2023 IEEE 第三届电力，电子和计算机应用国际会议(ICPECA) - 978-1-6654-7278-4/23/$31.00©2023 IEEE - DOI: 10.1109 / ICPECA56706.2023.10075946

人工智能技术下基于用户需求的网络信息安全服务模型研究

徐李
四川工商学院智能制造与信息工程学院
中国成都
470792941@qq.com

***摘要:*本文提出了一种基于人工智能技术的通用网络安全框架。然后阐述了安全目标、安全边界、安全系统要素、安全服务和安全风险评估之间的关系。利用统一建模语言 UML 的强大功能和通用性，给出了安全目标、安全边界和安全系统要素的建模方法。本文在构建网络场景的基础上，从网络数据库安全漏洞、数据孤岛风险和网络安全防护能力三个角度，建立了网络信息安全事件检测关联规则，构建了信息安全风险度量模型。最后，通过一个典型网络实例，分析了上述模型和算法在网络安全评估和最优主动防御中的应用。分析结果表明，本文提出的模型和方法是可行和有效的。**

关键词:人工智能，用户需求，网络信息，安全服务

I. 介绍

网络安全体系是一个涵盖“攻击、预防、检测、控制、管理、评估”多阶段安全管理与安全技术相结合的完整体系。　鉴于网络安全体系的重要性，国内外研究机构和人员开展了广泛的研究，根据主要研究对象的不同，可分为三类:安全技术体系研究、安全管理体系研究、综合安全体系研究[1]。许多研究者在等级保护方面取得了很大的成就。有学者将信息安全绩效度量与信息安全等级分配相结合，建立了多维度的信息安全指标体系。他们提出了一种基于安全指标的信息安全等级保护量化模型。有学者提出了一种基于威胁建模与实施指南相结合的软件安全需求分析方法，通过威胁攻击图(TAG)对攻击进行评估，将分层防护思想融入软件安全设计阶段。这样，该解决方案可以更好地改进软件设计有效提升软件安全性。有学者提出了企业网络安全等级保护的实现方案，包括安全域、网络边界和网络环境三层。通过具体案例，实现了企业服务器域和桌面终端域的划分、域间路由的动态计算以及各网关和链路的热备冗余。全面提高了网络和业务系统的容错性和稳定性，取得了良好的效果。有学者利用 DeMatel- ANP 方法和灰色系统理论建立了信息安全风险评估模型。通过对控制措施之间的不确定性关系进行灰色关联分析，得出安全风险等级，从而找出需要改进的控制措施。这将把风险降低到可接受的范围内。　然而，目前企业部署的工业信息安全系统大多基于传统的信息安全理论，建立基于密码学、反病毒和网络边界保护的静态被动防御体系[2]。面对日益复杂的网络环境和持续不断的大规模网络攻击，这种静态被动防御系统已经不能满足用户对工业信息安全防御的需求。为了实现工业信息安全系统的动态主动防御，有必要引入新的信息安全防御理论来丰富传统的信息安全理论体系。　本文介绍了关联规则的概念。关联规则反映了一件事物与另一件事物之间的相互依赖关系。关联规则的应用有望减小网络信息安全风险度量分析模型输出结果与实际风险值之间的差异，即提高风险度量分析模型的准确性。

II. 人工智能技术下的信息网络安全内容

鉴于以上对云计算网络信息安全的威胁分析，结合中国网络安全等级防护工作，本文提出云计算网络安全策略，模型如图 1 所示。

978-1-6654-7278-4/23/$31.00©2023 ieee

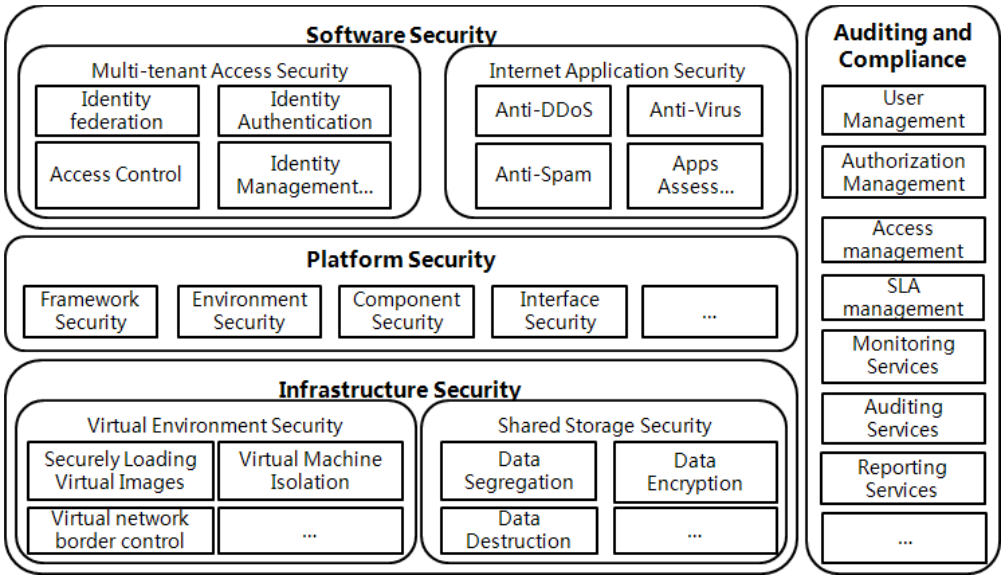

图 1 所示。云计算网络信息安全架构

A. 物理和环境安全

在物理和环境安全方面，为物理选址、物理门禁、防盗毁损、防雷、防火、防水防潮、防静电、温湿度控制、供电、电磁保护等提供安全保护[3]。由于云计算环境中物理位置的分布，每个机房需要满足相同的物理安全防护要求。

B. 网络与通信安全

在网络和通信安全方面，主要从网络架构、通信传输、边界保护、访问控制、入侵防御、恶意代码防御、安全审计、网络级集中控制等方面进行保护。在云计算中，采用虚拟化技术对物理进行抽象资源分为虚拟网络、虚拟计算机、虚拟存储等资源。因此，需要同时考虑物理资源和虚拟资源的安全保护。

C. 设备与计算安全

在设备和计算安全方面，从身份认证、访问控制、安全审计、入侵检测、恶意代码防御、资源控制等方面保护主机和操作系统。

D. 应用及数据保安

在应用和数据安全方面，需要考虑应用层的身份认证、访问控制、安全审计、软件容错、资源控制、接口安全，以及数据完整性、数据机密性、数据备份与恢复残留信息保护等方面的安全保护。

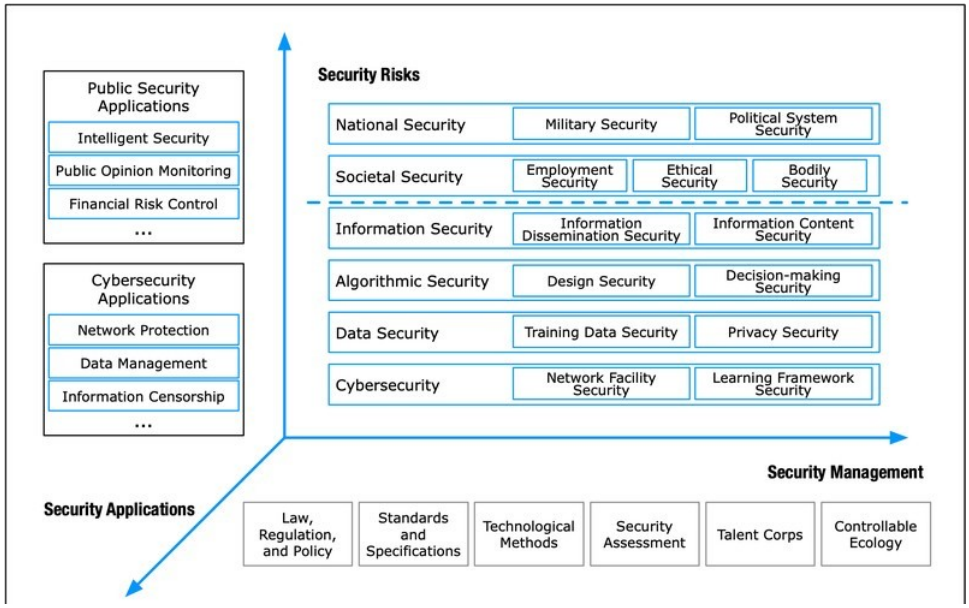

图 2 所示。网络安全架构图

III. 网络安全体系框架

图 2 所示的安全体系框架包括安全目标、安全边界、安全系统要素、安全服务、安全风险评估和 OSI 参考模型，其中安全目标分为业务需求目标和安全需求目标，安全系统要素分为安全技术要素和安全管理要素[4]。按照 OSI 安全体系结构的分类方法，安全技术要素可分为 8 类:数据签名机制、加密机制、访问控制机制、数据完整性机制、认证交换机制、反服务填充机制、公证机制和路由控制机制。安全管理要素分为信息安全组织、网络信息安全管理、人力资源安全、物理与环境安全、通信与运营管理、访问控制、信息系统采集开发与维护、信息安全事件

管理，业务连续性管理，合规性等，按照 ISO 27000 系列标准的要求。这种分类方法可以保证与上述标准体系的兼容性，便于扩展本文构建的安防系统框架的适用范围。

在图 3 中，可以根据安全目标确定安全体系框架的安全边界和安全体系要素，安全边界的划分和安全体系要素的建立将为安全目标的实现提供支持。安全服务一方面是由特定的安全系统要素决定的，另一方面又受到安全边界划定的影响[5]。安全风险评估提供了一种动态改进和完善安全体系框架的手段，通过分析安全边界内的安全体系要素来实现安全目标。安全系统要素的建立需要满足 OSI 参考模型的要求，以保证各个层面的安全。

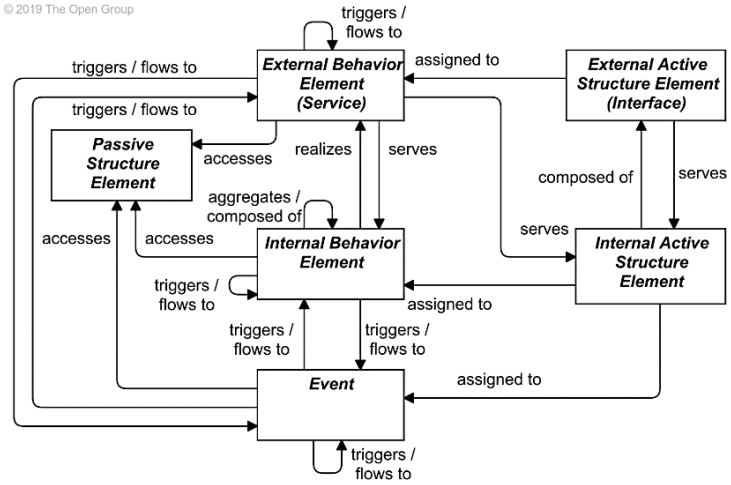

图 3 所示。安全体系结构框架元素的示意图

IV. 网络信息安全风险度量分析模型的设计

网络安全。根据上述理论，网络信息安全风险度量与分析模型的基本框架如图 4 所示。

A. 风险分析

一般来说，信息安全风险的价值与信息的价值、威胁和脆弱性有关

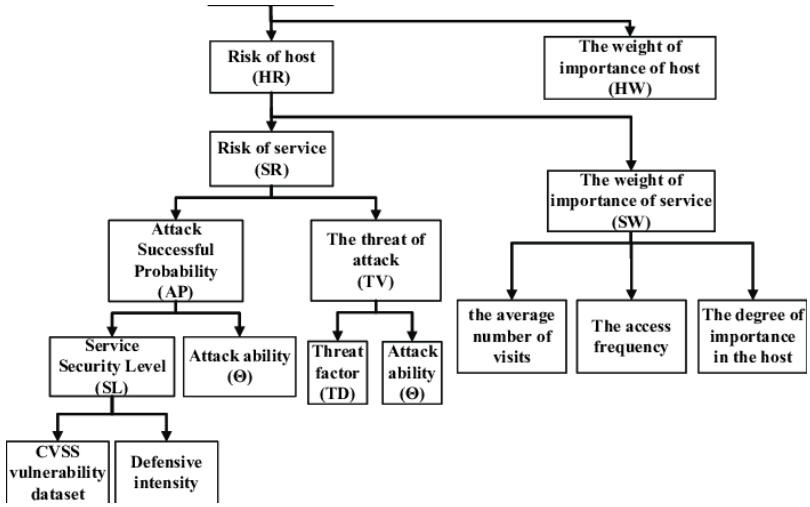

图 4 所示。网络信息安全风险度量分析模型框架

网络信息安全，威胁和漏洞是风险的三个要素。财产是指对企业具有价值的一切，包括有形资产和无形的网络信息安全，如软件、数据、提供服务的能力等[6]。通过分析上述网络信息安全的损害程度，可以量化风险造成的损失。网络信息安全风险可以表述为:

$$R \equiv \{(E1, L1), \ldots, (Ei, Li), \ldots, (En, Ln)\} \quad (1)$$

地点: En 和 Ln 分别为安全风险事件及其发生概率。风险造成的损失可以用网络信息安全价值和损失份额来衡量[7]。将网络信息的 j 个网络信息的网络信息安全值定义为 Aj，然后是损失

过程中，可以根据网络信息的损失和收益得到风险的量化结果。

科学的安全测量过程一般包括提出测量目标、确定测量要求、设定测量指标、建立测量模型、制定安全测量标准、实施安全测量等步骤[8]。遵循上述安全风险度量的基本步骤，关联
规则用于挖掘网络的实时信息数据，分析关联关系

由安全风险事件 Ei 引起的:

网络风险事件，确定当前网络的运行状态，进而保证安全风险度量的准确性。

$$Di=\mathrm{Pij}\sum_{j=-1}^{*} Aj \quad (2)$$

在那里，j 损失的份额是由信息引起的吗

j 网络的安全性。M 是网络信息安全的数量。在此基础上，将安全风险事件 Ei 造成的绝对损失效应定义为:

$$Ui=(\mathrm{Di})\mu \quad (3)$$

地点: $\mu()\cdot$为风险事件引起的不满程度。同理，相对损失效应可得:

$$\text{外}:\mu\text{我}\leftarrow \sum_{j=-1} Aj \quad (4)$$

概率意义上的相对损失效应，考虑安全风险事件发生的概率，应计算预期损失效应，其表达式为:

$$U=\sum_{i1=}^{n}\mu(\mathrm{Di})\mathrm{Li} \quad (5)$$

式(5)的最终计算结果 U 和 F 分别为预期绝对损失效应和预期相对损失效应。在实际的安全风险度量中

下面将详细描述这四个部分完成的评估功能。

A. 网络信息安全评估

网络信息安全评估主要是根据网络信息安全调查结果确定被测信息系统中的网络信息安全类型，即确定集合 a 中的各个要素 Nai。根据安全调查结果得出的决定网络信息安全价值的相关属性，计算出各网络信息安全价值，即

{ai - *value}已确*定。

B. 基于关联规则的网络安全信息模型

首先，使用关联规则检测网络安全事件，基本流程如图 5 所示。

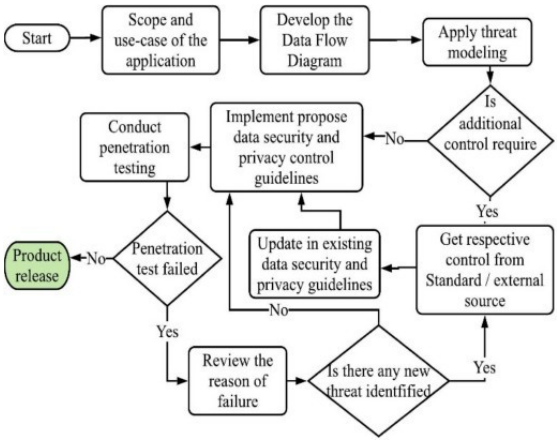

图 5 所示。关联规则检测网络安全事件的流程

数据孤岛风险的风险度量主要从数据孤岛的影响程度角度进行分析，其过程如下:

$$Atd=\mathrm{Atn}+Ast+R(Asd) \quad (6)$$

最后一个 d 自闭症

地点: $Atdd$ 为数据孤岛的影响程度。为数据孤岛程度的量化值。$Astd$ 是信息重要性的量化值

岛上。美国培训信息的比例是

湖巨大的和 Vasd 分别是数据的严重性

孤岛，信息网络信息安全的重要性和信息的权重值效率损失。R+是损失函数。

V. 应用网络信息安全风险模型

网络信息安全风险关联规则模型的应用分为网络信息安全评估、威胁评估、漏洞评估和风险计算四个步骤[9]。的

B. 威胁评估

威胁评估主要是根据入侵检测和问卷调查的结果来确定被测信息系统所面临的威胁，即确定集合 t 中的每个元素 ti，计算威胁

频率，即确定{ti - fren}。分析网络信息安全面临的威胁，即确定 AT (ai, tj)。

C. 漏洞评估

漏洞评估主要是根据漏洞扫描结果、BIOS 安全检测结果、WLAN 检测结果、设备有效性检测结果来确定被测信息系统的漏洞，即确定 setV 中的各个元素 vi。确定每个漏洞的严重程度及其可被利用的程度，即确定{vi - serious, diff}。分析威胁可以利用的漏洞，即确定 TV (ti,vi)。

D. 风险计算

风险计算主要分析漏洞之间的相互作用，即确定 VV (vm,vn)。 分析网络信息安全之间的安全依赖关系，即确定 AA(am, an)。根据模型过程确定的网络信息安全风险计算方法，计算出网络信息安全的风险值。

VI. 实验检测

本实验选取某省某大数据平台运营商的网络数据作为测试样本，在一个月的采集周期内每 10 分钟保存一组数据，以评估运营网络的信息安全[10]。将选取的数据资源分成样本，按照平均分配原则处理成三组数据包。测试前，邀请 10 位专家对网络安全指标进行选择和评分，进行不同指标水平下的网络安全评价设置。为了保证实验的准确性，引入了一组传统模型进行比较。 测试平台获得分级结果后，将两组模型依次接入测试平台，分别对网络信息样本的安全等级进行评估。具体等级评价结果如表 1 所示。

表 1 运营商网络信息安全水平评估结果

样本数	示例 1	示例 2	示例 3
安全	0.2387	0.1073	0.2185
更安全的	0.3864	0.3585	0.0298
一般安全等级	0.0461	0.0467	0.1777
危险的	0.2552	0.2732	0.1707
非常危险的	0.0736	0.2143	0.4033
实际结果	更安全的	更安全的	非常危险的
新模式	更安全的	一般	一般
原始模型	安全	更安全的	非常危险的

根据表 1 所示的原始模型在信息安全等级评估中，其危险性一般低于实际结果中的某一等级。本文模型的应用可以匹配实际数据的分级结果，在综合考虑各指标主观因素的情况下，将内部数据的等价性联系起来，从而获得更准确的评价结果。综合实验结果表明，本文设计的模型可以通过所选择的指标类型重新描述等级特征，并综合考虑不同等级指标的重要属性，从而评价具有实际应用效果的网络信息安全等级。

VII. 结论

为了全面、准确地度量网络信息安全风险，关联规则的引用有效地提高了网络信息安全风险的度量精度。然而，在不同的网络环境中，由于对网络信息的攻击方式不同，安全风险测量结果也会有很大差异。

参考文献

[1] 左晓军，陈泽，董立联，等。基于信息安全框架“金三角模型”的网络安全评估方法研究。《Bond Bonding》，vol. 41, pp.54-59, 2020 年 2 月。

[2] 杨志远，张世鹏，孙浩，关晓红。基于 Cyber-net 和学习算法的变电站网络威胁风险评估。电力系统自动化，第 44 卷，第 91-94 页，2020 年 12 月。

[3] 张凯，刘敬举。基于漏洞动态利用的网络入侵路径分析方法。信息网络安全，vol. 11, pp.62-72,April 2021。

[4] 张欣，董黎明。攻防博弈模型下的网络节点信息安全定量仿真。计算机仿真，vol. 037, pp.18-21,98, 2020 年 6 月。

[5] 张祥云，周子，蒋友新，等。基于卷积神经网络的离焦颗粒尺寸和位置测量。光学学报，vol. 42, pp.191-200,December 2022。

[6] 方绍峰，周仁军，彭媛媛，等。风险规避型电力零售商的均衡市场交易模型。电力系统与自动化学报，vol. 32, pp.69- 74, 2020 年 2 月。

[7] 秦中原，胡宁，方兰亭。基于免疫仿生机制和图神经网络的网络异常检测方法。信息网络安全，第 11 卷，pp.10-16, 2021 年 8 月。

[8] 李伟刚，李强。基于零信任网络模型的环境监测网络安全性分析。《四川环境》，第 40 卷，第 49-51 页，2021 年 3 月。

[9] 孟金。基于因子分析和神经网络的信息系统风险评估模型。现代电子技术，vol.43, pp.58-62,December 2020。

[10] 彭子祥，焦科，王俊杰，等。基于贝叶斯网络的建筑结构安全评价模型。建筑技术，vol. 52, pp.49-59, 2021 年 10 月。