PhD thesis topic proposal.
Strengthening the reliability and safety of AI methods in a medical context.

Supervisor: J.-F. Couchot, MCF, HDR, FEMTO-ST, France

Summary

The general objective of this PhD is to improve the reliability/security of Artificial Intelligence (AI) methods when applied to hospital medical data. It takes place in a context of collaboration between the Computer Science Department of FEMTO-ST and the Hôpital Nord Franche-Comté (HNFC) located in Belfort in Burgundy-Franche-Comté, France.

The medical input data are multi-types: they come from the Medicalization Program of Information Systems (PMSI) of the SNDS which is a standardized synthetic description of the medical activity of health institutions, medecine classification (Anatomical Therapeutic Chemical code) and data to be extracted from the computerized patient file of the Hôpital Nord Franche-Comté (mixing text, codes, numerical values) for which the Department of Medical Information (DIM) of the HNFC has the expertise. They must be handled with the utmost rigour and confidentiality, in compliance with the RGPD as they are personal data. A collaboration agreement between the two entities FEMTO-ST and HNFC is being set up and will be established before the beginning of the PhD. In particular, methods for anonymization of multi-type longitudinal medical data (medical reports, numerical values, etc.) based on differential confidentiality will be defined, theoretically validated and validated by the medical team of the DIM, then applied to the data present in this study to allow the implementation of AI on them. The AI approaches will aim to isolate from the PMSI atypical care trajectories that could be explained by combinations of medicines (pharmacovigilance), by Care Associated Infections (CAI). The analysis algorithms will also need to integrate other types of data such as textual medical reports, numerical and/or textual results of analysis, CIM-10 codes... If necessary, the variables that best explain the problem cases will be extracted.

Analyses of anonymized medical data will first of all be based on recent AI approaches such as the automatic processing of natural languages by Deep Learning [DCLT19, AMB$^+$19] or gradient boosting approaches, methods on which FEMTO-ST has experience [CGR19]. They will be continued using very recent approaches [ACG$^+$16, Mir17], particularly implanted in pytorch-dp[1] and performing analyses on raw data (*i.e.* identifying and personal data) but guaranteeing on the fly privacy through differential confidentiality. The objective will be to improve the reliability and security of these two dual approaches.

Necessary Skills

The candidate must have a Master's degree in Computer Science or Mathematics and have certified competence in:

- probabilities;
- setting up AI schemes (DeepLearning, GAN, XGBoost).

Application

All correspondence should be sent to couchot@femto-st.fr. The candidate must send by e-mail:

- her/his detailed resume;
- her/his master's transcripts;
- letters of recommendation from her/his teachers and supervisors.

.

[1] https://github.com/facebookresearch/pytorch-dp

References

[ACG$^+$16] Martín Abadi, Andy Chu, Ian J. Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 308–318. ACM, 2016.

[AMB$^+$19] Emily Alsentzer, John R. Murphy, Willie Boag, Wei-Hung Weng, Di Jin, Tristan Naumann, and Matthew B. A. McDermott. Publicly available clinical BERT embeddings. *CoRR*, abs/1904.03323, 2019.

[CGR19] Jean-François Couchot, Christophe Guyeux, and Guillaume Royer. Anonymously forecasting the number and nature of firefighting operations. In Bipin C. Desai, Dimosthenis Anagnostopoulos, Yannis Manolopoulos, and Mara Nikolaidou, editors, *Proceedings of the 23rd International Database Applications & Engineering Symposium, IDEAS 2019, Athens, Greece, June 10-12, 2019*, pages 30:1–30:8. ACM, 2019.

[DCLT19] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. BERT: pre-training of deep bidirectional transformers for language understanding. In Jill Burstein, Christy Doran, and Thamar Solorio, editors, *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, NAACL-HLT 2019, Minneapolis, MN, USA, June 2-7, 2019, Volume 1 (Long and Short Papers)*, pages 4171–4186. Association for Computational Linguistics, 2019.

[Mir17] Ilya Mironov. Renyi differential privacy. *CoRR*, abs/1702.07476, 2017.