**武汉理工大学本科生毕业设计（论文）任务书**

学院： 信息工程学院 专业班级：\_\_信息2001 \_\_\_

姓名： 胡姗 学 号：\_\_0122015710114\_

毕业设计（论文）题目：面向隐私保护深度学习的变换数据分类方法

任务书包含以下方面的内容：

1. 设计（论文）主要内容：

本次毕业设计的主要内容是研究面向隐私保护深度学习的变换数据分类方法，运用深度学习方法，设计和实现一种面向隐私保护深度学习的变换数据分类方法，采用现有的主流的隐私保护深度学习模型来产生训练数据与标签，再基于训练数据构建分类模型，并分析分类模型的效率，通过实验验证模型的准确率和有效性。包括以下任务：（1）掌握并复现差分隐私、同态加密等主流的隐私保护深度学习模型的原理，并运用其方法生成模型训练数据集与标签；（2）搭建深度学习神经网络模型，划分数据集后进行训练分类网络，对模型评估与调优；（3）集成上述工作，给出一种完整的可解决隐私保护中变换数据分类问题的理论方案，并搭建神经分类网络对所提方案进行量化的性能分析。

（二） 完成的主要任务及要求：

1、查阅不少于15篇的相关参考文献资料（其中，近5年外文文献不少于3篇)。

2、完成至少1500字开题报告等规定的毕业设计文档。

3、研究隐私保护方法与技术分类问题的相关工作，设计一种完整的可解决隐私保护中变换数据分类问题的理论方案，并对所提方案进行量化的性能分析。

4、撰写不少于12000字的毕业论文并完成答辩的相关工作。

5、完成不低于5000汉字（20000英文印刷符）的教师指定的相关文献英译汉翻译。

（三） 完成任务的时间节点：

第1-3周：确定选题，查阅相关中、英文文献资料，外文翻译和撰写开题报告；

第4-5周：完成论文开题工作，完成英文专业文献翻译任务；

第6-12周：完成系统方案设计、深度学习网络设计与实现、系统测试与完善，并撰写论文初稿；

第13-15周：修改完善毕业论文；

第16周：进行论文答辩工作。

1. 必读参考文献：
2. Sousa, S. and Kern, R. How to keep text private? A systematic review of deep learning methods for privacy-preserving natural language processing. Artificial Intelligence Review, 56(2), pp.1427-1492, 2023.
3. M. Campbell, Privacy-Preserving Computation: Doomed to Succeed, in Computer, vol. 55, no. 8, pp. 95-99, Aug. 2022.
4. Rehman, M.U., Shafique, A., Ghadi, Y.Y., Boulila, W., Jan, S.U., Gadekallu, T.R., Driss, M. and Ahmad, J. A novel chaos-based privacy-preserving deep learning model for cancer diagnosis. IEEE Transactions on Network Science and Engineering, 9(6), pp.4322-4337, 2022.
5. 沈传年,徐彦婷,陈滢霞.隐私计算关键技术及研究展望[J].信息安全研究,2023,9(08):714-721.
6. 白晓雷,张海岩,王硕.联邦学习隐私攻击与保护技术研究综述[J].网络安全技术与应用,2023(12):34-35.

指导教师签名： 马小林 2023 年 12月 17日

系主任签名： 阮幼林 2023 年 12月 18日

院长签名（章）： 李政颖 2023 年 12月 18日