基于人工智能的信息共享安全防护系统

亚文米 1 号
国防科技大学基础军政教育学院，中国长沙
miyawen624@126.com

2 号恩多高
中南大学物理与电子学院，长沙 1263551501@qq.com

2022 IEEE 第二届移动网络与无线通信国际会议(ICMNWC) | 978-1-6654-9111-2/22/$31.00 ©2022 IEEE | DOI: 10.1109 / ICMNWC56175.2022.10031986

***摘要*随着信息共享安全问题的日益严重和网络攻击的不断防御，用于解决信息共享安全问题的防护技术必须不断更新。为了解决现有信息共享安全防护研究的不足，本文基于递归神经网络的函数方程和信息共享安全要素，简要讨论了本文提出的防护系统的测试环境和参数配置。讨论了基于递归神经网络的信息共享安全保护系统的软件结构和功能，并将所设计的信息共享安全保护系统应用于信息误用(IM)、信息异常(IA)和安全响应(SR)进行了实验测试。实验数据表明，在所有信息样本中，信息误用保护检测的准确率平均达到 97.5 左右。信息异常(IA)保护检测的准确率平均达到 97.2 左右。安全响应(SR)保护检测准确率平均达到 96.7%。由此验证了本文设计的信息共享安全防护系统具有良好的防护效果。**

关键词:人工智能，信息共享，安全防护，神经网络

I. 介绍

随着计算机技术的逐渐普及。在各种各样的信息交换和共享环境中，每个用户的生活变得越来越便利，带来了大量的网络安全问题，信息安全和隐私保护迎来了新的挑战。

如今，越来越多的学者通过各种技术和系统工具对信息共享安全防护系统进行了大量的研究，也通过实践研究取得了一定的研究成果。El-Latif AA 认为，网络信息共享的威胁已经成为各个领域和部门关注的问题。虽然有许多现有的对策，但在各个领域和部门的网络安全专业人员中常用的是网络安全威胁响应。该方法是指通过网络信息对信息共享的威胁进行识别、评估、检测和响应的任何信息。 它包括威胁的指标、威胁的方法和程序。CTI 共享被认为是提高信息共享安全防护能力的一种科学方法[1]。为了在网络中发展和实践信息共享和安全保护系统，需要科学有效的保护协议和程序。Romansky R P 提出了两种方法算法和保护系统的假设。但是在网络密码解析中有一个最容易受到攻击的环节。初始信息参数的敏感性和可控性理论上可以为防护已知攻击提供更大的密钥空间。Romansky RP 提出了一种科学的基于 qw 的信息共享安全保护机制。然后进行性能分析，实验表明该方法在网络信息共享中具有高安全性和高稳定性[2]。Haque S 的研究目标是提供一个可靠的保护环境，以确保网络信息安全。由于网络信息的复杂性，通过一定的信息监控手段，将安全信息放到云端已经成为一种监控标准。在各种情况下，这些信息安全问题都涉及到信息向云的传输，提出了一种实现个人信息向云传输的方法，并限制这些信息进入云环境的威胁。对传输到云端的信息进行检测，保护用户的信息，列举了网络信息的风险和保护技术[3]。 虽然现有的航空管制安全风险评估体系研究非常丰富，但基于层次分析法的航空管制安全风险评估体系研究仍存在一定的局限性。

因此，为了丰富现有的信息共享安全防护系统的研究，本文首先介绍了递归神经网络函数方程的概念和人工智能技术的应用，以及信息共享安全的构成要素，其次讨论了本文提出的信息共享安全防护系统的测试环境和参数配置;最后将设计的信息共享安全防护体系结构具体应用于信息误用(IM)、信息异常(IA)和安全响应(SR)进行实验测试，最后实验证明了本文设计的信息共享安全防护体系的有效性。

II. 基于人工智能的信息共享安全防护

A. 人工智能技术

人工智能技术在这种信息共享安全保护中的应用[4]。

1) 建立规则生成专家系统; 本系统是指具有丰富专家经验的检测系统。管理者可以根据入侵情况编制标准，利用系统的检测功能识别系统的安全程度系数[5]。

978-1-6654-9111-2/22/$31.00 ©2022 ieee

2) 人工神经网络系统: 该系统的研发是一支高效的科研团队在对人脑的长期模拟中形成的一种学习技能。除了具备上述有利条件外，它还具有良好的学习能力和自适应能力，能够实现对入侵情况的快速识别[6]。

3) 人工免疫技术: 该技术的原理是基于人体免疫系统，人体通过信息安全技术对外界环境产生自我保护现象并进行训练[7]。

B. 信息共享安全

信息共享安全的要素

1) 信息资产: 信息包括所有形式的数据、文件、信息等。信息资产是指对组织有价值的、以任何方式存储的信息[8]。

2) 安全风险: 信息资产面临着信息误用、信息异常等诸多安全威胁。由于存在一些可以利用或破坏的薄弱环节，信息资产可能会遭受损失[9]。

*3) 漏洞: 指*可能被威胁利用，造成资产损失的薄弱环节。这些漏洞可能存在于软件、硬件、工作流程、人员等方面[10]。

C. 循环神经网络

遗忘门根据前一个循环网络单元输出的信息状态和当前循环网络单元输入的信息状态，共同控制前一个循环网络单元的监控状态有多少信息需要保护，即按比例调整前一个循环网络单元输出的信息[11]。其具体公式如下:

$$ks = P(Rk \cdot [ts\text{-}1, us] + ck) \quad (1)$$

$$N^{\wedge} = {}_{ks} * as\text{-}1 \quad (2)$$

其中，Rk 为信息共享安全防护权值矩阵，tx-1, us 为之前信息的保护状态 tx-1 与当前保护的输入信息 us 的组合，ck 为信息异常，P 为分类激活函数。这个函数可以将(-∞，∞)映射到(0,10)，所以 kx 的值在 0 到 10 之间，使得前一个保护状态的检出率进入当前保护状态的信息可以进行调整。

信息共享首先需要安全防护计算当前信息的保护状态 $n^{\wedge}{}_{x}$，这就决定了在当前的安全保护中需要检测到什么样的新信息进入安全保护状态。其计算公式为:

$$N^{\wedge} = \tan(Rn \cdot [ts\text{-}1, us] + cn) \quad (3)$$

其中，Rn 为信息共享安全防护权值矩阵，cn 为信息异常，tanh 是循环网络中常用的激活函数。

III. 基于信息共享安全防护系统的调查与研究

人工智能

A. 基于人工智能的信息共享安全防护系统测试环境

1) 硬件环境

a) *监控主机(Web 服务器):* Pentium(R) Dual-CoreCPUE54002.70G, 2G 内存，320G 硬盘服务器主机

b) *控制终端:* 奔腾(R) dual - CoreCPUE53002.60GHz, 1G 内存，250G 硬盘。

2) 软件环境

a) 操作系统: 监控 web 服务器采用 Windows server 2003 SP2 操作系统。

b) 控制终端:采用 WindowsXPSP3 操作系统的网站服务器软件; IIS6.0.3。

3) 网络环境

a) 网络类型: 局域网。

b) 网络带宽: 100 米。

c) 网卡速度: 10/100M。

B. 基于人工智能的信息共享安全防护系统参数配置

本文在实验测试中采用了不同的信息共享安全保护参数。用户可以通过浏览器登录系统的前端界面，添加信息共享安全保护对象，并设置信息共享安全保护的相关参数。添加信息共享安全保护对象时，需填写相关网络的名称、IP 地址和组字，信息共享安全保护参数可根据用户业务需求和系统实际情况进行配置。具体参数配置如表 1 所示:

表 1 .信息共享安全保护对象参数

保护类别	保护参数
服务器	网络 ID、时间间隔、IP 地址、性能指标阈值
中间件	网络 ID，网络类型，时间间隔，端口号，网络版本
数据库	网络 ID、信息库类型、用户名和密码、计数器阈值
网络设备	网络 ID、网络类型、IP 地址、时间间隔、性能指标阈值

IV. 基于人工智能的信息共享安全防护系统应用研究

A. 基于人工智能的信息共享安全防护系统软件结构设计

本文的信息共享安全防护系统的软件开发是基于 Linux 的环境，并使用 QT 作为开发工具。设计了信息共享安全防护系统的软件结构，主要包括三个模块:输入层、隐藏层和输出层。信息共享安全防护系统的具体软件结构如图 1 所示:

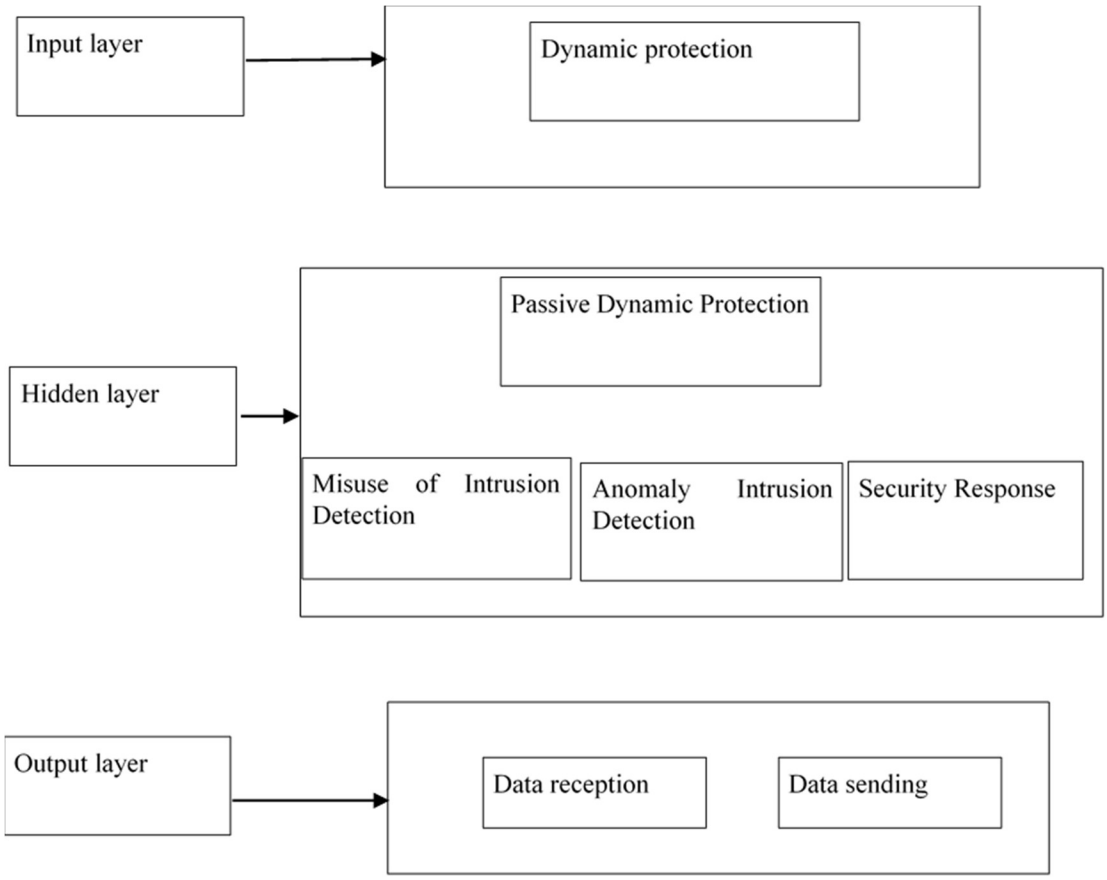

图 1 所示。信息共享安全防护系统的软件结构

基于人工智能中递归神经网络技术的信息共享安全防护系统的详细软件功能如下:

1) 输入层: 输入层主要负责信息共享安全防护系统状态信息和可视化显示，主要对信息共享安全进行动态防护。

2) 隐藏层: 隐藏层主要是信息共享的被动动态安全保护部分。被动动态首先对系统的状态进行入侵检测。一方面，通过递归神经网络对系统信息进行实时分析，通过特征匹配检测已知信息攻击;通过预测信息通信报文的时间间隔，及时发现信息异常。安全响应模块检测到异常信息后，生成并下发安全响应命令，保护系统的动态安全。

3) 输出层: 输出层负责与部署在信息共享安全站点的分布式安全交换机进行数据通信，包括通过镜像和发布获取的网络信息

由安全监管中心生成的安全指令。

B. 基于人工智能的信息共享安全防护系统应用

为了评估信息共享安全防护系统的防御效果，本文考虑了信息误用(IM)、信息异常(IA)和安全响应(SR)两种类型的信息安全。并分别选取 50%、100%、150%和 200%的信息样本进行检测和保护准确率的测试。首先计算梯度集中单个梯度与其他梯度的欧氏距离和值，然后选择欧氏距离和值最小的梯度作为最新的梯度，更新递归神经网络模型的权值。具体实验结果对比如图 2 所示:

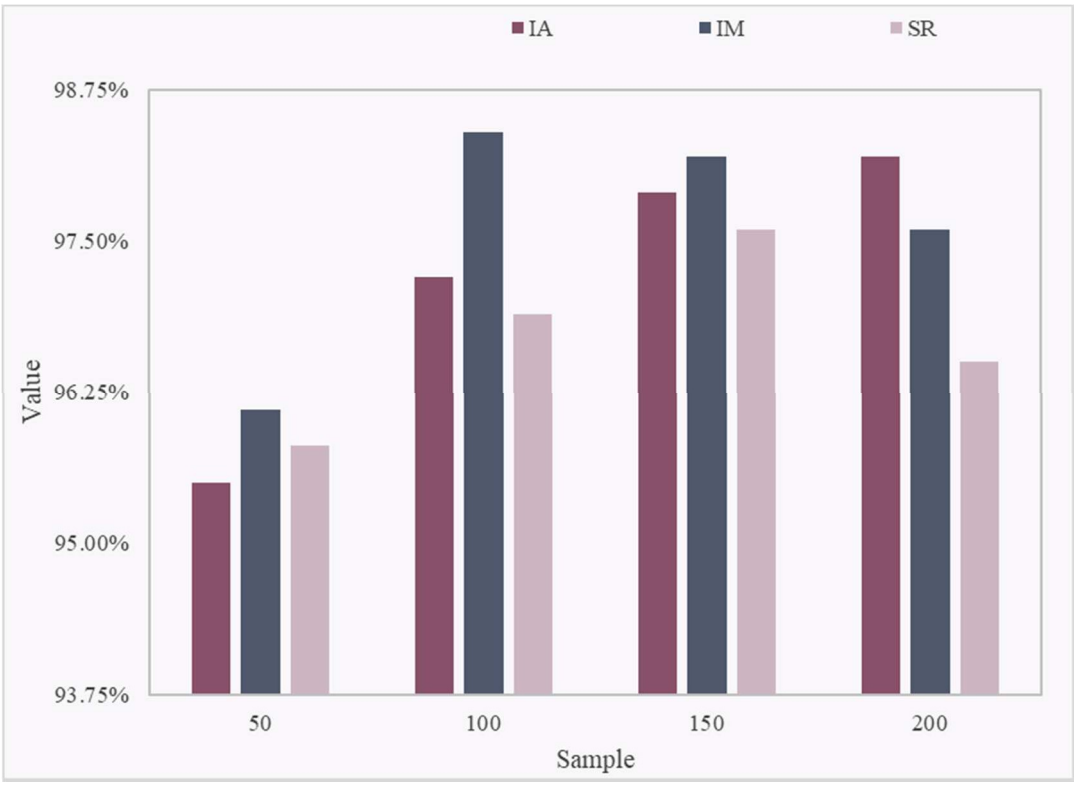

图 2 所示。保护精度实验结果的比较

从图 2 的实验数据可以看出，基于递归神经网络的信息共享安全防御效果更好。在 50% ~ 200%的信息误用(IM)样本检测与防御中，基于(RNN)的信息共享安全防护系统准确率分别达到 98.4%和 96.1%。在 50% ~ 200%的信息异常(IA)样本检测与防御中，基于递归神经网络(RNN)的信息共享安全防护系统的准确率在 95.5% ~ 98.2%之间。在 50% ~ 200%的信息安全响应(SR)样本的检测和防御中，信息共享安全防护系统(RNN)的准确率分别达到 95.8%和 97.6%。

V. 结论

本文阐述了基于信息共享的人工智能技术建立安全防护系统，神经网络包含一个环路方程，并对信息共享中应用人工智能技术的安全防护及安全信息共享要素进行描述，并对基于信息共享的人工智能安全防护系统的设计、系统环境和参数配置进行了调查研究。同时设计了基于人工智能的信息共享安全防护系统流程框架。通过实验验证了基于人工智能的信息共享安全防护系统的优越性。

参考文献

[1] El-Latif A A, Abd-El-Atty B, Venegas-Andraca S E，等。5G 网络信息共享和数据保护的高效量子安全协议。下一代计算机系统，2019,100(11):893-906。

[2] 刘建军，刘建军。数字时代对隐私和个人数据保护的挑战。数学与生物科学，2020,17(5):5288-5303。

[3] 李建军，李建军，李建军，等。物联网安全的区块链技术。土耳其计算机与数学教育杂志(TURCOMAT)， 2021, 12(No 7):549-554。

[4] Parfenov D I, Bolodurina I P, Torchin V .。多云平台下网络安全节点规则形成算法的开发与研究。信息系统建模与分析，2019,26(1):90-100。

[5] 王晓明，王晓明。网络社交网络中隐私保护行为与信息披露问题的分析与评价。工程机械学报，2009(2):444 - 444。应用科学，2018,31(8):1234-1239。

[6] Tom N, Izabela P, Ian M 等。 使用基于人工智能(AI)的聊天机器人提供性健康和生殖健康咨询的障碍和促进因素:定性分析。性健康性。卫生，2021,18(5):385-393。

[7] Idowu S O, Fatokun A A.人工智能(AI)的拯救: 利用机器学习弥合抗氧化检测中的生物相关性差距:。sla 技术，2021,26(1):16-25。

[8] 人工智能(AI)、基于知识的系统(KBS)和机器学习(ML)在石油行业应用的最新进展和新发展。石油学报，2012,6(4):319-320。

[9] 金海伟，李金生。基于人工智能和大数据的融合型人才培养(STEAM)项目的开发与应用成果。体育学报，2021,26(2):37-51。

[10] Mohammad M, Saleh A, Jawabreh O 等。 人工智能(AI)对约旦亚喀巴分类酒店财务报表一致性和解释的影响战略管理学报 2021,20(3):1-18。

[11] 公众对医疗保健和人工智能的看法: 一项调查研究。国际创新教育与研究学报，2021,9(7):1-8。