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

Plug, R.B.F.

Curriculum Vitae

Ruduan Benjamin Franklin Plug was born on the 12th of July 1991 in Leiden, Netherlands. After completing his primary and secondary education, he started working as an independent contractor in web development for a couple of years before enrolling in Leiden University. There he attained a BSc. in Informatics and a MSc. in Computer Science. He graduated on the master thesis "*Methods for Federated Data Analysis*", which was a joint research project between Leiden University and Stanford University. He was awarded the Honours and Cum Laude distinctions.

During his studies Ruduan has attended the International Leiden Leadership Programme, has assisted in the teaching of twelve courses and was one out of two people in Netherlands that was awarded the prestigious Google Scholarship of 2021. He has also been part of the research group led by his supervisor, Prof. Dr. Mirjam van Reisen. There he contributed to the ongoing research in the VODAN consortium.

After graduating he has continued his research as an external PhD researcher at LUMC under supervision of Prof. Dr. Mirjam van Reisen. His work primarily revolves around the theory and application of FAIR, machine learning and federated learning in the healthcare domain. His research has practical grounding and application within VODAN, collaborating cross-discipline with clinicians and researchers in Africa as well as global experts in clinical informatics, data science and computer science. During his research he has served as an ambassador for GO FAIR and has been a member of the GAIC expertise network.

Ruduan has previously worked as a junior scientist and later scientist in ML/AI at the Netherlands Organisation for Applied Scientific Research (TNO). His work focused on energy grid analysis and optimisation, working on topics such as net congestion and load balanc-

ing. Currently he works at Booking as a machine learning engineer. Ruduan's areas of expertise includes machine learning and software engineering. He specialises in topics of distributed machine learning, federated learning, language modelling and computer vision.

ORCID: 0000-0001-5146-6116

List of Publications

Publications included in this dissertation

1. **Plug, R.B.F.**, Jati, P.H.P., Amare, S.Y., & van Reisen, M. (2025). *Benchmarking TinyML Encrypted Federated Learning with Secret Sharing in Medical Computer Vision*. In A.L. Imoize, D. Dinh-Thuan, & H.H. Song (Eds.), Tiny Machine Learning: Design Principles and Applications (Ch.19). Wiley-IEEE Press. ISBN: 978-1-394-29454-1

2. **Plug, R.B.F.**, Amare, S.Y., Jati, P.H.P., Kievit, R., Kawu, A.A., Liang, Y., & van Reisen, M. (2025). *Secure Distributed Machine Learning for Edge Computing*. In A.L. Imoize, F. Xhafa, M.S. Obaidat, & H.H. Song (Eds.), Cybersecurity Defensive Walls in Edge Computing (Ch.10). Elsevier Academic Press. ISBN: 978-0-443-34109-0. doi: 10.1016/B978-0-443-34109-0.00001-2.

3. **Plug, R.**, Liang, Y., Basajja, M., Aktau, A., Jati, P.H., Amare, S., Taye, G.T., Mpezamihigo, M., Oladipo, F.O., & van Reisen, M. (2022). *FAIR and GDPR Compliant Population Health Data Generation, Processing and Analytics*. In *Proceedings of the 13th International Conference on Semantic Web Applications and Tools for Health Care and Life Sciences (SWAT4HCLS)*. CEUR Workshop Proceedings, Vol-3127. ISSN 1613-0073. urn:nbn:de:0074-3127-1

4. **Plug, R.**, Liang, Y., Aktau, A., Basajja, M., Oladipo, F., & van Reisen, M. (2022). *Terminology for a FAIR framework for the Virus Outbreak Data Network-Africa*. Data Intelligence, 4(4), 698–723. doi: 10.1162/dint_a_00167

Other publications during doctoral candidacy

5. Amare, S.Y., Taye, G.T., **Plug, R.**, Medhanyie, A.A., & van Reisen, M. (2025). *Federating tools for FAIR patient data: Strengthening maternal health and infectious disease surveillance from clinics to global systems*. Langaa Research and Publishing Common Initiative Group. doi: 10.5281/zenodo.15382870

6. Aktau, A., Amare, S.Y., van Reisen, M., Taye, G.T., Gebremeskel, T.G., Purnama Jati, P.H., & **Plug, R.** (2025). *GO TRAIN: A protocol for metadata creation for the FAIRification of patient data health records*. Langaa Research and Publishing Common Initiative Group. doi: 10.5281/zenodo.15382836

7. van Reisen, M., Amare, S.Y., **Plug, R.**, Taye, G.T., Gebreslassie, T.G., Kawu, A.A., Smits, K., Woldu, L.M., Stocker, J., Heddema, F., Folorunso, S.O., Kievit, R., & Medhanyie, A. (2024). *Curation of federated patient data: A proposed landscape for the African Health Data Space*. Elsevier Academic Press. doi: 10.1016/B978-0-443-13897-3.00013-8

8. Gebreslassie, T.G., van Reisen, M., Amare, S.Y., Taye, G.T., & **Plug, R.** (2023). *FHIR4FAIR: Leveraging FHIR in health data FAIRfication process: In the case of VODAN-A*. FAIR Connect, 1(1), 49–54. doi: 10.3233/FC-230504

9. Amare, S.Y., Taye, G.T., Gebreslassie, T.G., **Plug, R.**, & van Reisen, M. (2023). *Realizing health data interoperability in low connectivity settings: The case of VODAN-Africa*. FAIR Connect, 1(1), 55–61. doi: 10.3233/FC-221510.

10. Trantas, A.[1], **Plug, R.**[1], Pileggi, P., & Lazovik, E. (2023). *Digital twin challenges in biodiversity modelling*. Ecological Informatics, 78, 102357. doi: 10.1016/j.ecoinf.2023.102357

11. van der Holst, B., Verhoeven, G., Matthijssen, E., Vrijlandt, M., **Plug, R.**, van der Meer, A., & Kok, K. (2023). *A dynamic bandwidth tariff assessment in a Dutch distribution network using a novel scalable distributed simulation framework*. CIRED 2023. IEEE IET. doi: 10.1049/icp.2023.0722

12. Jati, P.H.P., van Reisen, M., Flikkenschild, E., Oladipo, F., Meerman, B., **Plug, R.**, & Nodehi, S. (2022). *Data access, control, and privacy protection in the VODAN-Africa architecture*. Data Intelligence, 4(4), 938–954. doi: 10.1162/dint_a_00180

[1] Authors contributed equally to this work.

13. van Reisen, M., Oladipo, F.O., Mpezamihigo, M., **Plug, R.**, Basajja, M., Aktau, A., Jati, P.H.P., Nalugala, R.M., Folorunso, S., Amare, S.Y., Abdulahi, I., Afolabi, O.O., Mwesigwa, E., Taye, G.T., Kawu, A.A., Ghardallou, M., Liang, Y., Osigwe, O., Medhanyie, A.A., & Mawere, M. (2022). *Incomplete COVID-19 data: The curation of medical health data by the Virus Outbreak Data Network-Africa*. Data Intelligence, 4(4), 673–697. doi: 10.1162/dint_e_00166

14. Basajja, M., Suchanek, M., Taye, G.T., Amare, S.Y., Nambobi, M., Folorunso, S., **Plug, R.**, Oladipo, F., & van Reisen, M. (2022). *Proof of concept and horizons on deployment of FAIR Data Points in the COVID-19 pandemic*. Data Intelligence, 4(4), 917–937. doi: 10.1162/dint_a_00179

Acknowledgements

I would like to begin by expressing my sincere gratitude to my supervisors, Prof. Dr. Mirjam van Reisen and Prof. Dr. Anna Fensel. Working under your guidance has been a privilege.

Mirjam, thank you for always believing in me and for opening the door for me to the VODAN consortium and the thought-provoking GAIC research group. Your vision and passion for human-centred research are what have inspired me to pursue this endeavour, resulting in countless memories and experiences that will remain with me.

Anna, I am grateful for your thoughtful insights and guidance throughout my doctoral research. You helped me see things from a different angle and provided feedback that strengthened the scientific quality of my writing.

I also want to specifically thank Prof. Dr. Mark Musen for taking the time to thoroughly review my dissertation and for the opportunity to collaborate with the Stanford Center for Biomedical Informatics Research. This collaboration initially motivated me to pursue research and represents an important milestone in my academic journey.

My heartfelt thanks go to the entire VODAN consortium. There are too many of you to name, but each of you has shaped me into the researcher I am today. You have made this journey meaningful, and I hope to have the opportunity to collaborate with you again in the future. I would also like to thank all the members of GAIC, and especially the PhD peer-group: Kai, Rens and Putu, for the feedback and support you have offered me.

Lastly, I would like to thank my family, my partner and her family for their unwavering support. I owe this to you, and undertaking this endeavour would not have been possible without your support.