中国大学生计算机设计大赛



软件开发类作品文档简要要求

作品编号：

作品名称：赛博哨兵--基于win的电脑监控软件防护平台

作　　者：　　陈鑫越、李新荣、沈宏远、周培翔

版本编号：

填写日期：　　2025年3月30日

填写说明：

1. 本文档适用于所有涉及软件应用与开发类的各个小类作品，包括：（1）Web应用与开发（2）管理信息系统（3）移动应用开发（非游戏类）（4）算法设计与应用（5）企业赛项；
2. 本文档为简要文档，不宜长篇大论，需简明扼要，建议设计二级目录，逻辑性强；
3. 一级标题采用二号黑体，居中，二级标题采用三号黑体，靠左，根据需要可以设计三级标题，正文一律用五号宋体；
4. 提交文档时，以PDF格式提交本文档；
5. 本文档内容是正式参赛内容组成部分，务必真实填写。如不属实，将导致奖项等级降低甚至终止本作品参加比赛。

目 录

[第一章 需求分析 4](#_Toc26017)

[1.1 需求背景 4](#_Toc17463)

[1.2 市场分析 4](#_Toc21891)

[1.3 用户需求 4](#_Toc15079)

[1.4 竞品分析 5](#_Toc7571)

[第二章 概要设计 5](#_Toc24822)

[2.1 系统架构 5](#_Toc10440)

[2.2 功能模块 6](#_Toc24275)

[2.3 数据流设计 6](#_Toc2525)

[2.4 技术选型 6](#_Toc46)

[第三章 详细设计 7](#_Toc23070)

[3.1 数据库设计 7](#_Toc27668)

[1.AppInfo表 7](#_Toc5005)

[2.MonitoringRule表 7](#_Toc3846)

[3.SystemMonitor表 8](#_Toc26915)

[4.AIAnalysisResult表 8](#_Toc20133)

[3.2 前端页面 9](#_Toc30274)

[3.3 界面设计 10](#_Toc7149)

[3.3.1 主控制台 10](#_Toc9877)

[3.3.2 应用管理界面 11](#_Toc24595)

[3.3.3 威胁监控界面 11](#_Toc484)

[3.4 API接口设计 12](#_Toc24961)

[第四章 测试报告 12](#_Toc9135)

[4.1 功能测试 12](#_Toc27013)

[4.2 性能测试 12](#_Toc9362)

[第五章 安装及使用 13](#_Toc30895)

[5.1 系统要求 13](#_Toc11190)

[5.2 安装步骤 13](#_Toc1785)

[5.3 使用指南 14](#_Toc20700)

[5.3.1 应用保护配置 14](#_Toc30236)

[5.3.2 监控与分析 14](#_Toc31695)

[5.3.3 日常管理 15](#_Toc20432)

[第六章 项目总结 15](#_Toc5171)

[6.1 项目成果 15](#_Toc30404)

[6.2 项目挑战与解决方案 15](#_Toc11539)

[6.3 未来展望 16](#_Toc26765)

[参考文献 16](#_Toc29085)

# 需求分析

### 1.1 需求背景

随着信息技术的飞速发展和企业数字化转型的深入，组织机构面临的网络安全威胁日益复杂多变。传统单点式、被动防御的安全方案已难以满足当今企业全面、主动的安全防护需求。市场调研显示，企业IT环境平均部署了420多种不同应用程序，而传统安全工具往往形成孤岛，导致安全管理碎片化，平均每个组织需部署45种以上安全工具才能覆盖基本防护需求。

### 1.2 市场分析

当前企业面临以下关键安全挑战：

1. 高级持续性威胁(APT)增长：针对性攻击显著增加，攻击持续时间长
2. 勒索软件攻击：全球勒索软件攻击频率和赎金要求不断上升
3. 内部威胁风险：数据泄露事件中有相当比例源自内部人员
4. 供应链攻击：第三方软件组件漏洞利用增加，开源依赖项安全隐患增多
5. 远程办公安全隐患：远程与混合办公模式扩大了攻击面

### 1.3 用户需求

本系统面向的用户群体包括：

1. 中大型企业的信息安全团队
2. 信息安全管理人员与系统管理员
3. 需要高级应用保护的开发团队
4. 对核心应用和数据有严格保护需求的行业（金融、医疗、政府、研发等）

这些用户需要一站式安全管理平台，整合应用监控、威胁检测、用户管理和文件安全功能，特别在进程保护、反录屏和AI安全分析方面提供独特优势。

### 1.4 竞品分析



# 概要设计

### 2.1 系统架构

软件安全管理系统采用分层架构设计，包括以下层次：

1. 数据采集层：负责从系统和应用收集各类监控数据
2. 核心处理层：实现进程伪装、反录屏等核心安全功能
3. 分析引擎层：包含AI分析引擎，提供智能安全分析
4. 存储层：管理系统各类数据的存储和访问
5. 表现层：提供Web界面和API接口

### 2.2 功能模块

系统主要由以下功能模块组成：

1. 应用管理模块：负责应用注册、信息管理及生命周期跟踪
2. 安全防护模块：提供进程伪装、反录屏保护和窗口保护功能
3. 威胁检测模块：监控恶意线程和文件修改操作
4. 资源监控模块：跟踪系统和应用资源使用情况
5. 用户管理模块：处理用户账户、权限和操作日志
6. 文件安全模块：提供文件加密和安全删除功能
7. AI分析引擎：处理安全事件分析和风险评估
8. 系统配置模块：管理全局配置参数

### 2.3 数据流设计

各模块间主要数据流向如下：

1. 应用管理模块收集应用信息，为安全防护模块和资源监控模块提供基础数据
2. 威胁检测模块捕获可疑行为，提交给AI分析引擎进行深度分析
3. AI分析引擎评估风险并向告警管理系统提供风险评分
4. 资源监控模块向所有其他模块提供性能指标参考
5. 用户管理模块控制所有操作的授权，并记录操作日志

### 2.4 技术选型

系统采用的主要技术包括：

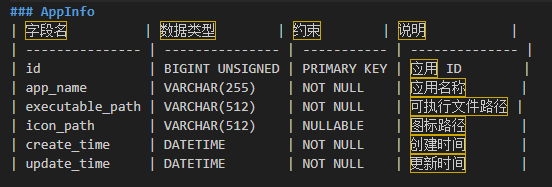
* 开发语言：C++
* 数据库：MySQL
* Web框架：httplib
* 前端技术：vue、ECharts
* 通信协议：HTTP/HTTPS
* 安全技术：RC4加密、Windows API钩子

# 详细设计

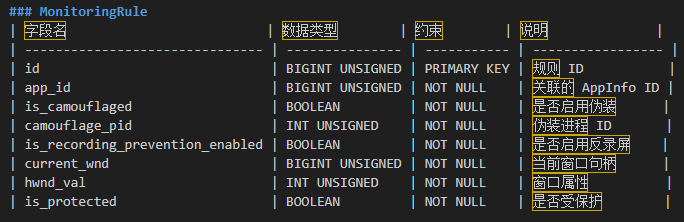
### 3.1 数据库设计

系统采用关系型数据库存储结构化数据，主要数据表包括：

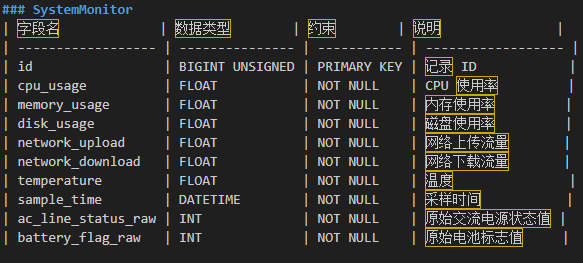
### 1.AppInfo表



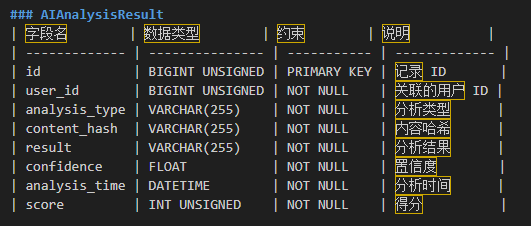
### 2.MonitoringRule表



### 3.SystemMonitor表



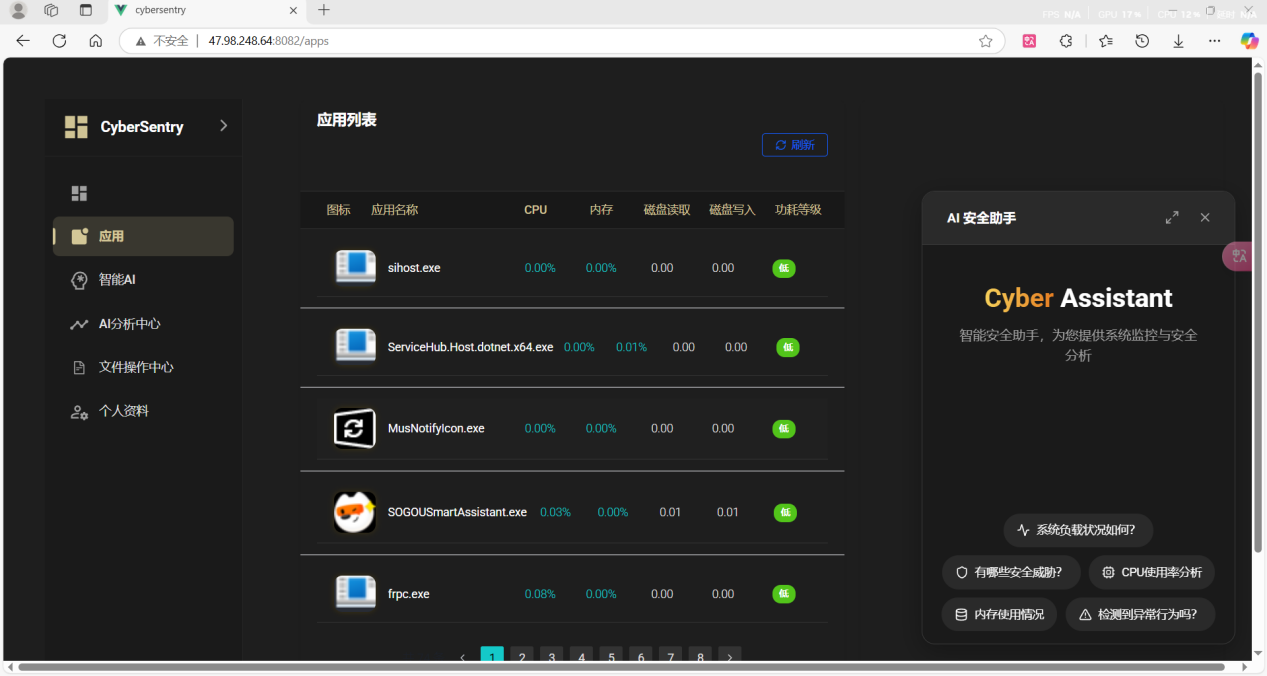
### 4.AIAnalysisResult表

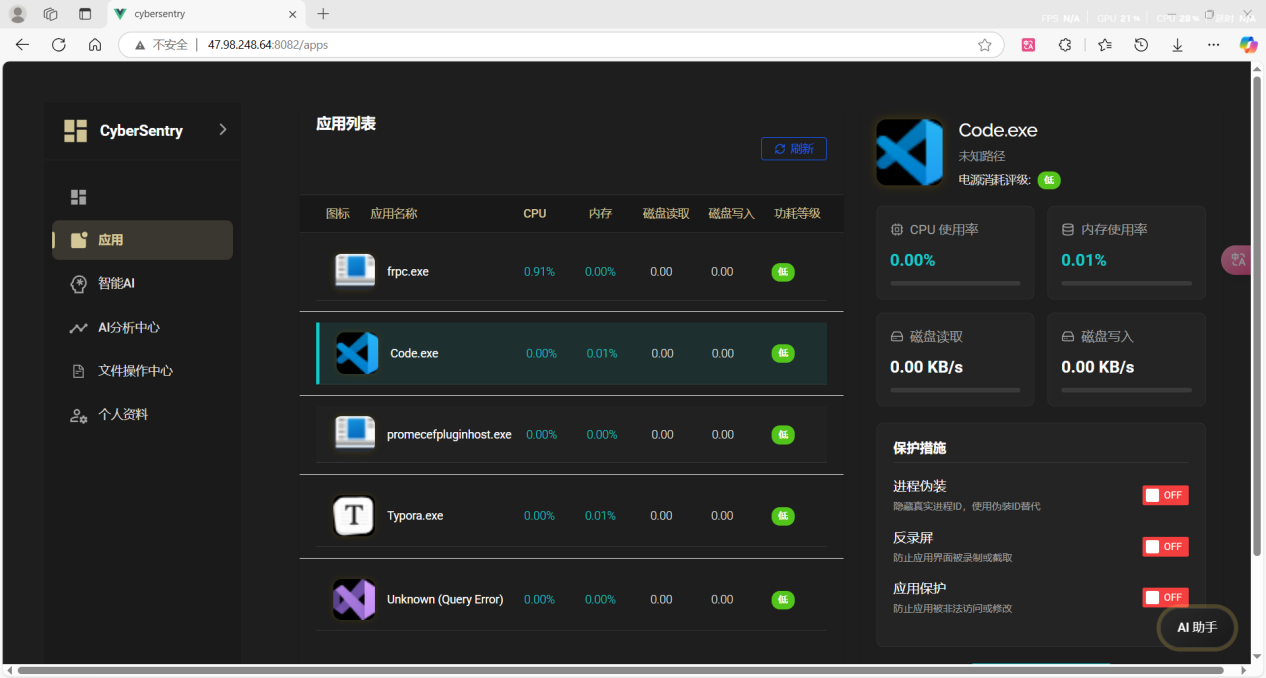


1. AppResourceMonitor表、MaliciousThreadLog表、FileModificationLog表、AIAnalysisResult表、SystemConfig表、UserInfo表、UserOperationLog表和FileInfo表的设计遵循类似结构。

### 3.2 前端页面









### 3.3 界面设计

### 3.3.1 主控制台

主控制台集中展示系统关键状态指标，包括：

1. 安全概览：当前系统安全评分、待处理告警数量
2. 资源使用情况：CPU、内存、磁盘和网络使用趋势图
3. 应用状态：受保护应用数量及其运行状态
4. 近期活动：最近检测到的威胁和用户操作
5. 

### 3.3.2 应用管理界面

应用管理界面用于注册和监控应用程序，主要功能包括：

1. 应用列表视图：展示所有注册应用基本信息
2. 应用详情视图：显示单个应用的详细配置和监控数据
3. 安全规则配置：设置进程伪装、反录屏等保护规则
4. 应用资源使用趋势：展示应用资源消耗历史数据

### 3.3.3 威胁监控界面

威胁监控界面集中展示检测到的安全威胁，包括：

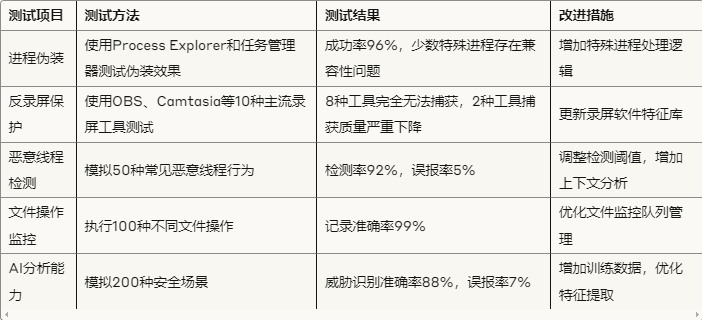
1. 恶意线程列表：展示检测到的可疑线程及其风险评分
2. 文件变更监控：显示敏感文件的修改操作记录
3. 威胁处理工作流：支持分析、隔离、恢复等操作
4. 威胁趋势分析：展示不同类型威胁的历史趋势

### 3.4 API接口设计

# 测试报告

### 4.1 功能测试

系统功能测试结果：



### 4.2 性能测试

系统性能测试结果：



# 安装及使用

### 5.1 系统要求

* 操作系统：window10
* 处理器：amd 5800
* 内存：16GB DDR4 ECC
* 存储空间：256GB NVMe SSD
* 数据库：MySQL
* 网络：双千兆以太网（1Gbps）

### 5.2 安装步骤

1. 准备工作：

* 下载安装包
* 准备数据库环境
* 关闭杀毒软件(避免误报)

1. 安装过程：

* 运行安装向导，选择安装目录
* 配置数据库连接参数
* 设置管理员账户
* 配置系统参数
* 安装驱动组件(需管理员权限)
* 重启系统完成安装

1. 验证安装：

* 登录管理控制台
* 检查系统状态指示器
* 添加测试应用验证功能

### 5.3 使用指南

### 5.3.1 应用保护配置

* 打开应用管理界面
* 添加需要保护的应用
* 配置保护规则(伪装、反录屏等)
* 启用保护并验证效果

### 5.3.2 监控与分析

* 查看系统监控仪表板
* 分析应用资源使用情况
* 检查威胁监控告警
* 查看AI分析报告

### 5.3.3 日常管理

* 用户和权限管理
* 系统配置调整
* 日志查询与分析
* 安全策略优化

# 项目总结

### 6.1 项目成果

软件安全管理系统成功实现了预期目标，提供了一套全面的应用保护和安全管理解决方案。系统整合了多种先进安全技术，特别是进程伪装、反录屏保护、AI安全分析和双粒度资源监控等特色功能，在企业应用安全领域具有显著优势。

系统具有良好的性能和扩展性，资源占用低，可靠性高，满足各类企业环境的部署需求。

### 6.2 项目挑战与解决方案

项目开发过程中面临的主要挑战包括：

* 技术创新难题：进程伪装和反录屏技术需要深入Windows底层，团队通过系统研究和反复测试，成功实现了稳定可靠的保护机制。
* 性能优化挑战：全面监控功能可能导致系统性能下降，通过优化采样策略和数据处理算法，将资源占用控制在极低水平。
* 兼容性问题：不同Windows版本和应用程序的兼容性是一大难题，团队建立了广泛的测试环境，确保在各种常见环境中稳定运行。
* 用户体验设计：安全软件往往操作复杂，团队注重用户体验设计，简化操作流程，提供直观界面，大幅提升了产品易用性。

### 6.3 未来展望

未来系统计划在以下方面继续发展：

* 平台扩展：开发Linux和macOS版本，满足跨平台企业需求
* 云安全整合：增强云环境安全防护能力，适应混合云架构
* 威胁情报集成：对接主流威胁情报平台，提升威胁检测能力
* 移动端增强：完善移动端应用功能，支持更多远程操作
* AI能力提升：持续优化AI模型，提高分析准确性和覆盖面

# 参考文献

1. Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.
2. William Stallings, Lawrie Brown. Computer Security: Principles and Practice. Pearson, 2018.
3. Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley, 2015.
4. Microsoft Corporation. Windows Internals, Part 1: System Architecture, Processes, Threads, Memory Management, and More. Microsoft Press, 2017.
5. Andrew S. Tanenbaum, Herbert Bos. Modern Operating Systems. Pearson, 2016.
6. Martin Fowler. Patterns of Enterprise Application Architecture. Addison-Wesley, 2002.
7. Michael Howard, David LeBlanc. Writing Secure Code. Microsoft Press, 2018.
8. Carsten Bormann, Mark Nottingham. The Hypertext Transfer Protocol Status Code 308. RFC 7538, 2015.