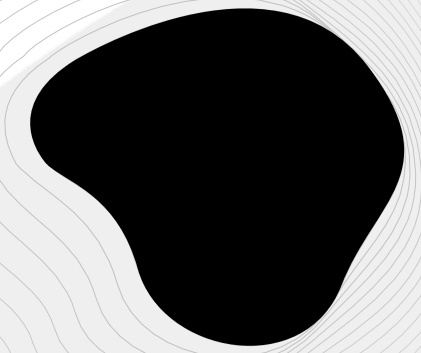
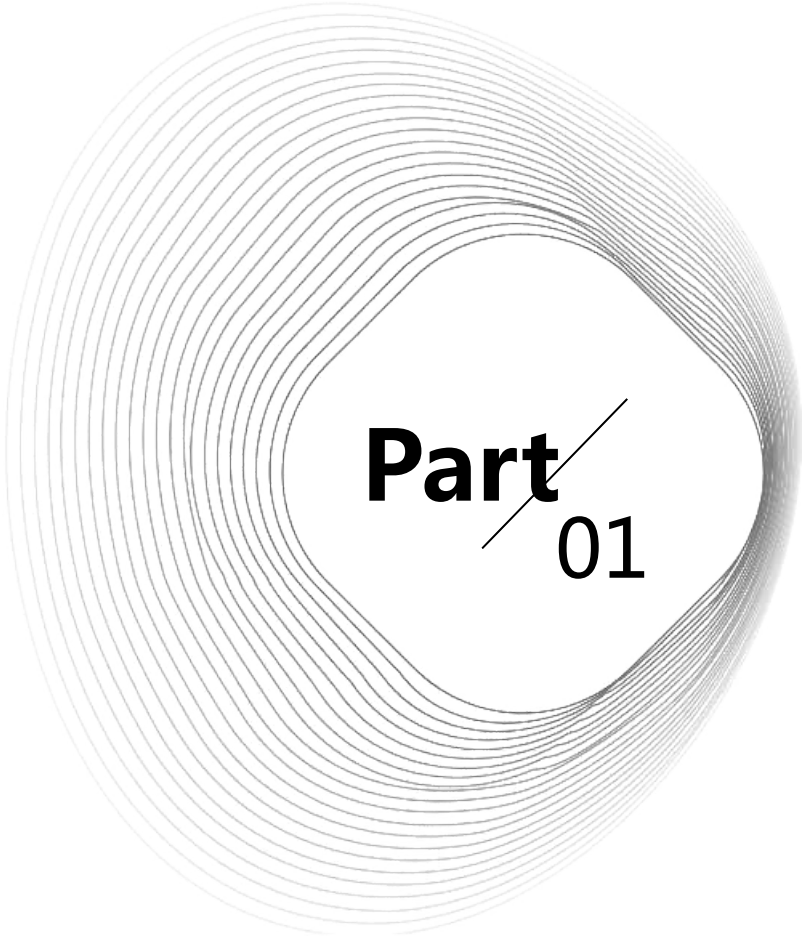


基于改进型循环神经网络的恶意代码分类检测

汇报人：

2024-02-01

目录



Part 01

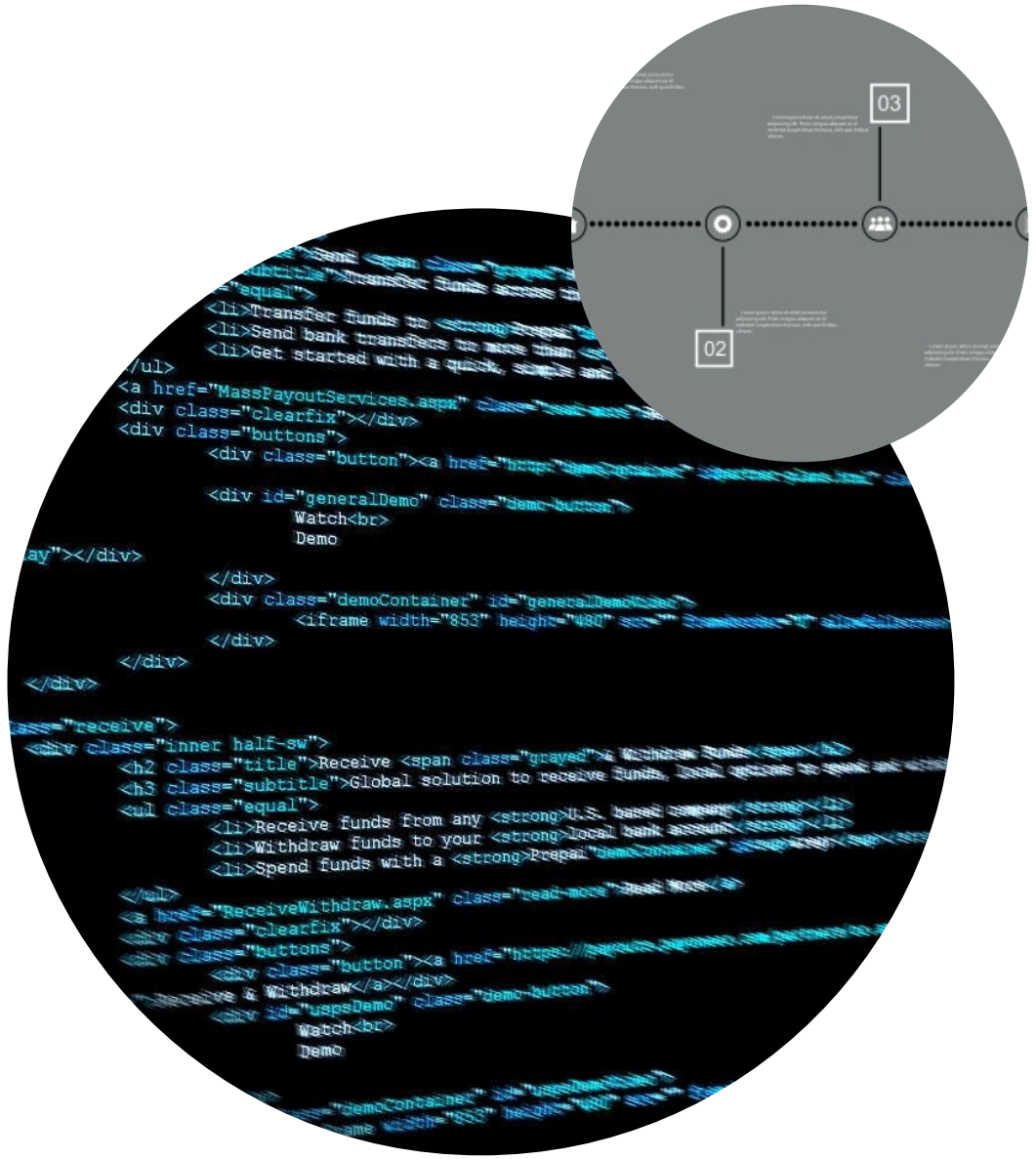
引言

背景与意义

随着互联网的快速发展，恶意代码数量急剧增加，对信息系统安全构成严重威胁。

恶意代码分类检测是信息安全领域的重要研究方向，有助于实现对恶意代码的有效防范和应对。

传统的恶意代码检测方法存在准确率低、泛化能力弱等问题，急需改进和优化。



国内外研究现状及发展趋势

目前，国内外研究者已提出多种恶意代码分类检测方法，包括基于静态特征、动态行为、机器学习等。

深度学习在恶意代码分类检测中取得显著成果，尤其是循环神经网络（RNN）及其改进型在处理序列数据方面具有优势。

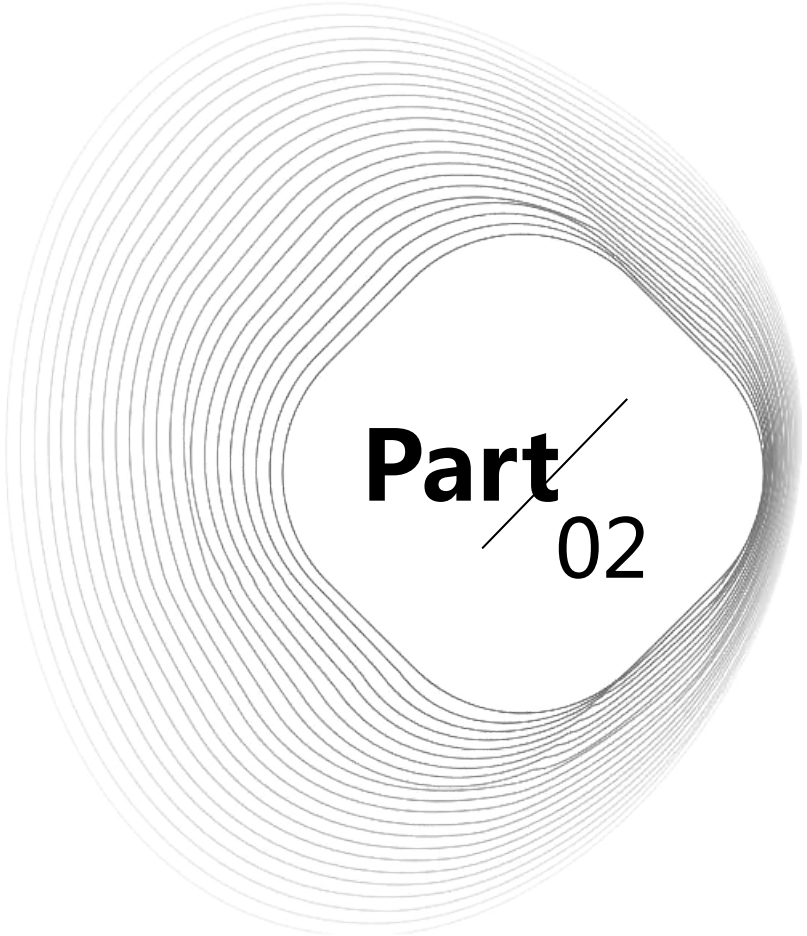
未来发展趋势将更加注重模型的准确性、实时性和可解释性，以及对抗样本攻击的鲁棒性。

本文研究内容与创新点

本文旨在研究基于改进型循环神经网络的恶意代码分类检测方法，提高分类准确性和泛化能力。

VS

创新点包括：提出一种新型的网络结构，结合注意力机制和残差连接，以更好地捕捉恶意代码序列中的关键信息；采用多种优化策略，如自适应学习率调整、批量归一化等，提高模型训练效率和稳定性；在公开数据集上进行实验验证，并与现有方法进行对比分析。



Part 02

基础知识介绍

神经网络基本概念

神经元与感知器

神经网络的基本单元，模拟生物神经元的结构和功能，通过权重和激活函数实现输入信号的加权和与非线性转换。

前向传播与反向传播

神经网络的学习和训练过程，前向传播计算输出值，反向传播根据误差调整权重。

网络结构与层数

神经网络的拓扑结构，包括输入层、隐藏层和输出层，不同层数和节点数影响网络的表达能力和复杂度。

循环神经网络原理及特点

循环连接与记忆单元

循环神经网络通过引入循环连接和记忆单元，使得网络能够处理序列数据和具有时序关系的信息。

参数共享与动态行为

循环神经网络中的参数在时间维度上共享，降低了模型复杂度，同时网络具有动态行为，能够适应不同长度的输入序列。

梯度消失与梯度爆炸

循环神经网络在训练过程中可能面临梯度消失或梯度爆炸问题，导致网络难以学习和优化。

改进型循环神经网络结构

长短期记忆网络（LSTM）

通过引入门控机制和记忆单元状态，有效解决了梯度消失问题，能够学习和记忆长期依赖关系。

门控循环单元（GRU）

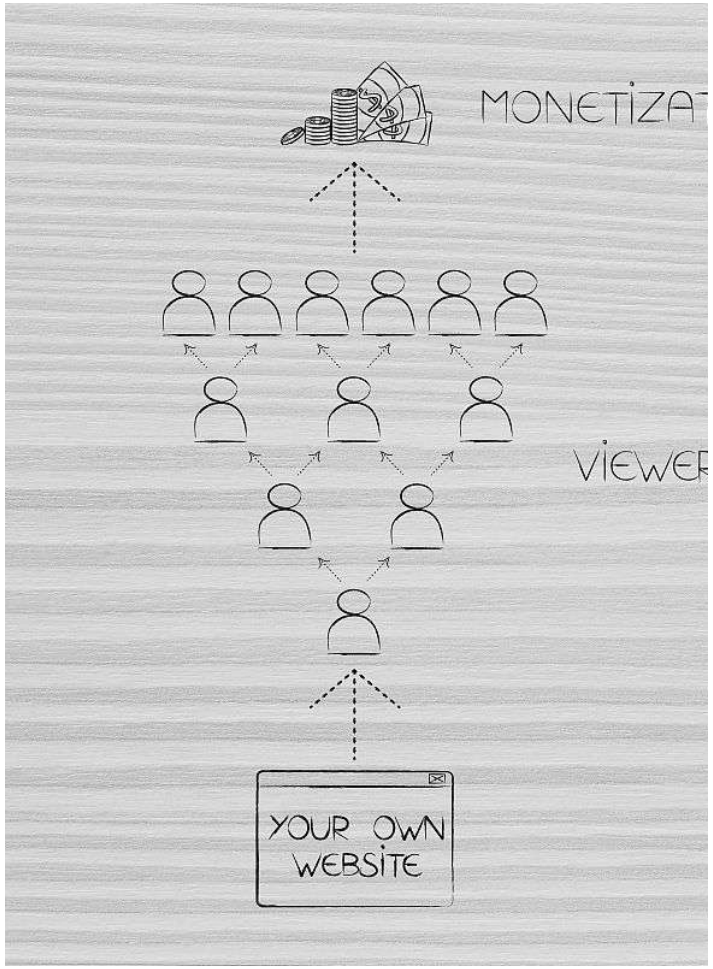
简化了LSTM的结构，将输入门和遗忘门合并为一个更新门，减少了参数数量和计算复杂度。

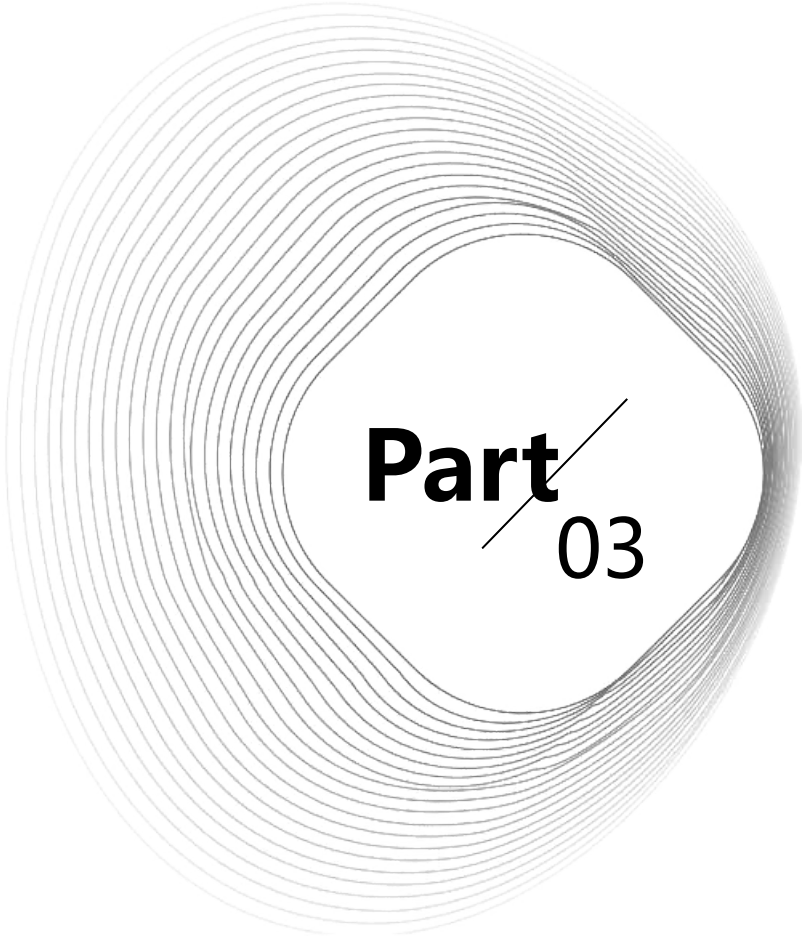
注意力机制

在循环神经网络中引入注意力机制，使得网络能够关注输入序列中的关键信息，提高了模型的表达能力和泛化能力。

双向循环神经网络（Bi-RNN）

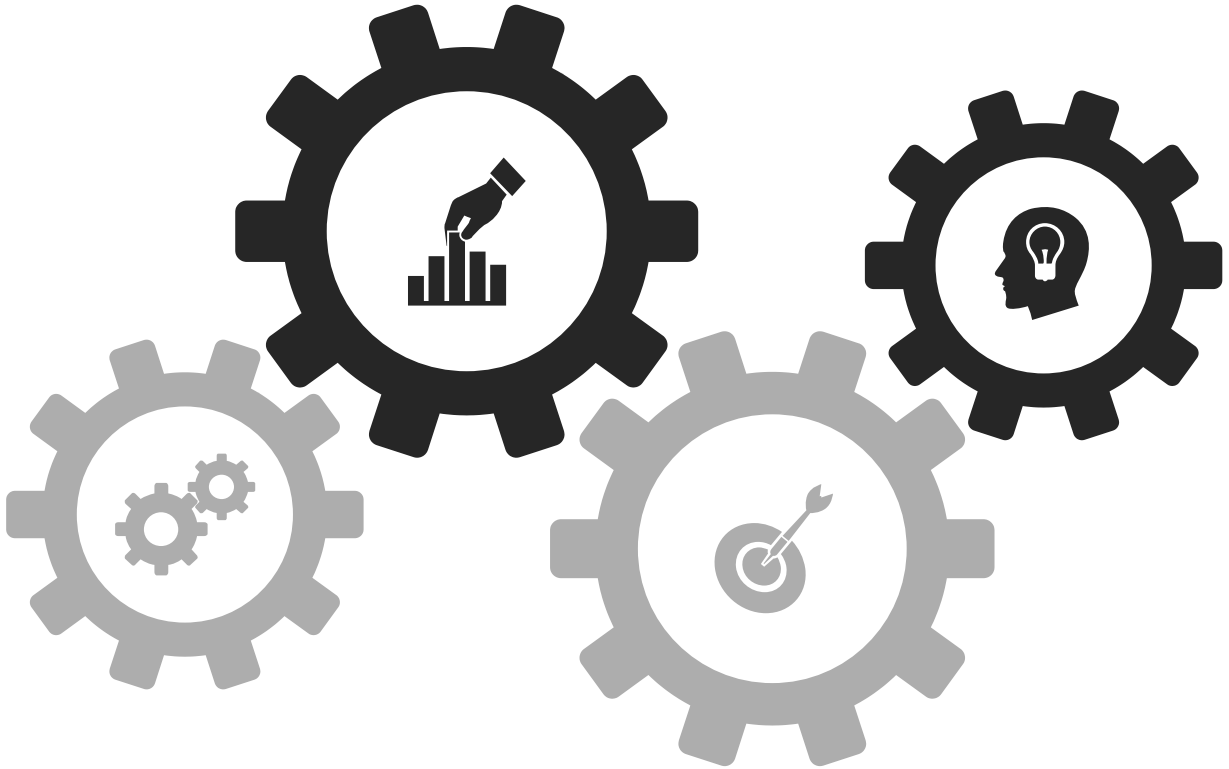
同时考虑输入序列的正向和反向信息，增强了网络的上下文感知能力。





恶意代码分类检测问题描述

恶意代码定义及危害性分析



恶意代码定义

恶意代码是指旨在破坏、干扰或未经授权访问计算机系统的任何程序或代码片段，包括病毒、蠕虫、特洛伊木马等。

危害性分析

恶意代码可导致数据丢失、系统瘫痪、隐私泄露等严重后果，对网络安全构成极大威胁。

传统恶意代码分类检测方法概述

01

基于签名的检测方法

通过比对已知恶意代码签名与待检测文件特征来识别恶意代码，但无法应对未知威胁。

02

启发式扫描方法

通过分析文件行为、代码结构等特征来推测文件是否为恶意，但误报率较高。

03

沙盒技术

在隔离环境中运行待检测文件，观察其行为并判断是否为恶意，但可能影响系统性能。