IoT) or blockchain, have propelled the development of innovative solutions to combat COVID-19. Such technologies have facilitated real-time monitoring of infected individuals and the identification of outbreaks, enhancing our capacity to respond effectively. However, the massive deployment of such technological solutions exacerbates security and data protection challenges. That is, ensuring the privacy of individuals, safeguarding data integrity, and enhancing cybersecurity to adapt to evolving work paradigms have become paramount concerns. The rapid digital transformation that accompanied the pandemic's challenges brought about not only opportunities but also significant cybersecurity and data protection challenges. As societies globally navigated these uncharted waters, it became evident that addressing these issues thoughtfully and comprehensively was essential. Indeed, the pandemic demonstrated that cybersecurity and data protection aspects go beyond technology, but they have legal and social implications that will continue evolving in the future.

While the World Health Organization declared "with great hope" an end to COVID-19 as a public health emergency in 2023, our society will have to face new emergency situations in the coming decades. We hope that the technological advancements of recent years and those to come as well as the lessons learned from the COVID-19 pandemic will serve to develop effective responses while cybersecurity and data protection are still properly addressed from a more multidisciplinary perspective, considering social and legal aspects. Indeed, we must ensure that cybersecurity and data protection remain at the forefront of our strategies, considering the complex interplay between technology, societal state transitions, and emergency preparedness.

The articles in this special issue highlight recent contributions in the areas of cybersecurity and data protection related to COVID-19 and the postpandemic world.

"Blockchain-Based Mechanism for Smart Record Monitoring During and After the COVID-19 Pandemic," by Geetanjali Rathee et al.,[A1] provides an overview of security and privacy mechanisms for facilitating efficient communication, decision making, planning, information recording, and management using smart devices in postpandemic scenarios. Furthermore, the authors explore the utilization of blockchain technology to establish a secure and trustworthy communication network.

In "The Changing Landscape of Privacy-Countermeasures in the Era of the COVID-19 Pandemic," Sherali Majeed and Seong Oun Hwang[1] analyze the aspects related to data privacy due to the COVID-19 pandemic and present developed countermeasures to

1520-9202 © 2023 IEEE
Digital Object Identifier 10.1109/MITP.2023.3322609
Date of current version 3 November 2023.

IN THIS ISSUE

There can be no question that COVID-19 has profoundly impacted society and, by extension, information technology. That is the topic of the September/October *IT Professional* special issue. At the same time, Hoda Diba[A4] has written "Employer Branding: The Impact of COVID-19 on New Employee Hires in IT Companies" for the IT Trends department. This article deals with subtle shifts in post-COVID employee attitudes that will likely necessitate changes in employer branding strategies. As this article touches the IT professional directly and aligns with the special issue, we elected to elevate this article to this edition's From the Editor column.

In the Formal Methods in Industry column, Axel Legay[A5] offers "Design, Validate, Implement, and Validate: From Dreaming Approaches to Realities." This article examines statistical model checking as a formal method to certify a strategic enterprise system as dependable, particularly in the era of AI. Although some limitations are inherent in this formal method, it also possesses some decisive advantages. Next, in his popular Life in the C-suite column, Steve Andriole[A6] asks, "How Competitive Are You?" Here, Andriole speaks directly to the importance of tackling competitive intelligence as a professionalized discipline as opposed to the less formal way by which many corporations often view their competition.

In the IT Security column, "Labeling Software Security Vulnerabilities," Irena Bojanova and John J. Guerrerio[A7] examine the methods by which the common weakness enumerations (CWEs) related to 228,000 common vulnerabilities and exposures (CVEs) in the National Vulnerability Database can be mapped to the Bugs framework. This detailed analysis reveals the value of refining the CWE definitions with the Bugs framework formalism to bolster a deeper understanding of CVEs. Finally, but highly timely as always, Nir Kshetri,[A8] in his powerful IT Economics department, examines "Generative Artificial Intelligence in Marketing." Here, he exposes the virtues of generative AI in marketing and counterposes with the barriers to entry, concluding that humans must remain in the loop. This article makes for an informative ending to a power-packed edition of *IT Professional*.

This edition also includes two feature articles, each dealing with machine learning as applied to an aspect of cybersecurity. The first feature, by Mohamed Saied Essa and Shawkat Kamal Guirguis,[A9] is "Evaluation of Tree-Based Machine Learning Algorithms for Network Intrusion Detection in the Internet of Things." Here, the authors present a literature review, identify salient research gaps, and then demonstrate the comparative value of six tree-based machine learning techniques to detect intrusion in an Internet of Things environment. The second feature article, by Michail Tsikerdekis and Sherali Zeadally,[A10] "Misinformation Detection Using Deep Learning," examines the effective use of various deep learning techniques in attacking differing forms of misinformation on social platforms. It then explores relevant challenges and opportunities in the deep learning approach toward curbing misinformation, concluding that further research may prove rewarding.

address these issues. The importance of implementing privacy strategies in epidemic-handling systems is emphasized, and key lessons for future similar pandemics are provided. This article was inadvertently published in the July/August edition of *IT Professional*. As such, it is available there to round out this special issue with a premature preview.

In "Enhancing Communication Among Remote Cybersecurity Analysts With Visual Traces," Chen Zhong et al.[A2] introduce an approach to enhance communication in collaborative cybersecurity analysis during the postpandemic era. This is done by utilizing visual traces of experts' analytical processes. Their method addresses the challenges of remote work and demonstrates its benefits through a case study. This provides insights for organizations aiming to improve communication in remote teams during collaborative problem solving in the postpandemic era.

All transformations that accompanied the pandemic's challenges brought about not only opportunities but also significant cybersecurity and data protection challenges. As societies globally navigated these uncharted waters, it became evident that addressing these issues thoughtfully and comprehensively was essential. Indeed, the pandemic demonstrated that cybersecurity and data protection aspects go beyond technology, but they have legal and social implications that will continue evolving in the future.

"Ransomware Attacks of the COVID-19 Pandemic: Novel Strains, Victims, and Threat Actors," by Zubair

APPENDIX: RELATED ARTICLES

A1. G. Rathee, C. A. Kerrache, and A. Cheriguene, "Blockchain-based mechanism for smart record monitoring during and after the COVID-19 pandemic," *IT Prof.*, vol. 25, no. 5, pp. 20–28, Sep./Oct. 2023, doi: 10.1109/MITP.2023.3310650.

A2. C. Zhong, J. B. Kim, and A. Yayla, "Enhancing communication among remote cybersecurity analysts with visual traces," *IT Prof.*, vol. 25, no. 5, pp. 29–36, Sep./Oct. 2023, doi: 10.1109/MITP.2023.3318485.

A3. Z. Baig, S. H. Mekala, and S. Zeadally, "Ransomware attacks of the COVID-19 pandemic: Novel strains, victims, and threat actors," *IT Prof.*, vol. 25, no. 5, pp. 37–44, Sep./Oct. 2023, doi: 10.1109/MITP.2023.3297085.

A4. H. Diba, "Employer branding: The impact of COVID-19 on new employee hires in IT companies," *IT Prof.*, vol. 25, no. 5, pp. 4–9, Sep./Oct. 2023, doi: 10.1109/MITP.2023.3321926.

A5. A. Legay, "Design, validate, implement, and validate: From dreaming approaches to realities," *IT Prof.*, vol. 25, no. 5, pp. 10–13, Sep./Oct. 2023, doi: 10.1109/MITP.2023.3314327.

A6. S. J. Andriole, "How competitive are you?" *IT Prof.*, vol. 25, no. 5, pp. 14–16, Sep./Oct. 2023, doi: 10.1109/MITP.2023.3314326.

A7. I. Bojanova and J. J. Guerrerio, "Labeling software security vulnerabilities," *IT Prof.*, vol. 25, no. 5, pp. 64–70, Sep./Oct. 2023, doi: 10.1109/MITP.2023.3314368.

A8. N. Kshetri, "Generative artificial intelligence in marketing," *IT Prof.*, vol. 25, no. 5, pp. 71–75, Sep./Oct. 2023, doi: 10.1109/MITP.2023.3314325.

A9. M. S. Essa and S. K. Guirguis, "Evaluation of tree-based machine learning algorithms for network intrusion detection in the Internet of Things," *IT Prof.*, vol. 25, no. 5, pp. 45–56, Sep./Oct. 2023, doi: 10.1109/MITP.2023.3303919.

A10. M. Tsikerdekis and S. Zeadally, "Misinformation detection using deep learning," *IT Prof.*, vol. 25, no. 5, pp. 57–63, Sep./Oct. 2023, doi: 10.1109/MITP.2023.3314752.

Baig et al.,[A3] analyzes the organizational vulnerabilities to threats exposed by the COVID-19 pandemic, focusing on the rise of ransomware attacks. It analyzes popular ransomware attacks during the pandemic and highlights the importance of preventing malware spread in corporate networks. The work identifies impactful ransomware strains and emphasizes the need for preventive and security measures.

REFERENCE

1. A. Majeed and S. O. Hwang, "The changing landscape of privacy– Countermeasures in the era of the COVID-19 pandemic," *IT Prof.*, vol. 25, no. 4, pp. 52–60, Jul./Aug. 2023, doi: 10.1109/MITP.2023.3287876.

JOSÉ L. HERNÁNDEZ-RAMOS is a Marie Sklodowska-Curie postdoc fellow with the Department of Information and Communications Engineering, University of Murcia, 30100, Murcia, Spain. Contact him at jluis.hernandez@um.es.

PAOLO BELLAVISTA is a full professor with the Department of Computer Science and Engineering, Alma Mater Studiorum, University of Bologna, 40136, Bologna, Italy. Contact him at paolo.bellavista@unibo.it.

GEORGIOS KAMBOURAKIS is a full professor with the Department of Information and Communication Systems Engineering, University of the Aegean, 83200, Karlovasi, Greece. Contact him at gkamb@aegean.gr.

JASON R.C. NURSE is a reader in cybersecurity with the School of Computing at the University of Kent, CT2 7NF, Kent, U.K., and the Institute of Cyber Security for Society, U.K. Contact him at j.r.c.nurse@kent.ac.uk.

J. MORRIS CHANG is a full professor with the Department of Electrical Engineering, University of South Florida, FL, 33620, USA. Contact him at chang5@usf.edu.