Modeling and Simulation 建模与仿真, 2021, 10(4), 973-983
Published Online November 2021 in Hans. http://www.hanspub.org/journal/mos
https://doi.org/10.12677/mos.2021.104097

Hans汉斯

基于QPSO-BP的云平台信息系统安全风险分析

杨志美[1]，潘　平[1]，潘俊宇[2]

[1]贵州大学，贵州　贵阳
[2]贵州省电子证书有限公司，贵州　贵阳

收稿日期：2021年9月2日；录用日期：2021年10月26日；发布日期：2021年11月2日

摘　要

云平台是云计算服务的重要载体，具有更开放、虚拟化、高度集成以及平台架构复杂等特性，更易受到各种威胁。论文在分析云平台架构及其服务模式的基础上，提出基于云平台信息系统的风险分析模型，引入量子粒子群优化BP神经网络(QPSO-BP)模型对信息系统安全风险进行分析，通过分析各风险因素对系统风险的影响，获得云平台风险因素敏感度评价，实现对风险的预测和管理。仿真表明，该方法能有效预测云平台信息系统风险，与GA-BP和PSO-BP神经网络预测方法相比有较好的网络性能和预测精度，为云平台信息系统风险管理提供一种科学有效的理论方法。

关键词

云平台，量子粒子群，神经网络，风险分析

Security Risk Analysis of Cloud Platform Information System Based on QPSO-BP

Zhimei Yang[1], Ping Pan[1], Junyu Pan[2]

[1]Guizhou University, Guiyang Guizhou
[2]Guizhou Province Electronic Certificate Company Country, Guiyang Guizhou

Received: Sep. 2nd, 2021; accepted: Oct. 26th, 2021; published: Nov. 2nd, 2021

Abstract

Cloud platform is an important carrier of cloud computing services, which is more open, virtualized, highly integrated and complex in platform architecture. It is more vulnerable to various

文章引用: 杨志美, 潘平, 潘俊宇. 基于 QPSO-BP 的云平台信息系统安全风险分析[J]. 建模与仿真, 2021, 10(4): 973-983.
DOI: 10.12677/mos.2021.104097

threats. Based on the analysis of cloud platform architecture and its service mode, this paper puts forward a risk analysis model based on cloud platform information system and introduces QPSO-BP model to analyze information system security risk. By analyzing the influence of various risk factors on system risk, the sensitivity evaluation of cloud platform risk factors is obtained, the risk prediction and management are realized. Simulation results show that this method can effectively predict the risk of cloud platform information system. Compared with GA-BP and PSO-BP neural network prediction methods, it has better network performance and prediction accuracy, provides a scientific and effective theoretical method for risk management of cloud platform information system.

Keywords

Cloud Platform, Quantum-Behaved Particle Swarm Optimization, Neural Network, Risk Analysis

1. 引言

云平台是一种基于互联网的后信息技术，相较于其他传统计算模式，具有动态可扩展、资源高度集中以及提供外包服务等特性，通过云平台，云计算服务提供商可向用户提供所需的服务，实现按需分配资源[1]。基于分布式服务器的云平台允许多用户从接入口获取数据资源并提供可视化窗口，同时云平台的用户群非常广泛，其中也掺杂着恶意的破坏者，并且服务器分布范围广等，导致云平台的监管力度不足，加剧云平台信息安全的管理难度[2]。较高的集成度以及大量的底层支撑技术也使得云平台的基础架构组成相对复杂，在当前的网络环境中更容易受到各类安全威胁，其安全性问题已然成为制约云计算发展的瓶颈。

信息系统日益更新以及网络环境的愈发复杂，导致网络安全威胁所带来的损失不断增加，信息系统的风险分析理论与方法倍受关注。刘国城[3]等人将层次分析法进行信息系统层级分类，并邀请专家为各层级因素打分赋权值，再计算其熵权值和风险向量，对风险向量进行排序比较得到其风险等级。尽管该方法实用性强可用性高，但该信息系统的层次系统结构设计科学性无法保证且熵权理论不能对每层中各指标进行横向比较，降低了风险评估的客观性。伍浏阳[4]采用因子分析法消除了风险因素间的相关性，再使用支持向量机方法进行网络训练，建立信息系统风险评价模型；该方法在一定程度上提高了信息系统风险评估的效率，但将众多风险因素提炼为几个指标会忽略小概率风险的影响因子，不利于风险评估与管理。令狐金花[5]等人用矩阵范式求解系统资产的证据距离并使用 D-S 证据理论计算威胁系统的证据距离，再将两种距离进行融合后计算出系统的风险值；该方法解决风险评估中专家评价意见主观性问题，但在其风险分析过程中没有考虑系统资产价值的损失对风险值的影响。王鑫[6]等人将模糊理论和贝叶斯正则化 BP 神经网络相结合进行风险评估，减少主观因素对评估结果的影响，增加指标量化的完整性，解决了神经网络过拟合问题，但该风险评估体系因素集较少且依赖专家评分，评估过程和网络设计过于复杂适用性不强；李森宇[7]等人使用改进的布谷鸟算法对 BP 神经网络进行优化并应用于信息安全风险评估，以提高信息系统风险预测的准确率；但后续没有对风险因素进行分析，且网络时间消耗大容易陷入局部最优解，不利于后续的风险分析和管理。

针对上述的问题，本文利用量子粒子群算法在求解局部最优解的基础上求全局最优解的优势用于优化 BP 神经网络并将此引入到风险评估中，提出基于量子粒子群优化 BP 神经网络的云平台信息系统安全风险分析模型。首先，根据云平台虚拟化、集成度高以及基础架构复杂等特性，以云平台信息系统作为评估对象，构建基于信息系统的云平台风险分析模型；其次，利用量子理论的相干性与对大数据量的未知信息处理能力对风险因素值求解最优初始权值和阈值[8] [9]；最后，将风险因素作为输入值进行网络训练输出风险值，再对风险进行单因素敏感度分析得出风险管理策略。

2. 量子粒子群优化 BP 神经网络

2.1. 量子粒子群算法

在量子理论中，薛定谔方程描述了微观粒子的状态随时间变化的规律，其解为波函数，而波函数描述了系统所有粒子的演化过程，则粒子行为存在于系统行为演化的波函数中。根据粒子群的基本收敛性质以及量子力学中的相关理论，2004 年 Sun 等人提出基于势阱模型的量子行为粒子群优化算法，并针对波函数的特征长度的特性，设计一种基于全局水平的参数控制方法，提出量子行为粒子群优化算法[10] (Quantum-behaved Particle Swarm Optimization, QPSO)。

在量子粒子群算法中，粒子有局部最优解和全局最优解，且粒子的搜索空间和求解空间性质不同。波函数描述粒子在搜索空间量子化的状态并规定粒子在势阱中的搜索范围，公式如下：

$$\Psi(x)=\frac{1}{\sqrt{L}}\exp\left(-\|P-X\|/L\right) \tag{1}$$

粒子 X 的位置进化方程为：

$$X(t+1)=P\pm\alpha*\left|mbest-X(t)\right|*\ln(1/u) \tag{2}$$

式中 α 为控制参数，决定粒子的进化位置和下一次搜索范围；u 为(0,1)上的均匀分布；P 是粒子的局部最好位置，每一维的第 i 个粒子位置 X_i 依概率收敛于 P_i；t 为迭代次数，及粒子群位置更新次数；L 为 δ 势阱的特征长度，是控制粒子搜索范围的重要参量，其进化方程为：

$$L(t+1)=2*\alpha*\left|mbest-X(t)\right| \tag{3}$$

mbest 为所有粒子的局部最好位置平均值，是此次进化粒子的全局最优位置。*mbest* 的表达式如式 4 所示，式中 M 为粒子个数。

$$mbest=\sum_{i=1}^{M}P_i/M \tag{4}$$

2.2. QPSO-BP 模型

BP 神经网络为有监督学习，通过误差信号反向传播修正权值，传统 BP 神经网络训练在之前会随机选取初始权值再进行网络训练，并基于梯度下降法，使实际输出值与期望输出值之间的误差平方和最小化；然而随机选取初始值会降低 BP 神经网络训练效率，降低迭代速率，造成学习收敛速度慢、陷入局部最优等问题。

针对传统 BP 神经网络的局限性，国内外很多学者采用免疫算法、遗传算法等仿生算法对 BP 神经网络进行优化[11] [12] [13] [14]，这些优化方法参数设置多并且易陷入局部最小值；然而，QPSO 是一种全局搜索的仿生算法，控制参数较少，有较强的鲁棒性。因此，本文采用 QPSO 优化 BP 神经网络，选取最优的初始权值和阈值，以提高网络的全局寻优能力和收敛速率。量子粒子群优化 BP 神经网络模型如图 1 所示，算法流程图如图 2 所示。

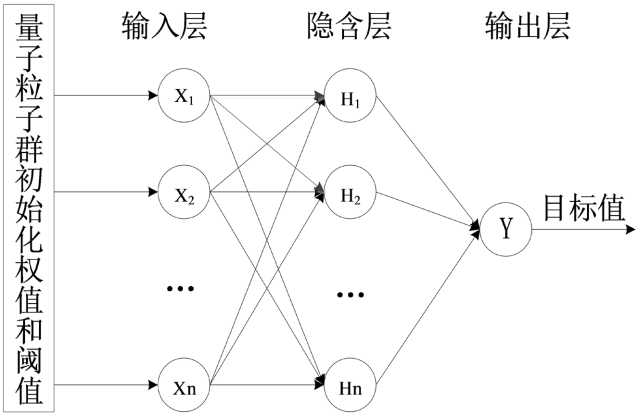

Figure 1. Quantum particle swarm optimization BP neural network model
图 1. 量子粒子群优化 BP 神经网络模型

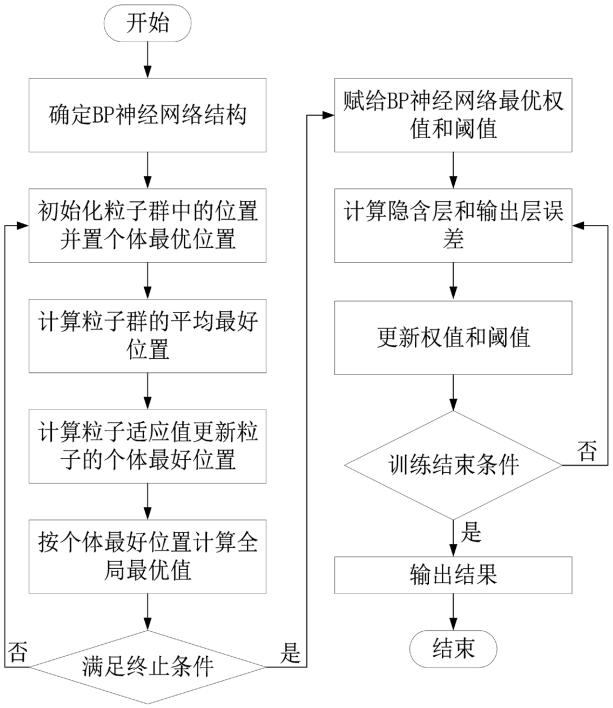

Figure 2. Quantum particle swarm optimization BP neural network algorithm flow
图 2. 量子粒子群优化 BP 神经网络算法流程

3. 基于云平台信息系统的风险分析模型

3.1. 云平台信息系统安全风险因素模型

云平台有 IaaS、PaaS 和 SaaS 三层云服务，每层都有相应的技术来支持该层的服务，可构建相应的独立“云”，也可基于下一层的“云平台”提供服务，每种“云”可直接提供给终端用户，也可以只用于支撑上层的服务。相对于其它两种底层服务形式，SaaS 提供最为集成化的功能，可以用于某些特定功能的应用，是云租户最常使用的云服务租用模式。与此同时，对于用户的个人数据信息的控制度也是最高的，在遭受到了安全风险的威胁时，面临着数据大量泄漏的危险。因此，以网络信息系统资产为切入点，主要针对云平台的 SaaS 层进行安全风险的评估与分析。

云平台由于自身架构过于复杂，较多的依赖于底层的支撑技术(例如分布式计算、虚拟化技术以及网络通信技术等)，造成一系列安全难题，国内学者针对此难题构建云计算环境的安全检查与评估指标体系[15]。因此，根据云平台信息安全资产，从物理安全、云网络安全、云虚拟化安全、云应用安全以及云数据安全五部分对系统进行风险的评估和分析，具体可分别：机房设施(r_1)、基础设备(r_2)、云网络加密措施(r_3)、云网络设备安全(r_4)、云网络访问控制(r_5)、云监视器(r_6)、云管理平台(r_7)、安全攻击及防御(r_8)、云应用隐私保护(r_9)、云数据安全存储(r_{10})、云数据安全共享(r_{11})，云数据安全加密(r_{12})，构建云平台信息系统安全风险因素模型，如图 3 所示。

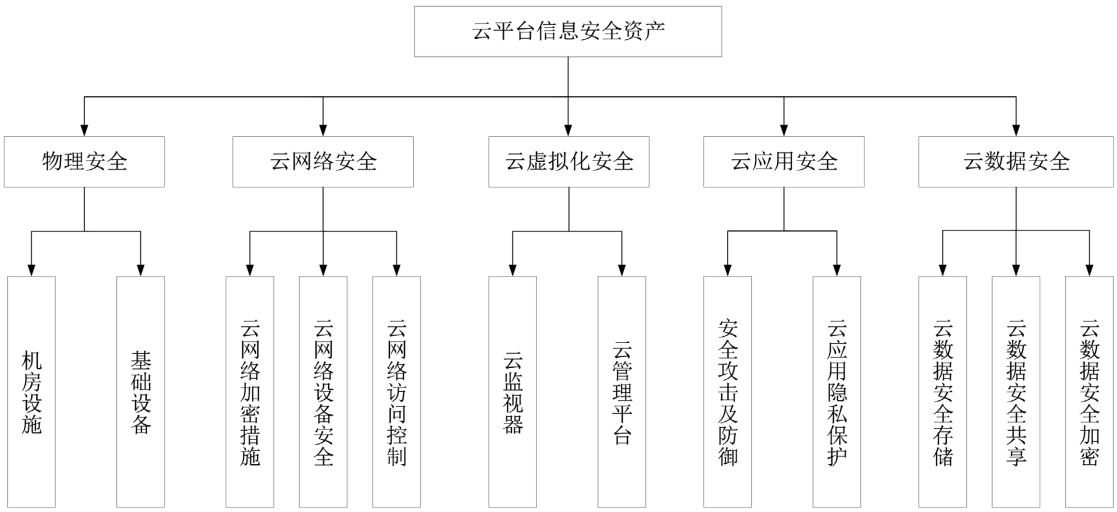

Figure 3. Cloud platform information system security risk factor model
图 3. 云平台信息系统安全风险因素模型

根据国家安全等级保护的安全控制项的要求，通过对云平台系统的信息系统安全配置项进行检查，并对调查数据进行统计分析，完成对云平台安全风险因素的量化，以实现对于风险的定量分析。传统风险分析模型为 $R = f(A,T,V)$，其中 A 为资产，T 表示威胁，V 表示脆弱性。根据 QPSO-BP 算法思想将信息系统风险分析模型抽象为：

$$R = f\left[Q(X)\right] \tag{5}$$

式中 $X = (X_1,\cdots,X_n)$ 表示各单位风险值向量，$X_n = (r_1,r_1,\cdots,r_{12})^T$ 是根据现场检测得到风险因素的风险值；Q 表示量子粒子群算法；f 表示 BP 算法；R 表示经 QPSO-BP 映射的系统风险值。

3.2. 云平台信息系统安全风险模型训练过程

云平台信息系统安全风险因素模型为三层的逻辑结构，而神经网络模型的三层网络模型中隐含层能拟合任意函数。运用量子粒子群 BP 神经网络对风险值预测，以云平台信息系统的风险因素值作为模型的输入，通过量子粒子群算法寻找 BP 网络的初始最优权值和阈值，最终输出值为信息系统的风险值。具体步骤如下：

步骤 1：信息系统风险因素特征参数初始化，将对系统检查得到的资产风险实值样本进行归一化处理后，得到粒子群算法的输入值。

步骤 2：粒子群初始化，将风险因素值作为输入粒子，设量子粒子群算法迭代次数为 t，置 $t = 0$，种群数为 12，设粒子的初始位置 $X_i(0)$，且 $P_i(0) = X_i(0)$。

步骤 3: 根据式(4)计算粒子群的 *mbest* 值和粒子 i 的适应值 $X_i(t)$; 若 $X_i(t)$优于 $X_i(t-1)$，则 $P_i(t)=X_i(t)$，否则 $P_i(T)=P_i(t-1)$。

步骤 4: 将 $P_i(t)$与全局最优位置 $D(t-1)$ 比较，若 $P_i(t)$优于 $D(t-1)$，则置 $D(t)=P_i(t)$；否则 $D(t)=D(t-1)$。

步骤 5: 根据公式(2)计算粒子的新位置。

步骤 6: 如果 $t<t_{\max}$，则 $t=t+1$，转入步骤 3，否则转入步骤 7。

步骤 7: 将 QPSO 算法得到的结果作为 BP 神经网络的初始权值和阈值，进行网络训练，计算输出误差值。

步骤 8: 根据误差，调整网络权值和阈值，进入下一次训练。

步骤 9: 若达到最大迭代次数或者预设精度则输出结果，否则转入步骤 8。

3.3. 云平信息系统安全风险分析

基于量子粒子群优化 BP 神经网络的云平台信息系统安全风险分析的过程如下：

步骤 1: 将待分析的云平台系统风险数据归一化处理，将归一化后的样本特征参数作为 QPSO 算法的初始粒子值。

步骤 2: 将 QPSO 的输出值作为网络的初始权值和阈值，进行网络训练得出风险值。根据样本的误差均值 $\bar{e}=\frac{1}{n}\sum_{i=1}^{n}e_i$，标准差 $\sigma=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(e_i-\bar{e})^2}$，调整网络参数，使网络输出值误差最小。

步骤 3: 根据网络输出值，计算第 i 个风险因素敏感度 $S_i=\left|R_i'-R_i\right|$，对云平台信息系统的安全因素做风险分析。云平台信息系统安全风险分析流程如图 4 所示。

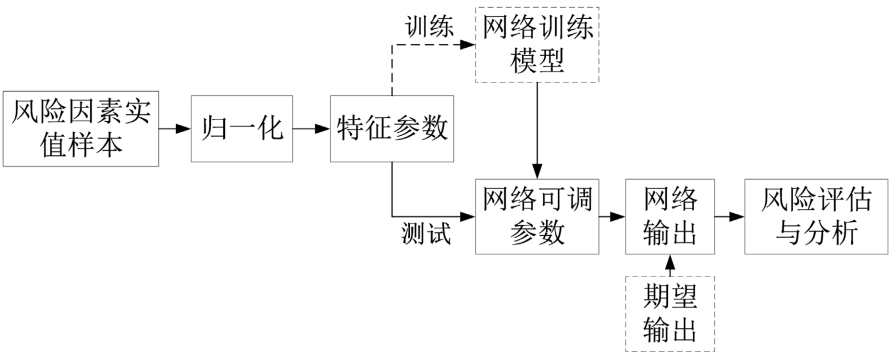

Figure 4. Cloud platform information system security risk analysis process
图 4. 云平台信息系统安全风险分析流程

4. 仿真实验

仿真使用 Windows10 和 Matlab R2019b 作为测试环境。数据源于对多家单位的云平台信息系统安全调查，以信息资产的保密性、完整性和可用性赋值为原始数据，根据影响程度对风险因素预处理得样本数据，归一化处理后的样本数据如表 1 所示。取前 30 组为训练样本后 12 组为测试样本。根据测试数据分析模型结构为 12-5-1，设最大迭代步数为 1000，误差精度为 0.0001。

在相同条件下，分别通过 QPSO-BP、粒子群优化 BP 神经网络(PSO-BP)、遗传算法优化 BP 神经网络(GA-BP)进行样本训练，根据实验可知，QPSO-BP 算法的收敛速度和预测拟合度明显优于另外两种网络。QPSO-BP 性能曲线图 5 所示、PSO-BP 性能曲线图 6 所示、GA-BP 性能曲线图 7 所示。

Table 1. Normalized sample data
表 1. 归一化样本数据

X	r_1	r_2	r_1	r_4	r_5	r_6	r_7	r_8	r_9	r_{10}	r_{11}	r_{12}	期望输出
X_1	0.66	0.71	0.67	0.51	0.50	0.81	0.82	0.70	0.81	0.44	0.87	0.71	0.62
X_2	0.16	0.25	0.25	0.15	0.14	0.19	0.68	0.30	0.23	0.13	0.17	0.21	0.19
X_3	0.49	0.69	0.56	0.61	0.75	0.83	0.76	0.32	0.77	0.71	0.51	0.75	0.53
X_4	0.42	0.79	0.68	0.5	0.2	0.2	0.36	0.47	0.37	0.66	0.7	0.41	0.39
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
X_{40}	0.2	0.63	0.65	0.75	0.44	0.9	0.26	0.32	0.4	0.7	0.56	0.3	0.43
X_{41}	0.37	0.36	0.77	0.54	0.50	0.20	0.30	0.34	0.46	0.32	0.20	0.54	0.32
X_{42}	0.23	0.32	0.62	0.30	0.40	0.39	0.60	0.48	0.20	0.32	0.20	0.20	0.29

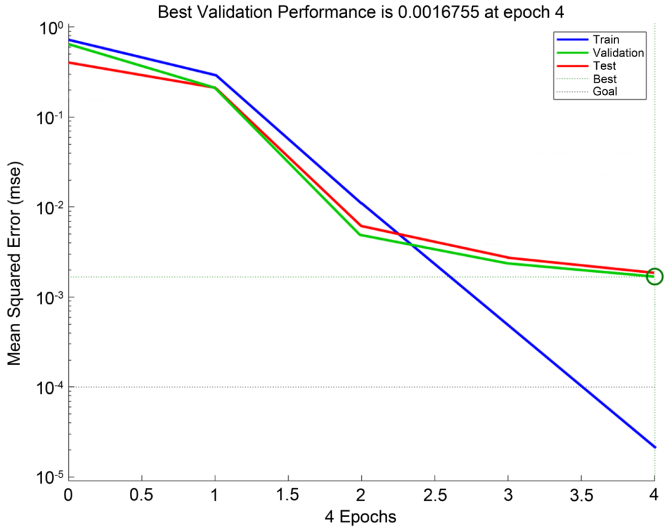

Figure 5. QPSO-BP performance curve
图 5. QPSO-BP 性能曲线

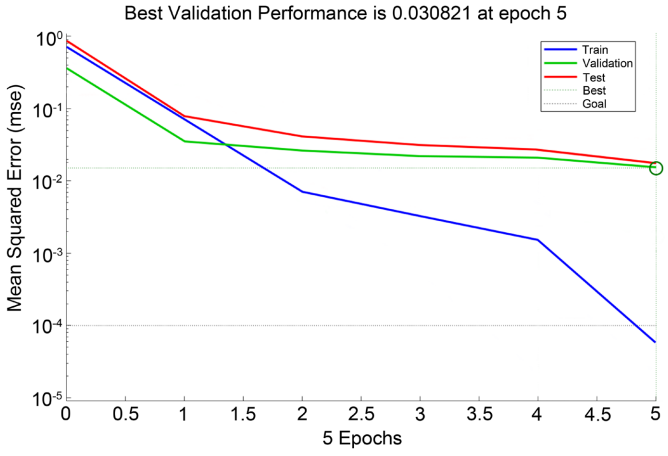

Figure 6. PSO-BP performance curve
图 6. PSO-BP 性能曲线

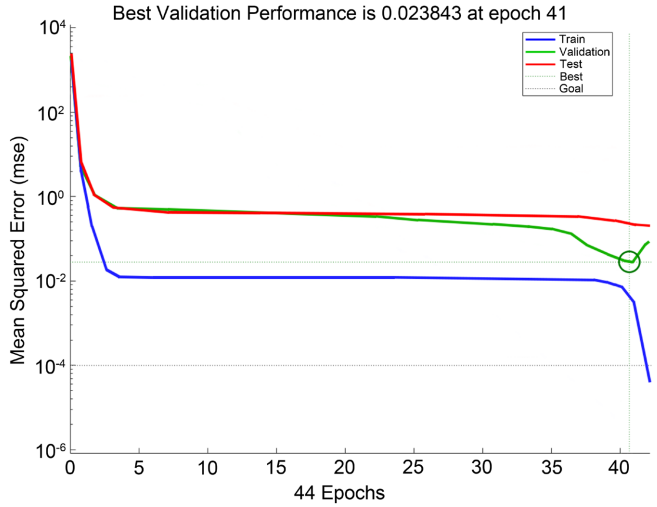

Figure 7. GA-BP performance curve
图 7. GA-BP 性能曲线

三种算法的预测结果比较如图 8 所示。实验结果表明，这三种算法都能对风险进行有效的预测，GA-BP 迭代次数多且达不到预测效果，PSO-BP 迭代次数少但拟合程度不够，QPSO-BP 则表现出良好的性能，迭代次数少网络效率高且能更准确进行预测，误差均值和标准差均优于另外两种网络，算法误差对比分析如表 2 所示。因此，QPSO-BP 预测算法更适用于云平台安全风险预测。

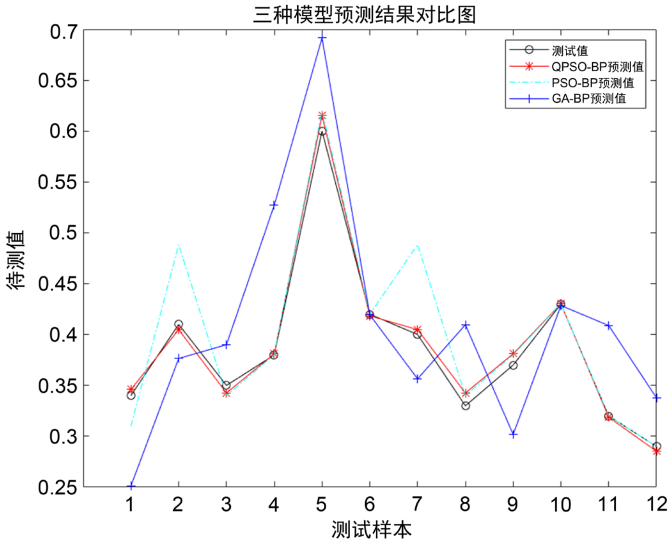

Figure 8. Comparison of test results
图 8. 测试结果对比

Table 2. Network output risk error
表 2. 网络输出风险误差

网络	$\overline{e}$	σ	收敛步长
GA-BP	0.0610	0.0729	41
PSO-BP	0.0304	0.0480	5
QPSO-BP	0.0060	0.0076	4

根据大小将风险值划分为五个等级，每个等级相应的给出风险评价，风险等级划分和评价如表 3 所示。计算出某一单位的风险值后，进行风险因素敏感度分析，即分析当某一风险因素出现波动时对系统风险造成的影响程度。以单位 X_1 为例对其进行风险敏感度分析；首先采用控制变量法计算单位 X_1 每个风险因素波动±10%后的变化值；再根据变化后的风险因素值预测风险值；最后分析云平台信息系统风险因素变化后的风险值波动情况如图 9 所示；由图知风险因素 r_{11} 变化后，风险值相较于原来风险波动最大；风险因素 r_{10} 变化后，对系统风险没有太大影响。

Table 3. Classification of cloud platform risk value levels
表 3. 云平台风险值等级划分

风险值	风险评价
$r < 0.2$	风险值很低，发生风险事件的概率很小，可忽略
$0.2 \le r < 0.4$	风险值较低，发生风险事件的概率低，采取适当的措施进行维护
$0.4 \le r < 0.6$	风险值中等，发生风险事件的概率中等，应采取措施预防风险
$0.6 \le r < 0.8$	风险值较大，发生风险事件概率较大，必须加强风险管理
$0.8 \le r < 1$	风险值极大，会发生风险事件，应马上采取紧急措施控制风险

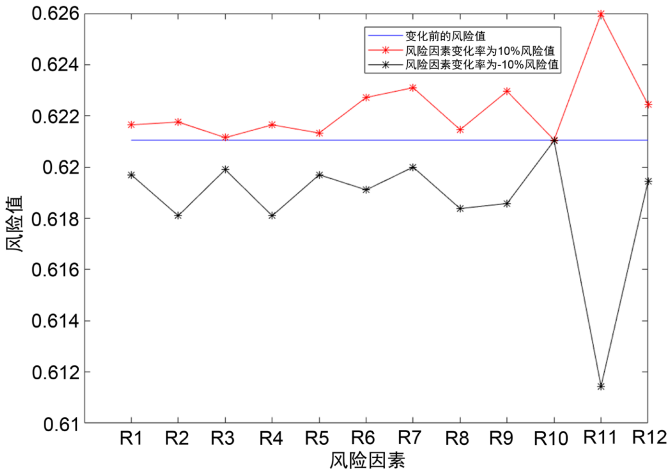

Figure 9. Risk wave after risk factors change
图 9. 风险因素变化后的风险波动

风险因素敏感度计算结果如表 4 所示，表中列出风险因素变化后的值、风险因素变化后的预测风险值以及风险敏感度。由风险因素敏感度分析得，X_1 单位的风险因素的敏感度为 0.0011 和 0.0009，相较于其他风险敏感度其值最小，则在本系统中风险因素 r_{10} 对系统风险影响最小；而风险因素 r_{11} 的敏感度为对 0.0060 和−0.0087，相较于其他因素其敏感度值波动较大，因此对系统风险值影响也较大，在该系统数据共享时加强数据的保护，避免敏感数据泄露和篡改等，应立即采取措施对数据进行加密管理和安全维护以规避风险。

Table 4. Sensitivity analysis of various risk factors of cloud platform
表 4. 云平台各风险因素敏感度分析

风险因素	变化率%	变化赋值	风险值	敏感度
r_1	10	0.7260	0.6217	0.0017
	−10	0.5940	0.6197	−0.0004

Continued

r_2	10	0.7810	0.6218	0.0018
	−10	0.6390	0.6181	−0.0021
r_3	10	0.7370	0.6212	0.0011
	−10	0.6030	0.6199	−0.0002
r_4	10	0.5610	0.6217	0.0017
	−10	0.4590	0.6181	−0.0021
r_5	10	0.5500	0.6213	0.0013
	−10	0.4500	0.6197	−0.0004
r_6	10	0.8910	0.6227	0.0027
	−10	0.7290	0.6191	−0.0010
r_7	10	0.9020	0.6231	0.0031
	−10	0.7380	0.6200	−0.0001
r_8	10	0.7700	0.6215	0.0015
	−10	0.6300	0.6184	−0.0018
r_9	10	0.8910	0.6296	0.0096
	−10	0.7290	0.6186	−0.0016
r_{10}	10	0.4840	0.6211	0.0011
	−10	0.3960	0.6210	0.0009
r_{11}	10	0.9570	0.6260	0.0060
	−10	0.7830	0.6114	−0.0087
r_{12}	10	0.7810	0.6224	0.0024
	−10	0.6390	0.6194	−0.0007

5. 结论

通过对云平台安全架构的理论分析，构建基于云平台信息系统的风险分析模型，该模型以信息系统作为评估对象，利用 QPSO-BP 算法有效地解决网络局部最优问题，实现对云平台风险的预测，再对高风险系统进行风险因素敏感度分析，为有效地转移风险提供了相应的理论依据。实验表明，QPSO-BP 神经网络适用于对云平台信息系统的安全风险值预测，实现对网络可调参数的更新，提高网络的收敛速率和未知风险的预测精度。通过分析各因素对风险值的影响，能更精准地对云平台信息系统风险进行管理，提高风险管理效率，为云平台信息系统风险分析提供一条新途径。

基金项目

国家社会科学基金资助项目[19BZX035]。

参考文献

[1] 赵波, 戴中华, 向骕. 一种云平台可信性分析模型建立方法[J]. 软件学报, 2016, 27(6): 1349-1365.

[2] 杨悦. 云平台信息安全整体保护技术探讨[J]. 中国管理信息化, 2021, 24(2): 200-201.

[3] 刘国城, 王会金. 基于 AHP 和熵权的信息系统审计风险评估研究与实证分析[J]. 审计研究, 2016(1): 53-59.

[4] 伍浏阳. 因子分析和支持向量机的信息系统风险评价[J]. 微电子学与计算机, 2016, 33(2): 144-148.

[5] 令狐金花, 潘平, 杜瑶瑶. 基于证据距离理论的信息系统安全风险分析[J]. 信息网络安全, 2019(9): 11-15.

[6] 王鑫, 唐作其, 许硕. 基于模糊理论和 BRBPNN 的信息安全风险评估[J]. 计算机仿真, 2019, 36(11): 184-189.

[7] 李森宇, 毕方明, 刘晋, 陈伟. ICS-BPNN 在信息安全风险评估中的应用[J]. 中国科技论文, 2018, 13(2): 171-175.

[8] 李士勇, 李盼池. 量子计算与量子优化算法[M]. 哈尔滨: 哈尔滨工业大学出版社, 2009.

[9] 李士勇, 李盼池. 求解连续空间优化问题的量子粒子群算法[J]. 量子电子学报, 2007(5): 569-574.

[10] Sun, J. and Xu, W.B. (2004) A Global Search Strategy of Quantum-Behaved Particle Swarm Optimization. *Proceedings of IEEE Conference on Cybernetics and Intelligent Systems*, Singapore, 1-3 December 2004, 111-116.

[11] Al-Shaikhly, R. and Mazin, H. (2018) Intelligent Cloud Computing Security Using Genetic Algorithm as a Computational Tool. *Journal of Physics*: *Conference Series*, **1003**, Article ID: 012024. https://doi.org/10.1088/1742-6596/1003/1/012024

[12] 曹林, 王之腾, 陈亮, 李洪顺, 高申, 张自立. 基于改进量子免疫算法的神经网络集成[J]. 计算机工程与应用, 2020, 56(22): 142-147.

[13] 张立仿, 张喜平. 量子遗传算法优化 BP 神经网络的网络流量预测[J]. 计算机工程与科学, 2016, 38(1): 114-119.

[14] Stepanov, L.V., Parinov, A.V., Korotkikh, L.P. and Koltsov, A.S. (2018) Approach to Estimation of Level of Information Security at Enterprise Based on Genetic Algorithm. *Journal of Physics*: *Conference Series*, **1015**, Article ID: 032141.

[15] 章恒, 禄凯. 构建云计算环境的安全检查与评估指标体系[J]. 信息网络安全, 2014(9): 115-119.