

## EDITORIAL

### Special Issue on Cybersecurity in Healthcare, Edition 1 Volume 4, April 2024

### ARIS<sup>2</sup> - Advanced Research on Information Systems Security an International Journal

Nuno Mateus-Coelho, PhD \*

#### 1. INTRODUCTION

In today's fast-evolving realm of cybersecurity, where technology advances swiftly and threats multiply incessantly, it's paramount to keep pace with cutting-edge research and fresh concepts [1], [2], [3], [4]. In this era of perpetual transformation and evolving obstacles, ARIS2 - Advanced Research on Information Systems Security remains steadfast, providing guidance to scholars, practitioners, and enthusiasts as they navigate the complex landscape of cyber defenses and digital security measures.

As we delve into this Special Issue on Cybersecurity in Healthcare, part of Volume 4, Issue 1, we find ourselves at a pivotal moment, fully aware of the urgent issues defining cybersecurity in today's era. With each passing day, new vulnerabilities surface, threat actors grow more sophisticated, and the digital frontier extends into uncharted territories. In this landscape, ARIS2 serves as an indispensable guide, steering discussions toward leading-edge research and fostering a deeper comprehension of the unique challenges and opportunities in healthcare and health technologies [5].

As we delve into the core of this Special Issue of the Volume 4, Issue 1, we extend an invitation to our readers to embark on a journey of discovery, navigating through the realms of social engineering resilience and the integrative capabilities of enterprise architecture in cybersecurity. In a landscape where cyber threats continue to evolve in complexity and diversity, ARIS2 remains unwavering in its dedication to providing a platform for research that not only confronts the challenges of today but also lays the foundation for a resilient and secure digital future.

## **2. STRUCTURE**

In an era where healthcare systems increasingly rely on digital technologies to deliver efficient and effective care, the importance of cybersecurity in safeguarding patient data and maintaining operational continuity cannot be overstated. As healthcare organizations continue to adopt electronic health records (EHRs), telemedicine platforms, and internet-connected medical devices, they become more vulnerable to cyber threats that can compromise patient privacy, disrupt clinical services, and undermine public trust. Consequently, addressing the ethical, legal, and technological dimensions of cybersecurity in healthcare has become a paramount concern for stakeholders across the industry.

### **Ethical and Legal Aspects of Cybersecurity in Health**

Discussion on ethical considerations related to patient privacy, data security, and informed consent in healthcare.

Examination of legal frameworks governing healthcare data protection and cybersecurity practices.

Insights into the ethical responsibilities of healthcare professionals and organizations in safeguarding patient information.

Recommendations for ensuring compliance with ethical standards and legal regulations in healthcare cybersecurity.

### **Exploring the Dynamics between Artificial Intelligence and Cybersecurity in Healthcare**

Exploration of the evolving role of artificial intelligence (AI) in healthcare cybersecurity. Analysis of AI-driven cybersecurity solutions for threat detection, incident response, and vulnerability management.

Discussion on the potential benefits and challenges of integrating AI into healthcare cybersecurity practices.

Case studies highlighting successful AI implementations and their impact on healthcare security.

### **Cyber Threats to Healthcare Technology Services: A Case Study**

Detailed case study of cybersecurity threats targeting healthcare technology services.

Examination of specific cyber threats faced by healthcare organizations, such as ransomware attacks, data breaches, and insider threats.

Analysis of the impact of cyber-attacks on patient care, data integrity, and healthcare operations.

Lessons learned and best practices for mitigating cyber threats and enhancing resilience in healthcare technology services.

### **Database Decomposition to Satisfy the Least Privilege Principle in Healthcare**

Explanation of the least privilege principle and its importance in healthcare data security. Discussion on database decomposition techniques for minimizing access privileges and reducing the attack surface in healthcare databases.

Case examples illustrating the implementation of database decomposition strategies in healthcare settings.

Recommendations for integrating database decomposition into broader cybersecurity frameworks to enhance data protection and compliance.

### **3. ACKNOWLEDGEMENTS**

We would like to thank the authors who have submitted their manuscripts and all the reviewers for their valuable contributions. The scientific importance of the publications in this Issue of the ARIS<sup>2</sup> - Journal is a strong reason for other authors to submit works for future Regular and Special Issues.

### **REFERENCES**

- [1] Mateus-Coelho, Nuno, and Manuela Cruz-Cunha, editors. Exploring Cyber Criminals and Data Privacy Measures. IGI Global, 2023. <https://doi.org/10.4018/978-1-6684-8422-7>
- [2] Daniel Jorge Ferreira, Nuno Mateus-Coelho and Henrique S. Mamede, Methodology for Predictive Cyber Security Risk Assessment (PCSRA), Procedia Computer Science, Volume 219, 2023, Pages 1555-1563, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2023.01.447>.
- [3] Mario Saraiva, Nuno Mateus-Coelho, CyberSoc Framework a Systematic Review of the State-of-Art, Procedia Computer Science, Volume 204, 2022, Pages 961-972, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2022.08.117>.
- [4] M. Saraiva and N. Coelho, "CyberSoc Implementation Plan," 2022 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey, 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800819.
- [5] Filipe Alves, Nuno Mateus-Coelho, Manuela Cruz-Cunha, Encryption File System Framework - Proof of Concept, Procedia Computer Science, Volume 181, 2021, Pages 1237-1246, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2021.01.322>.

### **How to cite this article:**

Mateus-Coelho, N. (2024). *The Editorial of ARIS<sup>2</sup> - Advanced Research on Information Systems Security, an International Journal*, Special Issue on Cybersecurity in Healthcare, Vol. 4, No. 1, 1-3.