



Universiteit
Leiden
The Netherlands

Secure distributed machine learning in healthcare: a study on FAIR, compliance and cybersecurity for federated learning

Plug, R.B.F.

Citation

Plug, R. B. F. (2025, December 17). *Secure distributed machine learning in healthcare: a study on FAIR, compliance and cybersecurity for federated learning*. Retrieved from <https://hdl.handle.net/1887/4285632>

Version: Publisher's Version
License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)
Downloaded from: <https://hdl.handle.net/1887/4285632>

Note: To cite this publication please use the final published version (if applicable).

Secure Distributed Machine Learning in Healthcare:

A Study on FAIR, Compliance and Cybersecurity for Federated Learning

Proefschrift

ter verkrijging van

de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof.dr.ir. H. Bijl,
volgens besluit van het college voor promoties
te verdedigen op woensdag 17 december 2025

klokke 16.00 uur

door

Ruduan Benjamin Franklin Plug

geboren te Leiden

in 1991

Colophon

Design and Layout: Ruduan B.F. Plug

Illustrations: Ruduan B.F. Plug

Printing: Print&Bind

Copyright © 2025 Ruduan Benjamin Franklin Plug

All rights reserved. No part of this thesis may be reproduced in any form without the written permission of the author.

Wageningen University & Research

University of Amsterdam
Heidelberg University
Leiden University
Amsterdam University Medical Center

Promotores

Prof. Dr. M.E.H. van Reisen
Prof. Dr. A. Fensel

Leden Promotiecommissie

Prof. Dr. T.H. van den Akker
Prof. Dr. P.T. Groth
Dr. L. Maxwell
Prof. Dr. M.M. Bonsangue
Prof. Dr. R. Cornet

Contents

1	Introduction	5
1.1	Research Context	5
1.2	Research Outline	13
I	Article 1	20
2	Terminology for a FAIR Framework for the Virus Outbreak	
	Data Network-Africa	21
2.1	Introduction	22
2.2	Data concepts	24
2.3	FAIR health data management	35
2.4	Jurisdiction and data governance	45
2.5	Discussion and conclusion	57
II	Article 2	66
3	FAIR and GDPR Compliant Population Health Data	
	Generation, Processing and Analytics	67
3.1	Introduction	68
3.2	FAIR and GDPR Standards	69
3.3	Study Results	71
3.4	Conclusion	76

III Article 3 82

4 Advancing Cyber Resilience in Edge Computing with Secure Distributed Machine Learning	83
4.1 Introduction	84
4.2 Federated Learning in Edge Computing	89
4.2.1 Properties of Federated Learning	90
4.2.2 Communication Efficiency of Federated Learning . .	93
4.2.3 Privacy-Preservation in Federated Learning	95
4.2.4 Ethical and Regulatory Considerations in Federated Learning	98
4.3 Secure Multi-Party Computation in Edge Computing	100
4.3.1 Security Methods of Secure Multi-Party Computation	101
4.3.2 Advanced Cryptographic Techniques for Secure Multi-Party Computation	104
4.3.3 Ethical and Regulatory Considerations in Secure Multi-Party Computation	109
4.4 Secure Distributed Machine Learning	111
4.4.1 Motivation behind Secure Distributed Machine Learning	112
4.4.2 Secure Distributed Machine Learning Architecture .	116
4.5 Discussion	122
4.6 Conclusion	126

IV Article 4 136

5 Benchmarking TinyML Encrypted Federated Learning with Secret Sharing in Medical Computer Vision	137
5.1 Introduction	138
5.2 Related Work	139
5.3 Methodology	141
5.3.1 MedMNIST Dataset	141
5.3.2 ResNet18 Model Architecture	143
5.3.3 Federated Learning Architecture	144

5.3.4	Encryption and Secret Sharing	147
5.3.5	Experimental Setup	150
5.4	Results	152
5.5	Conclusion	157
6	Discussion	163
6.1	Main Findings	164
6.2	Future Research	169
A	Appendix	181
	Summary	181
	Samenvatting	183
	Curriculum Vitae	185
	List of Publications	187
	Acknowledgements	190