CSA GCR cloud security alliance ®
GREATER CHINA REGION

基于IAM的数据安全技术研究

@2023 云安全联盟大中华区－保留所有权利。你可以在你的电脑上下载.储存.展示.查看及打印，或者访问云安全联盟大中华区官网（https://www.c-csa.cn）。须遵守以下：（a）本文只可作个人.信息获取.非商业用途；（b） 本文内容不得篡改；（c）本文不得转发；（d）该商标.版权或其他声明不得删除。在遵循 中华人民共和国著作权法相关条款情况下合理使用本文内容，使用时请注明引用于云安全联盟大中华区。

联盟简介

云安全联盟(Cloud Security Alliance,CSA)是中立、权威的全球性非营利产业组织,于2009年正式成立,致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识,推动数字安全产业全面发展。

云安全联盟大中华区(Cloud Security Alliance Greater China Region, CSA GCR)作为CSA全球四大区之一,2016年在香港独立注册,于2021年在中国登记注册,是网络安全领域首家在中国境内注册备案的国际NGO,旨在立足中国,连接全球,推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《基于 IAM 的数据安全技术研究》由 CSA 大中华区 IAM 工作组专家撰写，感谢以下专家的贡献：

工作组联席组长：

戴立伟　　于继万　　谢琴

主要贡献者：

谢江　　蔡国辉　　林鹭　　包宏宇　　郭立文　　李凌宇

参与贡献者:

崔崟　　黄鹏华　　鹿淑煜　　石瑞生　　王亮　　于振伟

张彬　　张淼　　周利斌

研究协调员：

蒋妤希

© 2023 云安全联盟大中华区版权所有

贡献单位：

安易科技（北京）有限公司
北京天融信网络安全技术有限公司
北京芯盾时代科技有限公司
杭州安恒信息技术股份有限公司
华为技术有限公司
江苏易安联网络技术有限公司
奇安信网神信息技术（北京）股份有限公司
三未信安科技股份有限公司
上海观安信息技术股份有限公司
上海物盾信息科技有限公司
深圳竹云科技股份有限公司

（以上排名不分先后）

关于研究工作组的更多介绍，请在 CSA 大中华区官网（https://c- csa.cn/research/）上查看。

在此感谢以上专家及单位。如此文有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱 research@c-csa.cn；国际云安全联盟 CSA 公众号

© 2023 云安全联盟大中华区版权所有

序言

随着数字化进程的加速推进，数据已成为现代企业最重要的资产之一。在大数据.云计算等技术发展以及数据要素市场化流通的背景下，数据的存储和使用方式发生了翻天覆地的变化，同时也带来了新的挑战——如何保护这些敏感的数据资产不被非法访问或者故意泄露？这就需要我们引入 IAM（Identity and Access Management）的解决方案。

IAM，即身份与访问管理，是一种用于管理和控制用户对资源访问的体系。它可以帮助企业建立一套完整的数据安全管理框架，确保只有得到授权的人员才能访问相关数据。基于 IAM 的数据安全管理不仅可以提高企业的信息安全水平，还能降低数据安全风险，提高企业运营效率。

《基于 IAM 的数据安全技术研究》一文以深入浅出的方式，详细阐述了 IAM 的基本原理.IAM 与数据安全的融合以及典型案例实践。我们将从 IAM 的基础概念开始，逐步探讨如何构建一个有效的数据安全访问控制体系，并通过案例分析，让大家更直观地理解 IAM 在数据安全中的应用。

我们希望通过本报告，让读者对 IAM 有更深入的理解，能够将 IAM 的理念和技术运用到自己的工作中，更好地保障网络数据和个人信息的安全。同时，我们也期待更多的人加入到 IAM 赋能数据安全的相关研究和实践中，共同推动数据安全技术的发展，为构建更加安全可靠的数字世界贡献力量。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

© 2023 云安全联盟大中华区版权所有

目录

致谢 2
序言 5
1 前言 10
1.1 研究背景 10
1.1.1 基础政策导向 10
1.1.2 数据安全形势严峻 10
1.2 研究范围 11
1.3 适用场景 11
2 数据安全合规 12
2.1 数据安全面临合规压力 12
2.2 我国数据安全相关法律法规 12
2.2.1 《中华人民共和国网络安全法》 12
2.2.2 《中华人民共和国数据安全法》 13
2.2.3 《中华人民共和国个人信息保护法》 13
2.2.4 《关键信息基础设施安全保护条例》 13
2.3 我国数据安全相关国家标准 14
2.3.1 安全要求类标准 14
2.3.2 实施指南类标准 18
2.3.3 检测评估类标准 20
3 数据安全风险 21
3.1 常见数据安全问题分析 21
3.1.1 数据泄露 21
3.1.2 数据篡改 22
3.1.3 数据勒索 23
3.2 数据处理活动安全风险 23
3.2.1 数据收集环节的安全风险 23
3.2.2 数据存储环节的安全风险 25
3.2.3 数据使用和加工环节的安全风险 25
3.2.4 数据传输环节的安全风险 26
3.2.5 数据公开安全风险 27
3.2.6 数据提供安全风险 28
4 数据安全与身份安全 28
4.1 数据处理活动中的数据安全技术措施 29
4.2 身份与访问管理（IAM）赋能数据安全 29
4.2.1 身份鉴别 29
4.2.2 授权管理 30
4.2.3 数据访问控制 31
4.2.4 数据安全审计 32
4.3 与数据安全相关的 IAM 技术挑战 33
4.3.1 身份管理挑战 33
4.3.2 访问控制挑战 34

© 2023 云安全联盟大中华区版权所有

4.3.3 审计溯源挑战 34
5 身份管理 35
5.1 身份定义 35
5.1.1 自然人身份 35
5.1.2 组织身份 36
5.1.3 设备身份 37
5.1.4 外部应用身份 38
5.2 身份数据收集 38
5.2.1 数据源同步 38
5.2.2 用户自注册 39
5.2.3 自动采集 40
5.2.4 人工录入 40
5.2.5 自助维护 40
5.3 身份认证 40
5.3.1 身份认证凭据 40
5.3.2 用户认证策略 41
5.3.3 身份认证技术 42
6 数据访问控制 43
6.1 数据权限管理 44
6.1.1 权限管理的基本要素 44
6.1.2 权限管理系统设计 47
6.1.3 用户管理 47
6.1.4 角色管理 48
6.1.5 权限管理 49
6.2 数据访问控制模型 50
6.2.1 自主访问控制Discretionary Access Control，DAC） 50
6.2.2 强制访问控制（Mandatory Access Control，MAC） 52
6.2.3 基于角色的访问控制（Role-Based Access Control, RBAC） 55
6.2.4 基于属性的访问控制（Attribute-Based Access Control, ABAC） 60
6.2.5 风险自适应访问控制（(RAdAC,Risk-Adaptable Access Control)） 65
6.2.6 下一代访问控制（NGAC） 66
7 数据安全审计 69
7.1 审计日志分类 70
7.1.1 单次数据使用审计日志 70
7.1.2 单会话内多次数据使用审计日志 72
7.2 审计日志获取能力 73
7.2.1 精准解析协议能力 73
7.2.2 加密算法解析能力 73
7.2.3 用户名补偿审计能力 73
7.2.4 三层关联能力 74
7.3 审计分析 74
7.3.1 自动分析 74

© 2023 云安全联盟大中华区版权所有

7.3.2 人工干预分析 75
8 用零信任实现数据安全 76
8.1 零信任介绍 76
8.2 零信任的实现 78
8.3 发展与展望 79
9 典型应用场景 80
9.1 政务领域典型场景 80
9.1.1 政务领域数据使用场景与访问控制威胁分析 80
9.1.2 政务领域身份管理与访问控制能力分析 80
9.1.3 政务领域数据访问控制防护场景与技术说明 81
9.2 企业领域典型场景 82
9.2.1 企业领域数据使用场景与访问控制威胁分析 82
9.2.2 企业领域身份管理与访问控制能力分析 86
9.2.3 企业领域数据访问控制防护场景与技术说明 87
10 数据安全新技术展望 89

© 2023 云安全联盟大中华区版权所有

1 前言

1.1 研究背景

2022 年 1 月 12 日，国务院发布《“十四五”数字经济发展规划》，强调数据要素是数字经济深化发展的核心引擎，到 2025 年数字经济走向全面扩展期，数字经济核心产业增加值占国内生产总值比重达到 10%，数据要素市场体系初步建立。2023 年 1 月，工信部等十六部门联合印发《关于促进数据安全产业发展的指导意见》，提出到 2025 年，数据安全产业规模超过 1500 亿元，到 2035 年，数据安全产业进入繁荣成熟期。2023 年 3 月《数字中国建设整体布局规划》要求数字基础设施高效联通，数据资源规模和质量加快提升，数据要素价值有效释放。2023 年 3 月《党和国家机构改革方案》方案提出组建国家数据局，负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，推进数字中国.数字经济.数字社会规划和建设等，推进数据要素基础制度建设。

数据已被视为国家基础性战略资源，各行各业的大数据应用正迅猛发展，但随之而来的数据安全问题也日益加剧，有时甚至限制了大数据应用的发展。基于此，无论是国家机关还是企事业单位，都在加紧数据安全体系的建设。数据安全是数据经济发展的必要条件，是促进数据分享.产生数据流动价值的基本保障。

1.1.1 基础政策导向

《中华人民共和国计算机信息系统安全保护条例》《网络安全法》《信息安全等级保护管理办法》《国家密码法》《关键信息基础设施安全保护条例》《数据安全法》《个人信息保护法》《关于促进数据安全产业发展的指导意见》等法律法规和政策文件也要求推动信息网络空间安全治理，并提出相关的规范与要求，将信息安全检查常态化。完整的识别组织内部的信息资产，并制定覆盖所有网络设备的信息安全策略，只有这样才能尽可能保护数据资产的安全性。

1.1.2 数据安全形势严峻

近几年政府.企业数字化转型进程不断加快，但随之而来的数据安全问题愈发严重。如 Facebook 在 2021 年曾遭遇数据泄露，其中 5.33 亿条数据记录被曝

© 2023 云安全联盟大中华区版权所有

光；印度某政府网站 800 万核酸检测报告被泄露。同时在国内此类事件也屡见不鲜，2023 年某大学学生创建颜值打分平台，学生的照片.姓名.学号.学院.籍贯.生日信息泄露；两名航空公司员工在 2020 年至 2021 年间利用职务之便，向粉丝出售明星个人信息；2020 年以来，有关电信运营商.航空公司等单位内网和信息系统先后多次出现越权登录.数据外传等异常网络行为。

1.2 研究范围

根据国家标准 GB/T 35274-2023《信息安全技术 大数据服务安全能力要求》，数据处理安全能力涵盖数据收集.数据存储.数据使用.数据加工.数据传输.数据提供.数据公开以及数据销毁等活动。而身份管理与访问控制是数据要素安全.合理.合法.合规流动与分享的基础条件，本研究报告重点关注身份与访问管理保障数据使用主客体身份安全.数据权限控制.数据使用身份风险以及事后审计等内容。

(1) 数据采集.存储.传输.使用过程中面临的身份安全问题

(2) 身份管理与访问控制在数据生命周期管理中可带来作用与价值

(3) 重点讨论数据访问控制策略与技术

(4) 结合零信任体系探讨数据安全保证模式

(5) 描述典型业务场景下，身份管理与访问控制如何保障数据正确安全使用

1.3 适用场景

本次研究成果关注身份管理与访问控制在数据安全中主客体身份安全管理.数据访问权限控制.数据使用风险管控等相关内容，可结合数据分级分类.数据加解密.DLP 数据防泄漏.数据情报获取等内容形成数据整体安全体系，保障数据安全流转，促进数字经济发展。

© 2023 云安全联盟大中华区版权所有

2 数据安全合规

2.1 数据安全面临合规压力

随着数字经济的发展，数据逐渐成为了经济增长的强大动力及核心资产，随着我国乃至全球数字经济的兴起，数据从一种信息的载体，转化成了具有独立经济价值，乃至国家安全价值的一种利益形态。随着国家层面对数据管理和个人信息保护需求的激增，社会公众对隐私及个人信息保护意识的加强，在过去几年中，在全球范围内各国纷纷出台相关法律法规，相关的监管活动也呈现出常态化趋势。

数据安全新监管趋势及行业趋势对数据安全管理提出了新的挑战和要求，政府. 企业等组织机构做好数据安全工作面临着较大的合规压力，例如数据处理安全. 个人信息保护. 数据跨网交换安全及数据出境安全等方面。

2.2 我国数据安全相关法律法规

近年来，随着《网络安全法》《数据安全法》《个人信息保护法》等上位法的发布，数据要素掌控和利用过程中面临刚性的数据安全合规要求。

从我们国家来看，从 2017 年《网络安全法》的施行开始，到 2021 年《数据安全法》和《个人信息保护法》相继的生效和施行，三部法律法规构成了我国网络安全和数据合规领域的基本法律规则框架，形成中国特色的三法并行的数据安全法律框架。

三部法律虽然明确了我国网络安全. 数据安全. 个人信息保护的顶层设计，但是在具体落地层面还有不少空白和规范细则需要完善。中央网信办. 工信部等多个部门针对热点. 重点问题，制定了相关领域的规章制度和指导文件，国家和各行业. 领域的数据安全标准体系也在不断健全当中。

2.2.1 《中华人民共和国网络安全法》

2016 年 11 月，第十二届全国人民代表大会常务委员会通过了《网络安全法》，2017 年 6 月 1 日正式施行。《网络安全法》中将“网络数据”定义为“通过网络收集. 存储. 传输. 处理和产生的各种电子数据。”要求“建设. 运营网络或者通

© 2023 云安全联盟大中华区版权所有

过网络提供服务，应当依照法律.行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全.稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性.保密性和可用性。”并“鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。”

2.2.2 《中华人民共和国数据安全法》

2021 年 6 月《数据安全法》发布，将个人.企业和公共机构的数据安全纳入保障体系，确立了对数据领域的全方位监管.治理和保护，既约束了数据的非法采集和滥用，又保护了数据提供方和民众的信息使用，推动以数据开放.数据保护.数据流动等为基础的数据规则进一步完善。作为我国数据安全领域内的基础性法律和我国国家安全领域内的重要法律，给企业数据经营合规.以及进一步的数据资产化治理与发展提供指引。《数据安全法》中给出了“数据安全”的定义，为“通过采取必要措施，确保数据处于有效保护和合法利用状态，以及具备保障持续安全状态的能力。”《数据安全法》中对于“数据处理”则定义为“包括收集.存储.使用.加工.传输.提供.公开等”7 个环节。

2.2.3 《中华人民共和国个人信息保护法》

2021 年 8 月《个人信息保护法》发布，规定个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息；个人信息的处理包括个人信息的收集.存储.使用.加工.传输.提供.公开等活动。《个人信息保护法》确立了个人信息处理应遵循的原则，强调处理个人信息应当采用合法.正当的方式，具有明确.合理的目的，限于实现处理目的的最小范围，公开处理规则，保证信息准确，采取安全保护措施等，并将上述原则贯穿于个人信息处理的全过程.各环节。

2.2.4 《关键信息基础设施安全保护条例》

2021 年 7 月 30 日，《关键信息基础设施安全保护条例》发布。条例涵盖总则.关键信息基础设施认定.运营者责任义务.保障和促进.法律责任等诸多方面，

© 2023 云安全联盟大中华区版权所有

旨在保障关键信息基础设施安全，维护网络安全。条例要求关键信息基础设施运营者应当“在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性.保密性和可用性。”并应成立专门安全管理机构，负责“履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度。”

2.3 我国数据安全相关国家标准

随着数字经济发展加速，数据要素的战略地位不断抬升，数据安全保护需求也日益旺盛。国家在加强对数据安全监管的同时，也加大了数据安全相关国家标准的制定和发布速度，方便政府.企业等组织机构在实践中进行参考，使数据安全治理和保护工作更加规范和更容易落地。截至目前，国家已经正式发布的数据安全相关标准已经超过 20 项，仅 2022 年发布的就有 10 余项。

数据安全系列国家标准分为三个类别：安全要求类标准.实施指南类标准和检测评估类标准，组织机构可根据实际需要有选择的参考采用。其中安全要求类标准如 GB/T 41479—2022《网络数据处理安全要求》.GB/T 35274—2023《信息安全技术 大数据服务安全能力要求》.GB/T35273—2020《信息安全技术 个人信息安全规范》和 GB/T 39477—2020《政务信息共享数据安全技术要求》等；实施指南类标准如 GB/T 27973—2019《大数据安全管理指南》.GB/T 39725—2020《健康医疗数据安全指南》和 GB/T 42447—2023《电信领域数据安全指南》等；检测评估类标准如 GB/T 37988—2019《数据安全能力成熟度模型》。以下分别进行简要介绍。

2.3.1 安全要求类标准

2.3.1.1 《信息安全技术 网络数据处理安全要求》（GB/T 41479—2022）

该标准规定了网络运营者开展网络数据收集.存储.使用.加工.传输.提供.公开等数据处理的安全技术与管理要求，适用于网络运营者规范网络数据处理，

© 2023 云安全联盟大中华区版权所有

以及监管部门.第三方评估机构对网络数据处理进行监督管理和评估。

该标准实质是对《网络安全法》《数据安全法》《个人信息保护法》所提出的网络服务提供者.重要数据处理者.个人信息处理者（即该标准所称的网络运营者）在开展数据处理经营活动中，针对数据处理活动全流程的具体技术要求和管理要求的规定。首先，从数据识别.数据分类分级.风险防控以及审计追溯方面对数据处理安全提出了总体要求；其次，对数据处理经营活动涉及的各个环节的安全技术要求做了具体的规定；最后，从数据安全责任人.人力资源能力保障与考核.事件应急处置三个方面提出了数据处理安全管理要求。

其中“5.12 访问控制与审计”提出：网络运营者开展数据处理活动时应基于数据分类分级，明确相关人员的访问权限，防止非授权访问；对重要数据.个人信息的关键操作（例如批量修改.拷贝.删除.下载等），应设置内部审批和审计流程，并严格执行。

2.3.1.2 《信息安全技术 大数据服务安全能力要求》（GB/T 35274—2023）（代替 GB/T 35274—2017）

国家标准 GB/T 35274-2017《大数据服务安全能力要求》于 2017 年首次发布。该标准规定了大数据服务提供者应具有的组织相关基础安全能力和数据生命周期相关的数据服务安全能力，适用于政府部门和企事业单位建设大数据服务安全能力，也适用于第三方机构对大数据服务提供者的大数据服务安全能力进行审查和评估。

2021 年信安标委立项对该标准进行修订，并于 2023 年 8 月 6 日正式发布，2024 年 3 月 1 日起实施。标准修订采用了数据安全风险管理的思路，基于数安法.个保法等法律法规要求和国内大数据服务提供者的最佳实践，在参考信息安全管理体系和网络安全等级保护制度基础上，制定了大数据服务提供者的大数据服务安全能力要求，以促进我国大数据服务产业的安全治理.安全监管以及个人信息和重要数据安全保护等。

© 2023 云安全联盟大中华区版权所有

该标准面向有大数据平台.大数据应用和大数据服务所需数据资源的组织。从大数据组织管理安全能力.大数据处理安全能力和大数据服务安全风险管理能力三个方面规定了大数据服务提供者的大数据服务安全能力要求，其中：

a）大数据组织管理安全能力：按照信息安全管理体系要求制定大数据安全策略与规程，从大数据服务组织与人员的安全管理，以及大数据服务所需的数据资产与系统资产管理视角制定数据安全管理等制度，满足大数据服务组织管理安全合规及数据安全风险管控要求；

b）大数据处理安全能力：针对数据收集.存储.使用.加工.传输.提供.公开.销毁等数据处理活动，从大数据平台和大数据应用业务及技术层面采取数据保护措施，满足大数据服务中数据处理活动相关的数据保护要求；

c）大数据服务安全风险管理能力：按照大数据服务中数据业务流转过程和数据处理活动安全保护要求，从风险识别.安全防护.安全监测.安全检查.安全响应和安全恢复六个环节建立大数据服务安全风险管理能力，采取风险应对措施使大数据服务及其数据资产始终处于有效保护.合法利用状态，保障大数据系统运营者所提供的大数据服务的可持续性。

该标准多处提及身份鉴别.授权管理.访问控制.审计监控等安全要求，对于开展大数据服务所涉及的身份安全与数据访问控制技术研究具有较强的指导作用。

2.3.1.3 《信息安全技术 个人信息安全规范》（GB/T 35273—2020）（代替 GB/T 35273-2017）

该标准针对个人信息面临的非法收集.滥用.泄漏等安全问题，规范各类组织在开展收集.存储.使用.共享.转让.公开披露.删除等个人信息处理活动时的相关行为，旨在最大程度地保障个人的合法权益和社会公共利益。

该标准对于如何判定个人信息及个人敏感信息给出了具体的方法和详细的示例，并对个人信息控制者（有能力决定个人信息处理目的.方式等的组织或个

© 2023 云安全联盟大中华区版权所有

人）在确保个人信息安全方面应遵循的基本原则.行为约束和应采取的保护措施等做出了明确的规定。

其中，对于个人信息控制者应采取的个人信息访问控制措施要求包括：

a）对被授权访问个人信息的人员，应建立最小授权的访问控制策略，使其只能访问职责所需的最小必要的个人信息，且仅具备完成职责所需的最少的数据操作权限；

b）对个人信息的重要操作设置内部审批流程，如进行批量修改.拷贝.下载等重要操作；

c）对安全管理人员.数据操作人员.审计人员的角色进行分离设置；

d）确因工作需要，需授权特定人员超权限处理个人信息的，应经个人信息保护责任人或个人信息保护工作机构进行审批，并记录在册；

e）对个人敏感信息的访问.修改等操作行为，宜在对角色权限控制的基础上，按照业务流程的需求触发操作授权。

2.3.1.4 《信息安全技术 政务信息共享 数据安全技术要求》（GB/T 39477—2020）

该标准从政务信息共享交换中的数据安全与保护出发，依据数据分类与分级原则及数据安全能力成熟度模型，规定了政务信息共享过程中共享数据准备.共享数据交换.共享数据使用阶段的数据安全技术要求以及相关基础设施的安全技术要求，用于指导政务信息共享交换数据安全体系建设，增强政务信息共享交换的数据安全保障能力，解决政务信息共享交换环节数据泄露.数据滥用等数据安全问题，对动态流转场景下的政务数据应用具有普适性和指引性。

该标准所提出的政务共享数据安全技术要求框架由数据安全技术要求和基础设施安全技术要求两部分组成。图 2-1 展示了共享数据准备.共享数据交换.共享数据使用等三个阶段分别涉及的数据安全技术措施：

© 2023 云安全联盟大中华区版权所有

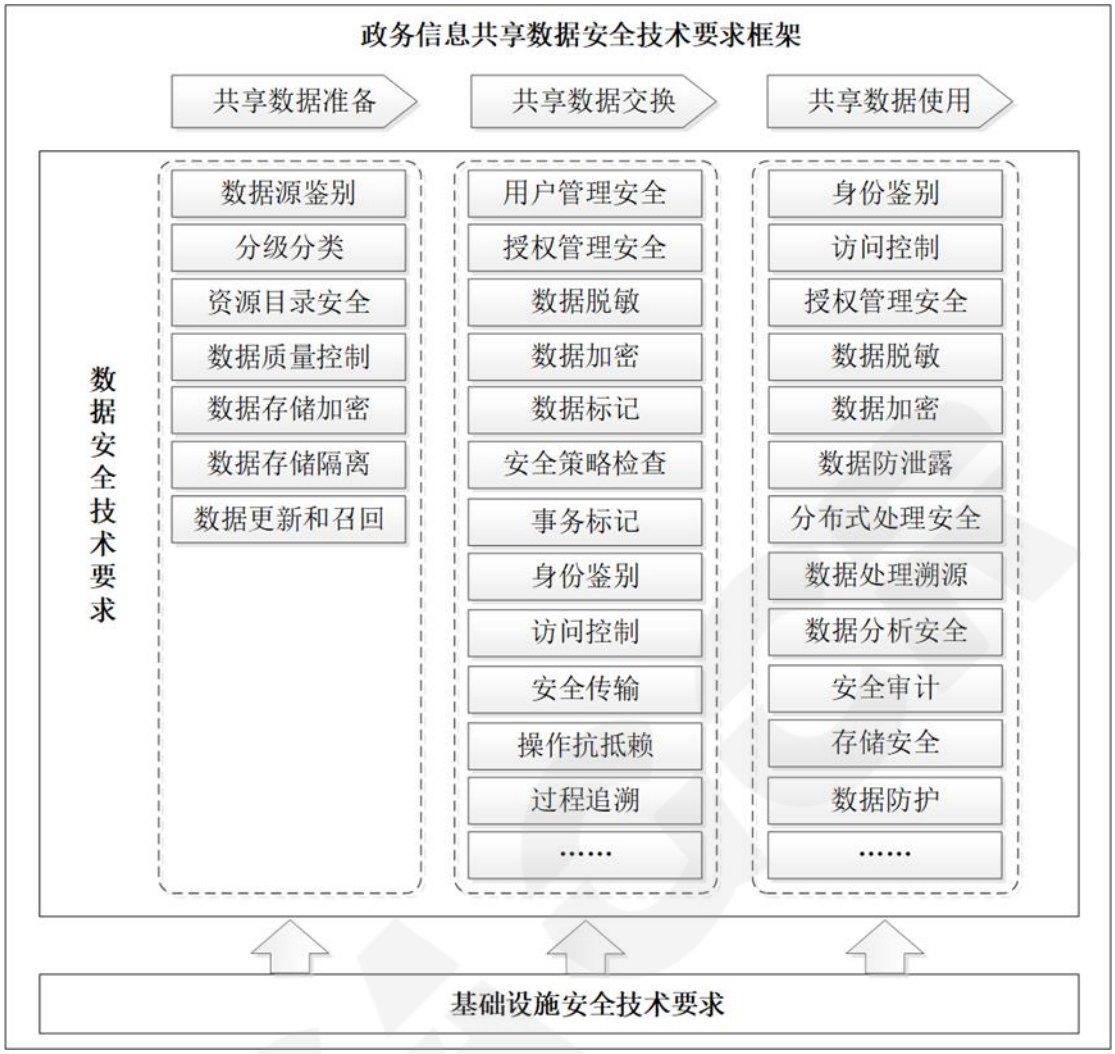


图 2-1 政务信息共享数据安全技术要求框架

2.3.2 实施指南类标准

2.3.2.1 《信息安全技术 大数据安全管理指南》（GB/T 37973—2019）

该标准提出了大数据安全管理基本原则，规定了大数据安全需求. 数据分类分级. 大数据活动的安全要求以及如何评估大数据安全风险，可指导拥有. 处理大数据的企业. 事业单位. 政府部门等组织做好大数据的安全管理. 风险评估等工作，加强数据采集. 存储. 处理. 分发. 删除等环节的技术和管理措施，使数据的安全风险可控，确保组织能够有效. 安全地应用大数据。

其中“最小授权”原则是指“控制大数据活动中的数据访问权限，保证在满足业务需求的基础上最小化权限”，具体要求包括：赋予数据活动主体的最小操

作权限和最小数据集；制定数据访问授权审批流程，对数据活动主体的数据操作权限和范围变更制定申请和审批流程；及时回收过期的数据访问权限。

另外，针对“数据处理”活动的安全要求中相应提出了“遵循最小授权原则，提供数据细粒度访问控制机制”。

2.3.2.2 《信息安全技术 电信领域数据安全指南》（GB/T 42447—2023）

该标准给出了开展电信领域数据处理活动的安全原则.通用安全措施，及在实施数据收集.存储.使用加工.传输.提供.公开.销毁等过程中宜采取的相应安全措施，适用于指导电信数据处理者开展数据安全保护工作，也适用于指导第三方机构开展电信数据安全评估工作。

其中对于“权限管理”的一般措施要求包括：

(1) 对开展数据处理活动的平台系统账号，明确审批流程和操作要求；

(2) 遵循安全策略和最小授权原则，合理界定数据处理权限，设置相关岗位角色并确保职责分离，形成并定期更新数据处理权限记录表；

(3) 对开展数据处理活动的平台系统,使用技术手段进行权限管理和账号管理,同时控制超级管理员权限账户数量；

(4) 涉及数据重大操作的，采取多人审批授权或操作监督方式。

增强措施要求包括:

(1) 明确重要数据和核心数据处理权限审批.登记方式和流程，控制权限范围，留存登记.审批记录；

(2) 对开展重要数据和核心数据处理活动的平台系统，具备基于 IP 地址.账号与口令等的用户身份认证和多因子认证的能力,并配备权限管理保

© 2023 云安全联盟大中华区版权所有

障功能。

2.3.2.3 《信息安全技术 健康医疗数据安全指南》（GB/T 39725—2020）

该标准给出了健康医疗数据控制者在保护健康医疗数据时可采取的安全措施，主体内容包括分类体系.使用披露原则.安全措施要点.安全管理指南.安全技术指南和典型场景数据安全等内容，适用于指导健康医疗数据控制者对健康医疗数据进行安全保护，也可供健康医疗.网络安全相关主管部门以及第三方评估机构等组织开展健康医疗数据的安全监督管理与评估等工作时参考。

该标准提出“可以根据数据保护的需要进行数据分级，对不同级别的数据实施不同的安全保护措施，重点在于授权管理.身份鉴别.访问控制管理。”并针对各类数据使用的典型应用场景下所采取的重点数据安全措施提供了详细的指导。

2.3.3 检测评估类标准

2.3.3.1 《信息安全技术 数据安全能力成熟度模型》（GB/T 37988—2019）

该标准给出了组织数据安全能力的成熟度模型架构，从组织建设.制度流程.技术工具.人员能力 4 个能力维度，按照 1-5 级成熟度，规定了数据采集安全.数据传输安全.数据存储安全.数据处理安全.数据交换安全.数据销毁安全.通用安全的成熟度等级要求，适用于对组织数据安全能力进行评估，也可作为组织开展数据安全能力建设时的依据。

该标准适合用来作为评估组织数据安全能力的方法和标准，在组织开展数据安全能力建设的过程中被用作参考目标和依据。基于该标准的数据安全能力评估结果，可以鼓励数据在同等安全能力水平的组织间安全有序流动，或者流向能力水平更高的组织，避免数据流向低安全能力的组织。

其中“9.3 PA12 数据正当使用”部分，从等级 3 开始提出了身份安全相关

© 2023 云安全联盟大中华区版权所有

的技术工具要求，并从等级 3 到等级 5 逐级增强。如下所示：

等级 3（充分定义）：应依据合规要求建立相应强度或粒度的访问控制机制，限定用户可访问数据范围；应完整记录数据使用过程的操作日志，以备对潜在违约使用者责任的识别和追责。

等级 4（量化控制）：应具备技术手段或机制，对数据滥用行为进行有效的识别、监控和预警。

等级 5（持续优化）：应研究并利用新的技术提升对用户的身份及访问管理能力，并通过风险监控与审计实现对数据使用的安全风险进行自动化分析和处理。

3 数据安全风险

3.1 常见数据安全问题分析

随着数字经济的快速发展，数据已经成为基础性资源和战略性资源，是决定数字经济发展水平和竞争力的核心资源。另一方面，近年来随着企业数字化转型，数据集中化、数据量大、数据价值高等特点的安全风险更加凸显。数据安全形势日益严峻，高价值数据泄漏、个人隐私信息滥用情况突出，针对数据的攻击、窃取、劫持、滥用等不断推陈出新。

3.1.1 数据泄露

根据 Verizon 发布的《2021 年数据泄露调查报告》可以看到，绝大多数的数据泄露事件是因为数据存储安全、数据处理安全和数据交换安全这 3 个方面安全措施薄弱，主要面临以下安全问题：

(1) 参与数据资源访问的主体复杂多样。涉及到数据交互的主体可分为人和非人实体（BYOD、IoT 设备、应用程序等），业务场景也从用户访问资源的场景拓展到泛终端访问场景、应用访问应用场景等，业务流程复杂

(2) 跨业务的数据调用大幅增加。传统基于网络边界的安全防护体系无法对

© 2023 云安全联盟大中华区版权所有

应用层跨业务数据交换，提供足够的防护能力和细粒度的访问控制。

(3) 数据访问请求的主体包含发生可能来自不同的部门或者外部人员，访问的区域也从内网逐渐扩散到互联网.云上等多种网络环境，现有的数据安全防护手段难以判定数据访问人员的身份可信度，默认信任访问用户。

(4) 数据访问主体可能随时随地在不同的终端设备上发起访问，现有的数据安全防护手段难以评估访问终端的设备可信度，默认信任访问终端。

(5) 访问过程中，难以有效地度量访问过程中可能发生的行为并进行持续信任评估，并根据信任程度动态调整访问权限。

(6) 缺少对敏感数据流动监控的措施，无法详细审计敏感数据被终端用户审计的情况，对可能存在的敏感数据泄露风险难以预警。

3.1.2 数据篡改

可以看到，绝大多数的数据篡改事件是因为错误.系统故障.意外修改等方面安全措施薄弱，主要面临以下安全问题：

1. 计算机和存储故障可能损害数据和损害数据完整性。

确保选定的存储基础设施是通过适当的冗余和将重要数据存档作为服务的一部分来构建的。建议使用完整性验证软件来验证和验证数据。

2. 数据损坏和数据篡改

由计算机或存储系统故障引起的数据变化，以及由恶意个人或恶意软件引起的数据变化。用户在修改重要数据时使用版本控制软件维护其存档副本。确保所有数据都受到防病毒软件的保护。维护基于角色的所有数据访问控制，基于最小权限原则，已知的工作功能和业务需求。测试使用完整性检查软件监控和报告关键数据的变化。保持对获取和管理数据的个人的培训。

© 2023 云安全联盟大中华区版权所有

3. 数据意外修改

缺少数据完整性和意外修改的最常见原因可能是用户故意更改数据，或者用户错误输入数据。

3.1.3 数据勒索

勒索攻击.撞库攻击等专门针对数据层面的攻击威胁愈演愈烈，数据非法收集.明文传输.恶意挖掘.滥采滥用.黑产交易.数据资产暴露等风险事件时有发生，因弱口令.漏洞.SQL 注入等网络安全问题导致的数据安全风险广泛存在。

当前的勒索软件已不再是简单针对单一终端的攻击。随着勒索团伙专注度的提升，他们已经将目标放到大型企业，并在锁定核心系统或核心数据前处于潜伏的状态。当企业中勒索软件后，大部分用户选择通过备份恢复数据。这个时候，备份数据是否完整.可靠.能够立即使用，就成为能否恢复企业业务的关键。通常用户会认为拥有数据备份系统，当基于数据的勒索攻击发生时，即可通过备份数据完成数据恢复。然而现阶段的勒索软件会在攻击备份数据后再大规模爆发，让用户无法使用备份数据，从而逼迫用户必须交纳赎金。因此，备份数据的安全性也应成为用户的关注点。

3.2 数据处理活动安全风险

数据安全风险处理活动围绕收集.存储.使用.加工.传输.提供.公开等 7 个环节展开分析，对每个环境进行安全风险描述和阐述，具体内容如以下章节。

3.2.1 数据收集环节的安全风险

1.数据收集过程的安全风险

数据收集一般采用人工或机器自动化方式。人工方式主要是以录入数据或导入数据或手工设置数据接口配置或 API 接口；机器自动化方式，使通过工具或 API 接口，自动读取源头数据，而写入目标系统或数据存储空间设备中。另外数据收集过程中如果采用人工方式，很容易被操作者窥探到数据或被留存，特别是

© 2023 云安全联盟大中华区版权所有

导入操作或配置数据接口 API，操作者获得操作权限后，很容易看得到数据。自动化录入数据，主要存在目标和源数据之间存在认证和鉴权行为，或者中断后能从配置文件中读取认证和授权，这个过程容易引发数据泄露风险，具体在收集过程安全风险包括以下几个方面：

(1) 恶意攻击所导致的安全风险，例如：恶意代码注入.数据无效写入.账号操控.配置文件被盗取.认证和授权不充分等所导致的。

(2) 数据泄露所导致的安全风险，例如：敏感数据丢失所导致的。

(3) 数据质量过低导致的安全风险，例如：数据无效写入.无作为或操作失误所导致的。

(4) 数据篡改导致的安全风险，例如：数据污染.非法数据源投毒所导致的。

(5) 越权或滥用所导致的安全风险，例如：数据分类分级或标记错误.采集数据过度获取.数据源与目标之间连接异常行为未做二次认证所导致的。

(6) 违法获取数据所导致的安全风险，例如：数据窃取.超范围收集所导致的。

(7) 手工方式收集数据，非法留存或窥探数据而导致泄密风险。

2. 数据收集活动的安全管理风险

在数据收集活动中，主要存在人员身份识别.鉴别.授权的风险，确保操作者是可信的人员，并且该人员能按照要求操作，而不允许对数据进行截留.备份.存储等行为，甚至是额外增加授权账户而导致数据泄露；整个过程需要技术上的认证.授权.监测.审计等保障对数据操作的安全。

3. 数据收集平台的安全风险

数据收集平台的安全风险是指平台自身的安全可信和可控，对收集的数据的

© 2023 云安全联盟大中华区版权所有

接口.操作员.导入内容等有安全措施，保障导入或接入的数据是在合法的用户下操作；另外平台外的或非授信的用户无法干扰或替换，而通过认证和授权后，数据能按照既定的路径导入到指定的问题。

3.2.2 数据存储环节的安全风险

1.数据存储过程的安全风险

常见的数据存储过程安全风险包括以下几个方面：

(1) 数据泄露：包括数据窃取.数据不可控.存储数据丢失.未授权爬取等所导致的风险。

(2) 数据被篡改：包括数据篡改.数据破坏所等导致的风险。

(3) 数据越权或滥用：包括数据分类或标记错误.权限滥用.过多特权账号.非授权访问或数据误操作所导致的风险。

2.数据存储活动的安全管理风险

数据存储活动中的安全管理风险主要源于安全管理不到位，例如：内部人员误操作.存储平台权限管理失效；缺少对第三方云平台.数据中心等的管控等所导致的风险。

3.2.3 数据使用和加工环节的安全风险

1.数据使用和加工过程的安全风险

常见的数据使用和加工过程安全风险包括以下几个方面：

(1) 恶意攻击：包括注入攻击.恶意盗取.中间人攻击所导致的风险。

(2) 数据被窃取：包括在使用加工过程中缺少监督管控机制，导致数据窃取所导致的风险。

© 2023 云安全联盟大中华区版权所有

(3) 数据越权或滥用：包括违反法律.法规规定的目的和范围使用加工数据，数据越权使用.使用权限混乱.数据过度获取.信任滥用威胁.分析结果滥用.违规操作所导致的风险。

(4) 数据泄露：包括数据不可控.敏感元数据未脱敏使用，去标识化或匿名化策略失效，对不同来源的数据整合后使得敏感数据被还原.泄露所导致的风险。

(5) 违法加工使用数据：未按有关规定或约定期限要求，超期使用有关数据所导致的风险。

(6) 数据技术处理不当，导致数据查询操作，出现水平越权.数据留存.数据截留存储等行为，终端设备管控不严格，导致留存的数据被拷贝或移动到其他存储设备，从造成数据泄露。

(7) 数据存储设备或运行设备因故障或使用生命周期终止后，未对存储设备进行数据处理，导致数据对外泄露。

2.数据使用和加工活动的安全管理风险

数据使用和加工活动中常见的安全管理风险主要源于安全管理不到位，例如：内部人员误操作.恶意授权等所导致的风险。

3.2.4 数据传输环节的安全风险

1.数据传输过程的安全风险

常见的数据传输过程安全风险包括以下几个方面：

(1) 数据泄露：包括数据窃取.网络监听.数据从高敏感区域传输到低敏感区域.重要数据明文传输.隐藏的通信隧道传输等情形所导致的数据泄露风险。

© 2023 云安全联盟大中华区版权所有

(2) 数据被篡改：包括数据篡改.数据传输缺乏完整性验证.伪装通信代理或通信对端等数据篡改所导致的数据被篡改风险。

2.数据传输活动的安全管理风险

数据传输活动中的安全管理风险主要源于管理不到位，例如：运维管理人员误操作.数据传输不合法等。

3.数据传输环境的安全风险

数据传输环境的安全风险包括未使用加密通道传输数据.使用弱加密算法加密等带来的数据被泄露.篡改的风险。

3.2.5 数据公开安全风险

1.数据公开过程的安全风险

常见的数据公开安全风险包括以下几个方面：

(1) 违反相关法规政策要求：包括国家和行业发布新的法律法规和行业规章，调整了数据公开的方式.受众范围.访问权限，导致公开目录未及时更新，或已公开的数据与现行合规要求不一致所导致的风险。

(2) 数据公开评估能力确实：包括缺少相关手段评估已公开数据或将公开数据，对国家安全.公共利益或者个人.本单位合法权益造成影响所导致的风险。

(3) 缺少数据防爬取手段：包括缺少公开的数据异常访问或异常操作检测手段， 如已公开的数据被超过设定阈值的频率访问，或访问操作超出设定的访问权限（如增加.删除.编辑.读取.导出等）等所导致的风险。

2.数据公开活动的安全管理风险

数据公开活动常见的安全管理风险主要源于安全管理不到位，例如：数据公

© 2023 云安全联盟大中华区版权所有

开的管理制度缺少或不完善，未对数据公开的方式.受众范围.访问权限，或本单位的数据公开情况底数不清并且未形成数据公开目录等所导致的风险。

3.2.6 数据提供安全风险

1.数据提供过程的安全风险

常见的数据提供过程安全风险包括以下几个方面：

(1) 数据泄露：包括未对数据进行去标识化等脱敏处理.数据提供过程缺少有效数据传输安全保护机制.接收方未对接收到的数据进行访问控制或有效保护所导致的风险。

(2) 违反数据合规提供原则：包括数据提供不具备正当.合法目的，提供个人信息缺少用户的单独同意，超出约定的处理目的.方式或范围处理数据，接收方缺少对接收数据存储期限.存储地点和到期后处理方式的明确规定所导致的风险。

(3) 越权或滥用：包括共享权限混乱.数据过度获取.数据不可控所导致的风险。

(4) 恶意攻击：包括中间人攻击.篡改攻击.重放攻击.数据信息监听.资源劫持.网络拒绝.撞库攻击所导致的风险。

2.数据提供活动的安全管理风险

数据提供活动中常见的安全管理风险主要源于安全管理不到位，例如：缺少对数据提供的安全管理制度.流程.内部人员权限管理失效.访问控制失效等所导致的风险。

4 数据安全与身份安全

© 2023 云安全联盟大中华区版权所有

4.1 数据处理活动中的数据安全技术措施

针对数据处理活动的不同环节中可能面临的安全风险，通常需要综合采用多种技术措施来进行数据安全保护，主要包括：

- 数据收集环节：数据来源管理.数据防泄露.数据源鉴别.授权管理.数字签名.数据识别.数据分类分级等；
- 数据存储环节：数据加密.数据安全隔离.数据备份.数据容灾.数据防泄露.身份鉴别.数据访问控制.数字签名.数据完整性校验等；
- 数据使用/加工环节：数据防泄露.身份鉴别.授权管理.数据访问控制.数据审计溯源等；
- 数据传输环节：数据加密.数据脱敏.数据防泄露.数据源身份鉴别.数据接收方身份鉴别.数据审计溯源等；
- 数据提供/公开环节：数据加密.数据脱敏.身份鉴别.数据访问控制.数字水印.隐私计算.数据安全交换.数据应用接口安全.数据审计溯源等；
- 数据销毁环节：数据擦除.介质销毁. 授权管理.数据访问控制.数据识别等。

4.2 身份与访问管理（IAM）赋能数据安全

根据 Gartner 的定义，身份与访问管理（IAM）是一个可有效控制人或物等不同类型用户访问行为和权限的管理系统，能够有效控制什么人或物体在什么时间有权限访问哪些资源。（Identity and access management (IAM) is the discipline that enables the right individuals to access the right resources at the right times for the right reason.）就数据资源而言，IAM 中所包含的身份鉴别.授权管理.访问控制.审计溯源等能力，均能对确保数据安全起到至关重要的作用。

4.2.1 身份鉴别

身份鉴别技术是指对实体和其所声称的身份之间的绑定关系进行充分确认

© 2023 云安全联盟大中华区版权所有

的过程，目的是为了解决网络通信或应用交互双方身份信息是否真实的问题，使各种信息交流可以在一个安全的环境中进行。身份鉴别技术可以提供关于某个人或某个事物身份的保证，这意味着当某人（或某事）声称具有一个身份时，鉴别技术将提供某种方法来证实这一声明是正确的。可靠的身份鉴别技术可以确保信息来源于正确的实体且只被正确的实体访问。不同的应用场景和安全需求可能需要不同级别的身份鉴别技术和措施。

身份鉴别技术对于数据安全能起到以下作用：

(1) 确保数据来源真实性：在数据收集环节，对数据源进行身份鉴别，有助于确保组织机构采集到的数据来自合法可信的数据源，防止采集到被恶意篡改或伪造的数据。

(2) 确保数据传输安全性：在构建数据传输通道前对两端主体身份进行标识和鉴别，确保数据传输的保密性.完整性，并通过记录通信双方身份和访问操作，监控和回溯敏感数据传输过程。

(3) 确保数据访问合法性：在数据收集.存储.使用.加工.公开.提供等各个环节，均可以使用身份鉴别技术确保只有合法的授权用户才能够查看和修改数据，有助于防止敏感信息的泄露和窃取。

(4) 确保数据操作可追溯：身份鉴别技术可以记录用户的登录行为和资源访问申请操作，有助于进行用户行为审计和非法行为追踪，这对于监控和回溯敏感数据的访问非常重要。

4.2.2 授权管理

授权管理（Authorization Management）和访问控制（Access Control）都是保护资源免受未经授权的访问和操作的重要手段。二者在含义上会有些重叠，但是各有侧重。授权管理也称权限管理，通常是指确定哪些用户有权访问网络.系统.应用.数据等资源，并管理这些用户对这些资源的权限级别；访问控制则是指通过控制用户访问和操作资源的方式来保护资源的安全性。

© 2023 云安全联盟大中华区版权所有

任何访问主体（人/设备/应用等）在被允许访问客体（网络/系统/应用/数据等）之前，都要经过授权。访问主体对客体的访问权限并非一成不变的，可以根据业务需要和风险（或可信度）的变化进行动态调整，并且分配访问权限时应遵循最小权限原则。授权管理技术与身份鉴别技术结合使用时，可以更好地满足不同场景下的数据安全需求。

授权管理技术对于数据安全能起到以下作用：

(1) 确保数据仅被授权的个体访问：授权管理技术允许管理员对数据资源的访问权限进行细粒度的控制，如可以根据用户角色.部门.任务等因素来精确定义谁可以访问什么数据以及可以执行哪些操作，对敏感数据的使用还可以要求进行二次授权，最大程度防止数据滥用.非法利用或越权使用。

(2) 根据上下文动态调整用户权限：授权管理技术可以支持动态权限管理，例如，当某个用户的角色或职责发生变化时，可以自动调整其权限，确保其仍然只能访问适当的资源，避免由于授权未及时更新而导致数据泄露或无法访问。

(3) 记录数据访问权限申请和变更：授权管理技术通常包括审计功能，可保留所有授权记录，以便在发生权限异常事件时可进行追查。

4.2.3 数据访问控制

访问控制的目标是防止对任何资源（如计算资源.通信资源或信息资源）进行未授权的访问，从而使资源在授权范围内使用，决定用户能做什么，也决定代表一定用户利益的程序能做什么。身份鉴别和授权管理通常被视为访问控制的基础。

数据访问控制是针对非法或越权访问数据资源的防御措施，通常包括身份鉴别.授权和控制等过程，以确保只有经过身份鉴别和授权的合法用户可以在权限许可范围内对数据资源进行适当访问操作，从而防止数据泄露和不当使用。

© 2023 云安全联盟大中华区版权所有

数据访问控制的主体包括用户.程序.进程等，客体包括存储介质.数据库.表.字段.文件目录.文件等，访问权限包括读取.增加.删除.修改.拒绝访问等。

数据访问控制措施需要贴近被保护的数据资源进行串联模式部署，作为各类主体访问被保护数据的唯一通道，可以作为 IAM 的一部分，或完全独立于 IAM 实现。当独立实现时，数据访问控制系统需要具备与 IAM 之间的交互接口，以便对访问主体进行身份鉴别并根据授权策略执行正确的数据访问控制。

4.2.4 数据安全审计

数据安全审计指为获得审计证据并对其进行客观的评价，以确定满足审计准则的程度所进行的系统的.独立的并形成文件的过程。审计数据的保留期限和管理也是一项关键工作，要求满足法规和合规性要求。目前，数据安全审计应符合《网络安全法》要求，审计日志留存时间应不少于六个月。

数据安全审计技术在数据安全处理过程中有助于监测和审计数据的访问.使用和处理情况，以确保数据的合规性.完整性和安全性。在实际应用中，数据安全审计技术通常涉及配置审计策略.收集审计数据.分析数据以及生成报告的过程。这些技术可以与其他安全措施（如身份鉴别.访问控制等）结合使用，以建立全面的数据安全策略，确保数据的安全和合规性。

数据安全审计技术具有以下作用：

(1) 合规性验证：数据安全审计技术可用于验证数据处理活动是否符合适用的法规.政策和标准。例如，对于 HIPAA.GDPR.SOX 等法规要求，审计可以帮助组织证明其数据处理活动的合规性。

(2) 合规性报告：审计记录通常用于生成合规性报告，以满足监管要求和证明合规性。这对于金融机构.医疗保健提供商等受监管行业尤其重要。

(3) 追踪数据访问：审计技术可以记录数据的访问和操作历史，包括谁访问了数据.何时访问.访问的内容和所采取的操作。这些记录有助于追踪数

© 2023 云安全联盟大中华区版权所有

据的使用情况。审计结果也可以用于验证用户或实体的身份，以确保只有授权的用户能够访问数据。它还有助于监控和强化访问控制策略。

(4) 监测不当行为：审计可以监测和检测不当行为，如未经授权的数据访问.篡改尝试.数据泄露等。这有助于及时识别潜在的安全威胁。

(5) 警报和通知：数据安全审计可以配置警报和通知系统，以在发生异常或潜在安全事件时及时通知安全团队，从而加快应对事件的速度。

(6) 取证和调查：如果发生数据安全事件，审计记录可以用于取证和调查。这些记录可以提供关于事件的详细信息，以便确定事件的原因和影响。

4.3 与数据安全相关的 IAM 技术挑战

数据安全是一个较大的课题，在数据收集到数据销毁的处理活动中，所涉及的数据本身的安全风险防范拘束以及数据处理行为的安全管控，前述章节已经有所描述，针对数据安全访问管控，我们将基于 IAM 进行简单说明。

4.3.1 身份管理挑战

数据在流通过程中，存在数据归属主体.数据访问主体以及第三方监管等多种身份体系，在身份管理方面存在多种挑战：

- 数据归属主体以及访问主体类型复杂，包括个人用户.企业用户.应用程序.物理设备等，缺乏统一的身份体系进行纳管
- 数据访问主体广泛存在于组织内部或者外部多种数据源，如何归类与定义访问主体身份
- 在数据归集阶段，涉及到多方数据源，各类身份数据不统一，组织范围内数据归属身份没有实现实名化

- 在数据资源目录管理阶段，身份数据与海量目录数据的关联带来的数据归属查询性能问题

- 在数据交换阶段，跨部门不同身份数据对接以及互认问题；

- 在数据使用阶段，相关联的身份数据的治理.命名规则以及使用规则不统一的问题。

4.3.2 访问控制挑战

数据访问便利性和安全性的平衡性挑战。当今疫情下的企业直面两大问题，其一是如何快速恢复并保持有序生产，其二是业务的开展受限于远程和多种非企业设备终端的情况下，如何保护企业数据的访问安全和合规使用。尤其是对于很多高科技企业，不仅要让员工能够远程接入，开展复杂的研发测试工作，而且还要保证敏感数据的安全传输交换与合规使用。

- 数据类型纷繁复杂，如何定义数据的访问控制策略与访问性能需要取得平衡。如是否定义基于访问主体的控制策略，或者被访问资源的控制策略，以及更复杂的 Policy-based 多种规则访问控制策略

- 在数据交换时，如何定义分级分类下数据.相对应的操作以及操作用户主体的访问规则

- 数据使用阶段，如何确保数据访问主体的安全性，即访问主体是否被正确鉴权以及主体是否存在冒用可能性

- 数据使用阶段，如何访问控制策略形成足够的鉴权点，比如在结构化数据从数据库中被读取时，或者非结构化数据在通过 API 等形式获取时，是否可以根据策略进行数据过滤控制；

4.3.3 审计溯源挑战

© 2023 云安全联盟大中华区版权所有

由于数据具备可复制性，当前广泛存在数据泄露后无法溯源的问题，故数据相关的审计溯源挑战也非常严峻：

- 海量的数据访问记录如何被存储
- 数据的共享. 访问以及操作记录如何确保不篡改
- 用户如何快速获知自己数据被第三方访问以及访问第三方数据的情况
- 数据在归集以及交换后，如何溯源数据来自于可信主体
- 数据多方操作时，其操作记录如何被多方可信
- 审计数据如何被合法存证

5 身份管理

身份管理是为了在数据的流通过程中正确的识别数据的提供者. 数据的使用者，它确保数据收集. 数据使用. 数据传输等数据活动的安全。身份管理需统一的管理组织. 自然人. 设备. 外部应用等主体的身份，建立身份库，通过身份鉴别技术识别主体身份，为数据的访问控制提供基础。

5.1 身份定义

身份定义是围绕数据处理活动来定义各个主体的身份，确定在数据处理活动中，谁是数据的提供者，谁是数据的使用者，谁可以参与数据的传输和交换。确保数据的来源可靠，数据的去向可查，数据的使用合规。

定义一套标准的身份数据模型是身份数据管理的基础。一方面身份数据模型定义应满足业务对身份数据的需求，满足数据访问控制的需求。另一方面，身份数据模型定义应充分考虑数据安全. 隐私保护的要求，最小化收集身份数据。

5.1.1 自然人身份

© 2023 云安全联盟大中华区版权所有

自然人是数据处理活动中最重要，也是最常见的主体，自然人自我的安全意识.所处的外部环境和主动的风险行为都会对数据安全产生影响。因此对于自然人用户身份的管理.鉴别和访问控制是数据安全的基本保证。

自然人身份是由各项身份属性定义的，自然人身份属性可以包含以下几个方面的信息：

- 个人属性：姓名.性别.年龄.电话.邮箱.地址.职业.兴趣爱好.教育背景.家庭状况.身份证件.社交媒体账户.偏好设置.健康信息等等
- 组织属性：所在部门.所处角色.岗位.区域.职级等等

注意，这些身份属性的收集和使用应符合相关隐私和数据保护法规，确保用户的个人信息安全和隐私保护。

自然人身份标识是用于唯一标识和识别一个自然人的标识符，它是一个独特的值或组合，用于在系统中区分不同的用户。自然人身份标识可以是任何形式的唯一标识符，通常由系统分配或用户自定义。常用的用户身份标识数据如下：

- 用户名：用户真实姓名.用户自设用户名等
- 用户 ID：组织内部 ID（如工号）.随机 ID.自增长 ID.OpenID 等
- 手机号码
- 邮箱
- 证件号码：身份证号码.护照号码.军人政号码等

系统应优先选择用户在系统内唯一且敏感度较低的数据作为用户的身份标识。

5.1.2 组织身份

© 2023 云安全联盟大中华区版权所有

组织就是指人们为实现一定的目标，互相协作结合而成的集体或团体，如党团组织.工会组织.政府部门.企业.军事组织等等。在数据处理活动中，组织可以作为独立的身份存在，如企业信息化系统中的供应商.代理商等合作实体。也可以和个人用户组合，用来定义用户身份，比如钉钉.企业微信等 SaaS 服务中的企业租户等组织。

组织的身份属性可以包含以下方面的信息：

- 组织属性：组织名称.组织机构代码.社会统一信用代码.组织类型.组织 logo.官方网址.官方邮箱.地址等等
- 代表人属性：法人信息.联系人信息等等

组织的身份标识一般采用组织编号，常见的组织编号有：

- 公开编号：社会统一信用代码.税务登记号等
- 内部编号：部门编码等

5.1.3 设备身份

在数据处理活动中，设备是指参与数据访问和加工的终端设备，如计算机.平板电脑.手机.传感器.物联网设备.嵌入式设备.虚拟终端等等。这些设备有些是数据的提供者，有些是数据的使用者，有些还参与数据的加工和传输，正确的识别这些设备才能有效的防止数据被恶意的访问或破坏。

设备的身份属性可以包含以下方面的信息：

- 设备属性：设备类型.设备编号.操作系统.位置.硬件信息.软件信息等等
- 设备所有人属性：所有人信息等等

常见的设备身份标识有以下几种：

© 2023 云安全联盟大中华区版权所有

- 硬件编号：IMEI.mac 地址等等
- 网络地址：IP 地址等
- 其它：数字证书.设备指纹等等

5.1.4 外部应用身份

外部应用可能参与数据处理活动的多个环节，如数据收集活动.数据使用活动.数据加工活动.数据传输活动等。在任何一个环节中，外部应用的身份都需要被正确的鉴别，否则将面临严重的数据破坏和泄露风险。

外部应用的身份可以包含以下方面的信息：

- 应用信息：应用名称.应用 ID.应用密钥.应用访问地址.应用类型等

常见的应用身份标识有：

- 应用 ID
- 数字证书

5.2 身份数据收集

收集身份数据，建立一套完整的身份数据库，用于满足身份标识.访问控制的需要。可通过以下几种方式收集身份数据：数据源同步.用户自注册.人工收集录入.自动采集和自助维护。

5.2.1 数据源同步

通过数据源系统同步身份数据涉及数据模型的兼容.多数据源数据的合并和清洗.以及多种数据同步方式。数据模型的兼容是指数据源的属性字段与自身属性字段的映射匹配，将来自数据源的数据转换为系统可识别的身份数据。多数据源数据的合并和清洗是指系统按照一定的规则和优先级，将来自不同数据源的数据合并为一套完整的身份数据，避免数据重复.数据覆盖等问题。系统与系统间

© 2023 云安全联盟大中华区版权所有

的数据自动同步可通过多种方式实现，常见的数据同步接口协议有以下几种：

- HTTPS：以安全为目标的 HTTP 通道，在 HTTP 的基础上通过传输加密和身份认证保证了传输过程的安全性。

- SFTP：Secure FTP 是一种数据流连线档案存取.传输和管理功能的网络传输协议。

- LDAPS：一种使用 TLS 或 SSL 保护 LDAP 客户端与 LDAP 服务器之间通信安全的协议。

- SCIM：跨域身份管理系统，用于规范不同系统间的身份数据共享原则和接口定义，以增强身份系统之间的互用性。

数据源同步常用于在企业内部传输和收集自然人身份数据。

5.2.2 用户自注册

用户自注册是一种常见的身份数据收集方式，面向公众的互联网应用和 SaaS 服务都会采用这种方式收集用户身份数据。用户自注册常用于收集自然人身份数据.组织身份数据和应用身份数据。

注意，采用用户自注册方式收集用户身份数据时，应对用户录入的部分关键数据进行校验，已确认用户身份数据的真实性，如手机号.邮箱.证件号码等数据，必要情况下还需要通过生物识别等方式校验用户的真实性。身份数据校验有以下两种类别：

- 真实性校验：即证实用户真实存在或数据真实有效，校验方式一般是采用权威系统进行验证，常见的权威系统有公安系统.运营商系统等。

- 归属性校验：即证实用户录入的数据确实归用户所有，如使用短信验证电话号码的归属，使用邮件验证邮箱的归属等等。

© 2023 云安全联盟大中华区版权所有

5.2.3 自动采集

在一些数据敏感度较高的信息化系统中，自动采集常用于收集设备身份数据，并针对设备的身份进行数据的访问控制。自动采集的设备身份数据有以下几种类型：

- 硬件数据：IMEI.mac 地址等
- 系统数据：操作系统版本.驱动版本等
- 网络数据：IP 地址
- 软件数据：软件名称.版本等

5.2.4 人工录入

由系统管理员收集和整理各类身份数据，通过文件或脚本导入系统数据库。

5.2.5 自助维护

自助维护是由用户自主的管理维护自身的身份数据，如修改个人信息，修改组织数据，管理可信终端等等。

5.3 身份认证

身份认证是以用户提交的信息.设备信息.应用信息作为身份凭据确认用户.设备.应用身份的过程。设备和应用的身份认证方式较为单一，一般是采用数字证书或密钥进行鉴别，在这里我们主要讨论用户的身份认证。

5.3.1 身份认证凭据

用户身份认证是对用户提交的身份凭据进行校验以确认用户身份。用户身份认证凭据是用户可以用来证明其合法身份的信息。从用户和凭据间的关系来看，用户身份认证凭据存在于用户所知.用户所持.用户所有三个维度。

- 所知：如口令.临时授权码等凭据，这些凭据的特点是只有用户才知道

© 2023 云安全联盟大中华区版权所有

这些信息，但是存在用户主动泄露.恶意获取或破解等风险。

- 所持：如U盾.手机等设备凭据，这些凭据的特点是这些设备归属于用户，但是存在设备丢失等风险。

- 所有：如人脸.声纹.指纹等生物特征凭据，这些凭据的特点是只有用户才拥有这些信息，基本不存在丢失.泄露等安全风险。

常见的用户认证凭据有以下几种：

- 口令：持续有效的用户身份凭据。

- 验证码：一次性.短时效的身份凭据。

- 动态口令/离线令牌：在固定设备上，通过特定算法计算出来的.短时效的身份凭据。

- 数字证书：安装在终端或特定设备上，通过加密算法证明自身存在并有效的身份凭据。

- 人脸/指纹/声纹/虹膜：以自然人的生物特征作为鉴别用户的身份凭据。

5.3.2 用户认证策略

用户认证策略是在综合考虑系统数据敏感度.使用环境的复杂度之后对用户认证方式.认证次数的定义。

认证策略考虑主体.客体.环境.行为等因子，在不同的场景下使用不同的认证方式，兼顾数据安全和用户体验。

- 主体因子：用户类型.用户安全等级.设备类型.设备风险.设备IP.应用安全等级等。

- 客体因子：数据类型.数据安全等级等。

© 2023 云安全联盟大中华区版权所有

- 环境因子：时间.地点等。

- 行为因子：敏感数据查询.数据修改.数据导出.数据删除等。

从要求用户提供的身份凭据数量来说，认证策略有以下两种：

- 单因素认证：用户提供一种用户凭据即可完成用户认证

- 多因素认证：用户需要一次性提交多种用户凭据才能完成用户认证，如口令+验证码。

从要求用户提供身份凭据进行认证的次数来说，认证策略有以下两种：

- 单次认证：用户只需要登录一次就可以按照用户权限访问数据。

- 二次认证：用户登录后，系统还需要根据主体因子.客体因子.环境因子.行为因子的变化，随时对用户发起认证挑战。二次认证并非指用户只认证两次，而是指对用户进行持续认证。

5.3.3 身份认证技术

随着互联网和企业数据化建设的发展，身份认证的安全性，用户的使用体验，都是推动身份认证技术发展的动力。比如，无口令认证技术旨在消灭安全性较低的用户口令，单点登录技术旨在给用户带来更好的使用体验。常见的身份认证技术包括：

- Kerberos 用于在包括 Windows.macOS 和 Linux 在内的操作系统中通过不安全的网络（例如 Internet）进行身份验证。Kerberos 与受信任的第三方合作以提供访问证书。
- CAS 是一种开源协议和 SSO 标准。CAS 通过 2 次前端重定向的过程完成用户的认证和用户票据的传递。
- SAML 是一种开源协议和 SSO 标准。SAML 在 IdP 和服务提供商之间通过签名的 XML 文档传递信息。

© 2023 云安全联盟大中华区版权所有

- Oauth 是一种开放标准的授权协议，允许用户让第三方应用访问该用户在系统上存储的数据，而无需将用户名和口令提供给第三方应用。
- OIDC 是用于身份验证和 SSO 的开源协议，用作 OAuth 2.0 授权框架的身份层。用户无需直接登录到各个网站，而是被重定向到 OIDC 站点进行登录。
- JWT 是为了网络应用环境间传递声明而执行的一种基于 JSON 的开发标准。JWT 的声明一般用来在 IDP 和 SP 之间传递被认证的用户身份信息，以便于从 SP 获取资源,该 token 也可以直接被用于认证,也可以被加密。
- 轻量级目录访问协议(LDAP)用于身份验证，以使用目录服务验证凭据。使用 LDAP 时，客户端请求存储在数据库中的用户数据，并在凭据匹配时提供访问权限。
- RADIUS 协议全称为远程身份验证拨入用户服务（Remote Authentication Dial-In User Service），是一种用于验证和授权用户访问的网络协议，访问范围囊括了远程和本地。RADIUS 多用于网络基础设施的访问。
- FIDO2 是多家科技巨头联合推动的一种安全标准,使用 Web 身份验证 API 和客户端到身份验证器协议,通过来自本地设备(例如令牌或智能手机)的公钥加密对用户进行身份验证。

6 数据访问控制

数据访问控制是在身份鉴别之后进行的。数据访问控制主要解决的是主体（人.应用.设备）对客体（本篇主要指数据）的安全访问问题，即：该行为是否可以作用于该数据以及能访问的数据范围这两个问题。本章主要从数据权限管理和数据访问控制模型两方面对数据访问控制展开介绍,数据权限管理主要是对权限要素概念的介绍,数据访问控制模型主要是介绍各要素之间的组织和交互关系模型。

© 2023 云安全联盟大中华区版权所有

6.1 数据权限管理

权限管理又名权限策略管理或者权限规则管理，一般是指根据系统设置的安全规则或者安全策略，用户（主体）可以访问而且只能访问一定范围内自身被授权的资源和数据。权限管理一般可以分为资源功能级权限管理和数据级权限管理，两者在管理上有相通性，但是随着云计算和大数据的发展，数据级权限管理面临更大的的挑战。

本节重点以当前业界流行的 RBAC 为模型介绍数据权限管理各要素，虽然该模型目前在权限管理的实践中遇到很多问题，比如角色爆炸.权限控制粒度不够精细.属性的标准化等问题，但这仍然是我们探讨数据权限管理的基础，随着 ABAC 以及其专门用于数据权限管理的分支 NGAC 的演进，我们在后续版本中会及时把业界相关的最佳实践同步进来。

6.1.1 权限管理的基本要素

在进行权限管理系统设计和选择的时候，首先需要考虑权限管理系统的核心对象模型.对象模型中包含的基本元素主要有：用户（Users）.用户组（Group）.角色（Role）.控制对象（Resource Class）.访问模式（Access Mode）.操作（Operator）。主要的关系有：分配角色权限 PA（Permission Assignment）.分配用户角色 UA（Users Assignment），分别描述如下：

(1) 控制对象：是系统所要保护的资源（Resource Class），可以被访问的对象。资源的定义需要注意以下两个问题：

- 资源具有层次关系和包含关系。例如，网页是资源，网页上的按钮.文本框等对象也是资源，是网页节点的子节点，如可以访问按钮，则必须能够访问页面。

- 这里提及的资源概念是指资源的类别（Resource Class），不是某个特定资源的实例（Resource Instance）。资源的类别和资源的实例的区分，以及资源的粒度的细分，有利于确定权限管理系统和应用系统之间

的管理边界，权限管理系统需要对于资源的类别进行权限管理，而应用系统需要对特定资源的实例进行权限管理。两者的区分主要是基于以下两点考虑：

- 一方面，资源实例的权限常具有资源的相关性。即根据资源实例和访问资源的主体之间的关联关系，才可能进行资源的实例权限判断。例如，在管理信息系统中，需要按照营业区域划分不同部门的客户，A 区和 B 区都具有修改客户资料这一受控的资源，这里“客户档案资料”是属于资源的类别的范畴。如果规定 A 区只能修改 A 区管理的客户资料，就必须要区分出资料的归属，这里的资源是属于资源实例的范畴。客户档案（资源）本身应该有其使用者的信息（客户资料可能就含有营业区域这一属性），才能区分特定资源的实例操作，可以修改属于自己管辖的信息内容。

- 另一方面，资源的实例权限常具有相当大的业务逻辑相关性。对不同的业务逻辑，常常意味着完全不同的权限判定原则和策略。

(2) 用户：权限的拥有者或主体。用户和权限实现分离，通过授权管理进行绑定。

用户仅仅是纯粹的用户，用来记录用户相关信息，如用户名.口令等，权限是被分离出去了的。用户（User）要拥有对某种资源的权限，必须通过角色（Role）去关联。

(3) 用户组：一组用户的集合。在业务逻辑的判断中，可以实现基于个人身份或组的身份进行判断。系统弱化了用户组的概念，主要实现用户（个人的身份）的方式。

(4) 角色：权限分配的单位与载体。角色通过继承关系支持分级的权限实现。例如，科长角色同时具有科长角色.科内不同业务人员角色。角色是使用权限的基本单位，拥有一定数量的权限，通过角色赋予

© 2023 云安全联盟大中华区版权所有

用户权限，对于基于角色的访问控制模型，访问权按角色名分组，资源的使用受限于授权给假定关联角色的个体。

(5) 操作（权限）：完成资源的类别和访问策略之间的绑定。

权限指用户根据角色获得对程序某些功能的操作，例如对文件的读.写.修改和删除功能。

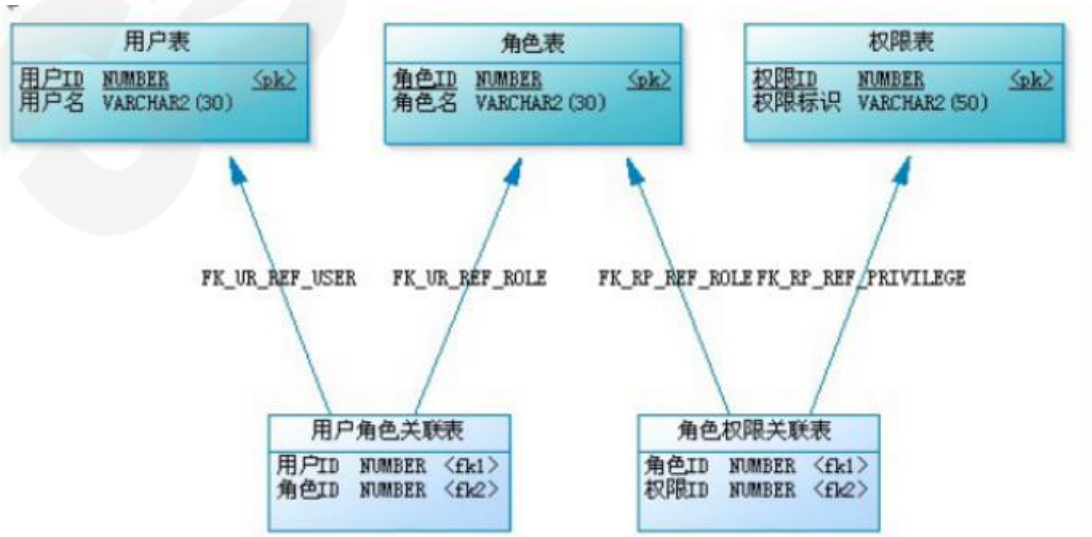
(6) 分配用户角色 UA：实现用户和角色之间的关联关系映射。

一个用户（User）可以隶属于多个角色（Role），一个角色组也可拥有多个用户，用户角色就是用来描述他们之间隶属关系的对象。用户（User）通过角色（Role）关联所拥有对某种资源的权限。

(7) 分配角色权限 PA：实现操作和角色之间的关联关系映射。

一个角色（Role）可以拥有多个权限（Permission），同样一个权限可分配给多个角色。

综合一下，基于 RBAC 模型的权限管理模型也可以用数据视图形象表示，如下图所示。



（图：RBAC权限模型）

© 2023 云安全联盟大中华区版权所有

6.1.2 权限管理系统设计

权限系统由三大部分构成：用户管理.角色管理.权限管理。

用户权限系统的核心由以下三部分构成：创造权限.分配权限和使用权限。

(1) 创建权限（Permission），在设计和实现系统时会划分。创建权限信息，指定系统模块具有哪些权限。

(2) 系统管理员(Administrator)创建用户和角色，并且指定用户角色(User—Role）和角色权限（Role—Permission）的关联关系。

1） Administrator 具有创建用户.修改用户和删除用户的功能

2） Administrator 具有创建角色和删除角色的功能

3） Administrator 具有建立用户和角色.角色和权限的关联关系功能

(3) 用户（User）使用 Administrator 分配给的权限去使用各个系统模块。

6.1.3 用户管理

用户管理是创建用户账号的一个过程，拥有账号之后，就可以登录系统。用户管理包括账号的创建.删除.冻结.解冻等操作。创建账号之后，使用对应账号可以登录系统，删除或者冻结账号之后，账号无法继续登录系统。

© 2023 云安全联盟大中华区版权所有

姓名.账号.口令为必须要素。其他的要素可根据企业自身需求增加，比如：手机号码.生日.联系地址.性别等信息。

账号创建完毕之后，需要为用户赋予角色（即在企业中的任职情况，如销售经理.销售主管.出纳.会计等）。

6.1.4 角色管理

权限系统中的角色大概率跟企业的组织架构是一致的，企业组织架构中的人在什么岗位要做什么事情？权限系统中的用户是什么角色被允许看那些东西进行什么操作？ 是一种对应关系，所以 企业架构的岗位.岗位职责跟别对应了权限系统的角色权限。

在企业中一个人可以兼任多个岗位，一个岗位也可能有多个人，所以岗位与人是多对多的关系。

岗位之间会有从属关系，比如：销售经理下设销售主管.销售主管下设销售专员，最终构成了组织架构，一般是树形关系。

© 2023 云安全联盟大中华区版权所有

角色管理需要我们可以灵活的配置角色，而且可以设置从属关系。

创建完毕角色之后，我需要为角色赋予权限（其在企业中对应岗位需要做什么事情，允许看到什么内容，进行什么操作？）

6.1.5 权限管理

权限一般是跟企业中的岗位职责对应的，在企业实际运营过程中，为了保证用户的隐私.企业数据的安全性，会对不同岗位设定不同的限制。比如客服不允许给用户退款转账，新媒体运营专员不允许查看用户手机等隐私信息，非高层管理者不允许批量导出用户信息等。

总结起来，我们可以将权限分为两大类：数据权限和操作权限。

（1）数据权限

数据权限，就是角色可以看到哪些内容（包括能看到哪些页面.字段.区域）

- 页面：假设有 10 个页面，管理员只给某个角色开通了 10 个中的 2 个页面查看权限，那么该角色就只能看到这 2 个菜单。

- 字段：假设某个菜单对应的页面列表中有 15 个字段，角色 A 被允许查看所有字段，角色 B 只允许查看其中的 10 个字段，那么 A 和 B 看到的内容就不同。

- 区域：假设为角色 A 开通了全国的数据查看权限，为 B 开通了北京的数据查看权限，那么 A 就可以看到全国的数据，B 就只能看到北京地区的收据。

（2）操作权限

操作权限就是角色可以进行哪些操作？包括增删改。比如客服不允许上下架商品，商品审核专员不允许操作退款等，都属于操作权限的控制，每个操作都可

© 2023 云安全联盟大中华区版权所有

以有权限控制。

6.2 数据访问控制模型

访问控制模型是规定主体如何访问客体的一种架构。1985 年美国军方发布《可信计算机系统评估准则》（Trusted Computer System Evaluation Criteria，TCSEC，也称“桔皮书”），描述了两种著名的访问控制模型，自主访问控制（DAC）和强制访问控制（MAC）。20 世纪 90 年代，大量专家学者和研究机构先后提出了不同类型的基于角色的访问控制模型（RBAC），其中美国 George Mason 大学信息安全技术实验室（LIST）提出的 RBAC96 模型得到了广泛认可。近年来，业内出现了一种基于属性的访问控制模型(ABAC)，被认为是可以弥补 RBAC 不足的新一代访问控制技术。随着动态安全能力越来越受到业界的关注，美国国家安全局（NSA）提出了一种风险自适应的访问控制模型（RAdAC）。本节将着重对上述访问控制模型进行说明。

6.2.1 自主访问控制 Discretionary Access Control，DAC）

自主访问控制（Discretionary Access Control，DAC）是根据主体（如用户.进程或 I/O 设备等）的身份及其所属的组来限制其对客体的访问。所谓的自主，是因为对某个客体拥有控制权的主体可以直接（或间接）地将对该客体的一种或多种访问权自主地授予其他主体，并在随后的任何时刻将这些权限回收。自主访问控制中，用户可以针对被保护对象制定自己的保护策略。

1.DAC 的具体实现

- 访问控制列表（Access Control List，ACL）

ACL 是最早也是最基本的一种自主访问控制实现方式。它的原理非常简单：每一项资源，都配有一个列表，这个列表记录的就是哪些用户可以对这项资源执行哪些操作（只读/读写/执行等）。当用户试图访问这项资源时，系统会首先检查这个列表中是否有关于当前用户的访问权限，从而确定当前用户可否执行相应

© 2023 云安全联盟大中华区版权所有

的操作。总的来说，ACL 是一种面向资源的访问控制模型，它的控制或保护机制是围绕“资源”展开的。

例如，对于一个文件对象，有如下的 ACL：

File1	
Alice	read, write
Bob	read

表示 Alice 可以对该文件进行读写操作，Bob 只能读取。

由于 ACL 的简单性，使得它几乎不需要任何基础设施就可以完成访问控制。但同时它的缺点也是很明显的，一方面，由于需要维护大量的访问权限列表，ACL 在性能上有明显的缺陷；另一方面，对于拥有大量用户与众多资源的应用，管理访问控制列表本身已变成非常繁重的工作。

- 访问控制矩阵（Access Control Matrix，ACM）

ACM 是通过矩阵形式描述主体和客体之间的权限分配关系。对每个主体而言，都拥有对哪些客体的哪些访问权限；而对客体而言，又有哪些主体可以对它实施访问；将这种关连关系加以阐述，就形成了访问控制矩阵。其中，特权用户或特权用户组可以修改主体的访问控制权限。

	Asset 1	Asset 2
Role 1	read, write, execute, own	execute
Role 2	read	read, write, execute, own

访问控制矩阵的实现很易于理解，但是查找和实现起来有一定的难度，而且，如果用户和文件系统要管理的文件很多，那么控制矩阵将会成几何级数增长，这样对于增长的矩阵而言，会有大量的空余空间。

- 访问控制能力列表（Access Control Capabilitis List，ACCL）

© 2023 云安全联盟大中华区版权所有

能力是访问控制中的一个重要概念，它是指请求访问的发起者所拥有的一个有效标签（ticket），它授权标签表明的持有者可以按照何种访问方式访问特定的客体。ACCL 是以用户为中心建立的访问权限表，其实现与 ACL 正好相反。

UserA	
File1	read, write
File2	read

定义能力的重要作用在于能力的特殊性，如果赋予哪个主体具有一种能力，事实上是说明了这个主体具有了一定对应的权限。能力的实现有两种方式，可传递的和不可传递的。一些能力可以由主体传递给其他主体使用，另一些则不能。

2.DAC 的典型应用场景

DAC 常见于文件系统，LINUX，UNIX.WindowsNT 版本的操作系统都提供 DAC 的支持。在实现上，先对用户鉴权，然后根据控制列表决定用户能否访问资源。用户控制权限的修改通常由特权用户或者管理员组实现。

3.DAC 的不足之处

DAC 最大缺陷就是对权限控制比较分散，比如无法简单地将一组文件设置统一的权限开放给指定的一群用户。同时，由于资源所有者（特权用户）的权限太大，无意间就可能泄露信息。此外，一旦系统遭遇特洛伊木马攻击，并且攻击者成功获取了特权账户权限，则系统中所有资源都将遭到侵害。

6.2.2 强制访问控制（Mandatory Access Control，MAC）

MAC 是为了弥补 DAC 权限控制过于分散的问题而诞生的。在 TCSEC 中有如下定义：“一种限制访问客体的手段，它以包含在这些客体中的信息敏感性和访问这些敏感性信息的主体的正式授权信息（如清除）为基础”。

1.MAC 策略

在 MAC 模型中，主体和客体分别被赋予一定的安全级别，主体能否访问客体由双方安全级别之间的关系决定。MAC 通常具有系统硬性限制，即系统强制主体服从访问控制策略，是一种强加给访问主体的访问方式。

MAC 利用下读/上写来保证数据的保密性,利用上读/下写来保证数据的完整性。

(1) 向下读（rd，read down）：主体安全级别高于客体信息资源的安全级别时允许查阅的读操作；

(2) 向上读（ru，read up）：主体安全级别低于客体信息资源的安全级别时允许的读操作；

(3) 向下写（wd，write down）：主体安全级别高于客体信息资源的安全级别时允许执行的动作或是写操作；

(4) 向上写（wu，write up）：主体安全级别低于客体信息资源的安全级别时允许执行的动作或是写操作。

2.MAC 安全标签

安全标签是附加在主体和客体上的一组安全属性信息。MAC 为访问主体和受控对象（客体）提供两类安全标签，一类是具有偏序关系的安全等级标签，另一类是非等级化的分类标签，它们是实施强制访问控制的基本依据。系统通过比较主体和客体的安全标签来决定一个主体是否能够访问某个客体。用户程序不能更改它自己以及任何其他客体的安全标签。

多级安全（MultiLevel Secure, MLS）是最常见的强制访问控制策略。在实际的应用中，可以通过访问控制标签列表（ACSLL）来限定一个用户对一个客体目标访问的安全属性集合。当用户在请求访问一个客体时，系统会判断它的安全级别是比所请求访问的客体高还是低，如果低的话，拒绝访问，如果高的话可以访问。通过分级的安全标签实现了信息的单向流通。

© 2023 云安全联盟大中华区版权所有

3.MAC 模型举例

MAC 模型中最著名的是 Bell-LaPadula 模型和 Biba 模型，其他较为常见的模型如 Chinese Wall 模型等。以下分别进行简单介绍。

（1）Bell-LaPadula（BLP）模型

Bell-LaPadula 模型通常是处理多级安全信息系统的设计基础，客体在处理绝密级数据和秘密级数据时，要防止处理绝密级数据的程序把信息泄露给处理秘密级数据的程序。BLP 模型的出发点是维护系统的保密性，具有只允许向下读（即不上读，NRU）.向上写（即不下写，NWD）的特点，可以有效地防止机密信息向较低安全级别的系统泄露。

（2）Biba 模型

Biba 模型是和 BLP 模型相对立的模型，Biba 模型改正了被 BLP 模型所忽略的信息完整性问题，但在一定程度上却忽视了保密性。Biba 模型使用不下读（NRD）.不上写（NWU）的原则来保证数据的完整性，在实际的应用中主要是避免应用程序修改某些重要的系统程序或系统数据库，这样可以使资源的完整性得到保障。

（3）Chinese Wall 模型

Chinese Wall 模型一般是用于多边安全系统（也就是多个组织间的访问控制系统）中的安全模型，应用在可能存在利益冲突的组织中，最初是为投资银行设计的。Chinese Wall 模型有两条基本原则：一是用户必须选择一个它可以访问的区域；二是用户必须自动拒绝来自与用户所选区域的利益有冲突的其他区域的访问。这种工作模式同时包含了 DAC 和 MAC 的属性，银行家可以选择为谁工作（DAC），一旦选择了之后，它就只能为这个客户工作(MAC)。一个典型的例子就是防火墙内部与外网相连的一台服务器，假如这台服务器暴露在外网之中，那么就禁止其转发数据，也就是说该服务器只能与外网通信，不能与内部网络通信。

© 2023 云安全联盟大中华区版权所有

4.MAC 的优缺点

MAC 策略一旦被制定，用户无法改变它。这种访问控制模型可以增强系统的安全性，因为它基于策略，任何没有被显式授权的操作都不能执行。MAC 一般在最重视保密性的机构或者其他等级观念强烈的行业中进行开发和实现，如军事系统。

MAC 的主要问题在于：

（1）实现工作量较大，授权管理不方便，不够灵活。

（2）过于强调保密性，对系统连续工作能力（可用性）方面考虑不足。

6.2.3 基于角色的访问控制（Role-Based Access Control, RBAC）

RBAC 是实施面向企业安全策略的一种有效的访问控制方式。其基本思想是，对系统操作的各种权限不是直接授予具体的用户，而是在用户集合与权限集合之间建立一个角色集合。每一种角色对应一组相应的权限。一旦用户被分配了适当的角色后，该用户就拥有此角色的所有操作权限。将用户和权限进行分离，彼此相互独立，使权限的授予更加灵活。管理员不必在每次创建用户时都进行分配权限的操作，只要分配用户相应的角色即可，而且角色的权限变更比用户的权限变更要少得多，这样将简化用户的权限管理，减少系统的开销。

1.RBAC 支持的安全原则

RBAC 支持以下公认的安全原则：最小特权原则.责任分离原则和数据抽象原则。

- 最小特权原则：通过限制分配给角色的权限的多少和大小来实现，分配给某用户对应角色的权限只要不超过该用户完成其任务的需要即可；

© 2023 云安全联盟大中华区版权所有

- 责任分离原则：通过在完成敏感任务过程中分配两个责任上互相约束的两个角色来实现，例如在清查账目时，需要设置财务管理员和会计两个角色同时参加。

- 数据抽象原则：借助于抽象许可权的概念实现，如在账目管理活动中，可以使用信用.借方等抽象许可权，而不是使用操作系统提供的读.写.执行等具体的许可权。

RBAC 并不强迫实现这些原则，安全管理员可以配置 RBAC 模型使其不支持这些原则。因此，RBAC 支持数据抽象的程度与 RBAC 模型的实现细节有关。

2.RBAC 概念模型

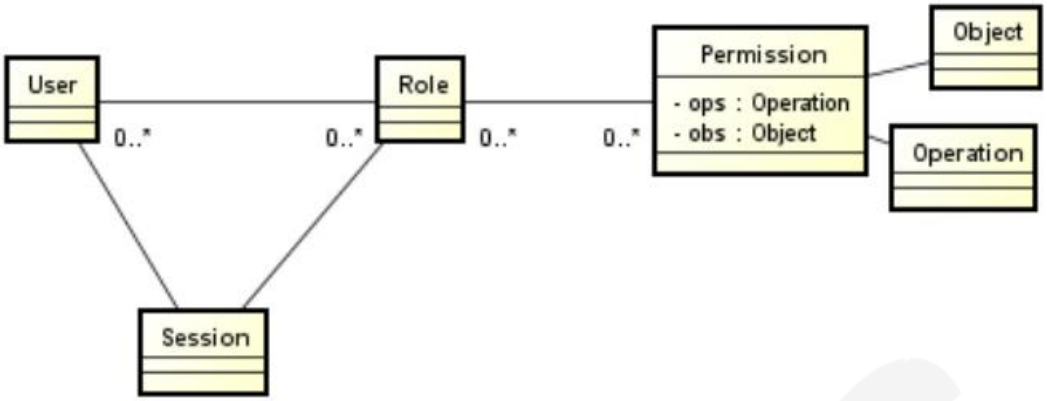
业界广为认可的 RBAC96 是一个模型族，其中包括 RBAC0~RBAC3 四个概念性模型。

（1）基本模型 RBAC0

RBAC0 定义了能构成一个 RBAC 控制系统的最小元素集合。RABC0 是 RBAC 的核心，其他版本都是建立在 RBAC0 的基础上的。

RBAC0 模型中包括用户（User）.角色（Role）.会话（Session）和权限（Permission)等 4 类实体集合。其中权限包括操作(Operation)和对象(Object）两个元素。图 6-2 展示了用户.角色.访问权限和会话之间的关系。

© 2023 云安全联盟大中华区版权所有



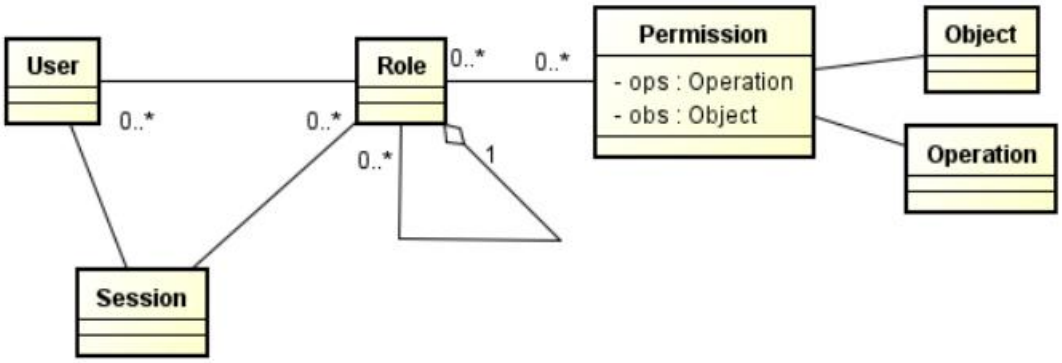
每个角色至少具备一个权限，每个用户至少扮演一个角色；可以对两个完全不同的角色分配完全相同的访问权限；会话由用户控制，一个用户可以创建会话并激活多个用户角色，从而获取相应的访问权限，用户可以在会话中更改激活角色，并且用户可以主动结束一个会话。

用户和角色可以是多对多的关系，权限和角色也是多对多的关系。一个用户在不同的场景下可以拥有不同的角色，例如项目经理也可以是项目架构师等；当然一个角色可以给多个用户，例如一个项目中有多个组长，多个组员等。一个角色可以拥有多份权限，同一个权限也可以授给多个角色。

（2）高级模型 RBAC1

RBAC1 在 RBAC0 模型基础上增加了角色分级的概念，即角色之间存在上下级的关系。同时引入角色间的继承关系，一个角色可以从另一个角色继承权限，并且在拥有其他角色权限的同时，自己还可以关联额外的权限。这种设计可以给角色分组和分层，一定程度简化了权限管理工作。

© 2023 云安全联盟大中华区版权所有



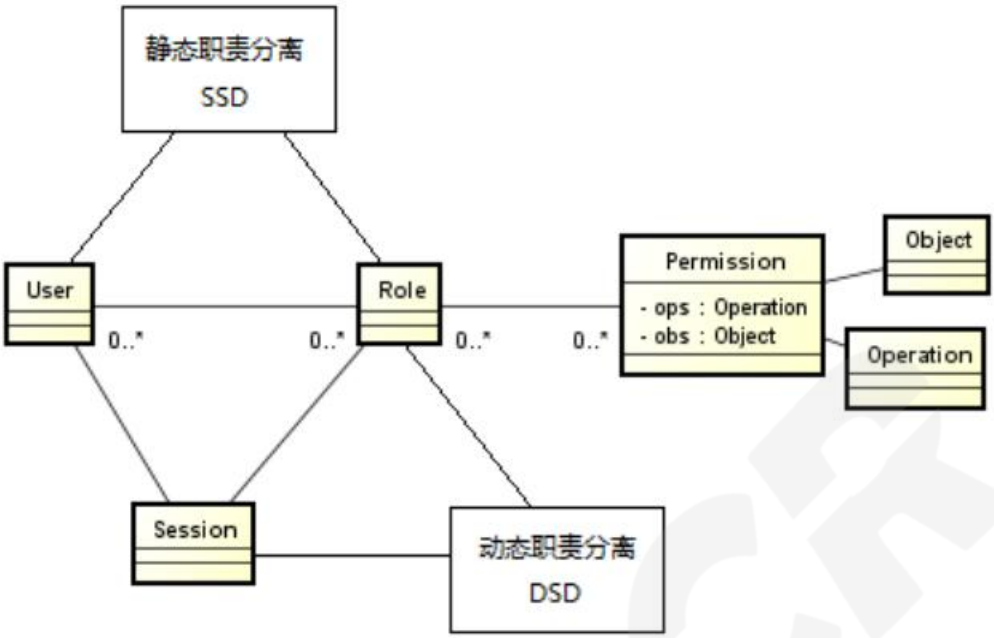
角色间的继承关系可分为一般继承关系和受限继承关系。一般继承关系仅要求角色继承关系是一个绝对偏序关系，允许角色间的多继承。而受限继承关系则进一步要求角色继承关系是一个树结构，实现角色间的单继承。

（3）高级模型 RBAC2

RBAC2 在 RBAC0 基础上增加了一些限制，强调 RBAC 的不同组件在配置方面的一些限制。

RBAC2 模型中添加了职责分离关系。RBAC2 的约束规定了权限被赋予角色时，或角色被赋予用户时，以及当用户在某一时刻激活一个角色时所应遵循的强制性规则。职责分离包括静态职责分离 (Static Separation of Duty，SSD)和动态职责分离 (Dynamic Separation of Duty，DSD)。

© 2023 云安全联盟大中华区版权所有



SSD 是用户和角色的指派阶段（授权阶段）加入的，主要是对用户和角色有如下约束:

a.互斥角色:同一个用户在两个互斥角色中只能选择一个,例如要么是会计，要么是出纳，不能兼任；

b.基数约束：一个用户拥有的角色是有限的，一个角色拥有的权限也是有限的，例如一个公司的领导岗位是有限的，每个领导岗的权限也是有限的；

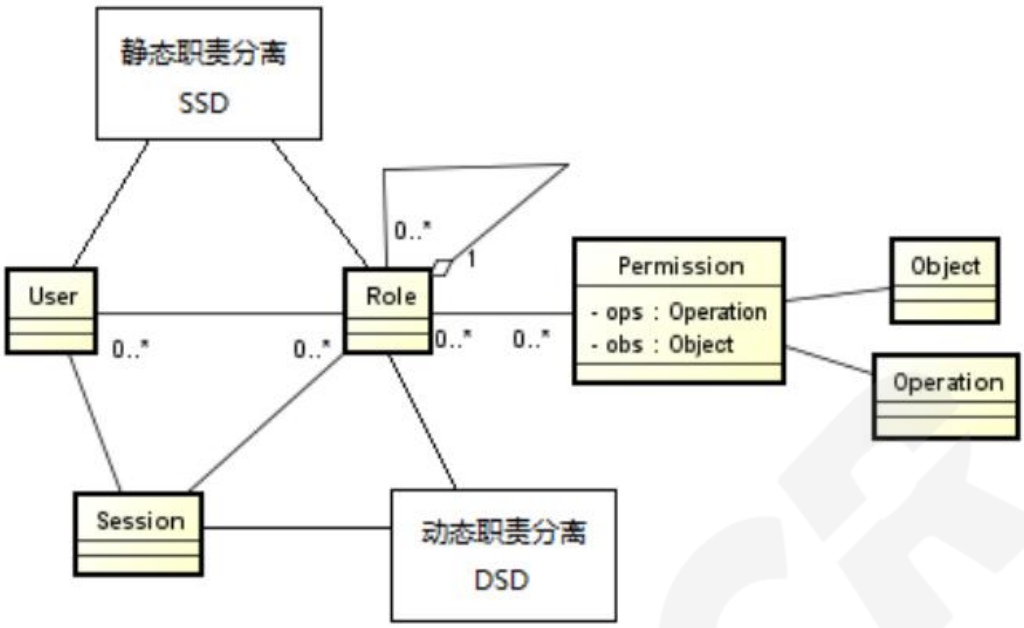
c.先决条件约束：用户想要获得高级角色，首先必须拥有低级角色，例如先要成为经理，之后才能升为总监。

DSD 是会话和角色之间的约束，可以动态的约束用户拥有的角色，例如一个用户可以拥有两个角色，但是运行时只能激活一个角色。

（4）统一模型 RBAC3

RBAC3 包含了 RBAC1 和 RBAC2，利用传递性，也把 RBAC0 包括在内。这些模型就构成了 RBAC96 模型族。

© 2023 云安全联盟大中华区版权所有



3.RBAC 的优缺点

RBAC 相对于 ACL 最大的优势就是它简化了用户与权限的管理，通过对用户进行分类，使得角色与权限关联起来，而用户与权限变成了间接关联。RBAC 模型使得访问控制，特别是对用户的授权管理变得非常简单和易于维护，因此有广泛的应用。但是它也有自身的缺点，那就是由于权限是以角色为载体分配的，如果某一角色下的个别用户需要进行特别的权限定制，如同加入一些其他角色的小部分权限或去除当前角色的一些权限时，RBAC 就无能为力了。此外，由于 RBAC 模型没有提供操作顺序控制机制，使得 RBAC 模型很难应用于那些要求有严格操作次序的实体系统，例如在购物控制系统中要求系统对购买步骤进行控制，在客户未付款之前不应让他把商品拿走，RBAC 模型对此也无能为力。

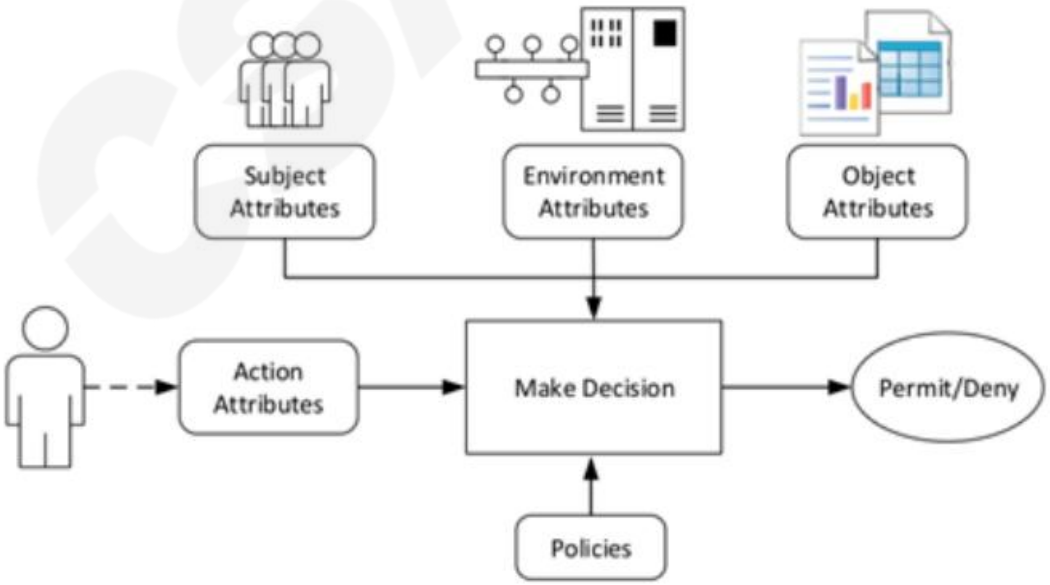
6.2.4 基于属性的访问控制（Attribute-Based Access Control, ABAC）

ABAC 是一种为解决行业分布式应用间可信关系的访问控制模型，它能够解决开放网络环境下资源保护所面临的细粒度问题以及网络系统所面临的大规模用户问题，为未来的开放网络环境提供了较为理想的访问控制策略方案。

1.ABAC 基本概念

现实中的实体可以通过实体特性（组合）来进行有效区分，这种可以对实体进行区分的实体特性称为实体属性。ABAC 利用相关实体(如主体.客体.环境)的属性作为授权的基础来研究如何进行访问控制。使用实体属性这个核心概念对主体.客体.权限及授权约束进行统一描述，用属性或属性组来区分不同的实体，用实体属性之间的关系对安全需求进行形式化建模，以期有效解决分布式开放环境下的细粒度访问控制和大规模用户动态扩展问题。

基于这样的目的,可将实体的属性分为四类：主体属性(如用户名.所在部门.所在用户组.职务.年龄等），环境属性（如访问客户端 IP.当前时间等），行为属性（如读取.修改.添加.删除等）和对象属性（如 URL.文件.数据库表.分类分级标签等）,这与传统的基于身份的访问控制（IBAC）不同。在基于属性的访问控制（ABAC）中，访问判定是基于请求者和资源具有的属性，请求者和资源通过属性来标识，而不像 IBAC 那样只通过 ID 来标识，这使得 ABAC 具有足够的灵活性和可扩展性，同时使得安全的匿名访问成为可能，这在大型分布式环境下是十分重要的。



图：NIST 的 ABAC 模型

ABAC 把实体属性（组）概念贯穿于访问控制策略.模型和实现机制中，把与访问控制相关的时间.实体空间位置.实体行为.访问历史等信息当作主体.客体.权限和环境的属性来统一建模，通过定义属性之间的关系描述复杂的授权和访问控制约束，能够灵活的进行访问控制。不同于常见的将用户通过某种方式关联到权限的方式，ABAC 是通过动态计算一个或一组属性是否满足某种条件来进行授权判断的，更适合大规模用户场景的使用需要。目前 ABAC 已经应用于 WEB 服务.网格计算.信息共享和消息管理中。

2.ABAC 体系结构

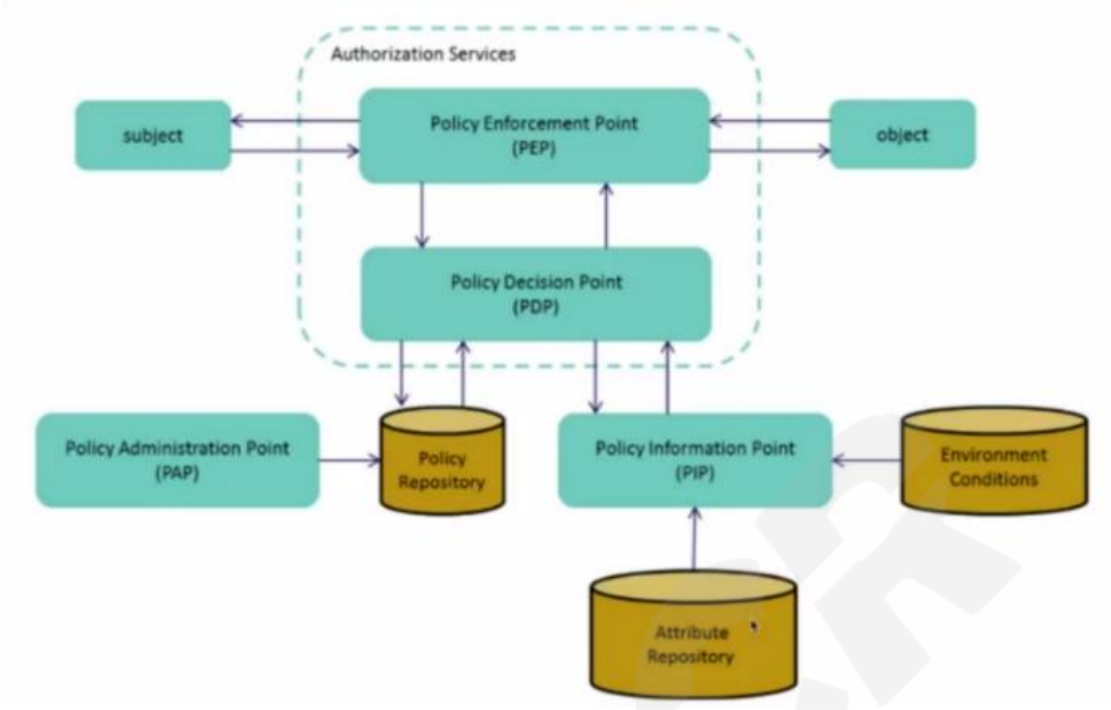
ABAC 的参考体系结构如图所示，该体系结构包括策略执行点（PEP）.策略决策点（PDP）.策略信息点（PIP）和策略管理点（PAP）四个服务节点。此外，PDP 和 PEP 功能可以是分布式的或集中式的，它们构成所谓的授权服务（AS）。对于访问请求，此体系结构的工作流描述如下：

（1）PEP 从经过身份验证的主体截获访问请求，并将该请求发送到 PDP。

（2）PDP 根据 PAP 生成的访问策略和查询 PIP 得到的主题.对象.环境等属性进行访问决策。

（3）PDP 给出的最终决策结果被发送给 PEP，然后 PEP 根据 PDP 的决策完成访问请求。

© 2023 云安全联盟大中华区版权所有



图：NIST 的 ABAC 参考体系结构

上述体系结构中还包括两个存储库和多个环境感知模块。两个存储库分别存储和管理公共访问规则和实体属性，环境感知模块可以获取与请求相关的当前时间的环境信息，其中这些信息可以包括当前时间.位置.威胁级别.设备类型等。

3.ABAC 实现方法

可扩展访问控制标记语言(Extensible Access Control Markup Language，XACML)是目前 ABAC 唯一的国际公开标准，已经在全球范围内被广泛采用，XACML 灵活的扩展性及丰富的规则及函数是实现复杂访问控制规则的科学选择。

© 2023 云安全联盟大中华区版权所有

图 基于 XACML 的 ABAC 策略

XACML 支持多种逻辑表达式和属性类型，具有很强的策略表达能力，非常适合对这种细粒度的大数据存储访问控制模型进行授权描述。同时具有可扩展性，能够支持大数据环境下的灵活.动态访问控制的需求。

4.ABAC 优缺点

ABAC 具有如下优点：

- 支持集中化管理；
- 可以按需实现不同颗粒度的权限控制；
- 不需要预定义判断逻辑，减轻了权限系统的维护成本，特别是在需求经常变化的系统中；

缺点则包括：

- 权限判断需要实时执行，规则过多会导致性能问题；
- 定义权限时，不能直观看出用户和对象间的关系，规则如果稍微复杂一点，或者设计混乱，会给管理者维护和追查带来麻烦。

跟 RBAC 相比，ABAC 对权限的控制粒度更细，如控制用户的访问速率。但是由于 ABAC 实现相对复杂，目前仍无法完全取代 RBAC。实际开发中可以结合 RBAC 角色管理的优点和 ABAC 的灵活性一起使用。

6.2.5 风险自适应访问控制（(RAdAC,Risk-Adaptable Access Control)）

在大规模应用场景中，安全管理员可能缺乏足够的专业知识，无法准确地为用户指定其可以访问的数据。风险自适应的访问控制是针对这种场景的有效解决方法。

1.RAdAC 概述

风险自适应访问控制（Risk-Adaptable Access Control，RAdAC）是美国国家安全局（NSA）研究的下一代动态访问控制方法，能够根据当前平台状态以及特殊情况灵活动态地对用户进行授权，给用户提供最严格的访问策略。由于系统在不同状态下（如网络繁忙.系统异常.用户违规操作.数据传输出错等）的访问安全风险是不一样的，因此，RAdAC 能提供动态的多级安全（Multi Level Security，MLS）级别的访问。RAdAC 具备动态分析安全风险和操作需求的能力，能够对分布式平台的访问安全风险进行评估，并与用户进行交互以确认其访问资源的必要性，最后综合两者对用户访问权限进行判定。

2.RAdAC 实现方法

RAdAC 是一种动态访问控制机制，通过实时评估用户操作需求并计算授权访问风险来动态调整访问控制策略。RAdAC 包含以下三部分：安全风险测量（Security Risk Measurement，SRM）.操作需求测定（Operational Need Determination，OND）以及最终访问决定（Final Access Decision，FAD）。

- 安全风险测量（SRM）：SRM 会根据用户的操作行为.用户状态.环境因素.上下文.访问目标特征等多种特性通过阈值判定.加权等计算方式得出本次访问风险值（实际是一个风险范围）。同时 SRM 还需具备一定的机器

© 2023 云安全联盟大中华区版权所有

自学能力，例如当用户在操作中多次访问核心数据资源，则必须提高风险等级。

- 操作需求测定（OND）：OND 使得用户在特殊情况下能够超越风险判定访问某资源。传统方式下，用户属于一个部门或者拥有某几个角色，能够访问的资源都是固定的，但是在紧急情况或者风险较大的时候，用户可能需要拥有超过自身权限的访问能力。系统需要结合用户权限和访问要求来得到最后的操作需求判定。

- 最终访问决定（FAD）：FAD 根据 SRM 和 OND 的结果，通过访问决定函数（Access Decision Function，ADF）来做出最终结果。由于用户每次操作的风险值和需求都是变化的，因此在多级安全系统中，用户的最终访问结果并不是固定的。FAD 的结果是二进制值，允许或拒绝。

3.RAdAC 优点

与当前较流行的 RBAC 算法相比，RAdAC 具有如下优点：

（1）平台扩展性好：RAdAC 可以在数据库或 XACML 的基础上，增加对平台安全性.用户属性的判定，依据相应的判定函数实施访问判决，克服了传统方式下的缺陷。

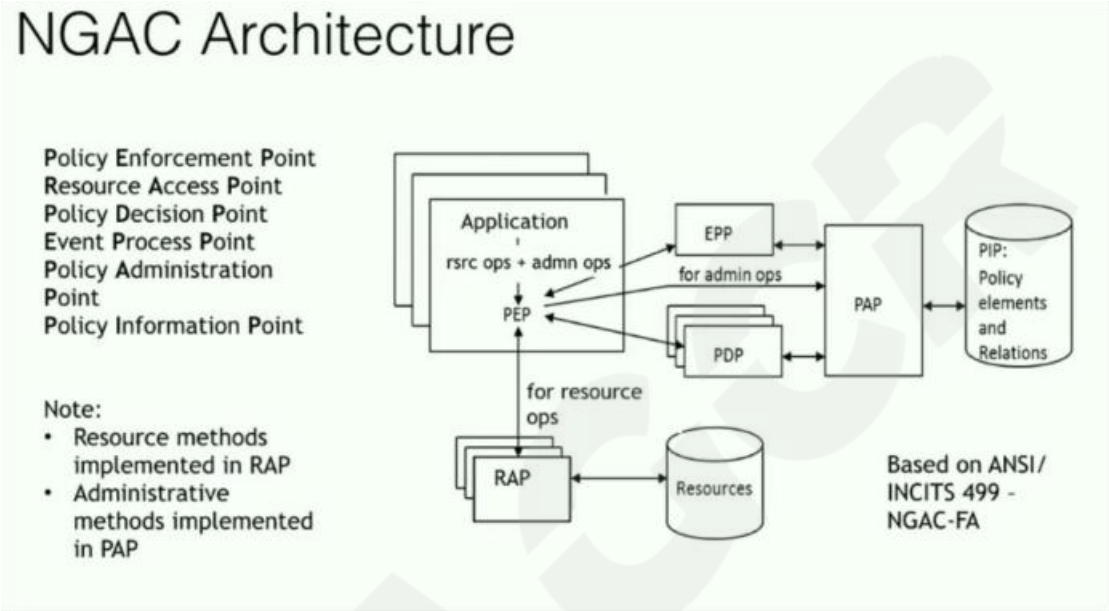
（2）策略灵活：目前大部分平台的安全策略工作采用 XACML 提供的集中式策略合成算法，为了数据的安全访问，往往直接遵守最小特权原则（deny override），无法根据具体情况作出不同判断。RAdAC 根据当前风险等级和操作需求，灵活确定资源访问权限，在保证数据安全的同时，尽可能满足访问需求。

6.2.6 下一代访问控制（NGAC）

1.NGAC 概述

NGAC，即下一代访问控制，采用将访问决策数据建模为图形的方法。NGAC 实

现了一种系统的.策略一致的访问控制方法，以细粒度授予或拒绝用户管理能力。NGAC 由 NIST（美国国家标准与技术研究院）开发。NGAC 研究的主要目标是寻求一个标准化的 ABAC 机制，降低 ABAC 中管理的复杂度和提高权限模型的通用性，它允许在 ABAC 策略的表达和执行中通过更改一组固定的数据元素和关系，来实现灵活的授权过程。



图：NGAC 架构图

NGAC 的功能架构与 XACML 一样，也分为 4 个功能层：实施.决策.管理和访问控制数据，各功能组件协同工作以实现受策略保护的访问和数据服务。在这些组件中，PEP 能够捕获应用程序的访问请求，包括进程 id.用户 id.操作以及该操作涉及的数据资源或访问控制数据元素和关系。管理操作例程在 PAP 中实现，资源读/写例程在 RAP 中实现。

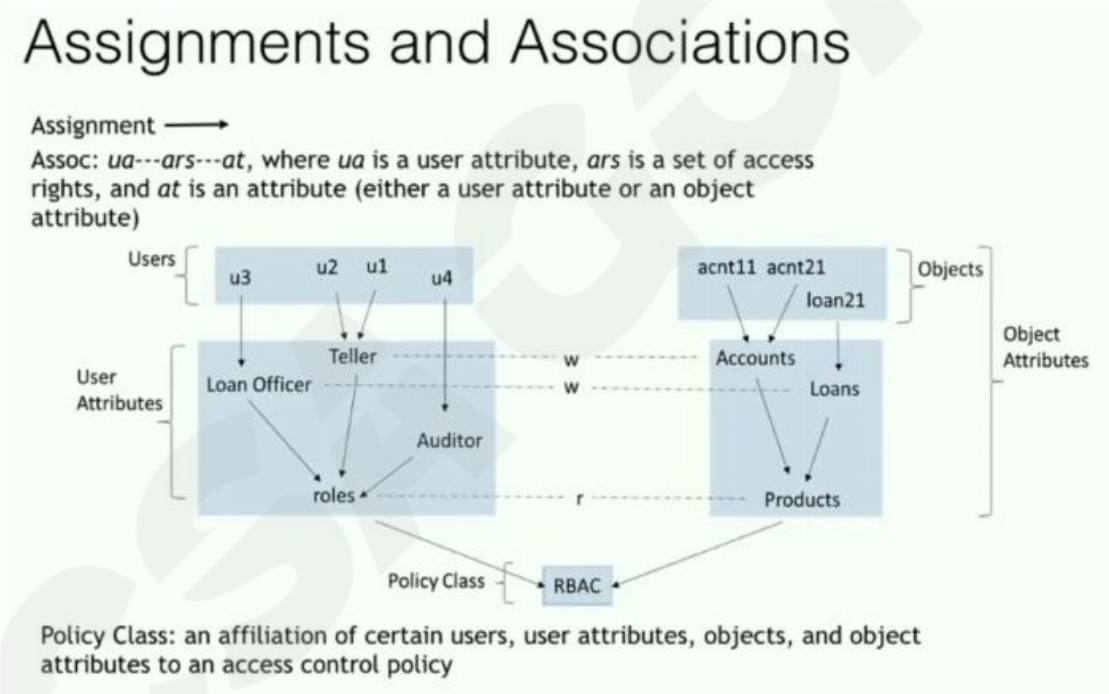
与 XACML 体系结构不同，来自 NGAC PEP 的访问请求信息以及 NGAC 关系（由 PDP 检索）提供了生成决策的完整上下文。PDP 将批准或拒绝的决定返回给 PEP。如果授予访问权限并且操作是读/写操作，PDP 还返回客体内容所在的物理位置，PEP 向对应的 RAP 发出对客体内容执行操作的命令，RAP 最后返回其执行的结果状态。在读取操作的情况下，RAP 还返回数据内容的类型（例如 PowerPoint），PEP 还要调用正确的数据服务应用来使用它。如果访问请求与管理操作有关，并且决策结果为准许，则 PDP 向 PAP 发出命令，使其对存储在 PIP 中的数据元素或

© 2023 云安全联盟大中华区版权所有

关系执行操作，并且 PAP 将状态返回给 PDP，而 PDP 再将状态转发给 PEP。如果 RAP 或 PAP 返回的状态为“成功”，则 PEP 向事件处理点（Event Processing Point，EPP）提交访问上下文。

如果该上下文与某个职责的事件模式匹配，那么 EPP 将自动执行该职责的管理操作，从而可能更改访问状态。注意，NGAC 是数据类型无关的，它将可访问的实体视为资源数据或访问控制数据的元素或关系，直到访问过程完成之后，数据的实际类型才对相应的应用程序起作用。

2.NGAC 标准规范



图：NGAC 标准规范

NGAC 通过一组标准化的.通用的关系（Relation）和功能（Function）来定义访问控制，这些关系和功能在策略的表达和执行中是可重用的。

（1）策略及其属性元素

NGAC 的访问控制数据由基本元素.容器（即属性）和可配置关系组成。

（2）关系

NGAC 不是通过规则来表达策略，而是通过配置 4 种类型的关系（Relation）来表达策略，这些关系包括：

- 指派（Assignment，用于定义容器的成员关系）

使用元组（x，y）来指代将元素 x 指派给元素 y，指派关系通常意味着包含（x 包含在 y 中）。

- 关联（Association，用于确定特权）

关联是一个三元组，用 ua---ars---at 表示，含义是，ua 中包含的用户可以对 at 引用的策略元素执行 ars 中的访问权限。

- 禁止（Prohibition，用于指定特权例外）

u_deny（u，ars，¬pe），ua_deny（ua，ars，¬pe）和 p_deny（p，ars，¬pe）是指用户 u.被指派给 ua 的用户和进程 p 不能对不在 pe 中的策略元素执行 ars 中的访问权限。

- 职责（Obligation，用于动态改变访问状态）

职责关系以(ep, r)对的形式表示，其含义为“当 ep 发生时，执行 r”，其中 ep 是事件模式，r 是一系列管理操作（称为响应）。

7 数据安全审计

GB/T 41479—2022《信息安全技术 网络数据处理安全要求》中明确提出，网络运营者应对数据处理的全生存周期进行记录,确保数据处理可审计.可追溯。GB/T 35274—2023《信息安全技术　大数据服务安全能力要求》中也提出，应具备对数据处理过程和存储数据使用与访问进行监测的能力,及时发现违规数据处理行为，记录并安全存储监控日志 6 个月以上，以满足数据处理活动安全审计要

© 2023 云安全联盟大中华区版权所有

求。本章主要以数据库数据使用审计为例进行介绍。

7.1 审计日志分类

数据使用审计日志通常应覆盖以下两个场景：

7.1.1 单次数据使用审计日志

1.信息粒度

单次数据使用审计日志中，至少应包括以下信息，才能够保障审计有效且有利于后期事件追溯：

(1) 发生时间：应详细到年-月-日-时-分-秒，便于用户准确追溯不同事件发生的时间，尤其保障业务量高峰时间的记录准确性；

(2) 是否告警：单词的审计日志需要有详细信息说明该行为是否出发了数据库审计系统的告警，便于用户识别高危行为与普通行为；

(3) 审计 ID：唯一识别标志，便于精准检索；

(4) 会话 ID：本次审计日志所在会话的唯一识别标志，用于精准检索；

(5) 资产名称：对应数据库资产的名称，便于用户识别；

(6) 客户端相关信息：包括但不仅限于客户端 IP.端口.MAC.客户端工具.主机名.操作系统用户名等；此外，为了满足快速阅读的需求，客户端 IP 等高频检索字段需要能够根据用户的使用习惯设置别名，提升使用体验；

(7) 服务端相关信息：包括但不仅限于服务端 IP.端口.MAC.数据库类型.数据库账号.数据库名/实例名等；此外，为了满足快速定位操作部门/操作人的需求，数据库账号等重点字段需要能够根据用户的实际情况设置别名，提升使用体验；

© 2023 云安全联盟大中华区版权所有

(8) 请求相关信息：包括但不仅限于操作类型.原始 SQL 长度.SQL 模板 ID 和对象，其中，对象应包括对应的库.表.字段.视图.存储过程.函数.触发器.索引.用户.角色.权限等数据库对象，展示报文原文和 SQL 模板，供客户回溯事件使用；

(9) 响应相关信息：包括但不仅限于响应行数.执行状态.执行时长.执行结果描述和返回结果集，其中，应支持用户以根据实际使用情况资产为单位进行返回结果集大小和行数的限制，以节约存储空间；

(10) 关联信息：对于通过应用访问数据库的情况，应审计到的信息包括但不仅限于关联账号.关联 IP.关联 URL 等。

2.审计功能

单次数据使用审计日志需要具备以下功能，以保障用户在检索.追溯时的易用性：

(1) 丰富的检索条件：至少应包括以下检索条件：报文.审计 ID.会话 ID.SQL 模板 ID.资产.数据库账号.客户端 IP.

(2) 分析筛选：为满足用户快速检索的需求，应提供分析筛选看板，便于用户在几个重要维度中对审计日志进行全面筛选，至少应包含的维度有：数据库账号.客户端 IP.客户端工具.操作系统用户名.服务端 IP.操作类型.数据库名/实例名.表名.主机名.执行状态.执行时长和影响行数；

(3) 一键取证：定位到安全事件相关日志时，需要提供一件取证的功能，从而以图片的形式保存对应的信息；

(4) TOP SQL 提取：为满足用户监测数据库性能的需求，数据库审计产品需要能够对访问数据库的 SQL 进行归类与排序，提取出平均执行时长 TOP.执行次数 TOP.总执行时长 TOP 和执行时长 TOP，便于用户定位数据库性能问题及采取针对性解决措施。

© 2023 云安全联盟大中华区版权所有

7.1.2 单会话内多次数据使用审计日志

单次数据使用可被视为单会话内多次数据使用的一个子集。单会话内每一次数据调用所需要的审计数据及审计功能与 7.1.1 章节单次数据使用审计日志的能力一致。以下表述为多次数据使用相对单次数据使用场景所需增加的内容。

1.信息粒度

多数场景下，单次会话中会包含多次数据使用行为，数据安全审计工作需要能够识别同一会话中的多个 SQL，且能够区分历史会话与在线会话，且会话相关的信息至少应有：

(1) 会话基本信息：唯一的会话标识如 ID 等.会话开始及结束时间.对应资产信息；

(2) 客户端信息，包括但不仅限于 IP.端口.MAC.客户端工具.主机名和操作系统用户名；

(3) 服务端信息，包括但不仅限于 IP.端口.MAC.数据库类型.数据库账号.数据库名/实例名等；

(4) 会话中所有的审计日志：即本次会话包含的所有 SQL 对应的单条审计日志信息，应详细记录发生时间.报文.影响行数.执行时长和执行状态等。

2.审计功能

对于单会话内多次使用数据的场景，建议能够对响应的日志进行一键式的查询分析，便于快速提取行为特征信息，同时需要审计日志能够自由导出，以便进行进一步的追踪溯源；

具备良好的在线会话信息审计能力，需要对在线会话的以下信息进行审计与记录：

© 2023 云安全联盟大中华区版权所有

(1) 客户端及服务端相关信息；

(2) 会话相关信息；

(3) 流量相关信息：累计请求流量及累计返回流量等；

(4) 活跃状态信息：该会话当前是否活跃.最后活跃时间等。

7.2 审计日志获取能力

7.2.1 精准解析协议能力

具备以上两个场景审计日志的收集，前提是需要对主流数据库有良好的解析能力，前提是具备较强的协议支持能力，包括但不仅限于支持以下数据库：

(1) 主流协议：Oracle.MySQL.SQL server.DB2.Cache.PostgreSQL 等；

(2) 国产化协议：DM.Oscar.Oceanbase.Kingbase.GBase 等；

(3) 大数据协议：HBase.Hive.HDFS.Greenplum.SSDB 等；

(4) 图数据库协议：Neo4j.OrientDB 等；

(5) 其他协议：Elasticsearch.Redis.HTTP 等。

7.2.2 加密算法解析能力

具备以上两个场景审计日志的收集，前提是需要对主流数据库有良好的解析能力，在解析无加密协议的基础上，要对部分 SSL 加密算法具备解密能力，否则加密流量无法在审计系统中留存，同时要具备解析 kerberos 认证加密的能力；数据解密需要获得数据所有者授权。

(1) Oracle：高级安全（AES-256）

(2) Oracle .SQL server MySQL：SSL

(3) Hive.Spark.HDFS.PostgreSQL：Kerberos 认证

7.2.3 用户名补偿审计能力

在没有任何其他干预的情况下，SQL server 较高版本会默认在用户登录认证时，对用户名加密，数据库用户通过客户端访问某 SQL server 数据资产，会

© 2023 云安全联盟大中华区版权所有

产生对应的访问流量，流量中账号相关信息被加密，在传统的审计中，此时即便获取了流量，也没办法解析出对应的数据库账号。

数据库账号等相关信息对于数据安全审计是至关重要的，在部分场景中，数据库账号是追踪溯源的重要线索，如果缺失，极大可能造成审计失效.无法追踪到操作人，进而无法追究数据安全责任且无法挽回数据安全事件导致的损失与声誉。

综上，数据安全审计工作中，需要在 SQL server 场景下能够获取数据库账号，作为审计工作的重要一环。

7.2.4 三层关联能力

当数据被业务应用访问.使用时，从网络流量中能够看到的信息中，来源会被定义为对应的业务应用，而并非使用业务应用的人，这会造成审计信息不全，导致无法将数据使用行为与具体的操作人进行准确关联。

完备的数据安全审计需要具备将登录业务应用的人和通过业务使用数据的行为进行关联的能力，此类能力应同时保障数据使用安全性和关联的准确性，仅有 100%准确关联，才能够认为是具备该项能力。

7.3 审计分析

在获取了全面.准确的审计日志后，数据安全审计工作的审计分析重点包含自动分析和人工干预分析两个方面。

7.3.1 自动分析

需要具备提供自动分析的能力，包括但不仅限于各种类型的仪表盘.实时监控和报表：

（1）仪表盘：按照不同事件范围自动统计审计趋势.告警趋势以及会话趋势，并以曲线图进行直观展示；同时自动统计数据库资产的只要指标，如审计数量.告警数量.会话数量.执行失败数量和登陆失败数量；

（2）实时监控：以资产粒度进行数据库资产性能主要指标的统计，例如慢 SQL.高峰.低谷等；同时进行平均耗时趋势.执行时长分布和慢 SQL 来源的自动统计，

© 2023 云安全联盟大中华区版权所有

帮助用户快速定位数据库资产性能问题的来源；

（3）报表：从不同的场景和维度，使用对应的审计数据进行报表的构造与呈现，以帮助用户迅速了解现状.总结问题：

1）塞班斯报表：以《2002 年萨班斯—奥克斯利法案》（简称萨班斯法案）为标准，制定的关于数据库安全审计方面的符合性报告。按照 PDCA 的理论模型，分成计划与组织（Plan and Organize）.确保和控制（Certify and Control）.评估风险（Assess Risk）三个部分全面分析数据库安全状况。 可以帮助管理人员.审计人员及时发现各种异常和违规行为，并对这些行为进行快速分析.定位和响应，为整体信息安全管理提供决策依据；

2）综合分析报告：包含 SQL 语句执行情况.会话连接.风险事件和 SQL 性能分析；

3）性能分析报表：包含性能变化趋势分析，同时列出性能最差的数据库资产.耗时最久的 SQL.性能最差的 SQL 模板.执行最多的 SQL 模板等；

4）等保参考分析报表：包含审计情况统计.入侵防范监控.恶意代码监控.安全审计监控和日志存储时间统计；

5）语句.会话.告警分析类报表

6）表分析

（4）应具备结合风控分析的能力。可识别各类风险包括但不仅限于 SQL 注入.漏洞攻击.账号安全.数据泄露和违规操作。通过数据分析监测数据库潜在风险：能够分析不同规则的触发情况，详细列举告警的资产信息.告警数量。

7.3.2 人工干预分析

数据安全审计工作需要进行人工干预分析，以审计日志为基础，进行多维度的复杂分析，以达成问题预防.问题定位或追踪溯源：

（1）审计日志分析筛选：从几个重要的维度进行单选或多选的筛选分析，例如数据库账号.客户端 IP.客户端工具.操作系统用户名.服务端 IP.操作类型.数据库名/实例名.表名.主机名.执行状态.执行时长和影响行数等，同时能够进行图形化展示，便于用户迅速获取有效信息；

© 2023 云安全联盟大中华区版权所有

（2）自定义报表：应具备自定义分析范围的能力，从数据安全审计获取的审计日志维度和指标中，进行自由选择和组合，从而进行定制化分析工作。

应具备风险分析及风险控制的能力，具备识别各类风险的能力，同时具备分析告警日志的能力：

（1）通过内置规则库识别各类潜在风险：包括但不仅限于 SQL 注入.漏洞攻击.账号安全.数据泄露和违规操作等；

（2）通过告警分析监测数据库潜在风险：能够分析不同规则的触发情况，详细列举告警的资产信息.告警数量，同时通过图标进行展示，详细列举告警的客户端 IP.数据库账号和对应的告警数量，详细列举告警的 SQL 模板和对应的告警数量。

8 用零信任实现数据安全

数字化时代，数据成为组织的核心资产，数据的生成.存储.传输和相关的应用都成为攻击者的目标。传统的安全理念基于边界，一旦通过了边界安全检查，用户（或设备.网络.连接等）就是隐式可信的。随着数字化建设的实施，组织的 IT 架构愈发复杂，传统边界逐渐模糊，传统的安全模型面临的大量的挑战。为了应对这一问题，近年来，零信任的相关产品和解决方案在安全领域占据的地位越来越重要。

8.1 零信任介绍

自 2010 年提出，零信任逐渐从一个理论概念发展为一种被广泛采纳的安全策略。作为一种安全理念而非具体技术或工具，零信任以身份为中心，强调“永不信任，始终验证”的核心原则，并要求在实体尝试访问任何资源时进行严格的验证和授权。

业界对零信任的理解不尽相同，但是其核心理念就是通过严格执行身份认证和资源访问授权，并通过持续且全面的安全态势评估动态调整授权，以实现安全

© 2023 云安全联盟大中华区版权所有

闭环。在不同应用场景下实施零信任安全，需要的融合的安全技术不尽相同，但是最小权限模型和对动态授权的实践是其中的基础。在数据安全领域，身份管理.动态访问控制.持续信任评估和安全代理是在数据零信任安全的实现过程中的关键要素。

身份在零信任中的定义不限于用户身份，还包括设备.服务.数据等所有在网络中交互的实体。每个实体的身份必须得到确认和验证，同时，在进行敏感操作时可能触发额外的身份验证步骤（例如，多因素认证）。动态访问控制关注实体的访问模式并实施“最小权限”原则。它基于实体身份.请求上下文和资源敏感性来授予或拒绝访问权限，并确保授予的权限不超出完成任务所需的范围。

传统上的访问控制在一次认证授权以后，除了定期复查（超时机制）之外，鲜有反映即时安全态势的能力。持续信任评估涉及对实体的持续监控和安全评估，并结合全面的安全信息，确保其行为符合预期，并实时更新实体的信任等级。这要求安全审计具备实时监控和自动化分析能力，以便在访问控制决策中利用最新的信任信息。

在零信任架构中，安全代理，例如 API 网关，扮演着关键的角色。安全代理负责实施安全策略并执行数据流的完全仲裁。作为数据和应用程序的守门人，安全代理确保只有经过严格验证和授权的实体能够访问资源。它执行定义的访问策略，例如基于角色的访问控制（RBAC）或基于属性访问控制（ABAC），确保实体只能访问其拥有适当权限的资源。安全代理不仅仅在实体首次请求访问时执行访问控制，它在整个会话期间持续监控和仲裁数据流，保证数据传输的安全性和符合政策，并在检测到可疑或不符合策略的活动时触发警报或采取预定义的响应行动。它甚至还可以负责数据的加密和解密，确保数据在传输和存储时的安全性，以及提供针对数据篡改和窃听的保护。在实际的零信任实施中，安全代理作为安全策略执行的关键环节，确保数据在整个生命周期内的安全，并使组织能够及时发现和响应潜在的安全威胁。它也使组织能够在复杂和动态的数字环境中维持对数据流的持续控制和可见性。

© 2023 云安全联盟大中华区版权所有

8.2 零信任的实现

尽管零信任的理念已经日臻成熟，但在实施过程中仍需秉持一种平衡的策略，充分考虑实际情况，并根据组织的特点选择和整合适宜的技术和策略。因此，需要企业或组织根据自身的安全能力.业务特点.应用及安全需求等因素，逐步建设，持续迭代。NIST 划分的零信任技术核心包括软件定义边界（SDP）.身份和访问管理（IAM）以及微隔离（Micro-Segmentation，MSG）三类。当前，与零信任相关的安全产品和解决方案基本上都是基于这些核心能力进行延伸或组合构建的。因此，企业在实际操作中应根据实际情况，选择相应的产品和解决方案并逐步实施。

软件定义边界（SDP）关注于确保网络资源的安全访问。它创建一个虚拟的网络边界，确保只有经过验证的实体才能访问网络中的指定资源，大幅度减小了潜在的攻击面。在如 SaaS.移动互联网.远程办公等应用场景中，SDP 为访问者提供了一个在需要时可以随时部署的安全边界，使服务与不安全的网络环境被隔离开。它确保数据的安全传输，并且能够与沙箱技术结合，实现数据不落地，防止数据泄露。此外，SDP 的网络隐身技术确保在身份验证和授权之前，后端业务系统对终端用户完全不可见，极大地减少了未经授权的恶意攻击者通过利用系统漏洞进行数据窃取的机会。

IAM 在零信任的实施过程中扮演着举足轻重的角色，它确保访问者的身份得到正确确认与授权。不仅依靠传统的登录认证，IAM 的部署，应要求它在每次访问尝试时都对每个用户进行信任识别.评估.认证和授权。通过与用户风险分析和动态权限控制的结合，IAM 可以适时调整用户访问权限，确保是合规用户在正常时间.正常设备，通过合规途径对相应数据进行访问。对于尚未完成身份管理能力建设的企业或组织，应优先从身份管理建设入手，而 IAM 的部署和应用就应被优先考虑。

微隔离（MSG）关注于通过精细化的网络划分来减小攻击面，并通过详细的策略控制不同划分间的流量，并为每个独立段提供控制与安全保障，实现了数据流与访问行为的精细管理。它允许 IT 团队使用网络虚拟化技术在数据中心内部

© 2023 云安全联盟大中华区版权所有

部署灵活的安全策略，为不同的安全段定义精准的安全规则，同时也阻止了未经授权的用户请求在内部进行横向移动。对于注重管理内部数据的横向流动，或者需要加强对后台的各类微服务及中间件的管理的场景，就需要优先考虑横向隔离进行有效管控的 MSG 类的产品或解决方案

在实施零信任的过程中，企业和组织应明确，完全的零信任是一种理想状态，而实际的建设过程则应适应组织的实际情况，逐步推进。组织可以选择与其实际情况.技术能力和业务需求最匹配的解决方案，逐步实施和优化，确保在实现数据和资源安全的同时，也能支持业务的灵活发展和技术的持续创新。

为确保零信任架构的实际效果能够切实满足新型 IT 环境下的安全需求，实践中需要遵循一系列基本架构原则。包括全面身份化原则.应用级控制原则.安全可闭环原则.业务强聚合原则.多场景覆盖原则和组件高联动原则。这些原则将确保零信任架构在实际实施过程中既具有强大的安全防护能力，也能够灵活适应多变的业务和技术环境。

8.3 发展与展望

零信任安全模型为我们提供了一种全新的视角和方法，帮助我们在面对复杂多变的安全威胁时，更加有效地保护数据安全。未来，随着技术的不断演进和新型安全威胁的出现，零信任模型也将持续发展和演变。我们可以预见，零信任模型将与更多的前沿技术相结合，比如通过区块链提供更加安全可靠的身份验证和数据完整性保障，或者利用人工智能优化动态访问控制和持续信任评估的智能决策过程。同时，零信任也将在更多的领域和场景得到应用，例如在物联网.边缘计算等领域解决设备身份和数据安全的问题。

在数据安全领域实施零信任模型无疑面临着多方面的挑战，包括技术实施的复杂性.组织文化的转变.人力和财力的投入等。特别是在技术集成方面，如何将现有的 IT 系统和零信任模型有机结合，保证业务的连续性，是一个值得深入探讨的问题。同时，对于许多组织来说，建设一个符合自身实际情况的零信任架构也是一项挑战。面对这些挑战，企业和组织也将迎来诸多机遇。例如，通过实施

© 2023 云安全联盟大中华区版权所有

零信任模型，组织不仅可以提高数据安全水平，也可以借此机会优化 IT 架构，提高业务灵活性和响应速度。同时，通过不断的技术创新和模型优化，企业和组织也可以在实践中积累宝贵的经验，推动零信任模型的进一步发展。通过持续的实践.学习和创新，我们相信零信任模型能够与更多的技术和领域相结合，发挥出更大的价值和潜力。

9 典型应用场景

9.1 政务领域典型场景

9.1.1 政务领域数据使用场景与访问控制威胁分析

政府侧已积累了海量的个人和企业的相关数据，而此类政务数据往往涉及安防.交通.医疗.教育等敏感信息，数据存量大，管理难度高；数据范围广，涉及多个部门；数据类型多，不乏敏感数据。当前政务领域数据访问控制管理存在以下特点：

（1）数据存放分散，数据类型不统一。很多职能部门自建系统，存放自有数据，导致各部门元数据统一，数据质量不同，形成烟囱式数据体系；

（2）数据无分级分类管理。数据本身大量存在于数据库.文件系统中，没有统一的指导思路针对数据进行分级分类管理，进而无法安全的将数据共享出去；

（3）数据访问主体无分类管理。数据往往被人或者应用访问，不同类别人员其所应该具备的数据访问权限不尽相同，需要针对访问主体进行分类分类管理；

（4）数据无统一访问控制体系。数据分散在不同的应用系统中，数据访问控制策略不相同，缺乏数据统一管理体系。

9.1.2 政务领域身份管理与访问控制能力分析

以特定系统为例，需要展开其系统所涉及的人员角色.存在数据以及数据与系统角色的关系进行初步分析，示例如下：

© 2023 云安全联盟大中华区版权所有

（1）整理系统角色，初步分为区领导.各局办领导.社区书记.区分拨人员.街道分拨人员.一级处置部门.二级处置部门.三级处置部门.街道督察员等内容；

（2)梳理系统存在的数据，分为实有人口.实有法人.疫情数据.民生诉求数据等。并分为定位这些数据的级别，分为公开级数据.普通级数据.敏感级数据.重要级数据（数据分类说明如 9.1.3 节所示）；

（3）定义数据级别和系统角色的关系，为角色授予数据权限。如普通级数据为那些角色可见，哪些角色脱敏可见等。

9.1.3 政务领域数据访问控制防护场景与技术说明

根据政府数据管控体系，需要将数据进行分级管理，示例如下：

级别	级别名称	定义
一级	公开级	依现行法律法规必须公开的信息；数据处理或泄露对数据对象（个人.企业.社会团体.党政机关及事业单位等）无负面影响，且不危害公共秩序.公共利益和国家安全
二级	普通级	数据处理或泄露会对数据对象（个人.企业.社会团体.党政机关及事业单位等）产生损害，或对公共秩序.公共利益产生轻微损害
三级	敏感级	数据处理或泄露会对数据对象（个人.企业.社会团体.党政机关及事业单位等）造成严重损害，或者对公共秩序.公共利益造成损害
四级	重要级	数据处理或泄露会对数据对象（个人.企业.社会团体.党政机关及事业单位等）造成特别严重损害，或对公共秩序.公共利益造成严重损害
五级	秘密级	依据法律.法规.规章不得共享和开放的数据；数据处理或泄露会对公共秩序.公共利益造成特别严重损害，甚至会损害国家安全（本办法不作讨论）

针对数据操作，需要进一步划分其安全级别，示例如下：

类别	级别	级别名称
操作级别	一级	低风险操作
	二级	中风险操作

© 2023 云安全联盟大中华区版权所有

	三级	高风险操作

根据数据敏感度不同建立数据主体.数据客体.数据操作的访问控制矩阵，示例如下：

角色		权限	公开级数据								普通级数据								敏感级数据								重要级数据							
			新增	修改	删除	批量修改	批量删除	查询	导入	导出	新增	修改	删除	批量修改	批量删除	查询	导入	导出	新增	修改	删除	批量修改	批量删除	查询	导入	导出	新增	修改	删除	批量修改	批量删除	查询	导入	导出
在编人员	区领导	区委	-	-	-	-	-	√	-	-	-	-	-	-	-	√	-	-	-	-	-	-	-	√	-	-	-	-	-	-	-	√	-	-
	处级领导	主要领导	-	-	-	-	-	√	-	-	-	-	-	-	-	√	-	-	-	-	-	-	-	√	-	-	-	-	-	-	-	√	-	-
		分管领导	-	-	-	-	-	√	-	-	-	-	-	-	-	√	-	-	-	-	-	-	-	√	-	-	-	-	-	-	-	√	-	-
	科室负责人	正职负责人	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	○	△	△	○	○	△	○	○	△	△	△	○	△	△
		副职负责人	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	○	△	△	○	○	△	○	○	△	△	△	○	△	△
	科级以下	公务员	√	√	√	○	○	√	√	√	√	√	√	○	○	√	√	○	○	○	△	△	△	○	○	△	△	△	△	△	-	△	△	△
非在编人员	在册不在编人员	雇员	√	√	√	○	○	√	√	√	√	√	√	△	△	√	√	△	○	○	△	△	-	○	○	-	△	-	-	-	-	△	-	-
		公共辅助员	√	√	√	○	○	√	√	√	√	√	√	△	△	√	√	△	○	○	△	△	-	○	○	-	△	-	-	-	-	△	-	-
	项目人员	常驻人员	√	○	○	○	○	√	√	○	√	○	○	△	-	√	√	△	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

注：√表示“低风险操作”，○表示“中风险操作”，△表示“高风险操作”，-表示“操作拒绝”

9.2 企业领域典型场景

9.2.1 企业领域数据使用场景与访问控制威胁分析

随着数字经济时代的序幕开启，企业数据作为核心生产要素被利用.开发而产生的价值日益凸显，数据的规模呈现爆发式增长态势，企业数据在使用场景中在不同行业有着相同的共性，又有着不同行业属性和特点，从数据类别来看一般企业数据主要包括业务信息数据和个人信息数据，从行业属性来看分为交通行业.能源行业.金融行业.教育行业.医疗行业.通信行业和互联网行业等。

通常企业的数据使用场景非常复杂，以电信领域为例，涉及办公环境.生产环境.研发运维环境等多种数据使用场景。从业务角度出发，可将数据分为以下类型：

- 通信记录：这包括电话通话记录.短信和多媒体消息的发送和接收记录。通信记录包括通话时间.通话持续时间.通话双方的号码.位置信息等。

© 2023 云安全联盟大中华区版权所有

- 位置数据：电信公司在提供移动电话服务时会收集和存储用户的位置数据，以支持定位服务和优化网络覆盖。这些数据用于确定用户的精确位置，通常以经纬度坐标的形式存储。

- 网络流量数据：电信公司监控网络流量，包括数据上传和下载速度.流量模式.数据包丢失率等，以确保网络性能和质量。这有助于识别瓶颈和改进网络基础设施。

- 账单数据： 电信公司生成客户账单，包括通信费用.数据使用费.漫游费用等。这些数据用于客户账单的准确计算和结算。

- 设备数据：电信公司会跟踪和管理与网络相关的设备，如手机.路由器.基站等。这些数据包括设备信息.注册状态.软件版本等。

- 用户身份数据：用户身份信息是电信领域的核心数据，包括用户姓名.电话号码.地址等。这些信息用于帐户管理.身份验证和客户支持。

- 业务支持系统数据：这包括电信公司内部的系统数据，如客户关系管理（CRM）.计费系统.网络管理系统等。这些系统用于管理业务流程和支持服务提供。

- 网络事件和警报数据：电信公司监控网络事件和警报，以检测异常活动.网络攻击和故障情况。这些数据用于网络安全和故障排除。

- 漏洞和安全事件数据：电信公司需要监视网络和系统以检测漏洞和安全事件。这些数据有助于及早发现潜在威胁，并采取适当的安全措施。

- 服务质量数据：电信公司测量和跟踪服务质量参数，如呼叫质量.数据速度.信号强度等。这有助于维护高质量的通信服务。

这些数据在电信领域中都是非常重要的，它们用于提供通信服务.网络管理.客户支持.账单生成.安全监控和业务优化等各个方面。电信公司需要有效地收集.

© 2023 云安全联盟大中华区版权所有

处理和保护这些数据，以提供可靠的服务并确保数据的安全和隐私。

大数据平台的建立，使得电信数据具有集中化等特点，但新的技术和架构使得电信大数据应用的系统边界变得模糊，传统基于边界的安全保护措施将变得不再有效，当前离散的数据安全防护和缺失的合规检测也不足以面对电信数据所面临的新的安全风险，因此，需要将重点放在数据本身的安全.身份管理和访问控制上才能适应大数据环境下的安全合规管控。

在保证数据流动（业务连续性）的情况下，要做好数据的安全防护以及满足合规要求，主要面临着以下挑战：

1.身份管理挑战

（1）口令管理困难：口令管理是一个常见的问题。许多人使用弱口令，重复使用口令，或者难以记住复杂的口令。这增加了口令泄露和入侵的风险。

（2）多因素认证难度： 尽管多因素认证提供了更高的安全性，但它也可能增加用户体验的复杂性。用户可能感到疲劳，因为他们需要不断验证自己的身份，尤其是在移动设备上。

（3）社会工程攻击：攻击者可能使用社会工程技术来获取用户的身份信息，如通过欺骗用户透露口令或其他敏感信息。这种类型的攻击不依赖于技术漏洞，而是依赖于欺诈。

（4）身份盗用：盗用身份是一种常见的问题，攻击者可能冒充合法用户，以获取访问敏感信息的权限。这种类型的攻击可能导致数据泄露和金融损失。

（5）隐私担忧： 用户对他们的身份信息的隐私担忧日益增加。数据泄露和滥用个人信息的事件导致用户担心他们的身份信息可能被滥用。

（6）技术复杂性： 一些身份识别技术可能需要大量的配置和管理，这对中小型企业来说可能是一项挑战。

© 2023 云安全联盟大中华区版权所有

2.访问控制挑战

（1）复杂的权限管理：随着电信业务规模的增长，权限管理变得越来越复杂。管理员需要管理数百甚至数千个用户的权限，这可能导致错误的配置和数据泄露。

（2）访问控制粒度不足：企业数据保护策略不够精确，使数据访问制控存在一定的风险，如授权管理与动态访问控制粒度不足等。

（3）过度授权：管理员可能存在过度授权用户，使他们获得了不必要的访问权限。这可能导致数据泄露和滥用。

（4）口令共享：用户可能共享他们的凭据，或者在未经授权的情况下使用他人的凭据来访问系统。这使得访问控制更加困难。

（5）监控和审计：监控和审计对于检测异常访问活动和滥用权限非常重要，但配置和维护这些系统可能很困难。

（6）复杂的环境：在混合云环境中，跨多个云提供商和本地数据中心的访问控制变得复杂。不同云环境可能有不同的访问控制机制。

（7）移动和远程访问：移动设备和远程访问增加了访问控制的复杂性。确保这些设备的安全性和合规性是挑战之一。

3.合规要求带来的挑战

缺少对大数据生命周期各环节即采集.传输.存储.使用.交换.销毁等作出数据安全合规检测和判断。

4.大数据安全管控挑战

（1）数据资产管理不清晰：数据量大且集中，分类分级管理开展难，数据资产梳理和识别不清晰，导致无法做到数据差异化和针对性的安全防护。

© 2023 云安全联盟大中华区版权所有

（2）现有数据安全防护手段离散：安全设备孤岛明显，无法形成安全联动，安全态势感知.应急处置能力亟需提升。

（3）数据开放增加了访问控制难度：大量的用户以及复杂的共享应用环境，导致大数据系统需要更准确地识别和鉴别用户身份，传统基于集中数据存储的用户身份鉴别难以满足安全需求。

（4）敏感数据共享风险：敏感数据跨部门.跨系统留存和使用，任一单位或系统安全防护措施不当，均可能发生敏感数据泄露。

9.2.2 企业领域身份管理与访问控制能力分析

企业领域身份管理与访问控制能力主要是从用户的身份管理.访问控制.权限管理和应用管理等维度进行监督与管控，基于用户数据使用风险研判结果进行动态处置，为参与到业务中的人.物.应用.服务等各类访问主体提供身份管理.访问控制.权限管理等能力。具体说明如下：

- 用户身份管理。用户身份主体定义与特征定义，如用户管理员.分级管理员.企业员工等身份定义。

- 用户访问控制。用户访问范围定义，如企业内财务部员工能访问财务系统.人事系统等访问规则，按照不同的员工标签设置规则。

- 用户权限管理。用户权限定义，如企业内财务主管能访问财务系统所有功能模块和数据，财务专员只能访问部分功能模块和部分数据。

- 用户应用管理。用户使用系统范围定义，如企业以公司名义购买云服务或设施，设置应用可见范围，并维护用户对应用的访问范围。①接入网关。设置用户对云平台和设施的访问范围，并依据风险指令自动更新网关控制策略。实现用户在不同网络环境.设备环境下使用应用防护.身份认证防护.传输加密防护等功能。②API 服务网关。设置用户及应用对 API 的使用范围.使用规则.控制规则，并依据风险指令自动更新网关控

© 2023 云安全联盟大中华区版权所有

制策略。以最小化原则设置 API“是否可见”“是否可用”“哪些能用”和“什么情况下能用”等属性。

- 使用风险研判结果动态处置用户权限与访问。当用户访问和被访问资源出现安全风险时，根据风险研判结果，下发处置指令，如通知.警告.回收权限(包括部分权限).阻断访问等。

9.2.3 企业领域数据访问控制防护场景与技术说明

保护好用户隐私和数据资产，持续强化大数据安全管理和保障，已成为发展大数据业务的关键。工信部在《大数据产业发展规划（2016-2020）》中将电信行业作为重点领域，在鼓励大数据业务发展创新的同时要求建设完善重要数据资源和信息系统的安全保密防护体系，防止其收集的众多用户数据受到侵害。然而，电信运营商的业务支撑网络存在区域和数据分散.系统繁多.环境复杂等特点，各个分散区域和系统中均会存储或使用大量的客户资料和企业核心数据，使得数据在不同的阶段都会存在不同的风险点。因此，必须综合考量，将离散的数据补救能力向综合的体系化数据合规检测与安全防护能力上延伸，提供针对性的信息安全技术措施和应用规范，采取合理的综合管控手段，以达到安全合规与安全防护的目标。

以电信大数据中心建设过程为例，重点对有价值类电信信息（客户积分.话费信息等）.客户类隐私信息（电话号码.轨迹等）.特征类识别信息（身份证.姓名等）在使用共享时开展智能化用户管理.访问控制和安全防护。通过统一数据安全管控平台的建设，以组件化.模块化方式，各个击破，实现对电信大数据的智能化安全合规检测与综合防护。在安全的基础环境下，通过融合数据分级分类管理.身份管理.访问控制.数据合规检测.数据动态/静态脱敏.数据水印追溯审计.UEBA(异常行为监测预警)等能力，建立一套完整的.创新的.实用的全生命周期数据安全合规检测与安全防护体系，激活电信数据生产力。

以实现统一数据安全管控为中心，将用户管理和数据访问控制融于“数据安全统一策略规则和分析展示平台”，针对电信各类业务平台.开发平台及运维平

© 2023 云安全联盟大中华区版权所有

所形成的数据，围绕数据安全全生命周期，从数据的采集.使用.存储.传输.共享等各个领域开展智能化安全合规检测与防护。依托数据安全管控平台的策略管理中心，对全生命周期合规检测与防护的各个组件进行统一策略设置.下发及部署，实现对电信大数据平台数据分级分类.用户管理鉴权.用户访问制控.用户行为分析（UEBA）.内容识别与管控等多项操作。通过分析统计中心，实现电信大数据安全态势的可视及数据安全风险管理，真正实现“一个中心，多级管控”的目标。

在用户管理建设方面，包括教育用户创建强口令，实施多因素认证，提高用户的身份意识，使用身份验证和访问控制技术，定期进行安全审查和更新。

在数据访问控制方面，包括精细的权限管理，教育用户不要共享凭据，实施监控和审计机制，使用现代身份管理和访问控制工具，定期审查权限配置，并确保移动和远程访问的安全性。

在电信大数据分级分类方面，实现用户个人信息安全保护的精细化管理，按各类用户信息的敏感程度，将用户信息进行分级。发现定位数据库中的敏感信息，分类并加密存储，同时跟踪哪些用户下载了敏感数据，控制敏感数据下载的生命期，个人信息做脱敏处理。对敏感数据保护；可对数据记录分配数据标签；可对应用用户分配用户标签，使用内置的算法实现对表的透明访问。同时，通过对电信大数据业务的全面摸底，进行敏感数据发现及梳理.数据资产分级.用户及敏感数据权限梳理等。避免一刀切的控制方式，在数据的安全管理上采用更加精细的措施。使数据在共享使用和安全使用之间获得平衡。

在电信大数据中心.云平台统一数据安全管控与合规检测方面，电信大数据平台离散数据安全问题，尤其是针对数据采集过程中的数据合规检测.数据使用安全管控（终端客户信息的水印追溯.终端异常行为管控.数据鉴权/业务鉴权<结构化数据>等）.数据传输安全管控（网络敏感数据传输监控.网络异常数据传输行为监控等）.数据共享安全管控（业务鉴权及业务数据访问控制）。

在电信大数据隐私数据开放共享防护方面，电信大数据的建设，关键是遵循数据流动的本质，大数据的开放与共享恰恰是遵照数据流动的本质出发，但是在

© 2023 云安全联盟大中华区版权所有

这个过程中，势必造成客户隐私信息.重要关键信息的泄露风险，因此在这个过程中既要保证数据的流动.正常使用，又要保障流动过程中的数据安全，通过数据脱敏泛化.数据模糊化技术，同时深度结合业务，根据不同的业务请求，实现对不同业务敏感数据的自动化动态脱敏。

从大数据全生命周期角度出发，综合考虑数据的合规使用以及安全防护，利用用户管理.访问控制.检测能力与数据安全防护技术，建立统一的认证.访问管理.安全合规检测和防护技术平台，改变数据安全防护离散的情况，解决数据安全合规检测缺失的难题，达到数据安全可控.风险可知的目标。

10 数据安全新技术展望

随着区块链技术.隐私计算等新技术体系的发展，数据安全管理与访问控制将迭代新办法与新场景。此刻，让我们先展望一下：

- 区块链技术与数字身份管理结合形成分布式的数字身份管理体系 DID，进而用户可以自主管理.授权以及回收个人身份信息。数据在流通过程中必然会涉及到多方数据访问与操作，而此时操作方的身份以及细粒度权限可以通过 DID 完成，保障多方共识后再进行数据操作，且此时数据访问与操作可以进行定位追溯；

- 隐私计算，其主要目标是实现“数据可用不可见，数据不动模型动”，从而使用户在不对外分享或者加密后再分享，即可获得数据处理结果，保护原始数据不被泄露。数据在分享时可以利用同态加密，以及结合用户身份信息（identity-based encryption， IBE）进行密文计算，此时可以在避免原始数据泄露的同时，并支持基于身份的数据访问控制，仅在身份被核验满足的情况下获取特定属性数据进行访问。当然，目前同态加密的性能还需要进一步增强；

- 机密计算，通过利用基于硬件的可信执行环境或 TEE 解决数据在内存的安全问题，敏感数据可以在内存中保持受到保护，直到应用程序告诉

© 2023 云安全联盟大中华区版权所有

TEE 对其进行解密以进行处理，从而保护工作负载免受未经授权的实体的侵害；

- 数字身份访问行为检测以及欺骗防御进行融合，从而保护数据的安全访问。近些年，身份威胁检测和响应 ITDR（Identity Threat Detection and Response）是相对较新的防御理念，是 Identity-First Security 中的重要组成部分。结合敏感数据特征可以建立欺骗陷阱，并与 ITDR 进行结合，从而防止数据被盗；

- 数据胶囊技术，通过访问者数字身份互信以及访问权限设定，可以设置数据的使用策略，并颁发对应的访问凭据，并连同加密后的数据.数据描述信息（声明）等封装成数据胶囊，并利用胶囊实行跨组织数据交换以及策略随行。

© 2023 云安全联盟大中华区版权所有

CSA GCR cloud security alliance
GREATER CHINA REGION

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网:https://c-csa.cn 电话:0755-86548359

地址:上海市浦东新区东育路255弄5号3FB30(前滩国际经济组织集聚区)/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905