 DOI: https://doi.org/10.12345/bdai.v5i6.18989

Analysis of the Current Status of Patent for Artificial Intelligence in Network Security Protection

Xiaoyi Xiao

Patent Examination Cooperation Sichuan Center of the Patent Office, Chengdu, Sichuan, 610213, China

Abstract

With the rapid development of information technology, the forms of cyber attacks have changed, making network security problems increasingly prominent. Artificial intelligence can better respond to threats by continuously learning from large amounts of data and making predictions and judgments. Applying artificial intelligence to network security protection is currently a hot research topic. This paper analyzes the application of artificial intelligence in network security protection from the perspective of patents. Based on the patent data retrieved, it analyzes the situation from multiple dimensions such as the overall situation of patents, the ranking of applicants, and the distribution of technologies, and provides corresponding suggestions based on the results to provide reference for innovative entities in related fields.

Keywords

AI; machine learning; network security; network attacks; patent analysis

人工智能应用于网络安全防护专利现状分析

肖小义

国家知识产权局专利局专利审查协作四川中心，中国·四川 成都 610213

摘　要

随着信息技术的快速发展，网络攻击形式不断变化，网络安全问题日益凸显。人工智能通过不断对大量数据的学习作出预测和判断，能更好地应对威胁，将人工智能应用于网络安全防护是目前研究的热点。论文从专利的视角对人工智能在网络安全防护中的应用进行分析，基于检索到的专利数据，分别从专利整体情况、申请人排名、技术分布等方面多维度分析，基于结果提供相应建议，为相关领域创新主体提供参考。

关键词

人工智能；机器学习；网络安全；网络攻击；专利分析

1 引言

近年来，互联网不断普及，计算机网络已经成为人们工作和生活中不可或缺的一部分。然而，随着网络技术的高速发展，网络安全问题也愈加严峻。人工智能技术是近年来的研究热点，其具备强大的数据处理能力、自我学习能力和预测能力 [1]，其对于目前层出不穷的新的网络安全问题能动态提供相应的防御策略。基于人工智能，可以实现高效的网络防御工具，用以识别恶意软件攻击、网络入侵、网络钓鱼和垃圾邮件、数据泄露等 [2]。专利地图通过对检索到的大量专利文献中的著录项目和技术方案进行分析，对相关信息进行提取、筛选、整理、归纳得到专利信息，并利用可视化图表来描述专利信息 [3]，论文利用专利地图从专利的视角分析人工智能应用于网络安全防护的专利现状。

【作者简介】肖小义（1990–），男，中国四川资阳人，硕士，助理研究员，从事网络通信、无线通信研究。

2 数据来源

论文数据来源于商业数据库 incoPat 全球专利综合文献数据库，该数据库对常用国家的专利数据进行特殊收录和加工处理，并提供相应的翻译文本，数据信息完善，便于阅读和检索。论文在 incoPat 数据库中通过分类号和关键词对人工智能网络安全领域的专利进行检索，获得专利 8842 件，检索时间为 2024 年 6 月 27 日。为确保数据准确有效，对检索的数据通过分类号进行初步去噪，然后通过人工筛选的方式进一步清洗，合并同族后最终获得有效专利 5829 项，论文以该数据为研究对象进行分析。

3 专利整体情况分析

3.1 申请趋势分析

首先对人工智能网络安全历年的申请量进行分析，由于从 2005 年开始，中国才有该领域的专利申请，在此之前，其他国家相关专利也仅为个位数，因此这里仅展示 2005—2024 年全球及中国的专利申请情况，如图 1 所示。从图 1

中可以看出，人工智能网络安全的发展可以分为三个时期，2005—2012 年属于技术萌芽期，每年有少量专利申请，2012—2018 年属于缓慢增长期，每年专利申请数量逐渐增加，2018 至今属于迅速增长期，每年专利申请数量呈爆发式增长。2024 年专利申请数量降低是由于检索时全年仅过一半，并且部分专利没有公开的原因，现在仍然处于快速增长期。另外，虽然中国比国外起步相对较晚，但是发展速度明显比国外更快，从 2019 年开始，中国申请量就超过全球申请量的一半，到 2023 年已经占到了全球申请量的近 70%，并且该占比还在逐年增加。可见中国在人工智能网络安全领域发展迅速，占据全球大部分比重。

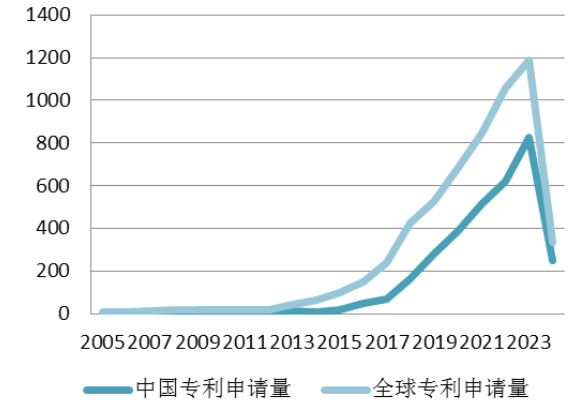

图 1 人工智能网络安全申请趋势

3.2 区域布局分析

在区域布局分布中主要分析全球地域排名，可以展示人工智能网络安全在各个国家或地区的专利数量分布情况，通过该分析可以了解人工智能网络安全在不同地区技术创新的活跃程度，以及主要的技术创新来源和市场。各国人工智能网络安全专利分布情况如图 2 所示。从图中可以看出，在中国公开的专利申请数量遥遥领先，达到了 3236 件，是第二名美国公开专利的两倍有余，是第三名印度的近六倍，可见人工智能网络安全技术在中国十分活跃。作为人工智能起源国的美国也具有较多的专利，达到了 1285 件。人工智能的本质是计算机程序，因此历来的软件强国印度在这方面也有相当一部分专利，达到 541 件。此外，韩国、欧专局也有一定数量的专利，而其他国家的专利数量较少。

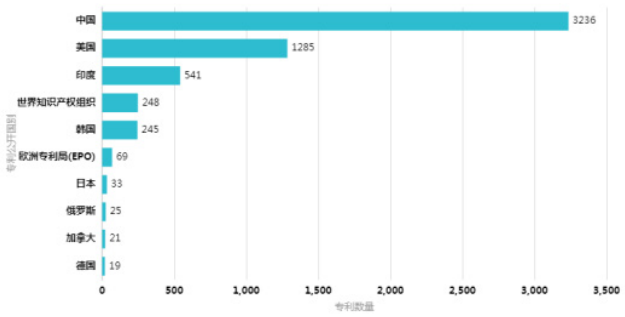

图 2 各国人工智能网络安全专利分布情况

4 申请人分析

4.1 申请人排名分析

论文统计了申请量排名前十的申请人，具体如图 3 所示。从图中可以看出，在排名前十的申请人中国占了 6 席，国外占 4 席，其中分别排名第一、第二的 CHITKARA UNIVERSITY 和 BLUEST METTLE SOLUTIONS PRIVATE LIMITED 为印度企业，排名第三的 CISCO TECHNOLOGY INC 和第七的 CYLANCE INC 是美国企业。排名前三的申请人属于第一梯队，申请量明显比其他申请人高出一截，其余申请人数量相差不大。结合图 2 可以得出，中国虽然申请总量较大，但是各申请主体相差不大，没有申请人跻身第一梯队，缺乏超大龙头企业。另外，在中国六席中有 5 个都是高校，说明高校是该领域的主力，在这方面投入了较多研究。

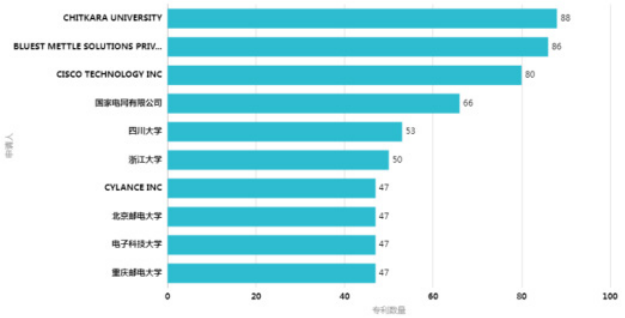

图 3 人工智能网络安全专利申请排名前十

4.2 申请人类型分析

论文还特意统计了人工智能网络安全领域中国专利申请的申请人类型，申请人类型占比如图 4 所示。从图中可以看出，高校和企业是该领域的主要创新主体，从申请数量上统计，高校占比超过一半，企业占比 46.76%，而其他剩余类型占比总和仅为 9.28%，需要注意的是，由于一件申请可能涉及多个申请人，也就可能对应多个申请人类型，因此各类型占比总和可能超过 100%，论文第 5 节技术分布也会出现类似情况。高校占比较高说明该领域偏向于基础研究，可能是因为人工智能主要是通过计算机来实现一些复杂的训练算法，理论性较强，并且成本较低，主要是计算设备成本，而这些方面都是高校的优势，方便开展科学研究。

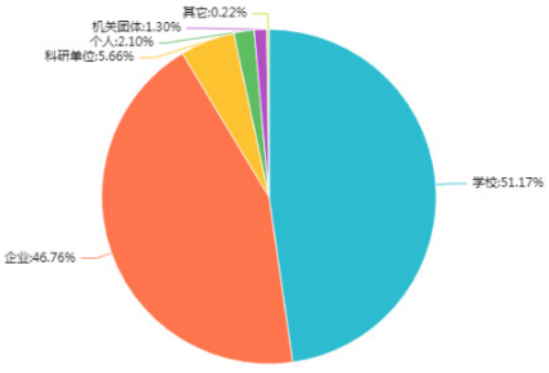

图 4 人工智能网络安全中国专利申请人类型

5 技术分析

5.1 技术分布分析

分析人工智能网络安全领域专利在各技术方向的分布情况，可以了解该领域涉及的技术类别和各技术分支的创新热度。由于小类分类不够精细，此处选择大组分类研究人工智能网络安全领域的专利技术分布情况，具体如图 5 所示。

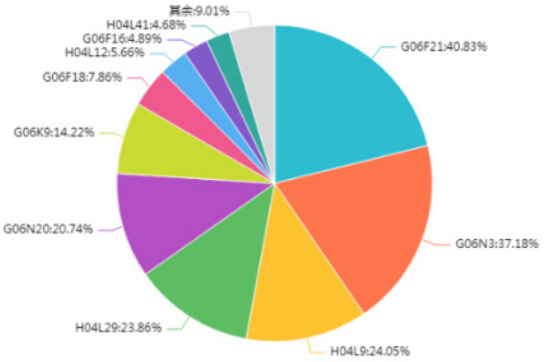

图 5 人工智能网络安全专利技术分布情况

从图中可以看出，分布最多的是 G06F21（防止未授权行为的保护计算机、其部件、程序或数据的安全装置），该领域的专利占到了所有专利的 40.83%，该领域涉及网络安全，正好是我们研究的重点。其次是 G06N3（基于生物模型的计算安排），占到了 37.18%，基于生物模型的计算安排实际就是通过计算机模型来模拟人的思维，本质就是人工智能。此外，人工智能网络安全技术占比较多的还分布在 H04L9（保密或安全通信装置；网络安全协议）、H04L29（H04L1/00 至 H04L27/00 单个组中不包含的装置、设备、电路和系统）、G06N20（机器学习）、G06K9（识别模式的方法或装置），分别占比 24.05%、23.86%、20.74%、14.22%。

5.2 重点代表专利分析

专利被引用次数越多、同族数量越多，代表该专利越可能是核心重点专利，此外 icoPat 提供的合享价值度也能作为是否为重点专利的参考，论文综合考虑这些因素选出了部分重点专利，对其专利技术进行分析。

Sourcefire 的专利（US20120210423A1）公开了一种通过上下文信息、类属签名和机器学习技术检测恶意软件的方法和装置，具体包括从软件应用中提取特征向量；提取关于所述应用的元数据，并收集关于所述应用所安装在系统的上下文信息；计算应用程序的通用指纹；将根据上述结果而获得的数据相关的信息发送到服务器应用程序；至少部分地基于上述发送的信息，从所述服务器应用程序接收关于应用程序是良性还是恶意的信息；以及基于从服务器组件接收的信息对应用程序采取动作。该技术能减少人工分析的工作量和系统中的误报风险， 使得能够通过使用自动化的手段来实现。微软的专利（US20120158626A1）公开了一种恶意 URL 的检测和分类方法，该方法公开了使用从 URL 提取的特征来检测恶意 URL 并将恶意 URL 分类为网络钓鱼 URL、垃圾邮件 URL、恶意软件 URL 或多类型攻击 URL 之一的技术。 所述技术使用一个或多个机器学习算法来使用一组训练数据来训练分类模型，所述训练数据包括已知的良性 URL 组和已知的恶意 URL 组。 然后使用分类模型来检测和 / 或分类恶意 URL。

国家电网的专利（CN107196910A）公开了一种基于大数据分析的威胁预警监测系统、方法及部署架构，包括，数据采集系统模块，对原始网络流量进行实时数据采集；数据存储系统模块，对数据采集系统模块采集的数据进行数据归并和数据清洗处理后再进行存储管理；实时威胁智能分析系统模块，利用数据挖掘、文本分析、流量分析、全文搜索引擎、实时处理对安全数据进行深度的分析与挖掘，结合入侵检测模型、网络异常行为模型和设备异常行为模型实时甄别未知的安全威胁；态势感知展示系统模块，采用了数据可视化工具库实时、立体地对安全威胁态势进行综合展示。用于多种业务场景下的网络安全威胁态势感知和深度分析，实现从攻击预警、攻击识别到分析取证的综合能力。中国电子科技集团公司第五十四研究所的专利（CN104935600A）公开了一种基于深度学习的移动自组织网络入侵检测方法与设备。包括数据采集模块、数据融合模块、预处理模块、存储模块、入侵检测模块和响应告警模块，将捕获到的无线数据包进行融合和去冗余后，提取网络行为特征并存储；深度学习网络行为特征后建立表达网络行为的深度神经网络模型；将待检测的网络数据输入深度神经网络模型，完成对入侵的判断和识别后响应告警。

6 结语

论文从专利的视角分析人工智能应用于网络安全防护的专利现状，从以上分析可以看出，中国在人工智能安全领域专利申请量占据较大优势，但没有形成超大龙头企业，和国外企业还有一定差距，并且目前主要在高校开展研究，专利储备量较大的企业较少。对此提出如下建议：一是政府要进一步加强政策引导，培育壮大一批人工智能网络安全领域的世界领头企业，加强建圈强链，形成全链条产业；二是要抓住目前行业快速增长期的发展机遇，加强海外专利布局，为进入国外市场打好基础；三是加强产学研结合，提高专利转化运用，将高校专利成果向市场推广。

参考文献

[1] 皮珣珣,吴立胜.基于人工智能技术的网络安全防御系统设计[J].无线互联科技,2023,20(18):25-27.

[2] 王跃强,张磊,陈鑫磊,等.人工智能技术在网络安全防御中的应用研究[J].网络安全技术与应用,2024(6):26-29.

[3] 蒋玉石,康宇航.基于专利地图的技术创新可视化研究[J].科研管理,2013,34(10):50-57.