分类号:　　密　　级：公开
学　号：20202108036　　单位代码：10759

石河子大学
硕 士 学 位 论 文

医疗机构网络安全态势评估与预测研究及系统实现

学 位 申 请 人	张明月
指 导 教 师	周杰 教授
申请学位类别	专业硕士
专 业 名 称	电子信息
研 究 领 域	计算机技术
所 在 学 院	信息科学与技术学院

中国·新疆·石河子
2024 年 10 月

分类号:　　密　　级：公开
学　号：20202108036　　单位代码：10759

石河子大学
硕 士 学 位 论 文

医疗机构网络安全态势评估与预测研究及系统实现

学 位 申 请 人	张明月
指 导 教 师	周杰 教授
申请学位类别	专业硕士
专 业 名 称	电子信息
研 究 领 域	计算机技术
所 在 学 院	信息科学与技术学院

中国·新疆·石河子
2024 年 10 月

Research and System Implementation of Network Security Situation Assessment and Prediction for Medical Institutions

A Dissertation Submitted to
Shihezi University
In Partial Fulfillment of the Requirements
for the Degree of
master of Engineering

By

Zhang Mingyue
Computer Technology

Dissertation Supervisor: Prof. Zhou Jie

October, 2024

石河子大学学位论文独创性声明及使用授权声明

学位论文独创性声明

本人所呈交的学位论文是在我导师的指导下进行的研究工作及取得的研究成果。据我所知，除文中已经注明引用的内容外 ，本论文不包含其他个人已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中作了明确的说明并表示谢意。

研究生签名：张明同　　时间： 2024 年 10 月 28 日

使用授权声明

本人完全了解石河子大学有关保留、使用学位论文的规定，学校有权保留学位论文并向国家主管部门或指定机构送交论文的电子版和纸质版。有权将学位论文在学校图书馆保存并允许被查阅。有权自行或许可他人将学位论文编入有关数据库提供检索服务。有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

研究生签名：张明同　　时间： 2024 年 10 月 28 日

导师签名：周杰　　时间： 2024 年 10 月 28 日

摘要

近年来，随着信息技术的迅速发展，网络的应用为人们的生活带来了极大的便利。医疗机构为了方便群众，提供了各种就医途径，但同时也增加了网络安全威胁的风险，造成大量患者的隐私泄露，导致患者被诈骗或勒索、医疗机构的经济与名誉受损等问题。传统的以边界为基础的安全保护手段，已经很难对医疗机构网络安全进行有效的防护，因此医疗机构的网络安全态势评估与预测技术便成为医疗机构和学术界关注的重点。本文从医疗机构网络安全态势评估、态势预测以及系统实现三个方面对医疗机构网络安全防护进行研究，具体的研究内容包括：

（1）基于改进的小生境草原犬鼠算法优化深度信念网络（Improved Niche Prairie Dog Optimization Algorithm - Deep Belief Network, INPDO-DBN）的医疗机构网络安全态势评估：设计改进的 INPDO 算法，以解决 DBN 网络在训练过程中可能出现的局部极小值、早熟收敛等问题，并利用 UNSW-NB15 基准数据集与 ECU-IoHT、WUSTL-EHMS-2020 医疗物联网数据集对该模型进行二分类和多分类评估验证。实验结果表明，在二分类结果中，与传统的 BPNN、CNN 和 DBN 相比，INPDO-DBN 在三个数据集上的召回率相比其他三种模型最好的结果分别提高了 2.94%、1.94%、2.38%；在多分类的结果中，平均召回率分别提高了 6.99%、3.98%、6.03%，证明了 INPDO-DBN 对于提升医疗机构网络安全态势评估性能的有效性。

（2）基于混沌精英粒子群算法优化门控循环单元（Chaotic Elite Particle Swarm Optimization - Gate Recurrent Unit, CEPSO-GRU）的医疗机构网络安全态势预测：采用改进的 CEPSO 算法对 GRU 网络结构的参数进行优化，进一步提升 GRU 的性能。针对态势评估的数据利用滑动窗口法处理后进行了一系列对比实验，实验结果表明，所提出的 CEPSO-GRU 态势预测模型的平均绝对误差、平均绝对百分比误差、均方误差、均方根误差四种指标在三组数据集上相比于 RNN、LSTM、GRU 至少降低了 13.81%、26.57%、50.00%、19.03%；使用拟合优度进一步验证预测的效果，结果表明，拟合优度相比于其他三种模型分别至少提高了 2.92%、2.67%、3.17%，证明了 CEPSO-GRU 对于医疗机构网络安全态势预测的准确性。

（3）医疗机构网络安全态势评估与预测系统的设计与实现：系统的后端采用了 Flask 框架，并使用 MySQL 数据库存储数据；前端采用 Vue.js 进行开发，在构建前端组件时融入了开源的 Echarts 可视化库，以图表形式清晰展示网络安全态势评估与态势预测的数据。经过充分测试，该系统各功能模块相互协作，能够准确地对上传的网络攻击数据进行分类检测，同时对网络态势进行相应的评估和预测。系统能够为医疗机构的网络安全防护提供重要的基础保障，具有一定的应用价值。

关键词：态势评估；态势预测；群智能优化算法；神经网络；医疗机构

Abstract

In recent years, with the rapid development of information technology, various network applications have brought great convenience to people's lives. Medical institutions have provided various ways of accessing medical care for the convenience of the public, but at the same time, they have also increased the risk of network security threats, resulting in the leakage of privacy of a large number of patients, leading to fraud or extortion of patients, and damage to the economic and reputational damage to the medical institutions and other issues. The traditional boundary-based security protection means has been difficult to effectively protect the network security of healthcare organizations, so the network security situation assessment and prediction technologies for medical organizations has become the focus of attention of healthcare organizations and academia. In this thesis, the network security protection of medical organizations is studied from three aspects: network security situation assessment, situation prediction, and system implementation. The specific research content includes:

(1) Network security situation assessment for medical organizations based on Improved Niche Prairie Dog Optimization Algorithm - Deep Belief Network (INPDO-DBN): The improved INPDO algorithm is designed to solve the DBN network's possible problems of local minima and premature convergence during the training process. Furthermore, evaluate and validate the model with binary classification and multi classification using the UNSW-NB15 benchmark dataset with the ECU-IoHT and WUSTL-EHMS-2020 medical IoT datasets. The experimental results show that in the binary classification results, the recall of INPDO-DBN on the three datasets is improved by 2.94%, 1.94%, and 2.38% compared to the best results of the other three models which are the traditional BPNN, CNN, and DBN, respectively. And in the multi classification results, the average recall is improved by 6.99%, 3.98%, and 6.03%, respectively. It proves the effectiveness of INPDO-DBN for improving the performance of network security situation assessment in medical organizations.

(2) Network security situation prediction for medical organizations based on Chaotic Elite Particle Swarm Optimization - Gate Recurrent Unit (CEPSO-GRU): The parameters of GRU network structure are optimized using the improved CEPSO algorithm to further enhance the performance of GRU. A series of comparative experiments is conducted on the data processed for the situational assessment using the sliding window approach, and the experimental results show that the proposed CEPSO-GRU situational prediction model reduces the average absolute error, the average absolute percentage error, the mean squared error, and the root mean squared error by at least 13.81%, 26.57%, 50.00%, 19.03%, respectively, in comparison to the RNN, the LSTM, and the GRU in the three datasets. And the effectiveness of the prediction is further

verified using the goodness-of-fit, which shows that the goodness-of-fit is improved by at least 2.92%, 2.67%, and 3.17% compared to the other three models, respectively. It proves the accuracy of CEPSO-GRU for the prediction of the network security situation of medical organizations.

(3) Design and implementation of network security situation assessment and prediction system for medical institutions: the back-end of the system adopts the Flask framework and uses a MySQL database to store the data; the front-end is developed using Vue.js, and the open-source Echarts visualization library is integrated into the construction of the front-end components, which clearly displays the data for network security situation assessment and situation prediction in the form of charts. After full testing, the system's functional modules collaborate with each other to accurately categorize and detect uploaded cyberattack data, as well as assess and predict the network security situation accordingly. The system is able to provide an important basic guarantee for the network security protection of medical organizations and has certain application value.

Key words: Situation assessment; Situation prediction; Swarm intelligence optimization algorithm; Neural networks; Medical Institutions

目录

第 1 章 绪论

本章将对医疗机构网络安全评估与预测的研究工作进行背景调研及研究意义的分析，在此基础上对国内外当前相关领域的研究现状进行总结归纳，提出本文的研究内容，最后对论文整体组织结构进行规划。

1.1 研究背景及意义

医疗行业作为关乎人们生命健康的重要领域，其信息系统的安全性直接关系到患者信息的保护和医疗服务的质量。信息技术的迅猛发展使得医疗服务与信息技术深度融合，为人们提供了便捷的智慧就医体验，如小程序挂号、线上问诊。然而，这一趋势也伴随着网络安全问题的不断增加，与此相关的信息安全管理变得尤为关键。由于医疗行业关乎民生，且涉及数据隐私性较强，具备重要的财富价值，因此针对患者个人信息、疾病诊疗隐私信息，以及医疗机构诊疗过程和费用信息等的网络安全攻击、数据窃取及更改、医疗机构勒索事件逐年增多。这些事件对医疗机构的管理造成严重影响，同时也会损害医疗机构和患者个人的合法权益[1]。

全球范围内的医疗机构正面临着日益严峻的网络攻击威胁。特别是随着网络攻击成本的降低和攻击方式的不断进步，大量重大的网络安全事件层出不穷。根据 GoUpSec 对国内外网络安全攻击事件的统计分析，2023 年全球遭受网络攻击的主要垂直行业中医疗行业排在第二名[2]。例如美国路易斯安那州医院遭勒索攻击，27 万名患者信息泄露；开源电子病历 OpenEMR 曝出严重漏洞，影响全球 10 万医疗机构；外包服务商被黑致使英国部分地区救护车系统瘫痪等等事件。2023 年 11 月国际数据公司 IDC 发布的《中国医疗行业网络安全市场洞察》总结了当前中国医疗行业在网络安全领域的建设情况及特征。相关攻击案例如 2022 年北京市朝阳区人民检察院裁定刘某等三人通过技术手段秘密接入数据库获取敏感数据后进行非法交易，导致了患者身份信息泄露等问题。2020 年，胶州市民的微信群里曝光了中心医院出入人员名单信息，引发了不良社会影响[3]。

近年来的案例以及研究报告均突显了医疗机构在网络安全方面存在的漏洞和风险，说明了治理医疗机构网络安全的紧迫性。医疗机构网络环境具有一定的隐私性及敏感性，患者可能会因医疗数据被修改导致错误诊断及错误的治疗，对患者生命安全造成伤害。这些事件不仅对患者的信息安全和身体健康造成了直接威胁，也对医疗机构本身构成严重威胁，甚至关系到国家安全[4]。这表明医疗机构需要不断关注和改进其网络安全防护措施，以确保患者数据的安全和医疗服务的持续稳定，保障国家安全。

为应对这一威胁，各国纷纷采取法律法规等手段对医疗行业网络安全进行规范。美国参议员提出了《2022 年医疗网络安全法案》，以提升医疗保健和公共卫生部门的网络安全，保护个人健康医疗数据隐私[5]。欧盟 2018 年实施的《通用数据保护条例》[6]也对医疗数据的处理和存储提出了更为详细的要求，以确保患者信息的隐私和安全。我国的《中华人民共和国基本医疗卫生与健康促进法》[7]等法律法规明确了医疗机构网络安全的基本要求和重要任务。2022 年 8 月，《医疗卫生机构网络安全管理办法》[8]的发布标志着卫健委首次出台了具体的医疗网络安全管理法规，将医疗卫生网络安全建设提升到一个新的高度。国家对医疗系统网络安全问题的高度关切和规范化管理有望提高医疗机构在网络安全领域的应对能力，保障患者和公众的利益。

医疗机构频繁受到网络攻击影响正常业务，各国纷纷制定网络安全法规，但仅靠法律约束存在不足，传统的安全保护手段，已经很难对医疗机构网络安全进行有效的防护，因此医疗机构的网络安全态势感知便成为医疗机构和学术界关注的重点。当前迫切需要在网络安全技术方面加强威胁检测和防御能力，构建科学、先进的网络安全态势感知平台[9]。网络安全态势感知（Network Security Situation Awareness，NSSA）被认为是一项重要工作，通过建立 NSSA 平台，可以在网络攻击发生前发现威胁，降低攻击成功率，从而在网络安全方面防范于未然。

鉴于此，综合分析医疗机构网络安全威胁和安全态势演变，以研究网络安全态势评估与预测模型为核心，建立网络安全态势感知系统，可以提升医疗机构的网络安全防范能力，早期发现潜在威胁，有效防止黑客组织利用互联网技术漏洞损坏医疗科研数据资源，同时依法保障互联网医疗患者信息的安全权益。这一综合措施有助于防护病人隐私，减少因隐私泄露造成的财产损失、诈骗、影响治疗等风险，降低网络安全攻击对医疗机构造成的经济、名誉、医疗技术的损失，对加强网络监控、应急响应，并在网络安全的发展趋势预测方面具有重要意义，是有效防护医疗机构网络安全的重要前提，能够确保医疗机构系统安全稳定地运行，网络安全水平的可持续提升。这不仅可以保障医疗机构的正常运作，也能为网络安全的发展做出积极的贡献。

1.2 国内外研究现状

本节将从医疗机构网络安全及网络安全态势感知两个方面对研究现状进行调研及分析，为之后开展态势评估与预测技术在医疗机构网络安全中的应用研究打下坚固基础。

1.2.1 医疗机构网络安全研究

国外对医疗机构网络安全方面的研究起步较早，积累了丰富的研究成果。计算机安全专家为提高网络防御水平提出了多种防御措施，涵盖了多个研究方向。

在网络安全威胁与防御策略方向，包括了对医疗机构面临的网络安全威胁的研究，以及提出的防御措施。Bhuyan 等人[10]研究了医疗保健组织面临的网络安全威胁类型，并分析了网络攻击者、防御者、开发人员和用户的角色，为政策制定者和医疗保健组织提供了加强网络安全的建议。Wyant 等人[11]提出了一个综合框架（DeTER），用于查看、理解和应对移动医疗保健中的网络安全问题，为系统开发生命周期中的决策提供了指导，并通过涉及 COVID-19 接触者追踪移动健康应用程序的案例研究展示了其应用。

在安全架构与身份验证技术方向，主要的研究成果有 Karmakar 等人[12]提出了一种安全架构与 OpenMANO 等未来网络框架兼容，通过虚拟网络功能（VNF）和加密通信协议，确保了只有经过身份验证的 IoMT 设备才能接入网络，强化了医疗保健网络基础设施的安全性和隐私保护。Yu 和 Park[13]提出了一种融合区块链技术和物理不可克隆功能（PUF）的身份验证协议，通过 AVISPA 模拟和 ROR 预言机模型进行的安全分析，实验验证了该协议能有效抵御中间人攻击等安全威胁，保障安全性的同时提高效率，为 WMSN 的医疗应用提供了一种可靠的解决方案。

在通信安全与性能优化方向，Chaganti 等人[14]提出了结合粒子群优化算法和深度神经网络的入侵检测系统（IDS），该系统利用网络流量和患者传感数据集，以 96%的高准确率有效识别潜在的网络入侵行为，有助于更有效地保护医疗物联网（IoMT）网络和医疗数据安全。Sönmez 等人[15]展示了医疗成本优化系统，并通过两种 IT 设置配置的案例研究说明了处理决策参数复杂性的方法。这些研究涵盖了医疗机构网络安全的多个关键领域，为医疗机构在面对网络安全挑战时提供了一系列的解决方案和策略。

在医疗机构网络安全技术研究领域，国内也有诸多研究者做出了重要贡献，特别是具有更多关于态势感知的最新研究。Zeng 等人[16]提出的自组织网络链路安全态势识别方法通过建立情境识别模型实现准确识别，但其在大型医疗单位内部网络的适用性仍需进一步验证。莫禹钧等人[17]从安全感知系统等 4 方面阐述基于网络安全态势感知的主动防御系统设计以及具体实现，极大提高了响应威胁的时效性和精准度。蒋科[18]基于数据挖掘算法提出了一种医疗网络安全风险评估方法，通过构建评估指标体系和模型，实验验证表明该方法能够实现高精度的风险评估，结果有效可信。石汤沐[19]结合了医院网络安全态势感知平台的构建和功能应用进行介绍，可为相关的医院提供参考和借鉴。王维[20]根据等保 2.0 要求，设计了一种医疗安全态势感应机制，通过智能学习创建了一种信息安全胁迫剖析模型，帮助医院随时掌控安全险度及态势。

同时，国内学者在提升医疗机构网络防御能力的技术和系统开发方面也做出了许多创新。卢熙[21]在其论文中介绍了新型医院网络安全防御技术，如深度包过滤、免疫网络和态势感知技术，这些技术有望提升医院网络的安全性。赵欣和郭建伟[22]建议医保机构采用快速、可信的数字签名和加密技术，以确保患者信息的可信性和完整性，同时防止医疗机构作假和提供虚假信息骗保。杨霞等人[23]探讨了基于蜜罐的防御技术，为医疗机

构网络安全提供了有益的思路。王伟昊[24]在医院网络安全系统建设中，应用了态势感知、日志管理和入侵监控技术，对威胁来源和系统安全性进行监控分析，实验测试的结果表明显著提升了入侵检测准确率和网络安全性。这些技术的应用和集成有助于构建更为坚固和可靠的医疗网络安全防线。

综上所述，国内外学者对于医疗机构网络安全领域做出了多种方向的研究，同时也取得了许多成果。在态势感知技术和防御系统构建方面的研究中，当前的研究可以有效地提高医疗机构网络的安全性，也为未来研究和实践提供了宝贵的经验和参考。然而，现有的研究往往局限于传统的网络安全技术。相比之下，态势感知作为一种新兴的网络安全防御技术，具有强大的潜力，能够通过动态分析医疗机构网络风险，以全局的视角提供全面保障，为医疗机构网络安全注入新的活力。因此，本文关注态势感知技术的应用，旨在于推动医疗机构的网络安全提升的有效性。

1.2.2 网络安全态势感知研究

网络安全态势评估与预测的概念来源于网络安全态势感知，该技术最初源自军事领域用于实时监测和分析战场环境，提高决策效果情景感知。随着互联网发展，该概念在网络安全领域推广。网络安全态势感知技术借鉴军事理念，实时监测和全面分析网络环境，及时识别和应对潜在威胁。

美国军事专家 Endsley 在 1998 年首次将安全态势分为安全事件提取、态势理解和态势预测三个部分[25]。然而，其模型主要关注航空安全，在网络领域尚未成熟。在此基础上，美国国防部提出了新的四级的 Joint Director of Laboratories 模型[26]，成为信息融合的标准。后 Bass[27]强调网络管理和入侵检测系统需统一协作，通过数据融合实现明智决策，并提出了入侵检测数据融合框架。发展到当前网络安全态势感知的研究方向主要集中在态势要素提取、态势评估、态势预测三个方面。

在态势要素提取方面，美国国家高级安全系统研究中心推出的安全事件融合系统则结合网络安全数据和人类认知能力，实现了网络安全状况的可视化，增强了安全事件的感知和理解[28]。Ghanem 和 Jantan[29]通过结合人工蜂群算法与蝶王优化算法，对神经网络进行训练提升了要素提取模型的精度。Mohan 等人[30]利用混合 Soergel 和 Lorentzian 方法从大量数据中提取出对入侵警报预测最为关键的特征进行特征筛选，随后送入深度最大网络（DMN）模型中，经过优化的模型性能出色。以上的研究工作表明，人工智能和机器学习技术可以有效地提取和分析网络数据，在态势要素提取领域不断发展和完善，从而提高对网络安全威胁的感知能力和响应速度。

NSSA 周期中，评估和预测是极为重要的阶段，因此更多的学者们对这两阶段开展了深入研究。在态势评估方面，国外的研究较早且成果颇丰。Skopik 等人[31]构建了一个

由关键事件指标组成的模型，并设计了高效的事件数据聚类算法，以实现对大型网络空间的态势感知评估。Wen 等人[32]建立了基于 LSTM 的典型时间序列网络安全态势评估模型。通过大数据深度学习算法，自动挖掘分析网络安全态势的隐性关系和变化趋势，大大提高了安全态势的评估精度。Devarakonda 等人[33]提出了一种简单而有效的数据预处理方法，并比较了四种 AI 方法来训练两个基准数据集，实验验证得到随机森林分类器的结果最为一致和准确。Chen 等人[34]提出了一种基于隐马尔可夫模型、PageRank 算法和 D-S 证据理论的网络安全态势整体评估模型，对不同融合阶段采用不同融合算法后的整体态势进行评估，比使用单一模型的方法更加准确和高效。这些深度学习和智能数据处理等技术的使用不仅提高了分类评估模型的性能，还有助于从复杂的网络数据中提取有价值的洞察。

网络安全态势预测领域发展较晚且研究方法和方向较为分散。常用预测方法如神经网络、时间序列分析法和 D-S 证据理论等。Kholidy 等人[35]提出了使用自适应风险方法的隐马尔可夫模型进行多阶段攻击预测，并在 DARPA 2000 数据集上验证了其有效性。此研究为网络安全态势预测提供了新的潜力方案，特别是在多阶段攻击的防范中有所成果。Sokol 等人[36]分析了时间序列的选择标准和适用性，比较了选定的统计模型，结果表明神经网络方法被证明是 NSSA 预测中比经典统计预测模型更准确的替代方案。Zhao 等人[37]融合自适应变异的跨层粒子群算法与传统的 D-S 证据理论，对当前网络安全态势进行评估，根据优化后的评估结果预测下一阶段的网络安全态势，提高了态势评估和预测的准确性。尽管网络安全态势预测领域的研究相对较新，但已经取得了显著的进展，先进的机器学习技术正在成为预测网络安全事件的有力工具。

国外在网络安全态势感知领域的研究起步较早，积累了丰富经验，形成了较为成熟的模型框架，每种模型框架都提供了独特的方法，以在不断变化的网络安全环境中提高态势感知的准确性和效率。同时，这也为国内研究者提供了宝贵的研究经验，有助于加速国内相关领域的发展。

在态势要素提取阶段，研究主要集中于运用机器学习等方法从复杂的网络数据中提取有价值的信息。王昕和孙磊[38]通过结合受限玻尔兹曼机和随机森林算法，提高了网络态势要素提取的精度，尤其在处理大规模网络数据方面。胡莹莹[39]开发了融合注意力机制、长短时记忆网络和卷积神经网络的方法，深入分析网络流量数据的特征，进行概率建模。张然等人[40]利用主成分分析法降维数据，去除冗余的态势要素，然后采用小波神经网络分类训练约简后的数据集。这些研究都为网络流量分析和异常检测提供了新的技术方案，有助于对潜在的安全威胁进行有效的预测和防范。

在态势评估的阶段，大量的研究为网络安全态势评估提供了多样化且有效的方法。Yang 等人[41]提出利用 DAE 进行特征学习，并将 DNN 作为网络攻击分类器，通过改变训练权重构建对抗性训练过程的网络安全态势评估方法。栗堃[42]提出了基于引力搜索算

法优化 SVM 参数的网络安全态势评估模型。龚嘉瑶和王钟庄[43]通过整合威胁子态势、脆弱性子态势以及基础运行子态势这三个维度来搭建了一个指标框架。在此基础上，运用了卷积神经网络算法，设计出了一个用于网络安全状况评估的模型。这些研究都在一定程度上提高了态势评估的准确性，特别是深度学习算法，如自编码器、深度神经网络和卷积神经网络，正在成为这一领域的重要工具。这些方法能够处理大量复杂的数据，并从中提取有用的信息以评估网络的安全状态。

在态势预测阶段的研究中，研究者们采用了多种方法，利用先进的机器学习技术提高对未来网络安全态势的预测能力。何梦乙[44]采用长短期记忆网络（LSTM）解决态势预测问题，并利用遗传算法优化 LSTM 的网络结构参数。彭兴维和袁凌云[45]提出了融合双向门控循环单元、多头注意力机制和残差结构的预测模型，经由自适应差分进化算法调优，可以更好地捕捉数据的复杂依赖关系，并进行多角度的数据分析。王可阳[46]采用双向 LSTM 网络安全预测模型，并结合了贝叶斯优化技术来确定模型的超参数进一步提升模型的性能。熊英等人[47]通过改进了 Elman 神经网络的激活函数、结构、参数三方面，建立了预测效果较好的预测模型。这些研究不仅展示了机器学习在网络安全态势预测中的应用，而且还强调了优化算法在提升模型性能方面的重要作用，为网络安全态势预测提供了有效的方法和思路。通过结合不同的机器学习架构和优化技术，能够构建出更精确、更高效的预测模型。

综上所述，尽管国内外研究者们已经做出了许多研究关于医疗机构网络安全态势感知的经典思路，仍然存在一定的局限性。例如，医疗机构对于网络安全较多的研究仍局限于传统防御技术；态势感知方面的大部分研究通常仅使用单一模型，较少融合群智能优化算法，而现代网络中对于数据信息的提取、态势评估与预测的工作量与复杂性上不断地提升，这使得原有的研究方法并不能很好地解决现有的行业问题，评估及预测的准确性不能得到保证。未来医疗机构网络安全的研究需要特别注重技术创新尤其是态势感知能力的提升，以更为有效地对抗不断演变的网络安全威胁。在这个过程中，必须综合考虑网络安全的态势评估、预测等关键因素，提升评估与预测的准确性，以确保医疗机构网络安全体系的全面健康发展，这也是本文研究聚焦的重点。

1.3 研究内容

对当前医疗机构网络安全及态势感知的研究现状进行归纳分析后，本文按照如图 1-1 所示的技术路线图，以群智能优化算法及神经网络模型为基础对医疗机构网络安全态势评估与预测技术进行研究，并实现相应的系统。具体研究内容如下：

（1）构建医疗机构网络安全态势评估指标及模型。参考现有研究与《信息安全技术-信息安全风险评估方法》[48]，选取重要要素构建指标，并设计公式量化态势指标。