Accepted Manuscript online: 2022-02-10 Article published online: 2022-08-19

Editorial for Focus Theme

Security and Privacy in Distributed Health Care Environments

Stephen V. Flowerday[1] Christos Xenakis[2]

[1] Department of Information Systems, Rhodes University, Grahamstown, South Africa
[2] Department of Digital Systems, University of Piraeus, Pireas, Greece

Methods Inf Med 2022;61:1–2.

Introduction

There is an increasing demand for distributed health care systems. Nevertheless, distributed health care environments do not come without risks. At the same time that distributed health care systems are growing, so are the cybersecurity threats targeting them. Additionally, the demand for compliance to new regulations increases as these distributed health care systems hold sensitive patient data. The use of data-driven technologies presents a promising opportunity for significant advances in the field toward improved health care for patients and the general public.[1,2] Several recent studies have highlighted the importance and the necessity of developing a data-driven approach where patient data are collected, analyzed, and leveraged for medical research purposes with the help of different types of artificial intelligence. To address the privacy-related challenges, novel methods, such as protection of personal health information, ensuring compliance, guaranteeing FAIR information processing, and building of trust, are required. In this issue, new paradigms and prominent applications are presented for secure, trustworthy, and privacy-preserving data sharing and knowledge representation to address the emerging needs.

Selected Articles

Three articles were selected after a rigorous peer-review process. Next, there are brief descriptions of the different articles:

Privacy-Preserving Artificial Intelligence Techniques in Biomedicine

Torkzadehmahani et al[3] in their recent work have reviewed the latest advances in privacy-preserving AI techniques applied to facilitate collaborative research in biomedicine that is currently being hindered by the privacy risks that emerge when training AI models on sensitive data. The numerous advantages of using AI in genomic and biomedical data analysis are counterbalanced by the serious privacy concerns raised regarding an individual's privacy. The paper goes beyond existing surveys by presenting a broader set of privacy-preserving AI techniques, including homomorphic encryption, secure multiparty computation, federated learning, and previously proposed hybrid approaches that combine characteristics from the above techniques to overcome their disadvantages. Comparing the different approaches in terms of efficiency, accuracy, and privacy revealed that the federated learning as a standalone approach or in combination with differential privacy is the most promising approach to be adopted in biomedicine.

A Privacy-Preserving Distributed Analytics Platform for Health Care Data

In recent years, data-driven medicine has gained an increasing importance in diagnosis, treatment, and research due to the exponential growth of health care data. However, data protection regulations prohibit data centralization for analysis purposes because of potential risk such as unauthorized disclosure. Therefore, this paper[4] aims to enable analyses on sensitive patient data by simultaneously complying with local data protection regulations by using an approach called the personal health train (PHT), which is a paradigm that utilizes distributed analytics methods.[1,2] The main principle of the PHT is that the analytical task is brought to the data provider and the data instances remain in their original location. This work presents the implementation of PHT and its novel features, which preserve the sovereignty and autonomy of the data providers.

Toward the Representation of Network Assets in Health Care Environments Using Ontologies

The article by Prieto Santamaría et al[5] describes the development of ontological models to represent distributed health care computer networks' data by reusing and

Address for correspondence
Stephen V. Flowerday, PhD, Department of Information Systems, Rhodes University, Eastern Cape 6139, South Africa (e-mail: s.flowerday@ru.ac.za).

DOI https://doi.org/10.1055/a-1768-2966.
ISSN 0026-1270.

Georg Thieme Verlag KG, Rüdigerstraße 14, 70469 Stuttgart, Germany

creating classes and properties consistent with the information context. Ontologies are a formal way to express knowledge employing triples composed of a subject, a predicate, and an object. The context is essential as health care environments are demanding as the systems deal with sensitive patient data, and thus cybersecurity becomes crucial. Therefore, this representation makes it possible for network administrators in health care institutions to clearly understand potential threats that may emerge in the network and monitor these threats in real time.

Conclusion

Within the context of distributed health care environments, technology has become critical as it processes and preserves sensitive patient data. Furthermore no matter how useful the data-driven technologies are for the advancement of medical science and for the effective health care delivery, they can only be used if they do not threaten patients' privacy. Various approaches and infrastructures have been developed to ensure that patients and research participants remain anonymous when data are shared and analyzed for research purposes. A set of relevant works has been presented in this issue targeting some of the domain's emerging security and privacy concerns.

Conflict of Interest

None declared.

Acknowledgment

The authors wish to thank the editors of *Methods of Information in Medicine* for supporting them through publishing this focus theme.

References

1 Chang K, Balachandar N, Lam C, et al. Distributed deep learning networks among institutions for medical imaging. J Am Med Inform Assoc 2018;25(08):945–954
2 Sheller MJ, Reina GA, Edwards B, Martin J, Bakas S. Multi-institutional deep learning modeling without sharing patient data: a feasibility study on brain tumor segmentation. Brainlesion 2019; 11383:92–104
3 Torkzadehmahani R, Nasirigerdeh R, Blumenthal DB, et al. Privacy-preserving artificial intelligence techniques in biomedicine. Methods Inf Med 2022 (e-pub ahead of print). Doi: 10.1055/s-0041-1740630
4 Welten S, Mou Y, Neumann L, et al. Privacy-preserving distributed analytics platform for healthcare data. Methods Inf Med 2022 (e-pub ahead of print). Doi: 10.1055/s-0041-1740564
5 Prieto Santamaría L, Fernández Lobón D, Díaz-Honrubia AJ, Ruiz EM, Nifakos S, Rodríguez-González A. Towards the representation of network assets in health care environments using ontologies. Methods Inf Med 2021;60(S 02):e89–e102

