福州大学计算机与大数据学院

课程技术报告

课题名称： **AI 模型攻击方法**

学　　号： **102102145**

姓　　名： **胡嘉鑫**

专　　业： **数据科学与大数据技术**

学　　期： **2023 学年第 2 学期**

2024 年 5 月

注意：*成稿后删除所有红色文字*。

总页数建议在 10 页左右，截图不宜过大，双面打印!!

XXXXXXX

比如：一种面向联邦学习模型的数据投毒方法及实验

【报告要求】从以下课题中任选 1 个课题，调研、学习、并撰写一个课程技术报告。

【可选课题】AI 模型攻击方法及实验实践，AI 模型防御方法及实验实践，去隐私技术及实验实践.

【报告内容建议】调研并学习针对数据集或 AI 模型的攻防技术方法，并进行一定的实验实践，尽量能够给出一定验证结果及描述。内容的书写可以参考以下几个部分来展开。

1、引言（或概述）

2、技术原理及方法

3、实验实践与结果分析

4、总结与发展趋势

参考文献（样例）

[1] 中国互联网协会 2006 年第一次反垃圾邮件调查结果.http://www.anti-spam.cnlShowArticle.php?id=2713

[2] 曹麒麟，张千里.垃圾邮件与反垃圾邮件技术[M].北京:人民邮电出版社，2003.

[3] 罗改龙.基于 SPI 的防火墙的研究与实现[硕士学位论文].武汉:武汉理工大学，2007
[4] 周茜，赵明生.中文文本分类中的特征选择研究[J].中文信息学报,2003,Vol.18 No.3