Computer Science and Application 计算机科学与应用, 2023, 13(11), 2062-2071
Published Online November 2023 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2023.1311205

Hans汉斯

安全驱动的边云数据协同策略研究

张王俊[1]，陈　宇[1]，赵忠军[2]，朱旻捷[1]，彭炜舟[1]

[1]国网上海市电力公司数字化工作部，上海
[2]上海欣能信息科技发展有限公司安全生产部，上海

收稿日期：2023年10月16日；录用日期：2023年11月15日；发布日期：2023年11月22日

摘　要

分布式计算虽然能弥补传统集中式计算网络拥堵、计算能力低的缺点，但对边缘设备隐私安全和可信感知存在不足。随着数字新技术的快速发展，利用新一代信息技术满足边云现场环境下的边云数据协同需求日益增长。本论文首先通过研究边缘计算和云计算的发展趋势，识别边云协同关键技术，然后分析边云数据协同面临的数据传输安全、数据通信安全、数据存储安全等问题，得出边云数据协同安全风险方法措施，最后结合边云现场环境下的工业信息物理系统数据协同安全需求，提出了一种基于边云协同的动态数据安全存储策略，该策略以“事前准备－事中防御－事后响应”为指导思想，既能够充分利用云计算和边缘计算的技术优势，又可以满足数据协同的安全性和实时性要求。

关键词

边缘计算，云计算，数据协同，安全存储策略

Research on Security Driven Edge Cloud Data Collaboration Strategy

Wangjun Zhang[1], Yu Chen[1], Zhongjun Zhao[2], Minjie Zhu[1], Weizhou Peng[1]

[1]Digital Work Department, State Grid Shanghai Electric Power Company, Shanghai
[2]Safety Production Department, Shanghai Xinneng Information Technology Development Corporation, Shanghai

Received: Oct. 16th, 2023; accepted: Nov. 15th, 2023; published: Nov. 22nd, 2023

Abstract

Although distributed computing can compensate for the shortcomings of traditional centralized computing network congestion and low computing power, it has shortcomings in privacy security and trustworthiness perception of edge devices. With the rapid development of new digital technologies, the demand for edge cloud data collaboration in edge cloud on-site environments is in-

文章引用: 张王俊, 陈宇, 赵忠军, 朱旻捷, 彭炜舟. 安全驱动的边云数据协同策略研究[J]. 计算机科学与应用, 2023, 13(11): 2062-2071. DOI: 10.12677/csa.2023.1311205

creasingly increasing through the use of next-generation information technology. This paper first identifies the key technologies of edge cloud collaboration by studying the development trend of edge computing and cloud computing, then analyzes the data transmission security, data communication security, data storage security and other issues faced by edge cloud data collaboration, and obtains the risk methods and measures of edge cloud data collaboration security. Finally, combined with the data collaboration security requirements of industrial information physics systems under the edge cloud on-site environment, a dynamic data security storage strategy based on edge cloud collaboration is proposed. The strategy takes "preparation in advance-defense in the event-response after the event" as the guiding ideology, which can not only make full use of the technical advantages of cloud computing and edge computing, but also meet the security and real-time requirements of data collaboration.

Keywords

Edge Computing, Cloud Computing, Data Collaboration, Secure Storage Policy

1. 引言

近年来，云计算的逐渐成熟，其已成为大数据处理与存储的技术支撑，大多用户能够利用不同终端对数据展开高效操作，满足了用户的需求。然而，在云计算应用过程中，仍存在数据安全问题，如：数据丢失、数据冗余、数据被窃取等，严重影响了用户安全与企业利益，为其带来较大损失。而边缘计算技术的出现，提供了计算分流、数据缓存、数据处理、快速响应和局部自治的能力，从而极大地缓解了云端网络通信、计算资源的负担，能够满足边云数据协同应用场景的需要。

2. 研究背景

当前，我国正处于新一轮工业革命的历史机遇期，随着工业物联网[1]的发展兴起和大数据[2]时代的来临，加快了云计算的出现和云存储技术的产生，打破了传统工业环境相对封闭可信的状态，因为其价格低廉、存储能力强，所以受到了大量用户的欢迎，越来越多的用户倾向于将生产设备现场产生的数据同步到云服务中心进行存储，主要依赖于集中式部署的云计算模型，对数据进行集中式处理。该模式虽然有很强的数据处理能力，但由于云计算固有的开放性，使得这种托管的云存储模式在提供更高的服务质量的同时也带来了隐私安全方面的挑战。一是云端更容易受到集中攻击，云服务提供商自身的可信度也值得评估。二是在集中式云存储模型中，数据收集终端通常距离云数据中心较远，这使得终端与云端通信时易产生高延迟。三是云数据存储中的隐私安全问题、云动态数据安全同步存储的问题、云数据存储中的数据完整性问题等。四是可靠性问题，如果用户直接将所有的数据上传到云，则无法保证数据的完整性、隐私和可靠性。五是更新效率问题，在一些实时性要求比较高的应用中，云和设备之间的通信延迟不可以超过其有界时延，若每次都更新整个文件将对实时性有很大的影响。

由此可见，工业领域应用中的数据聚合、数据处理、数据分析和数据决策等不同环节，往往也会产生各种各样的业务约束要求，如海量任务的快速响应、资源的层次化和异构性、能耗与延迟的均衡、任务的多样化和混合性、数据传输安全与效率等。传统的云中心智能无法很好地满足此类业务需求，而边云协同智能技术为解决上述问题提供了一条可行的道路，即通过端、边、云之间的协同优化，实现安全、

敏捷、低成本、低时延、隐私保护的大数据服务。边云协同技术由于具有对任务进行迁移决策、降低移动设备能耗、降低计算任务延迟、保护数据隐私安全等诸多优点，已经受到工业界和学术界的关注，并广泛应用于工业物联网、移动互联网等多个领域。因此，边云协同智能技术成为了工业控制领域中的新模式。然而，工业领域各大企业数据传输产生的安全问题尤为显著，如何解决工业信息物理系统数据传输安全问题成为了当前重点研究内容。从当前取得的研究成果来看，对于工业信息物理系统数据共享交互安全问题尚未形成有效的解决方法[3]。本文通过整理大量资料，归纳总结数据存储、传输、通信安全风险，引入更多数据安全技术，提出了一种基于边云协同的动态数据安全存储策略。

3. 边云协同技术概述

3.1. 国内外研究现状

云计算是基于网络的一种计算范式，传统的云计算把计算资源、存储资源和网络资源集中到云端数据中心统一处理，客户可以按需付费。云计算在一定程度上解决了设备内存不足、算力薄弱、效率低下等问题。云计算的处理流程是：任务从设备上传到云数据中心，处理完成后再把结果返回用户。但随着用户需求越来越多，延迟也在增加，以致客户需求得不到及时满足。延迟是衡量客户满意度和设备灵敏度的重要指标，尤其是在无人驾驶、智能救援等领域，系统延迟是无法容忍的。因为反应快 1 ms 可能就避免一场交通事故。因此，云计算不适用于延迟敏感的应用。为了缓解上述问题，边缘计算应运而生。

边缘计算并不是一个新词汇，早在 20 世纪末就已经被提出。边缘计算在更靠近设备的网络边缘测提供服务，大量任务在近设备端快速进行处理，使得数据的传输具有较短线路，不仅可以减小任务的计算延迟，支持任务的实时性要求，还能缓解数据传输过程中的带宽压力。而边缘计算的分布式多节点服务架构使得网络具有高可扩展性和弹性，单设备故障不会影响网络运行，其运行成本相对云计算也更加低廉。除此之外，这一架构还使得任务在处理过程中数据集中度低，数据泄露的风险低，有利于保护敏感数据的隐私与安全。边缘计算的概念自提出后引起国内外广泛的关注，各国对于边缘计算技术都各自提出了相应的研究战略。2015 年，欧洲电信标准化协会发布移动边缘计算白皮书，同时成立多介入边缘规范工作组。2016 年，中国成立了边缘计算产业联盟。同时，边缘计算也受到中国自动化学会的重视，成立边缘计算专委会，努力推动相关标准和技术的发展，并在多类业务场景下开展了边缘计算技术的应用。

从上述表述中可以看出，边缘计算与云计算之间是技术协同与优劣互补的关系，因而边缘计算实际上是研究边缘计算和云计算的协同合作问题。边云协同的核心是云计算和边缘计算，非常适用于物联网应用场景，可以广泛应用于智能电网、物联网、工业制造等实际应用场景。目前，边云协同概念已经开始应用于智能电网相关应用研究之中，并取得了一些成果。

3.2. 边云协同关键技术及实现方式

边云协同是云计算与边缘计算之间的协同，目的是为了更好地满足客户需求，降低建设和运营成本。边云协同的模式主要有数据协同、算法协同、应用协同、资源协同等多种典型模式。

数据协同：主要指边缘端对于现场采集到的数据先进行一轮处理然后再同步到云端。为了使资源利用率与服务效率提升，一般会在边缘端对数据进行预处理，筛选提炼关键数据，如对于不上传原始高频时序数据而只上传波动幅度超过一定范围的数据，如部分与目标相关性不大的字段从上传范围中进行剔除。提炼后的数据再同步上传至云端进行运算与应用。

算法协同：主要指云端到边缘端的模型下放。一般边云协同场景下，边缘端只负责模型的执行运算，而不会对算法模型直接进行构建。构建工作交由云端完成，云端可以汇聚更为丰富的数据，利用更加充足的计算资源构建更为可靠、有效的算法模型。算法协同实现了算法模型构建完成后，从云端到边缘端

的同步，其一般以时间、数据波动程度、模型波动程度为参考依据对算法模型进行更新。通过云端模型的建立与下放协同，保证边缘端执行计算的准确性与有效性。

应用协同：主要指将边缘计算节点与云主站相结合，从资源、数据、接口、通信、安全等多方面、多维度切入，遵循边缘计算自身的就近原则、边云层级对应原则以及云主站统一管理原则，减少数据往返云端等待时间和网络带宽成本，满足终端侧实时需求，同时提高云主站承担复杂工作的效率，降低边云管理的难度和系统资源成本，共同完成更多更复杂工作目标的过程。

资源协同：主要指在上层应用的支持下，对分布在边缘云的存储资源与中心云的存储资源进行协同处理，提高存储资源的利用率和计算资源的效率，节约传输带宽和传输成本。

3.3. 边云数据协同技术路线和模型原理

边缘计算与云计算协同服务作为桥接云和用户的一种有效的方式，主要包括两个方面内容：边缘计算完成现场局部自治，及时对现场采集到的数据计算执行，并精炼数据上报云端，提升反应速度；云端服务则完成面向数据的综合处理与模型建立，并构建完成的模型下放到边缘端，保障整体处理与运算效果。通过边缘计算与云计算协同服务，一些工作负载可以从云端卸载到边缘，从而减轻云中心的压力，与云计算相比，边云协同支持实时分析，协同服务，执行速度更快，成本更低。

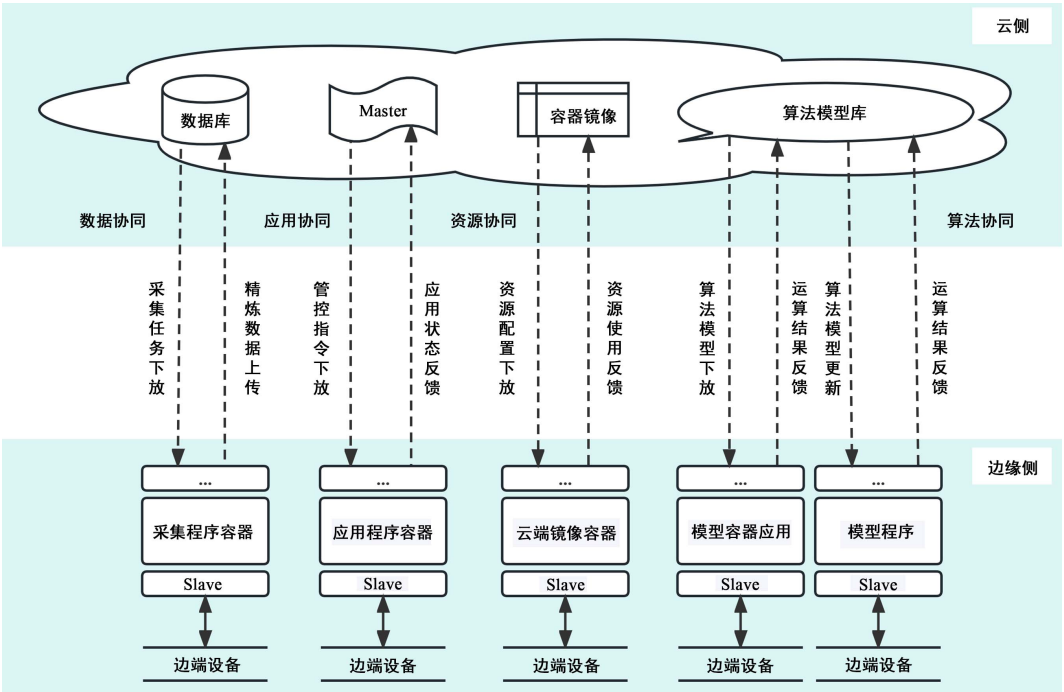

Figure 1. Route and model principles of edge cloud collaboration technology
图 1. 边云协同技术路线和模型原理

上图 1 中，边缘节点负责对于现场采集到的数据先进行计算、存储、网络、虚拟化等基础设施资源的协同，以及边缘节点设备自身的生命周期管理协同处理，然后把处理后的数据按照云端要求的格式发送给云端。因为现场采集数据很多时候往往会有较大的规模，而其本身信息密度并没有那么高，如果将所有数据都上传到云端，一方面会占用大量的网络资源，另一方面云端在汇聚众多边缘端数据后整体数据规模也会非常巨大，从而使得后续的运算开销较高。为了使资源利用率与服务效率提升，一般会在边

缘端对数据进行预处理，筛选提炼关键数据，如对于不上传原始高频时序数据只上传波动幅度超过一定范围的数据，如剔除部分与目标相关性不大的字段。提炼后的数据再同步上传至云端进行运算与应用。

由于电子文档、多媒体等的出现，使得云端的数据不再是简单的文本，而是集文字、图表、图片、图像、音视频等多样化媒体于一身的综合性信息传播媒介，数据的描述和管理也因此呈现出细粒度、对象化的特点，为了保证云端数据访问过程中的机密性、完整性，云端对海量数据进行存储，挖掘和分析和模型优化，并通过详细的数据分级和用户分级实现对数据的安全管理和维护，进而在边缘和云端两侧进行云边数据协同，从而缓解边缘服务器的计算压力，确保云端资源和服务被合法的用户所获取并使用。

4. 边云数据协同面临的安全威胁

边云数据协同面临的安全威胁主要体现在以下几个方面：

数据访问安全：由于网络、计算机等技术的发展，涌现出了大量类型各异的终端设备和接入方式个性化的网络计算模式。用户能够使用任何终端设备，在其方便的时间、地点，经由任何网络对其感兴趣的资源进行访问，这在为用户提供资源使用便利的同时，也导致了资源访问的随机和不可控问题。此外，云端数据多级管理的特点，使得访问控制技术的研究面临多要素和多级管理相结合的问题。

数据传输安全：在边云协同应用数据传输过程中，用户需要通过数字认证授权以后，才能进行其他操作。如果此种认证授权被篡改，那么攻击者就可以伪造被认证授权的数据，从而获得传输系统的操作权，威胁到整个网络系统的安全运行。

数据生成安全：防止云服务提供商利用其特权对用户隐私的窃取或泄露，或基于数据挖掘等手段对用户数据进行搜集，分析其隐私数据；防止恶意用户的攻击和对其他用户数据的非法获取、破坏。

数据通信安全：在边云协同应用中，对于没有实现的数据，需要利用网络传递至云计算中心，在传递过程中，数据极易被窃取，导致数据漏洞。现有工业物联网单一路经通信方法不能有效保证敏感信息传输的机密性、完整性和真实性，因此需要建立一直多路径冗余协同安全通信方法和通信缺失数据预测方法。

数据存储安全：用户的一些重要数据和资源、相关程序和应用通常都存储在云端，虽然目前云存储服务商对用户的数据进行集中存储、统一管理和实时监控，最大限度地保证系统和数据的安全。但是，云存储系统具有多层结构，是一个极其庞大、复杂的系统，这就涉及到了存储数据的完整性、机密性、可用性问题。

5. 边云数据协同安全风险防范措施

5.1. 有线数据传输安全风险规避方法

针对当前有线数据传输中存在的安全风险，常用的规避方法有差分平衡传输控制、Modbus 控制指令加密、跟踪端口访问动态、用户身份认证、实时监测、访问授权保障、CIP 安全协议、线缆冗余技术、TSN 技术[4]。这些方法虽然具有一定数据传输安全防御功能，但是对应用条件要求较高，并且部分技术单独使用情况下并不能充分发挥安全风险规避作用。所以，需要根据互联网有线传输安全风险，合理选取几种技术，搭建数据安全传输体系。

5.2. 无线数据传输安全风险规避方法

针对无线数据传输的安全风险问题，常用的风险规避方法有数据加密处理、网络远程监控、主动式冗余处理、用户身份认证和访问权限认证等。目前，这些方法的作用各不相同，可以用于数据发送终端、数据传输通道、数据接收终端[5]。由于数据传输的整个过程中任意一个访问端口和访问渠道都可能遭受

攻击，所以风险规避完整性显得尤为重要。

5.3. 云存储下数据存储安全风险规避方法

针对云服务环境下的数据存储安全，可以通过实施虚拟安全技术、物理安全技术、数据隐私管理、数据传输加密、数据访问控制、认证服务、安全审计等一系列的安全机制来保证云存储系统数据的可用性、保密性和不可抵赖性，从而提高数据的安全性。

5.4. 边缘计算数据通信安全风险规避方法

在密码学上，Bob、Alice 通信问题是常见问题，当前，为保障边缘计算数据安全，无论是对信息进行加密还是直接在 Bob、Alice 间设置访问控制协议，都各有利弊。为保障边缘计算数据的安全性，还可利用链－链、端－端的计算机网络通信加密技术，对信道进行加密，有效保障边缘计算数据通信的安全。

6. 基于边云现场的数据协同安全策略

6.1. 边云现场环境下的工业信息物理系统数据协同安全需求分析

随着云计算在工业领域的应用，工业信息物理系统(ICPS)正逐步向着扁平化的趋势发展并逐渐向“工业云平台－企业私有云－通信网络－现场控制－物理系统”的典型架构演变。其中，工业云平台提供大数据存储、大数据分析与挖掘以及通用的行业设计制造辅助等开放服务，企业内部部署私有云(边缘云)以支撑系统正常有序的生产、运营和管理，现场层控制工业系统的生产制造过程，通信网络负责云和现场的连接。由此可见随着信息化的加深，ICPS 中大量的生产装置以及仪器仪表等现场设施暴露于外部网络攻击之下，系统面临的安全威胁和挑战愈发严峻。

在边缘计算环境下的 ICPS 中，信息域物理域高度耦合、工序繁多、机理复杂、系统行为动态变化，边云协同体系更加复杂，需要充分利用历史数据、实时数据和系统知识进行准确的安全决策，以适应系统的动态变化。以上安全策略决策需求以现场系统的实时安全防护为中心，其实现依赖于智能化的评估和决策方法，如具备快速量化计算和具有动态自适应功能的风险评估模型，具备及时决策和具有全局视角分析能力的安全策略决策模型等，采用边云协同的模式以及模型与数据相结合的策略是实现途径之一。

6.2. 安全驱动的工业信息物理系统数据协同风险评估

根据信息安全风险评估相关标准 GB/T 31509-2015，GB/Z 24364-2009 和 GB/T 20984-2007 等的规范，风险评估是在了解威胁、脆弱性、资产等要素关系的基础上，通过对系统的综合分析得出系统风险，信息安全技术国家标准中给出的风险评估原理图如图 2 所示。

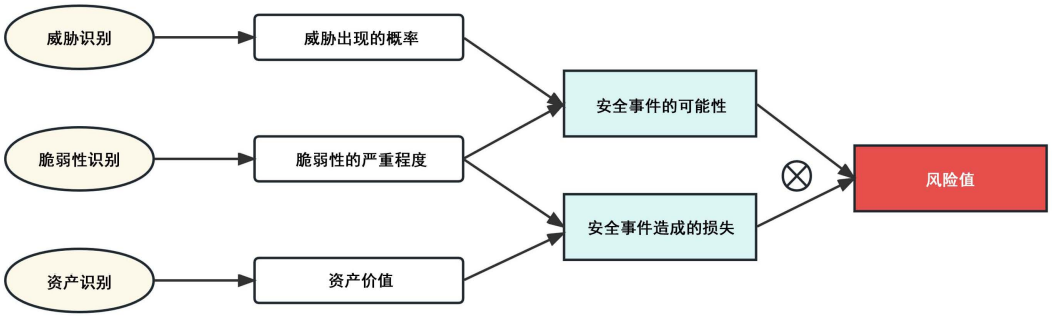

Figure 2. Principles of risk assessment for industrial information physics systems
图 2. 工业信息物理系统风险评估原理

根据标准规范，系统的风险通常可表示成安全事件发生的概率和安全事件造成的后果的乘积。ICPS 风险评估的目的是基于入侵检测证据预测攻击行为并评估系统安全状况，本质上 ICPS 的风险评估和信息安全风险评估类似，ICPS 的安全风险分析也应参考该框架，只是对于资产等要素需要结合 ICPS 实际进行评估。所以开展 ICPS 风险评估重点是获得安全事件发生的可能性和对资产的量化评估，可以基于贝叶斯网络建立风险传播模型以获得安全事件的概率，基于模糊综合评价法进行资产评估以获得安全事件造成的损失，并利用云计算的大数据处理能力训练贝叶斯网络的参数。

于是提出了一种数据和模型驱动的 ICPS 的风险评估方法。在充分分析攻击特点与过程及 ICPS 结构与功能的基础上，设计了基于贝叶斯网络的风险传播模型用来进行概率推理；在对 ICPS 信息安全需求进行分析的基础上，设计了基于模糊综合评价法的资产评估以评估安全事件造成的损失，二者共同完成基于模型的风险评估。然后利用边缘计算的大数据处理能力，在云端设计了贝叶斯网络的参数学习方法，具体地，设计了基于 MapReduce 的 EM 算法采用分布式计算可处理大规模数据，完成贝叶斯网络的模型参数训练。通过边云智能协同，实现了安全驱动的 ICPS 风险评估。

6.3. 边云数据协同的安全策略决策总体框架

针对上述边缘现场环境下的工业信息物理系统的数据协同安全需求，结合风险评估模型，提出如图 3 所示的边云数据协同的安全策略决策总体框架，从安全防护流程角度主要分为安全风险评估环节(图中蓝色部分)和安全策略决策环节(图中红色部分)，从边云协同角度主要包括在云端的安全知识提取环节和在边缘计算节点的本地安全决策环节。

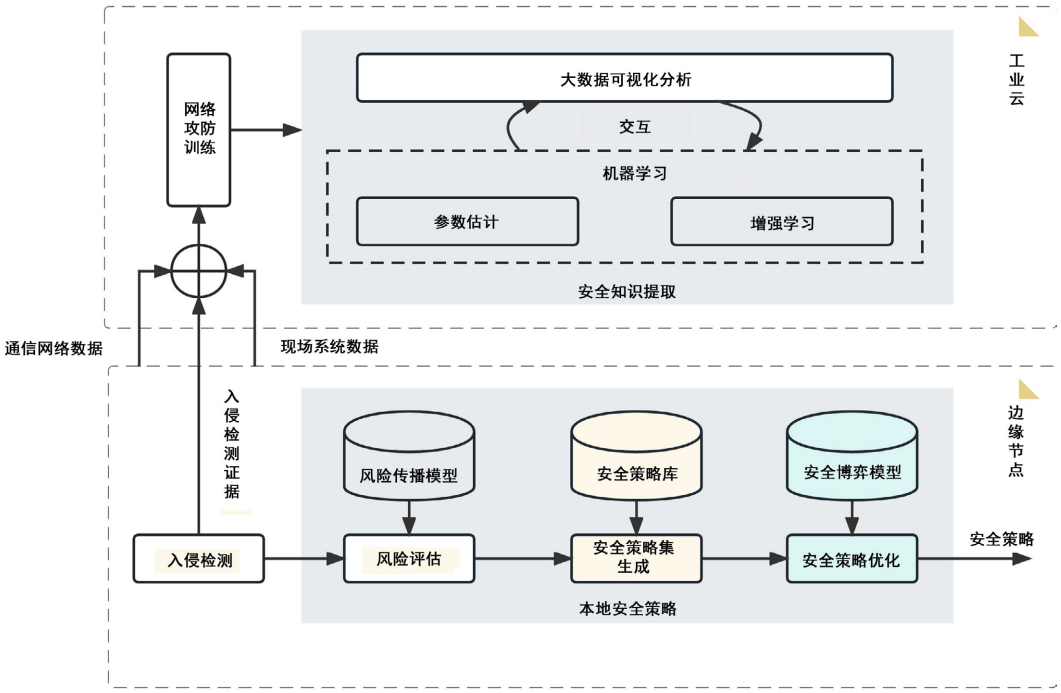

Figure 3. Security policy decision framework for edge cloud data collaboration
图 3. 边云数据协同的安全策略决策总体框架

云端的网络攻防训练是数据预处理过程，主要在云端融合系统全局时空的历史运行数据，包括现场系统数据、通信网络数据和入侵检测证据，进而构造真实物理实体的虚拟映射系统。在虚拟系统中模拟

典型网络攻击，通过攻防演练生成攻防过程仿真数据，然后利用生成对抗网络技术对得到的仿真数据进行修正得到用于安全知识提取的攻防数据集。

云端的知识提取环节是离线的大数据分析处理过程，主要对风险传播模型(如贝叶斯网络模型)进行分布式的参数学习(如基于MapReduce的EM算法)以及对安全博弈模型(如随机博弈模型)进行强化学习的博弈训练，采用数据和模型驱动的方法利用云计算的大数据处理能力、资源优势和全局视角构建起用于安全策略决策的模型。同时，模型的训练过程可以通过可视化技术进行直观展示，结合工业及安全领域的专业背景知识，可以发掘数据中隐含的知识和模式，提高知识提取过程的准确性。当安全模型训练完成后，将模型下发到边缘侧部署，以实现本地的安全决策。

边缘侧的本地安全决策环节是在知识提取环节获得的安全模型的基础上，对融合的实时多源入侵检测证据，通过贝叶斯网进行动态风险评估，预测攻击者可能的攻击目标、路径以及相应的概率，建立攻击策略集，并结合系统安全策略库以及基于功能树的系统功能模型生成安全防御策略集，进而建立安全策略集。同时风险评估得到的量化结果作为博弈的收益(payoff)量化参考，建立收益量化模型。然后，将收益量化模型作为随机博弈判别条件进行攻防博弈以生成最优防御策略。

在边云数据协同的安全策略决策框架中，安全策略决策是核心，边云协同是辅助的运行模式。

6.4. 边云数据协同的基本内涵和流程

边云数据协同主要包括三个方面：数据协同，智能协同和管理协同。在图 4 中，云计算主要完成模型参数学习和全局数据分析；边缘计算基于训练后的模型执行智能推理，以实现本地快速安全策略的生成。边云协同过程在图 4 中用序号①~⑦标记，下面简要介绍边云协同在 ICPS 安全策略决策场景下的基本内涵和流程。

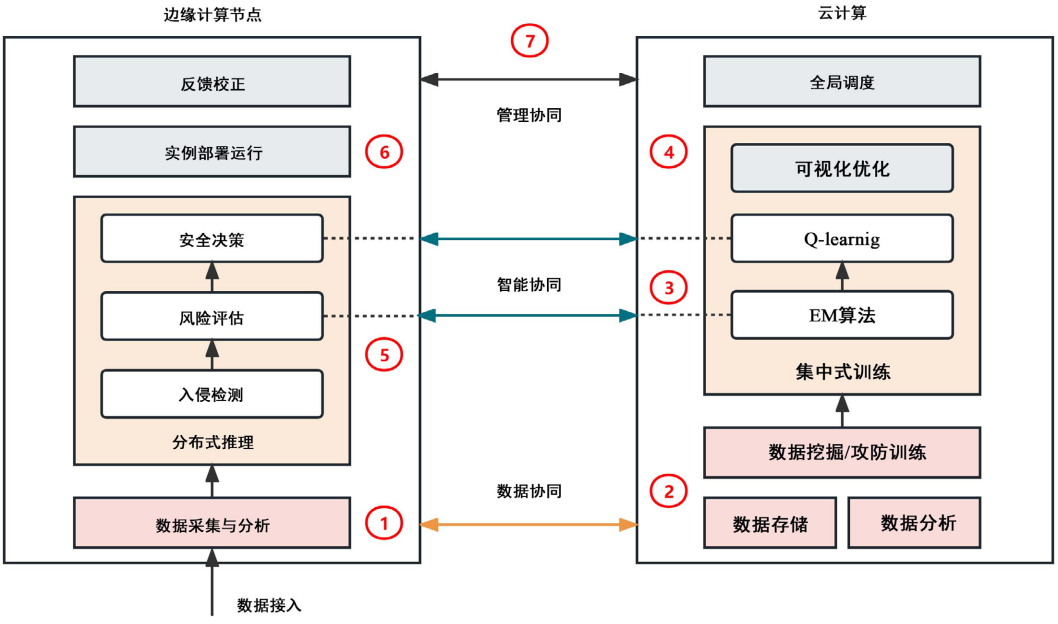

Figure 4. The connotation and process of edge cloud data collaboration
图 4. 边云数据协同的内涵和流程

数据协同支持边缘和云之间的数据的有序可控流动[6]。首先，边缘计算节点收集 ICPS 现场/终端数据，根据相应规则或模型对数据进行预处理，然后将处理结果和相关数据上传到云中，云端提供海量数

据的存储、分析和挖掘。考虑到工业现场运行数据量很大，但攻击数据相对较少，数字孪生等技术可用于构建云中物理实体的虚拟映射，通过对攻击和防御模拟来生成攻防数据集，这是执行算法之前的数据预处理过程，对应图 4 中的①和②。

智能协同可以简单理解为“训练在云端，部署在边缘”。首先，云端的集中式训练对应于图 4 的安全知识提取模块。主要有基于 MapReduce 的 EM 算法用于贝叶斯网络的参数学习和基于 Q-learning 强化学习用于随机博弈参数确定，此外，可视化技术结合专家经验可用来进一步优化模型，最后将模型下发给边缘节点，对应图 4 中的③和④。而边缘节点的分布式推理对应于图 4 中的本地安全决策模块。它基于云端训练的模型，根据实时的多源入侵检测证据，开展动态风险评估和安全策略决策等环节的智能推理，实现本地快速的安全决策，对应图 4 中的⑤。

管理协同是对于实际环境(实验室级仿真，工业现场部署等)开发的软件应用程序甚至硬件设备的管理调度。边缘计算节点提供应用程序部署和运行环境，它管理和调度每个节点的多个应用程序的生命周期，并同时将结果反馈到云端，对应图 4 中的⑥和⑦。云端提供了应用程序的开发和测试环境，应用程序的生命周期管理以及业务编排，此外云端接收边缘节点的反馈，并使用其全局视角来完成系统的整体监控和调度管理，对应图 4 中的⑦。

6.5. 基于边云协同的动态数据安全存储策略

与集中控制结构由云平台完成所有计算任务不同，为提高数据的分析精度，解决传感云系统中数据存储的隐私安全问题，并利用边缘计算提高存储效率与审计效率，提出了一种基于边云协同的动态数据安全存储策略，该策略采用基于数据隐私的数据分区策略，将完整的数据块划分为多个分片，进一步提高了在云和边缘共谋场景下的数据隐私性，同时设计了一种基于边缘的数据更新机制，利用边缘智能中的协同计算技术来支持同步。该策略的系统模型由三层组成：云端、边缘端和终端，如图 5 所示，采用了云边协同的集中－分布联合控制方式，能够充分利用云计算和边缘计算的协同优势，既实现了实现边缘云系统和云计算中心资源的充分利用，又可以满足边云数据协同安全性及实时性要求。

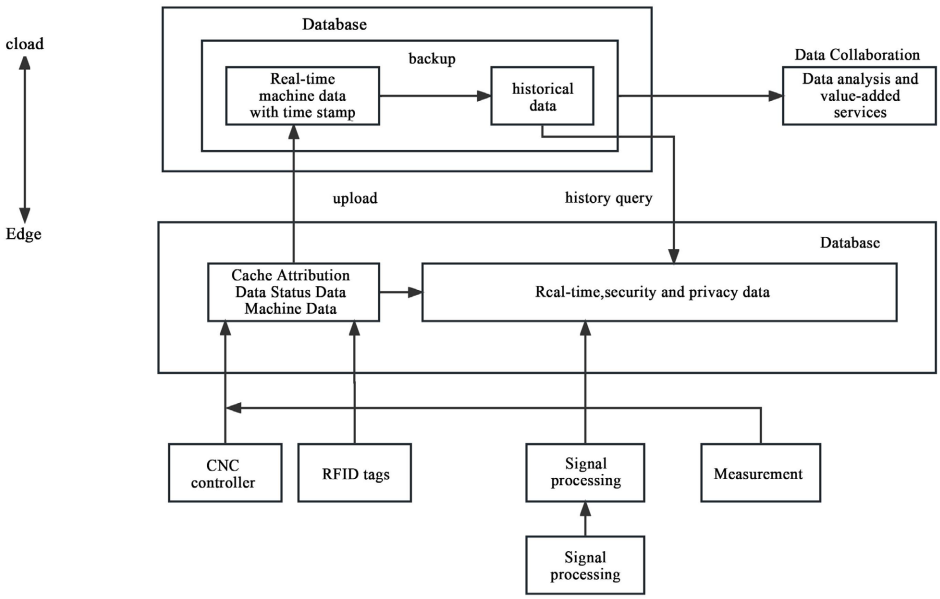

Figure 5. Implementation principle of dynamic data security storage strategy based on edge cloud collaboration
图 5. 基于边云协同的动态数据安全存储策略实现原理

7. 结语

工业云数据的存储问题一直是近些年的研究热点。国内外研究者们对其展开了研究，然而很多却牺牲了效率来换取安全性的提高。随着边缘计算的研究与发展，利用边缘计算的计算能力及存储能力并将其引入工业云成为了一种有效解决其自身安全效率问题的可行手段。本论文基于边缘计算范式，对工业云的存储安全问题与效率问题展开了递进研究，通过实验和理论分析证明了这种基于边云协同的动态数据安全存储策略模式是有效的。

参考文献

[1] 王秋华, 吴国华, 魏东晓, 等. 工业互联网安全产业发展态势及路径研究[J]. 中国工程科学, 2021, 23(2): 46-55.

[2] 伍育红, 胡向东. 工业互联网网络传输安全问题研究[J]. 计算机科学, 2020, 47(1): 360-363.

[3] 陈园, 陈铁明, 宋琪杰, 等. 一种面向工业互联网终端的通用安全服务框架[J]. 电信科学, 2020, 36(3): 19-26.

[4] 汪允敏, 李挥, 王菡, 等. 区块链在工业互联网标识数据管理策略研究[J]. 计算机工程与应用, 2020, 56(7): 1-7.

[5] 徐雪松, 金泳, 曾智, 等. 应用于工业互联网数据安全的分层轻量级高通量区块链方法[J]. 计算机集成制造系统, 2019, 25(12): 258-266.

[6] Climent, J.-J., Napp, D., Perea, C., *et al*. (2015) Maximum Distance Separable 2D Convolutional Codes. *IEEE Transactions on Information Theory*, **62**, 669-680. https://doi.org/10.1109/TIT.2015.2509075