

数据安全治理

第五章 数据加密技术

(重点章节)

商用密码

商用密码指对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品。

密码分为核心密码、普通密码、商用密码。

密码算法

常见的数据加密算法的分类

1. 对称加密算法

常见的对称加密算法：DES、AES、SM4，祖冲之密码ZUC

2. 非对称加密算法（公钥密码算法）

常见的非对称加密算法：RSA、SM2、SM9

3. 散列算法

常见的散列算法：MD5、SHA系列、SM3

4. 随机数生成算法

密钥管理

密码协议

数据加密技术作用

作用：真实性、机密性、完整性、不可否认性

DES对称加密算法

AES对称加密算法

RSA非对称加密算法

MD5散列算法

SHA1散列算法

SHA2散列算法

国内主要数据加密算法

国产加密算法分类

对称密码算法：SM4

非对称密码算法：SM2, SM9

密码杂凑算法：SM3

SM2椭圆公钥密码算法(ECC)

SM3散列算法(MD5)

SM4分组对称加密算法(AES & DES)

SM9椭圆加密算法

数字签名

确认数据的来源和完整性，防止他人更改和伪造

性质

不可伪造、不可抵赖、可信、不可复制、不可篡改

签名方案的过程

1. 系统初始化过程
2. 密钥对生成过程
3. 签名过程
4. 验证过程

经典数字签名算法

RSA数字签名算法

基于椭圆曲线的数字签名算法

基于身份的数字签名算法

第六章 数据脱敏技术

(此节基本上没怎么划重点)

数据脱敏

对敏感数据通过一定的规则对其 进行数据变形、屏蔽或仿真处理，从而实现对其可靠保护

数据脱敏的原则

有效性、真实性、高效性、一致性、合规性

数据脱敏流程

1. 识别敏感数据
2. 脱掉敏感数据
3. 评价敏感数据

数据脱敏类别

1.结构化数据脱敏

结构化数据指由二维表结构来逻辑表达和实现的数据

在数据库脱敏中，包含了静态数据脱敏和动态数据脱敏

2.非结构化数据脱敏

非结构化数据是指没有明确结构约束(或数据结构不规则、不完整)、没有预定义的数据模型、不方便用二维逻辑表来 表现的数据。主要包括图像数据、视频数据、非结构文本数 据等

在图像数据脱敏中，相关技术手段包括AI学习、差分隐私、去标识化、遮罩、添加噪声等。

数据脱敏方法类别

经典数据脱敏方法

1. 泛化类方法
在保留敏感数据原始值局部特征的情况下，使敏感数据总体特征被泛化。
截断方法、取整方法、归类方法
2. 抑制方法
在保持敏感数据相同长度的情况下，对原始数据部分信息或全部信息进行隐藏。
3. 扰乱类方法
对敏感数据加入噪声来进行干扰，以扰乱原始数据的精确值。
加密方法、散列方法、混淆方法
4. 仿真类方法
是指在对真实数据集的敏感信息脱敏后且 仅保留其基本特征前提下，重新构建数据集，以便在数据实 验或数据分析过程中，对数据集的关键特征做出模拟的行为 过程。

现代隐私保护方法

- 1. K-匿名化
对原始数据集进行脱敏，脱敏后的任意用户标识信息相同组合都至少出现K次
K值越大，保护个人隐私的强度就越大。
- 2. L-多样化
在k-匿名化的基础上，每一个等价类数据集里的敏感属性 必须具有多样性，即敏感属性至少有L个不同的取值
- 3. T-接近性
在L-多样化基础上，如果一个等价类敏感数据集的敏感属性概率 分布与全局数据库的敏感数据的敏感属性概率分布的距离比较接 近，小于阈值T，则称该等价类满足T-接近性约束。
- 4. ϵ -差分隐私
略

第七章 数据资产保护技术

数据资产

资产的定义

资产是指特定主体拥有或者控制的，由过去的交易或事项形成的，能持续发挥作用且能带来经济利益或提高工作效率的资源。

资产分类

有形资产和无形资产

数据资产的定义

是指特定主体合法拥有或者控制的，能进行计量的，能带来经济和社会效益的数据资源。

显然，数据资产是典型的无形资产。

数据资产的特性

增值性、共享性、控制性、计量性、非实体性、依托性、多样性、加工性

数据资产的五大要素

数据要素、法律要素、价值要素、业务要素、类别要素

数据资产管理的基本原则

治理先行原则、价值导向原则、权责分明原则、成本效益原则、安全合规原则

数据资产识别策略

1. 梳理数据资源
2. 识别数据资产
3. 登记数据资产

数据资产确权策略

1. 确认数据资产权属
2. 存证数据资产特性

数据资产应用策略

1. 识别数据资产来源
2. 评估数据资产价值
3. 溯源数据资产应用过程

数据资产盘点策略

1. 编制数据资产盘点计划
2. 组织数据资产盘点人员
3. 实施数据资产盘点计划
4. 处理数据资产盘点问题

数据资产变更策略

1. 建立数据资产变更机制
2. 评审数据资产变更方案
3. 实施数据资产变更方案

数据资产处理策略

1. 建立数据资产处理机制
2. 评审数据资产处理方案
3. 实施数据资产处理方案

成本评估法

数据资产评估值 = 重置成本 X (1 - 贬值率)


Advantage:

容易理解、计算简单、便于操作、落地

应用对象:

一次数据资产、二次数据资产、三次数据资产

收益评估法

 image-202311111114355438

Advantage:

能充分反映数据资产的经济价值、容易被交易各方接受

应用对象:

二次数据资产、三次数据资产

市场评估法

数据资产价值评估值 = 可比案例数据资产的价值 × 技术修正系数 × 价值密度修正系数 × 期日修正系数 × 容量修正系数 × 其他修正系数

Advantage:

能客观反映数据资产的市场情况、评估参数及指标来源于市场，相对真实可靠

应用对象:

一次数据资产、二次数据资产、三次数据资产

数据资产评估体系（不考）

数据资产安全保护

目标：确保数据资产安全可控，进行真实性、机密性、完整性、不可否认性的保护。

第八章 数据资产交易技术

数据资产交易

概念

是一种对数据进行买卖的行为，是数据供给方与数据需求方通过交易机构或者双方契约合法合规地完成数据买卖的过程

基本组成

数据资产、交易平台、数据供给方、数据需求方

主要特点

资产形态、交易主体、交易模式、交易内容

资产形态

1. 一次数据资产

指有价值的原始数据

eg. 个人文献数据(如笔记、手稿等)、企业业务数据(如会议记录、生产现场实时数据等)、政务专题数据(如干部基本信息、窞井盖位路信息等)，等等

2. 二次数据资产

指对有价值的原始数据进行初加工(如标注、加密、脱敏、融合、汇聚等)后形成的数据集

eg. 个人数据集(如人脸数据、健康数据等)、企业数据集(如AI训练数据集、AI测试数据集、某城市居民用水记录等)、测绘数据集(如地图数据集、遥感数据集等)、政务数据集(如城市管网数据集、行业数据报表等)、文献数据(如文摘、索引等)、数据算法、数据模型，等等

3. 三次数据资产

指在二次数据资产基础上，对某一范围内的原始数据进行深加工(如专题分析、研究、开发等)后形成的数据系统或产品

eg. 人脸识别系统、人体体态分析系统、OCR文字识别系统、语音识别与合成系统、商业数据专题分析报告、文献数据资源平台(如超星、维普等)等相关数据产品

交易主体

卖方(数据供给方)、买方(数据需求方)以及中介方(数据交易中间商，如数据交易平台)

交易模式

按交易对象：数据资产交易分为企业/企业(B2B)模式、企业/个人(B2C, C2B)模式、个人/个人(C2C)模式。

按产权转让：数据资产交易分为所有权转让模式、使用权转让模式、收益权转让模式。

按金融模式：数据资产交易分为一级市场模式、二级市场模式。

交易内容

1. 可交易内容
2. 不可交易内容

数据资产交易面临的问题

1. 数据真实性
2. 数据合规合法
3. 数据安全
4. 其他(如数据的确权、定价等问题)

数据资产确权

概念

数据资产确权是指确定数据在全生命周期过程中产生数据资产的所有权、使用权、收益权、管理权、安全权的归属和职能。

问题

- 1. 数据资产确权不同于物质资产确权
- 2. 数据资产确权边界难以划分
- 3. 数据资产确权缺乏法律依据

原则

- 1. 利益平衡原则
- 2. 数据资产分类原则
分为个人数据资产、企业数据资产、社会数据资产
- 3. 数据资产分级原则
分为私有品数据资产、准公共品数据资产、公共品数据资产

准则

- 1. 效益优先准则
- 2. 先易后难准则
- 3. 先公后私准则

数据资产定价

方法

静态定价法

- 1. 固定定价法
- 2. 差异定价法
- 3. 拉姆齐定价法

动态定价法

- 1. 自动定价法
- 2. 协商定价法
- 3. 拍卖定价法

数据资产交易监管

原则

- 1. 安全第一原则
- 2. 权责一致原则
- 3. 分级监管原则

模式

- 1. 监管机构宏观监管模式
- 2. 行业组织自律监管模式
- 3. 交易主体内部监管模式

事前监管

事中监管

事后监管

数据资产交易平台

主要特征

平台类型、数据来源、产品类型、产品领域

第九章 数据审计技术

数据审计

概念

是指依照数据安全策略，对ICT设施设备系统的数据安全事件进行数据采集、事件审计、统计分析，从而发现系统漏洞、入侵行为或改善系统性能的过程

分类

- 1. 数据库审计
- 2. 主机审计
- 3. 网络审计
- 4. 应用审计

流程

- 1. 数据采集
- 2. 事件审计
- 3. 统计分析

作用

1. 事前
2. 事中
3. 事后

数据库审计

数据采集模式

1. 镜像模式（流量转发）
2. 探针模式

采集内容

1. 用户基本信息
2. 数据定义语言信息
3. 数据操作语言信息
4. 数据控制语言信息
5. 操作时间信息
6. 操作结果信息

主机审计

网络审计

应用审计

第十章 数据司法存在技术

电子数据

定义

电子数据是指基于计算机应用和通信等电子化技术手段形成的信息数据，包括以电子形式存储、处理、传输、表达的静态数据和动态数据

基本特性

1. 复制性
2. 虚拟性
3. 易变性
4. 稳定性

电子数据存证

电子数据司法存证是指服务方通过互联网或电子存证服务平台向使用方提供电子数据证据保管和验证的服务过程，以提升其司法证明力。

方式

1. 自行存证
2. 公正存证
3. 第三方存证平台存证

数据存证的基本原则

1. 合法性原则
2. 及时性原则
3. 保密性原则
4. 全面性原则

具体要求

1. 存证数据要求
2. 存证数据传输要求
3. 存证数据验证要求
4. 存证数据验证结果要求
5. 数据检索要求
6. 隐私保护要求

第三方数据存证平台

独立型存证平台、公证型存证平台、鉴定型存证平台

采用的技术

PKI技术、时间戳技术、商用密码技术、区块链技术