|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **分类号** |  | **密级** |  | |
|  |  |  |  |  | |
|  | | | | | |
| **重庆邮电大学研究生学位论文**  **中期考核报告** | | | | | |
|  | | | | | |
|  | **中文题目** | **针对不平衡样本分布的安全漏洞** | | |  |
|  | **分类方法的研究** | | |
| **英文题目** | **Research on Security Vulnerability** | | |
|  | **Classification Methods for** | | |
|  | **Unbalanced Sample Distribution** | | |
| **学 号** | **S211231083** | | |
| **姓 名** | **朱思宇** | | |
| **学位层次** | **硕士研究生** | | |
| **学位类别** | **工程硕士** | | |
| **学科专业** | **软件工程** | | |
| **研究方向** | **软件智能与测评技术** | | |
| **指导教师** | **韦庆杰 正高级工程师** | | |
| **完成日期** | **2023年 12月 24日** | | |
|  | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **一、研究生简况** | | | | | | | | | | | | | | | | |
| 姓名 | 朱思宇 | | | 性别 | 男 | | | 年龄 | | 24 | | 专业类型 | | 专业型 | | |
| 导师 | | | | 韦庆杰 | | | | 所在团队名称  团队负责人 | | | | 重庆邮电大学图像智能与软件工具团队 钱鹰 | | | | |
| 外出实习单位 | | | | 无 | | | | 外出实习时间 | | | | 无 | | | | |
| 开题时间 | | | | 2023.2.27 | | | | 开题状态 | | | | 正常开题 | | | | |
| 学籍异动情况 | | | | 无 | | | | | | | | | | | | |
| **二、学位论文工作进展自查** | | | | | | | | | | | | | | | | |
| **分项** | **开题报告内容** | | | | | | | | **中期完成情况** | | | | | | | |
| 论文  题目 | 安全漏洞分类方法的研究 | | | | | | | | 针对不平衡样本分布的安全漏洞分类方法的研究 | | | | | | | |
| 研究  目标 | 1.拟提出一种过采样方法，该方法考虑了生成样本对分类模型过拟合度的影响，并将该方法融入到安全漏洞分类方法中。  2. 拟提出一种特征词提取算法，该方法通过引入外部特征来提高提取文本语义特征的能力，并将该方法融入安全漏洞分类方法中。 | | | | | | | | 1.使用过采样方法解决了安全漏洞分类数据集存在的样本分布不平衡问题。  2.解决了过采样方法易导致安全漏洞分类模型过拟合度过高的问题。  3.通过添加漏洞危险等级信息，提高了安全漏洞分类模型的分类准确度。 | | | | | | | |
| 研究  内容 | 1.研究样本分布不平衡问题的处理方法。本研究将比较不同处理方法之间的差异和优劣，选择恰当的处理方法。  2.研究特征词提取算法。研究Word2vec、TF-IDF等特征词提取算法之间的差异和优劣，选择恰当的特征词提取算法，同时引入漏洞描述中共有的外部特征来提高特征词提取算法的准确度。  3.研究分类模型。研究分析BILSTM、BERT等分类模型之间的差异和优劣，将样本生成方法、特征词提取算法和不同分类模型进行融合，提升模型的效率与准确度。 | | | | | | | | 1.研究现有的样本分布不平衡问题的处理方法，并进行归纳总结，最终使用过采样方法解决了样本分布不平衡问题。  2. 改进过采样方法。使用预训练模型GPT2生成与少样本数据存在差异的新样本，以此解决了高相似生成样本易导致分类模型过拟合度过高的问题。最后使用一个筛选模型去除生成样本中的低相似度样本，以此确保生成样本的有效性。  3. 研究现有的安全漏洞分类模型，并进行归纳总结，分析各个分类模型的优缺点。  4．构建融合漏洞危险等级的安全漏洞分类模型。将漏洞危险等级作为外部特征输入安全漏洞分类模型，提高模型对漏洞描述中语义特征的提取精度。 | | | | | | 完成百分比  1.100%  2.90%  3.100%  4.90% | |
| 创新 | 1.针对安全漏洞分类数据集，改进样本分布不平衡处理方法。  2.针对安全漏洞分类数据集，改进特征词提取算法。 | | | | | | | | 1.目前常见的过采样技术，如回译、同义词替换，存在无法改变句子结构的缺陷，容易导致模型出现过拟合问题。相比之下， GPT2生成的样本与输入样本之间存在结构性差异，这有效地降低了模型的过拟合度。  2. 目前的研究证明了漏洞描述与漏洞危险等级、漏洞类型之间存在潜在联系，因此引入漏洞危险等级作为外部特征可以提高安全漏洞分类模型对漏洞描述的语义特征的提取精度。 | | | | | | | |
| 学术  指标 | 提出一种考虑生成样本对分类模型过拟合度的影响的过采样方法  引入公共外部特征来提高安全漏洞分类模型提取语义特征的能力 | | | | | | | | 1.完成了以GPT2为基础的过采样方法的设计和实验。通过实验对比，本研究的方法相较于目前的过采样方法在精确率和F1-measure指标上分别提升了2.0%、4.6%。  2.完成了融合漏洞危险等级的安全漏洞分类模型的构建和实验。通过实验对比，本研究构建的模型相较于未融合漏洞危险等级的模型在精确率和F1-measure指标上分别提升了2.1%、0.8%。 | | | | | | | |
| 成果  指标 | 拟发表EI检索会议或期刊1篇或专利一项 | | | | | | | | 已发表一项发明专利  计划申请一项发明专利 | | | | | | | |
| 其他  情况 | 实际采用的研究方法：  1.数据的收集和处理，使用网络爬虫技术从公开数据库NVD中获得了漏洞描述、漏洞危险等级、漏洞类型等相关漏洞信息。使用这些信息构建安全漏洞分类数据集，分析数据集中的相关属性，以便后续研究工作的开展。  2. 通过阅读论文分析现有的安全漏洞分类方法与过采样方法；学习并熟悉 tensorflow 深度学习框架，完成了论文实验的复现；阅读实验源代码，结合论文，学习安全漏洞分类的流程。  3.通过阅读论文和实验复现，发现现有方法存在问题。根据所发现的问题，进一步阅读相关论文。改进安全漏洞分类方法以提高度量指标精确率、召回率及 F1-measure。  4. 根据实验结果及理论依据，完成研究成果的撰写。 | | | | | | | | | | | | | | | |
| 实际执行的进度安排：  第一阶段（2022.12-2022.04）阅读相关文献资料，对安全漏洞分类相关的技术与理论进行研究，了解各种处理样本分布不平衡的方法和各种特征提取算法的研究现状。  第二阶段（2023.05-2023.07）对现有的样本分布不平衡方法进行研究，深入理解各种方法的理论原理，构建实验数据集并分析数据集，确定实验中可使用的数据。  第三阶段（2023.08-2023.9）完成以GPT2为基础的过采样方法的设计和实验，分析实验结果。  第四阶段（2023.09-2023.12）完成了融合漏洞危险等级的安全漏洞分类模型的构建和实验，分析实验结果。  第五阶段（2024.01-2024.03）完成论文的初稿并定稿。  第六阶段（2024.04-2024.06）毕业论文送审并完成毕业答辩。 | | | | | | | | | | | | | | | |
| 中期考核时提交的材料清单（含系统演示文档、发表成果等）：  1.中期报告  2.专利受理通知  3.中期演示文档 | | | | | | | | | | | | | | | |
| 工作  小结 | 是否按开题报告执行 | | | | | | 部分 | | | | | | | | | |
| 对变更开题内容的说明 | | | | | | 对于开题内容中的研究目标“提出一种融合公共外部特征的特征词提取算法”，在经过进一步实验后，发现使用分类模型能更充分地提取漏洞描述中的语义信息。因此将该研究目标修改为“一种融合漏洞危险等级的安全漏洞分类模型” | | | | | | | | | |
| 工作进展情况说明 | | | | | | 目前初步完成了以GPT2为基础的过采样方法的设计和实验和融合漏洞危险等级的安全漏洞分类模型的构建和实验。正在完成两者的结合实验。 | | | | | | | | | |
| 目前存在的问题和举措 | | | | | | 目前融合漏洞危险等级的安全漏洞分类模型的对比试验不够充分，需要进一步补充实验。 | | | | | | | | | |
| **三、毕业条件自查** | | | | | | | | | | | | | | | | |
| 课程  学分  情况 | | 学位课 | | **19** | | 是否完成规定学分？如无，说明原因及补救措施：  **是** | | | | | | | | | | |
| 非学位课 | | **14** | |
| 成果  情况 | | 排名 | 类型  (论文、专利、获奖等) | 内容  (按文献格式) | | | | | | | 级别 | | 状态  (发表/录用/已投/计划中) | 是否论文工作相关 | | 可否获得毕业资格 |
| 2 | 专利 | 一种基于行为文本处理的语音内容识别方法 | | | | | | | 发明专利 | | 已受理 | 否 | | 是 |
| 2 | 专利 | 一种针对不平衡样本分布的安全漏洞分类方法 | | | | | | | 发明专利 | | 计划中 | 是 | | 是 |
| 1 | 获奖 | 第13届蓝桥杯大赛 | | | | | | | 省甲 | | 省二等奖 | 否 | | 否 |
| 其他  情况 | | 如有其他和毕业相关的情况，在此说明：  无 | | | | | | | | | | | | | | |
| **四、学位论文写作计划** | | | | | | | | | | | | | | | | |
| 列出学位论文的目录计划，一般应给出全部章节的一级和二级标题（此部分对梳理学位论文工作并按期完成撰写很重要，务必在导师指导下撰写并提交）。  部分样例：  摘要  Abstract  目 录  第一章 绪论  1.1 研究背景及意义  1.2 国内外研究现状  1.3 论文主要工作  1.4 论文组织结构  第二章 相关理论  2.1 安全漏洞分类  2.2 安全漏洞特征  2.3 词嵌入模型  2.3.1 词嵌入模型概述  2.3.2 Word2Vec模型  2.4 本章小结  第三章 针对不平衡样本分布的安全漏洞分类方法  3.1 相关定义  3.2 问题分析  3.3 研究方法  3.3.1 欠采样方法  3.3.2 过采样方法  3.4 实验与分析  3.4.1实验数据与处理  3.4.2实验设计  3.4.3实验结果与分析  3.5 本章小结  第四章 融合外部特征的安全漏洞分类模型  4.1 相关定义  4.2 问题分析  4.3实验与分析  4.3.1实验数据与处理  4.3.2实验设计  4.3.3实验结果与分析  4.4 本章小结  第五章 系统设计与实现  5.1 可行性分析  5.2 系统设计  5.3 系统实现  5.3.1开发环境  5.3.2开发技术介绍  5.3.3系统展示  5.4 本章小结  第六章 总结与展望  6.1 主要结论  6.2 研究展望  致谢  攻读硕士学位期间从事的科研工作及研究成果  参考文献 | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | |

注：以上内容根据情况添页。