探讨大数据和人工智能在数据安全保障方面的新思路

刘博升
天津市静海区网格化管理中心　天津　301600

摘　要：本文聚焦大数据与人工智能在数据安全保障领域的新思路。剖析了传统数据安全防护在静态防御及隐私与效用平衡方面的局限性，进而提出大数据与AI融合的新框架，阐述其设计原则与核心模块。随后从内部威胁发现、威胁狩猎与溯源等多个维度，详细论述基于AI与大数据的安全保障创新思路，旨在为大数据时代的数据安全提供更可靠、高效的解决方案。

关键词：数据安全；大数据分析；人工智能

引言：在大数据与人工智能蓬勃发展的当下，数据成为关键生产要素，数据安全的重要性愈发凸显。传统数据安全防护模式，如静态防御，面对复杂多变的网络环境和新型攻击手段时，显得力不从心；在隐私与效用的平衡上也陷入两难困境。为有效应对这些挑战，探索大数据和人工智能在数据安全保障方面的新思路迫在眉睫，这成为推动数据安全领域发展的关键所在。

1 传统数据安全防护的局限性分析

1.1 静态防御的脆弱性

传统数据安全防护以静态防御为主，核心依赖防火墙、入侵检测系统、杀毒软件等固定安全设备，遵循“被动防御、事后补救”的模式，难以适配当前复杂多变的网络环境和攻击手段。这类防护方式本质上是基于已知威胁特征构建防御规则，对未知漏洞、零日攻击等新型威胁缺乏有效识别能力，一旦攻击手段超出预设规则范围，防御系统便会形同虚设。同时，静态防御多采用“一刀切”的防护策略，未结合数据重要性、业务场景进行差异化防护，既无法对核心敏感数据实施重点保护，也可能因过度防护影响业务正常运行[1]。另外，静态防御体系缺乏动态适配能力，无法随着数据量增长、业务模式迭代实时调整防护策略，面对大数据时代海量数据的高速传输与交互，防御响应滞后、防护效率低下的问题尤为突出，难以抵御持续性、针对性的高级威胁攻击，整体防护体系脆弱性显著。

1.2 隐私与效用的平衡难题

传统数据安全防护在隐私保护与数据效用之间难以实现有效平衡，往往陷入“重隐私、轻效用”或“重效用、轻隐私”的极端。一方面，为保障数据隐私安全，传统防护多采用严格的加密、隔离手段，将敏感数据完全封闭，导致数据无法被有效共享、分析和利用，限制了数据价值的发挥，与大数据时代“数据作为生产要素”的核心需求相悖；另一方面，部分场景下为追求数据效用，过度开放数据访问权限，简化安全防护流程，导致用户隐私信息、企业核心数据被非法获取、滥用，引发隐私泄露风险。此外，传统隐私保护技术缺乏灵活性，无法根据数据敏感等级、使用场景动态调整防护强度，对于半结构化、非结构化数据的隐私保护能力不足，既难以满足隐私合规要求，也无法充分释放数据价值，形成隐私保护与数据效用相互制约的困境，成为传统数据安全防护的重要局限。

2 大数据与 AI 融合的数据安全新框架

2.1 框架设计原则

大数据与AI融合的数据安全新框架，需遵循“动态适配、全面管控、隐私优先、价值协同”四大核心设计原则，打破传统防护的局限性，实现安全与效用的双重提升。动态适配原则要求框架能够实时感知数据量、业务模式、攻击手段的变化，通过AI算法自动调整防护策略，实现从静态防御向动态防御的转型；全面管控原则聚焦数据全生命周期，覆盖数据产生、采集、传输、存储、使用、销毁各环节，构建连贯、闭环的安全管控体系，消除碎片化防护漏洞。隐私优先原则以隐私合规为前提，将隐私保护嵌入框架各模块，通过隐私计算、智能加密等技术，在保障数据隐私安全的基础上，实现数据合规共享与利用；价值协同原则兼顾安全防护与数据效用，避免过度防护对数据价值释放的限制，通过AI与大数据的深度融合，让安全防护服务于数据价值挖掘，实现“安全护航价值、价值反哺安全”的良性循环，为大数据应用提供可靠的安全保障。

2.2 核心模块构成

2.2.1 大数据感知层

大数据感知层是新框架的基础支撑模块，核心功能是实现对全场景数据的全面采集、实时监测与精准识

别，为后续安全决策提供数据支撑。该层依托大数据技术，构建多源数据采集体系，覆盖网络流量、终端行为、数据流转、应用日志等各类数据，实现结构化、半结构化、非结构化数据的统一采集与汇聚。通过AI算法对采集的数据进行实时清洗、分类与分析，精准识别数据敏感等级、异常行为特征、潜在安全隐患，建立动态更新的数据安全态势画像。感知层具备实时告警能力，当检测到数据异常流转、非法访问、攻击行为等风险时，立即触发告警信号，推送至AI决策层，为快速响应提供及时支撑[2]。

2.2.2 AI决策层

AI决策层是新框架的核心大脑，负责基于大数据感知层提供的数据，通过AI算法实现安全风险的精准研判、决策制定与策略优化。该层集成了机器学习、深度学习、强化学习等多种AI技术，构建多维度安全决策模型，能够对感知层上报的异常数据、攻击行为进行深度分析，精准判断威胁类型、攻击来源、影响范围及危害程度，区分虚假告警与真实威胁，避免无效响应。同时，AI决策层具备自学习、自优化能力，能够通过持续学习历史攻击数据、安全事件，不断优化决策模型，提升威胁识别与研判的准确性，实现对未知威胁的提前预判。另外，该层可根据数据敏感等级、业务场景需求，自动制定差异化的防护策略，分配安全资源，指导响应执行层开展防护操作，实现安全决策的智能化、精准化、高效化，解决传统防护决策滞后、主观性强的问题。

2.2.3 隐私计算层

隐私计算层是实现隐私与效用平衡的关键模块，核心是通过隐私计算技术，在不泄露原始数据的前提下，实现数据的安全共享、分析与利用。该层集成了联邦学习、差分隐私、同态加密等主流隐私计算技术，针对不同数据类型、应用场景，选择适配的技术方案：联邦学习实现多主体数据“数据可用不可见”，无需汇聚原始数据即可开展联合建模；差分隐私通过添加噪声干扰，保护数据集中个体隐私，同时保证数据统计特性不变；同态加密实现对加密数据的直接运算，避免数据解密过程中的隐私泄露风险。隐私计算层与AI决策层深度协同，将隐私计算技术融入AI建模、风险研判全过程，既保障数据隐私安全、满足合规要求，又能充分挖掘数据价值，破解传统防护中隐私与效用难以平衡的难题，为大数据协同应用提供安全支撑。

2.2.4 响应执行层

响应执行层是新框架的落地执行模块，负责将AI决策层制定的防护策略转化为具体的安全操作，实现对安全风险的快速处置与闭环管控。该层依托自动化技术与安全设备，构建智能化响应执行体系，涵盖数据加密、访问控制、攻击阻断、漏洞修复、数据恢复等多种安全操作，能够根据决策指令自动执行相应的防护动作，无需人工干预，大幅提升响应效率。另外，响应执行层具备日志记录与复盘能力，对所有安全操作、响应过程进行详细记录，为后续安全事件复盘、策略优化提供依据，形成“感知-决策-执行-复盘”的闭环防护，确保安全风险得到及时、有效处置。

3 基于 AI 与大数据的安全保障创新思路

3.1 新思路一：基于用户与实体行为分析（UEBA）的内部威胁发现

基于用户与实体行为分析（UEBA）的内部威胁发现，是破解传统内部防护薄弱问题的创新思路，核心是通过AI与大数据技术，建立用户与实体的正常行为基线，精准识别异常行为，防范内部泄露、违规操作等风险。传统内部防护多依赖静态权限管控，难以识别合法权限下的恶意操作，而UEBA技术通过采集用户登录行为、数据访问记录、操作习惯、终端运行状态等多维度数据，利用机器学习算法构建个体行为基线，明确正常行为的范围与特征[3]。当用户或实体出现偏离基线的行为，如异常登录时间、违规访问敏感数据、批量下载核心文件等，系统可快速识别并告警，同时通过AI算法研判行为的恶意程度，区分无意操作与恶意攻击。该思路打破了传统“以权限为核心”的内部防护模式，实现了“以行为为核心”的动态防护，能够精准发现内部员工、合作伙伴等主体的恶意行为，提前防范内部威胁，弥补传统内部防护的短板，保障核心数据安全。

3.2 新思路二：自动化威胁狩猎与溯源

自动化威胁狩猎与溯源，是提升威胁处置效率、降低安全风险的重要创新思路，核心是利用AI与大数据技术，实现对潜在威胁的主动挖掘、快速溯源与精准处置，改变传统“被动等待告警”的防护模式。传统威胁狩猎依赖人工操作，效率低下、漏报率高，难以应对大数据时代海量威胁数据的挑战，而自动化威胁狩猎通过AI算法对全网数据进行持续扫描、分析，主动挖掘隐藏在正常数据中的潜在威胁，包括未知攻击、隐藏恶意程序、潜伏性入侵等，实现威胁的提前发现与预警。同时，当安全事件发生后，利用大数据技术整合攻击链路、日志数据、行为记录等信息，通过AI算法快速追溯攻击来源、攻击路径、影响范围及攻击目的，明

确攻击主体与攻击手段，为后续处置、追责提供精准依据。

3.3 新思路三：智能加密与隐私增强

智能加密与隐私增强思路，聚焦传统加密技术灵活性不足、隐私保护能力有限的问题，通过AI与大数据技术优化加密方案，提升隐私保护的精准度与灵活性，实现隐私与效用的深度平衡。传统加密技术多采用固定加密算法与密钥管理模式，难以适配不同敏感等级、不同应用场景的数据加密需求，而智能加密技术利用AI算法自动识别数据敏感等级，根据敏感程度动态选择适配的加密算法、密钥长度与加密方式，对核心敏感数据采用高强度加密，对普通数据采用轻量化加密，在保障安全的同时降低性能损耗。结合隐私增强技术，如差分隐私、联邦学习等，将AI算法融入数据加密、解密、共享全过程，实现数据“可用不可见”，既防止原始数据泄露，又能满足数据共享、分析的需求。该思路打破了传统加密技术的局限性，实现了加密与隐私保护的智能化、个性化，既能满足隐私合规要求，又能充分释放数据价值。

3.4 新思路四：对抗性机器学习与模型安全

对抗性机器学习与模型安全思路，针对AI技术在安全防护应用中存在的模型脆弱性问题，通过对抗性训练、模型加固等手段，提升AI安全模型的抗攻击能力，保障整个安全框架的稳定性与可靠性。随着AI技术在安全领域的广泛应用，攻击者通过生成对抗样本、模型投毒等方式，干扰AI模型的判断，导致安全防护失效，而对抗性机器学习通过模拟攻击者的攻击手段，生成对抗样本，对AI安全模型进行对抗性训练，提升模型对对抗样本的识别能力，增强模型的鲁棒性。通过模型加密、权限管控、行为审计等手段，加强AI模型本身的安全防护，防止模型被篡改、窃取或滥用，保障模型的完整性与安全性。利用大数据技术持续收集对抗攻击数据，不断优化对抗性训练方案，实现模型安全的动态提升，破解AI模型自身的安全隐患，为整个安全框架提供可靠的技术支撑。

3.5 新思路五：生成式AI（AIGC）在安全运营中的应用

生成式AI（AIGC）在安全运营中的应用，是提升安全运营效率、降低人工成本的创新思路，核心是利用AIGC技术自动生成安全运营所需的各类内容，辅助安全人员开展防护工作，提升安全运营的智能化水平。传统安全运营依赖大量人工完成日志分析、告警研判、策略编写、漏洞扫描等工作，效率低下、人工成本高，而AIGC可自动生成安全告警分析报告、漏洞修复方案、安全防护策略等内容，为安全人员提供决策辅助，减少人工工作量[4]。例如，AIGC可根据日志数据自动分析告警原因，生成详细的分析报告，帮助安全人员快速定位问题；可模拟攻击者的攻击手段，生成攻击场景与测试用例，辅助开展安全测试；可根据业务场景变化，自动优化安全防护策略，提升防护的适配性。同时AIGC与大数据、AI决策层深度协同，实现安全运营的自动化、智能化，大幅提升安全运营效率与质量，缓解安全人才短缺的困境。

结束语

大数据与人工智能为数据安全保障带来了新的契机与思路。通过构建融合大数据与AI的新框架，以及提出多种创新思路，能在动态适配、隐私保护、威胁处置等多方面实现突破。这不仅有助于克服传统防护的局限，更能适应大数据时代复杂多变的安全需求。未来，持续探索与完善相关技术，将为数据安全构筑更坚实的防线，推动数据领域健康、稳定发展。

参考文献

[1]唐铁军.大数据和人工智能时代数据安全风险及应对策略[J].通讯世界，2026，33(2):46-48.

[2]聂立泽,王祯.生成式人工智能对数据安全保护的挑战及刑法应对[J].河南社会科学,2025,33(1):56-63.

[3]徐翼.生成式人工智能应用中个人数据安全风险及其法律规制路径[J].征信,2025,43(5):9-16,28.

[4]张瀚文.生成式人工智能监管视角下数据安全治理研究[J].河北经贸大学学报（综合版）,2025,25(1):49-54.