

Alma Mater Studiorum Università di Bologna
Archivio istituzionale della ricerca

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

This is the final peer-reviewed author's accepted manuscript (postprint) of the following publication:

Published Version:

Hernández-Ramos, J.L., Bellavista, P., Kambourakis, G., Nurse, J., Chang, J.M. (2023). IT Professional Special Issue on Security and Data Protection During the COVID-19 Pandemic and Beyond. IT PROFESSIONAL, 25(5), 17-19 [10.1109/MITP.2023.3322609].

Availability:

This version is available at: <https://hdl.handle.net/11585/952082> since: 2024-01-04

Published:

DOI: <http://doi.org/10.1109/MITP.2023.3322609>

Terms of use:

Some rights reserved. The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

This item was downloaded from IRIS Università di Bologna (<https://cris.unibo.it/>).
When citing, please refer to the published version.

(Article begins on next page)

This is the final peer-reviewed accepted manuscript of:

J. L. Hernández-Ramos, P. Bellavista, G. Kambourakis, J. R. C. Nurse and J. M. Chang, "IT Professional Special Issue on Security and Data Protection During the COVID-19 Pandemic and Beyond," in *IT Professional*, vol. 25, no. 5, pp. 17-19, Sept.-Oct. 2023.

The final published version is available online at:
<https://dx.doi.org/10.1109/MITP.2023.3322609>

Terms of use:

Some rights reserved. The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

This item was downloaded from IRIS Università di Bologna (<https://cris.unibo.it/>)

When citing, please refer to the published version.

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

José L. Hernández Ramos¹, Paolo Bellavista², Georgios Kambourakis³, Jason R.C. Nurse⁴, and J. Morris Chang⁵

¹University of Murcia, Spain

²University of Bologna, Italy

³University of the Aegean, Greece

⁴University of Kent, UK

⁵University of South Florida, USA

I. INTRODUCTION

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 artificial intelligence, as well as the use of technologies like the Internet of Things (IoT) or the Blockchain, have propelled the development of innovative solutions to combat COVID-19. Such technologies have facilitated the 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 exacerbate 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.

While the World Health Organization (WHO) 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 cyber-security and data protection are still properly addressed.

A. In This Issue

The articles in this special issue highlight recent contributions in the areas of cyber-security and data protection related to COVID-19 and the post-pandemic world.

The article “A Blockchain-based Mechanism for Smart Record Monitoring during and after the COVID-19 Pandemic”, by Geetanjali Rathee, Chaker Abdelaziz Kerrache

and Anissa Cheriguene provides an overview of security and privacy mechanisms for facilitating efficient communication, decision-making, planning, information recording, and management using smart devices in post-pandemic 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”, Abdul Majeed, and Seong Oun Hwang analyze the aspects related to data privacy due to the COVID-19 pandemic and present developed countermeasures to address these issues. The importance of implementing privacy strategies in epidemic handling systems is emphasized, and key lessons for future similar pandemics are provided.

In “Enhancing Communication among Remote Cybersecurity Analysts with Visual Traces in the Post-Pandemic World”, Chen Zhong, Joo Baek Kim and Alper Yayla introduce an approach to enhance communication in collaborative cybersecurity analysis during the post-pandemic 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 post-pandemic era.

The article “Ransomware Attacks of the COVID-19 Pandemic: Novel Strains, Victims, and Threat Actors” by Zubair Baig, Sri Harsha Mekala and Sherali Zeadally, analyzes the organizational vulnerabilities exposed by the COVID-19 pandemic to cyberthreats, 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.

José L. Hernández-Ramos is a Marie Skłodowska-Curie Postdoc Fellow at the Dept. of Information and Communications Engineering, Uni-

versity of Murcia, Spain. His research interests include the application of machine learning techniques to enhance cybersecurity. Contact him at: jluis.hernandez@um.es

Paolo Bellavista is a Full Professor with the Department of Computer Science and Engineering (DISI), Alma Mater Studiorum - University of Bologna, Italy. His research interests span from middleware for mobile computing to edge/fog computing, from QoS management in 5G/6G applications with ultra-low latency requirements to container-based edge-deployed digital twins for industrial IoT. Contact him at: paolo.bellavista@unibo.it

Georgios Kambourakis is a Full Professor at the Dept. of Information and Communication Systems Engineering, University of the Aegean, Greece. His research interests are in fields of mobile and wireless networks security and privacy, VoIP security, IoT security and privacy, DNS security, and security education. Contact him at: gkamb@aegean.gr

Jason Nurse is a Reader in Cyber Security in the School of Computing at the University of Kent, UK and the Institute of Cyber Security for Society (iCSS), UK. His research interests include security risk management, cyber insurance, corporate communications and cyber security, secure and trustworthy Internet of Things, insider threat, and cybercrime. Contact him at: j.r.c.nurse@kent.ac.uk

K. Morris Chang is a Full Professor at the Dept. of Electrical Engineering, University of South Florida, USA. Dr. Chang's research interests include cyber security, wireless networks, energy-aware computing and object-oriented systems. Contact him at: chang5@usf.edu