

谈云计算环境下电子信息工程数据隐私保护机制

俞飞

江阴众和电力仪表有限公司 江苏 无锡 214400

摘要: 在当今数字化时代,云计算环境下的电子信息工程蓬勃发展,但数据隐私保护问题日益凸显。文章主要以云计算环境下电子信息工程数据隐私保护机制为重点,首先从四方面分析电子信息工程数据隐私风险,其次从多源数据融合监测机制、动态阈值与概率评估机制、分布式协同学习机制等方面深入探讨,致力于提升云计算环境下的数据隐私保护效果,在个机制协同融合基础上,为云计算环境下电子信息工程数据隐私建筑一条牢固的安全防线,更为相关研究提供参考资料。

关键词: 云计算环境;电子信息工程;数据隐私;保护机制

DOI: 10.63887/ssrp.2025.1.4.20

引言

数字化发展背景下,云计算具有一定的存储功能、计算功能,在电子信息工程领域得到广泛应用,尽管为企业、个人等都带来全新的数据处理手段、资源共享模式,但迎来了新数据隐私问题。电子信息工程涵盖诸多数据,其中有很多敏感信息,如个人隐私、企业技术参数等,一旦数据脱离本地安全管控,存储在云端服务器,就容易出现网络攻击,严重情况还会出现数据泄漏的问题。针对这一情况,为提升电子信息工程数据在云计算环境的安全程度,相关人员需要探索更有针对性的数据隐私保护机制,一方面维护用户权益,另一方面助力电子信息工程尽早实现可持续发展目标。

1 云计算环境背景

云计算环境是建立在互联网基础上的一种新计算模式,将大量的服务器、存储、网络等进行整合,通过虚拟化技术,依据所需完成分配^[1]。针对企业来说,不需要再创建大规模的数据中心,可节省一定的硬件购置成本、维护成本,还能更灵活的缩减资源规模;针对开发者来说,可在短时间获取开发环境,进一步推进项目发展。同时云计算环境,还有一定的数据备份功能、恢复功能,从多方面入手维护数据安全。

2 云计算环境下电子信息工程数据隐私风险

分析

2.1 数据存储风险

云计算背景下,大多数数据都存储在云服务提供商对应的数据中心。一旦用户数据没有在物理管控范围中,就容易面临云服务提供商人员的非法访问、篡改等诸多可能^[2]。若云储存系统自身的安全防护机制不完善,黑客也会以此为攻击点,从存储服务器中得到用户的隐私信息。比如某一大型企业,将电子信息工程有关研发资料,一直存储在云端,一旦存储安全不灵敏、出现失控问题,这些关键技术信息都可能出现泄露,进而为企业带来严重的经济损失。

2.2 数据传输风险

电子信息工程中,数据从网络传输到云计算平台,或者是数据在云平台中各阶段传输期间,如果没有在传输通道中设置相应的加密协议,易出现网络监听、中间人攻击等问题。攻击人员会得到传输数据,解析数据涵盖的敏感内容,如没有加密的用户登录凭证,严重影响数据隐私效果。比如某一互联网电子信息工程应用过程中,依托智能设备采集各项数据,涵盖用户健康数据、家庭环境数据等,这些数据上传到云端分析的时候,若传输安全受损,就会面临暴露用户生活隐私的可能性。

2.3 多租户共享资源风险

云计算环境中,一般使用多租户模式,诸多用户

一起共享计算资源、存储资源等，容易造成不同用户数据，在存储中存在相邻位置，导致数据存储之间无法隔离问题。一些恶意租户，就会采用侧信道攻击等方式，获取其他租户的隐私数据，对电子信息工程数据保密对产生严重影响。

2.4 云服务提供商可靠性风险

从数据隐私方面进行分析，云服务提供商的运营现状、信誉等要素，都会对其产生关键影响。若供应商面临经营困境，或者存在被收购现状，会面临无法保障用户数据安全的可能性，严重情况还会出现数据丢失等问题^[3]。

3 云计算环境下电子信息工程数据隐私保护机制

3.1 多源数据融合监测机制

3.1.1 数据采集整合工作，电子信息工程涉及多样化数据源，如传感器、智能终端和各种业务系统产出的数据，多源数据融合监测机制最先要做的是把分散于不同地方、不同格式的数据进行收集、整合，采用统一的数据接口规范，把不同源头的的数据以标准化格式汇聚在一起。例如，针对某一个电子产品研发的电子信息工程项目，无论是生产线上传感器收集到的产品性能参数数据，还是研发人员在设计系统中输入的

图纸相关数据，亦或是测试部门反馈的测试结果相关数据等，都能被统一收拢收集，集成一个相完整的数据集合，为后续的监测与分析工作打下基础^[4]。

3.1.2 智能分析监测。采用先进的数据分析、人工智能技术，对融合后的实施深度探查，实时查看数据的访问情形，通过分析访问时的 IP 地址、访问时间、访问的频繁程度以及操作类型等多方面因素，评估是否存在异常访问情形。一旦发现某个 IP 地址在短时间内频繁地试着去访问某核心电子信息工程数据，且 IP 并非授权许可的常用地址，系统随即就能识别并发出预警内容，持续留意数据的变动轨迹；详细记录数据的修改、删除、添加等，一旦发现不契合正常业务逻辑的变动，能迅速发觉并实施相应办法，防范数据隐私遭恶意篡改或毁坏。

3.1.3 持续优化更新。多源数据融合监测机制并非始终如一，它需要结合实际业务的发展进程以及新出现的威胁局面不断做优化更新。依靠机器学习算法，从既往的监测案例当中学习，持续增进对异常行为和潜在隐私威胁的辨认能力，当网络里新的攻击手段出现，监测机制能凭借学习新的攻击特征，及时改进分析策略，增长对新型数据隐私风险的抵御实力，始终做到对电子信息工程数据隐私的有效监测。

表一：多元数据融合监测表

阶段	描述	优点
本地数据处理	各数据源节对自身数据做初步处理与学习，采用机器学习算法，提取特征、完成模型训练	1.降低数据在传输中面临的隐私泄露风险 2.利用各节点计算资源，提高数据处理的成效
加密通信与信息共享	节点利用加密通信方式，把本地学习产生的关键参数、模型更新信息等跟其他节点与云端进行交互共享，采用高端的加密技术，如同态加密、差分隐私	1.保证数据传输与共享期间，让数据隐私更加安全可靠 2.实现知识共享与协同优化
协同整合与全局优化	云端对各个节点所传的加密信息做协同整合与优化，生成一个既综合又精准的全局模型，并重新反馈到各个节点去使用	1.展现云计算的分布式长 2.各个环节守护数据隐私 3.保证电子信息工程数据安全，实现高效利用与价值挖掘

3.2 动态阈值与概率评估机制

3.2.1 动态阈值设定

对不同的电子信息工程业务场景，数据各项指标的正常波动范围不同。处于动态阈值与概率评估机制

的环境中，动态阈值设定阶段会依据具体业务需求、数据过往表现以及当下运行环境等要素，实时判定数据指标的合理阈值范围，尤其在电子通信工程进行网络流量监测的场景里面，工作日白天业务的高峰阶段，数据流量会显著超过夜间以及节假日。系统会通过分析以往不同时段的数据流量，结合当前业务的开展情形，动态地去设定流量的上下限阈值，若实时发现流量超出这一动态阈值，会第一时间在系统出现警示，提示是否存在数据被恶意海量下载等，协助工作人员开展后续的排查工作，如表一所示。

3.2.2 概率评估分析

从概率学的角度进行分析，综合考量云计算环境下各种影响数据隐私的因素^[5]。对数据隐私面临威胁的程度做量化评估，要对外部网络攻击发生的概率、内部人员违规操作的可能性、数据共享时出现泄露的风险概率等多方面进行分析，通过对过往网络攻击的次数、内部违规事件的频率以及以往数据共享里的问题案例等进行统计分析。组建对应的概率模型，给每一次的数据交互、访问这类行为赋予一个风险概率值，依照此概率值的大小，分辨当前数据隐私面临的风险等级，进而判定是否需采取紧急的保护手段——如限制访问的权限、增强数据加密强度等，实现对数据隐私更妥当的守护。

3.2.3 协同配合作用

动态阈值和概率评估机制里的这两部分并非孤立运行，而是彼此协同联动的。动态阈值的设定为迅速发现数据指标异常给出了直观判断依据，而概率评估分析则进一步深入探查异常背后的隐私风险状况，可更全面、确切地把握数据隐私情形，在云计算复杂又变化多样的环境当中，能够快速察觉潜在隐患，保证电子信息工程数据隐私的安全可靠。



图一 流量监控系统界面

3.3 分布式协同学习机制

3.3.1 本地数据处理

在电子信息工程的范畴之内，数据一般分散于众多终端设备和不一样的业务节点上，分布式协同学习机制先激励各数据源节点在本地对自身数据做初步处理与学习；再采用本地的机器学习算法，终端设备可对本区域内收集到的电子信息工程数据做特征提取、简单的模型训练等处理。通过这种做法的好处，无需将原始的、大概含有大量隐私信息的数据全部上传至云端进行统一处理，大幅降低了数据在传输阶段隐私泄露的风险，还可充分利用各节点现有的计算资源，提高数据处理的成效^[6]。

3.3.2 加密通信与信息共享

各节点学习本地的数据之后，需要利用加密通信方式，把本地学习产生的关键参数、模型更新信息等跟其他节点与云端进行交互共享，采用高端的加密技术，如同态加密、差分隐私这般，保证在数据传输与共享期间，哪怕资料被第三方截取，也无从获取到有价值的隐私数据。例如，当某一大型电子信息工程项目，涉及多个子项目团队一起协作的时候，各个团队通过加密通道把本地训练好的模型参数发送至总协调的云端服务器，实现知识共享及协同优化，同时也保证了数据隐私的安全可靠^[7]。

3.3.3 协同整合与全局优化

云端收到各个节点所传的加密信息后，会按照相应的算法跟规矩，对这些以分布式传来的内容做协同整合与优化事宜，最终生成一个既综合又精准的全局模型。这个全局模型会重新反馈到各个节点去使用，让各个节点能凭借更全面、更确切的信息开展后续电子信息工程业务，整个进程里采用分布式协同学习机制，既充分展现了云计算的分布式长处，以及在各个环节守护数据隐私的成效，一方面让电子信息工程的数据在保障安全的基础上，实现高效利用与价值挖掘。

结语

探索云计算环境下电子信息工程数据隐私保护期间，相关人员充分意识到数据隐私保护这项工作的重要性，依据可能面临的数据隐私风险，制定一系列数

据隐私保护机制，全面提升数据隐私保护效果与水平。未来云计算技术、电子信息工程必定会取得更好的发展前景，也会迎来更多新挑战，呼吁相关人员能持续关注数据隐私保护工作，引入更多新理念、新方法完

善现存保护机制，促使电子信息工程数据即使面对云计算环境，也能完成安全存储、安全传输等，进一步推动相关行业高质量发展。

参考文献

- [1]刘永亮,冯庆云,夏辉福.基于大数据技术的电子信息安全保护策略分析[J].电子技术,2025,54(02):144-145.
- [2]项洁.低碳经济下电子信息工程在工业领域中的应用探讨[J].中国电子商情,2024,(19):91-93.
- [3]师文锦.基于人工智能驱动的电子通信网络优化研究[J].中国宽带,2024,20(09):139-141.
- [4]陈丹霞,曾鹏.交通数据隐私保护技术研究及其在智能交通系统中的应用[J].中国高新科技,2024,(09):69-71.
- [5]季奥颖,柳伟,丁页顶,鲍喜妮,高源.支持数据隐私保护的恶意加密流量检测确认方法研究[J].中国高新科技,2024,(09):75-76.
- [6]林龙.基于可信数字身份与电子证照的多因素认证与数据隐私保护技术研究[J].中国高新科技,2023,(21):47-49.
- [7]韩卫宏.“互联网+”背景下现代化电子信息技术的发展及应用[J].中国设备工程,2023,(17):244-246.

作者简介：俞飞，1987-09，男，汉，江苏无锡江阴，本科，研究方向或从事工作：电子信息 硬件设计