基于 AI 智能技术的计算机网络信息安全保护措施

彭廖
上饶学前教育学院，中国上饶
zhaoqiang20191@163.com

摘要

文摘: 目前，计算机网络是人们工作和生活中的主要应用对象。计算机网络在诸多优势的光环下，也依然存在劣势，因为网络系统易受外部和内部因素的影响，加上自身易受攻击的特点，使得网络安全问题很容易出现。所以在实施时需要充分了解影响计算机网络安全的要素，在融合实际情况的同时，采用科学的防护方案，提高计算机网络的安全水平和用户的人身财产安全，关系到社会的顺利运行，不良影响将严重损失，给国家和社会都带来好处。这是网络安全信息如此引人注目的原因之一。各种网络信息安全事件的频繁发生，极大地加剧了网络用户的焦虑。本文在研究网络信息的性质和保护方案的基础上，对网络信息安全管理进行分析研究，重点对网络信息的区分、重要性、安全危机来源等进行研究，旨在帮助网络警察首先从理论上收集违法犯罪的踪迹并打击网络犯罪，顺利构建网络环境，保障用户信息安全以及虚拟空间的健康发展。

关键字

大数据、人工智能、网络信息安全

ACM 参考格式:

彭廖。2020.基于 AI 智能技术的计算机网络信息安全保护措施。第三*届信息技术与电气工程国际会议(ICITEE2020)*， *2020 年 12 月 03-05 日*，中国湖南常德市。ACM，纽约，美国，3 页。https://doi.org/10.1145/3452940.3453070

1 介绍

人类智能通过计算机模拟和扩展的应用操作称为人工智能。在
利用人工智能的过程，人类的智能就可以了
增强了扩展能力，提高了计算机的灵敏度

https://doi.org/10.1145/3452940.3453070

通过优化服务于人们的工作和生活需求。当前的人工智能需要依靠计算机技术来发展，才能充分发挥人工智能对社会生产力的推动作用。在人工智能和计算机技术齐头并进的同时，计算机技术也取得了重大突破和成就，推动了计算机技术的更新和发展。人工智能与计算机技术相互作用，共同发展。人工智能已广泛应用于社会管理和生产中。计算机网络安全主要体现在日常运行中使用相应的技术保证计算机系统的信息安全，减少关联数据受到恶意攻击、系统障碍等因素的影响，避免信息数据被篡改、损坏、丢失等，保证计算机系统的顺利、安全运行。计算机网络安全涉及信息安全，对计算机技术、密码技术等要求非常高，计算机在信息时代的应用对网络系统的要求越来越高，因此在信息时代计算机网络安全面临着新的突破。在实践中对于计算机网络的安全和效率必须着重于事前预测保护。[1]

2 算法原理

BP 计算方法的主要理论是将学习过程模拟成一个有 n 个节点、L 层的虚拟网络，使每一层单元与上层的输出信息单元、下层的输入信息单元一一接触，Sigmoid 型成为各单元或节点的特征。通过设置输出 y，使操作流程简单高效。设 N 个样本(xk, yk)(k= 1,2，⋯， N)，假设样本上节点 I 的输出为 Oi，输入为 Xk, yk 表示网络输出，节点 I 的输出为 Oik。现阶段对第一层的 JTH 单元进行分析，节点 J 的输入为 KTH 样本输入时的输入[2-3]。

$$洗鼻_{我} = .wl\, i_{-}\mathbf{1}_{j} \; 我_{jk}$$

$$^{jk}_{I} = f\,(netl)^{jk}$$

其中 JK 表示网络层，当输入样本 K 时，JTH 单元的节点输出为 JK。误差函数如下所示

$$埃_{j} = (\mathbf{y}。 \quad 2)$$

式中，y 为单位 j 的实际输出，总误差如公式所示

$$E = \frac{1}{2N}\sum_{k=1}^{k}$$

$$\delta_{jk} = \frac{\partial E_k}{\partial net_{jk}}$$

所以

$$\frac{\partial E}{\partial w_{jk}} = \frac{\partial E}{\partial net_{jk}} \cdot \frac{\partial net_{jk}}{\partial w_{jk}} = \delta_{jk} \cdot o_{jk}^{l-1}$$

如果节点 J 是输出单元，则

$$\delta_{jk}^{l} = \frac{\partial E_k}{\partial y_{jk}} \cdot \frac{\partial y_{jk}}{\partial net_{jk}} = (y_k - y_k) F'(net_{jk})$$

如果节点 J 不是输出单元，则

$$\delta_{jk}^{l} = \frac{\partial E_k}{\partial net_{jk}^{l}} = \sum_{j} \frac{\partial E_k}{\partial net_{jk}^{l+1}} \cdot \frac{\partial net_{jk}^{l+1}}{\partial y_{jk}} \cdot \frac{\partial y_{jk}}{\partial net_{jk}^{l}} = f'(net_{jk}^{l}) \sum_{j} \delta_{jk}^{l+1} w_{jk}^{l+1}$$

总结上述结果，有

$$\frac{\partial E_k}{\partial w_{ij}^{l}} = \delta_{jk}^{l} o_{jk}^{l-1}, \quad \delta_{jk}^{l} = f'(net_{jk}^{l}) \sum_{j} \delta_{jk}^{l+1} w_{jk}^{l+1}$$

通过遗传算法的计算，得到了控制码的交叉和变异过程。当变异计算中剔除一个神经元时，对应的权重指标代码重置为 0;当在变异计算中加入一个神经元时，相应的权重指标代码将开始随机初始化。由于加权指数是用浮点数编程的，因此需要重新设置新的变异算子和交叉算子，并用 CP 的概率对交叉个体进行过滤。以个人为例，我首先看到一个人的行为相互交叉。[4-6]

$$X_{i+1} = c_i \cdot X_i + (1 - c_i) \cdot X_i$$

式中，X_i, X_{i+1}为交点前的个体对;x_{ii}、x_{ii+1}为交点后一;ci 是区间[0,1]内的均匀分布随机数。算法实现过程如图 1 所示

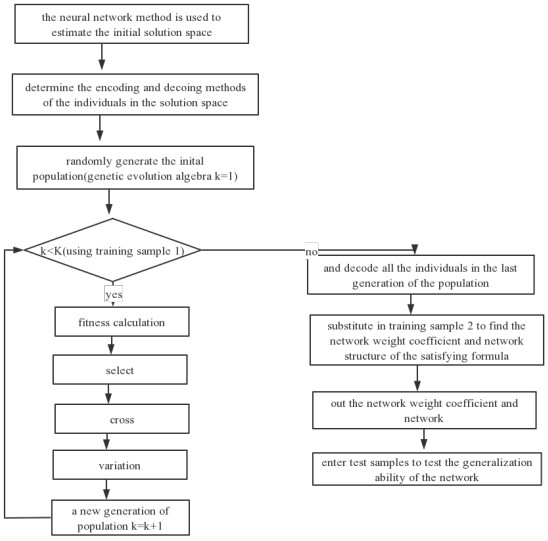

图 1: 算法实现流程图

3 系统设计

支撑平台由管理控制、资金筛选、在线检测、安全事件检测、渗透检测、恶意代码检测、漏洞检测、安全趋势预测评估等八个单元组成，如图 2 所示[7]。

由于本次构建的支撑平台各子系统都是独立的个体，能够应对复杂多变的安全检测与评估过程，提高了支撑平台其他应用的灵活性。主要体现在各子系统和硬件分别承载的平台显示上。此外，各子系统可以在自己的计算机上独立运行，并开始建立和运行检查评估工作。该计划将常用的接口设置为控件、数据和

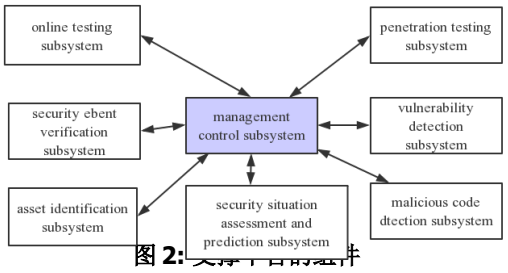

图 2: 支撑平台的组件

协作。新的支持平台覆盖范围广，是通过这些子系统和接口生成的。同时，完善的第三方检测评估方法和支撑平台也可以集成。文件传输方法以移动存储(如 u 盘)为媒介，体现控制和协调两个接口，子系统之间的交互用 XML 表示。利用基于 TCP/IP 协议的数据接口来传输检测评估的数据。

4 系统测试

在子系统开始安全事件检查之前，从被测试子系统的其余部分收集所需的信息称为渗透测试。渗透测试子系统除了可以在线检测出 IDS、防火墙等安全设备信息外，还可以检测出各子系统的恶意代码、间谍软件、木马等威胁数据，并为系统提供弱弱性需求

In this system database design, AQPJ is used to store all the business data. There is only one table space under AQPJ, and the SQL statement of table space is created:

```
--Create the tablespace
create tablespace AQPJ datafile F:\oracle\product10. 1.0\oradata\news\news_ data.dbf size 500M autoextend on next 10m maxsize unlimited;
```

图 3:代码

The AQPJ is the table space name F: \oracle\product\10.1.0\oradata\news\news_data.dbf' is the physical file stored in the data ,500 M is the initial size of the table space, and the space is automatic, adding 10 M space each time.
The user AQPJ the database is the sql statement AQPJ, creating the table user:

```
--Create the user
create user AQPJ indentified by "" default tablespace AQPJ temporary tablespace TEMP profile DEFAULT quota unlimited on AQPJ;
--Grant/Revoke role privileges
grant connect to AQPJ;
grant dba to AQPJ;
```

图 4:代码

To create user AQPJ AQPJ for spatial AQPJ and assign database permissions to users AQ_CO_Communication AQ_CO_Persons all of the above data tables are created using standard creation database predicates, such as:

```
- ( reate table
create table AQ RC_ _Subject
(
FID
VARCHAR2(100) not null,
VERSION NUMBER,
(Data table field)
tablespace AQPJ
pctfree 10
initrans 1
maxtrans 255
storage
(
initial 128
minextents 1
maxextents unlimited
);
-- Create/Recreate primary, unique and foreign key constraints
alter table AQ_ RC_ Subject
add primary key (FID)
using index
tablespace AQPJ
pctfree 10
initrans 2
maxtrans 255
storage
initial 128K
minextentsl
maxextents unlimited
);
```

图 5:代码

在漏洞安全筛选数据中提供我们的 IDS 和杀毒系统预警信息和客户端信息。

基于上述数据库结构的实现算法如图 3-5 所示:

总体上描述了网络安全评估的内容，主要由支撑平台架构网络安全评估单元、工作计划和系统动作单元等组成。

5 结论

网络信息存储广泛应用于人们的工作和生活中。随着网络技术的飞速发展，网络安全也应与时俱进。因为之前的检测效率、覆盖范围、检测系统不匹配等因素使得入侵检测成为人们关注的焦点。 现在通过人工智能中的信息识别，专家系统、神经网络和信息挖掘系统等产生了新的入侵监管体系，完善了以往的缺陷、潜在的网络安全威胁和恶意入侵的最高水平，可用于检测分析评估，以及防范恶意软件入侵病毒对计算机用户的危害，提高检测精度。计算机网络安全防御对于快速发展的人工智能技术尤为重要，人工智能技术对恶意软件的有效拦截、对计算机病毒入侵的强制防护，构建更高质量的安全防护体系，使人工智能在计算机网络安全中的应用得到进一步的实践和拓展。

参考文献

[1] 刘毅，袁兴良，熊泽辉，康家文，王晓飞，Niyato Dusit。6G 通信的联邦学习: [J]。中国通讯,2020,17(9):105 - 118。
[2] 张平，徐晓东，秦晓琪，刘一鸣，马楠，韩树军。6G Ubiquitous-X 下的物联网人工智能演进[J]。哈尔滨工业大学学报(新编)，2020,27(03):116-135。
[3] 白玉阳，黄艳浩，陈思远，张军，李柏青，王飞跃。 云边缘智能: 电力系统运行控制的边缘计算方法及其应用现状与展望[J]。自动化学报，2020,46(03):397-410。
[4] 吴文军，黄铁军，龚珂。 中国人工智能伦理原则及其治理技术发展[J]。工程,2020,(03):212 - 229。
[5] 陈兴远，高元钊，唐慧林，杜学华。大数据安全技术研究进展[J]。中国科学:信息科学，2020,50(01):25- 66。
[6] 杨林尧，陈思远，王晓，张军，王成红。数字孪生与并行系统的现状与展望[J]。化学学报，2019,45(11):2001-2031。
[7] 周骥，周艳红。白王。臧存继元。面向新一代智能制造的人-信息-物理系统(HCPS) [J].中国工程，2019,5(04):71-97。