

源于社区 服务社区

 中国DevOps社区峰会 2023 · 广州



应对挑战：剖析数据传输的安全难题

张晓辉 Flomesh 高级架构师





张晓辉 Flomesh 高级架构师

- 资深程序员
- CNCF Ambassador
- LFAPAC 开源布道师
- 云原生社区管委会成员
- 微软 MVP
- 公众号“云原生指北”作者
- 多年的微服务和云原生实践经验，主要工作涉及微服务、容器、Kubernetes、DevOps 等



目录

- 1 数据传输基本概念和模型的介绍
- 2 数据传输在数据治理中的角色
- 3 数据传输的安全难题
- 4 数据传输的安全性保障实践
- 5 Q&A





数据传输基本理念和模型

- 数据传输的定义
- 常见的数据传输模型和协议

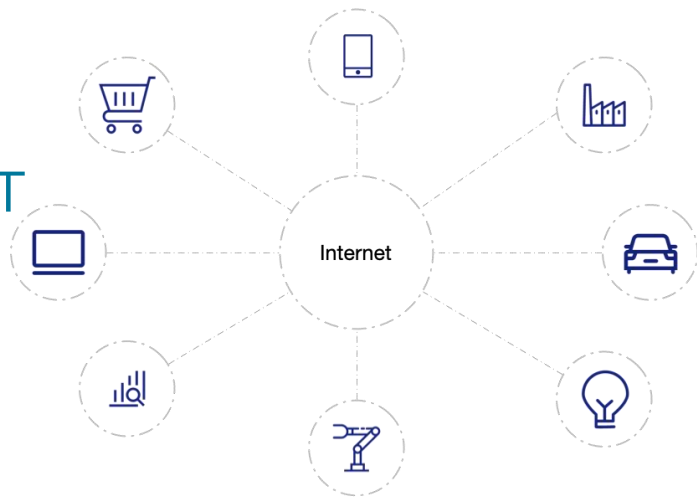




数据传输 - 定义

在不同系统、设备或网络之间移动或复制数据的过程。

它是信息技术、云计算、物联网IoT等领域的基础。





数据传输模型

客户端/服务器、点对点、发布/订阅、请求响应

- 网络协议

- Wi-Fi
- LTE CAT 1
- LTE CAT M1
- NB-IoT
- Bluetooth/BLE
- ZigBee
- LoRaWAN

- 数据协议

- AMQP
- MQTT
- HTTP
- CoAP
- DDS
- LwM2M





数据传输在数据治理中的角色

- 数据治理的定义和重要性
- 数据传输在数据生命周期中的作用



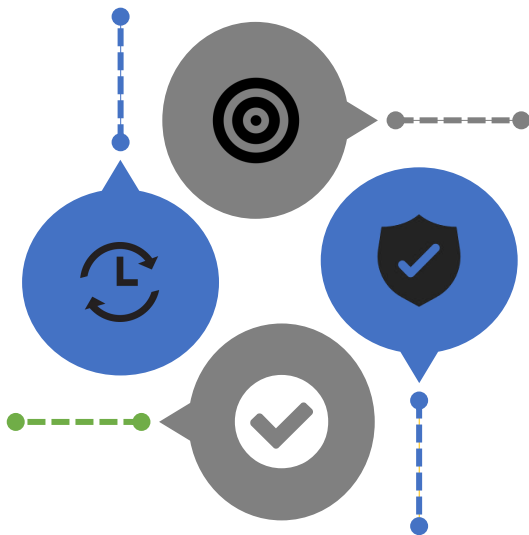
数据治理

可用性

确保数据在需要时总是可访问和可用的。如冗余机制、负载均衡、高可用性架构、监控等。

可靠性

确保数据在传输过程中准确无误地从源头传达到目的地，且在传输过程中不会丢失或损坏。如确认和重传、数据校验、流量控制、网络监控、端到端加密等。



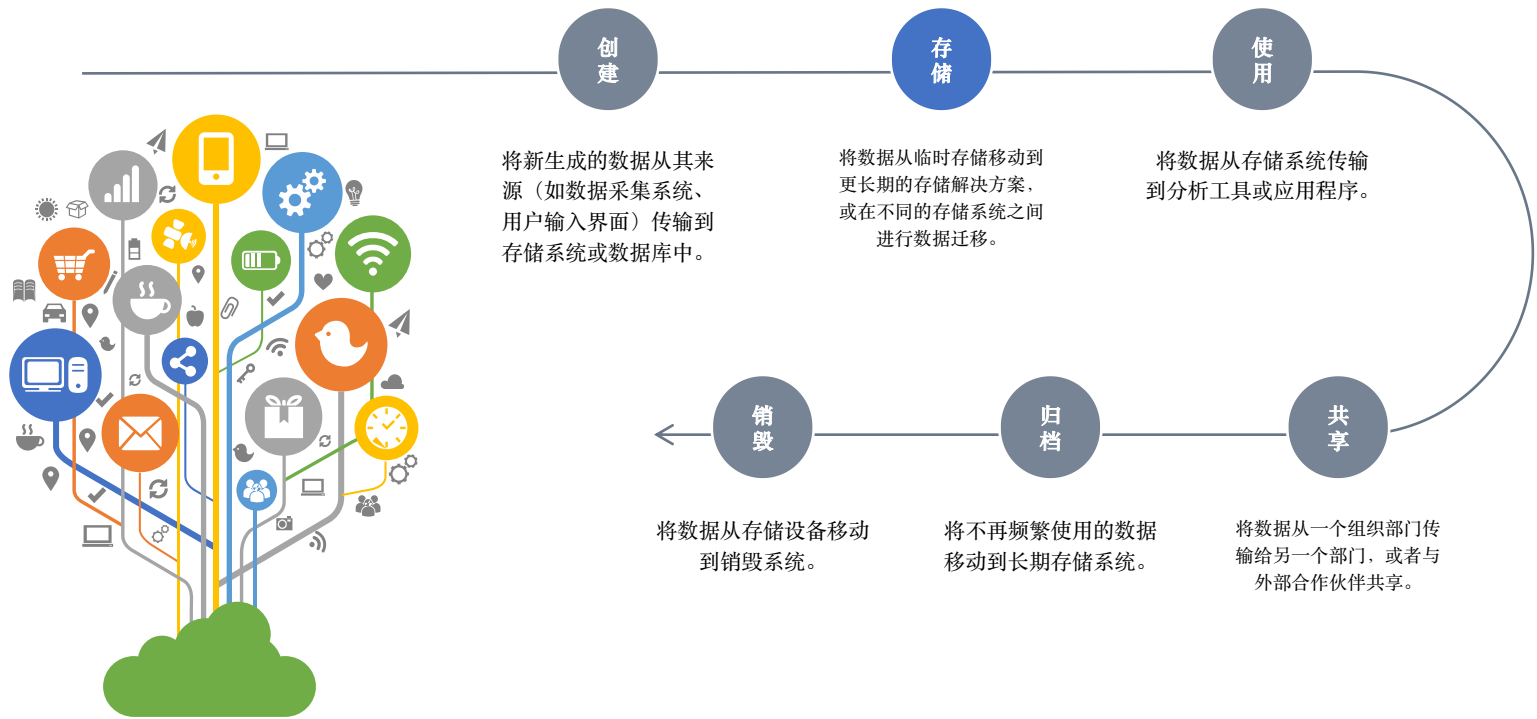
完整性

确保信息在源头和目的地之间未被篡改的关键。如散列值、签名、机密、序列号和时间戳、确认和重传等。

安全性

确保在传输过程中数据不被未经授权访问、泄露、篡改或破坏的关键。如加密、身份验证授权、安全协议、VPN和隧道、策略。

数据传输在数据生命周期中的角色





数据传输的安全难题

- 常见的安全挑战



数据传输的安全挑战



身份验证

确保数据安全和维护有效数据治理。保护数据免受未经授权访问，维护数据的完整性和可靠性，同时支持合规性和审计要求。

- 非授权访问
- 身份盗用



数据加密

在数据传输过程中，加密确保只有授权的接收者能够访问和理解数据内容。保护数据隐私、确保合规性、防止数据泄露和篡改、增强用户信任以及支持安全的数据共享等

- 加密算法的强度
- 密钥管理问题

其他挑战

- 网络拦截和数据截获，中间人攻击
- 数据完整性问题，由于网络错误、恶意攻击或系统故障而遭到篡改或损坏
- 端点安全问题，因为恶意软件、钓鱼攻击、用户失误或未经授权的访问而受到威胁。





数据传输的安全性保障实践

- 身份验证强化
- 数据加密传输
- 信创保障方案
- 隧道技术
- 防御恶意流量和负载过滤

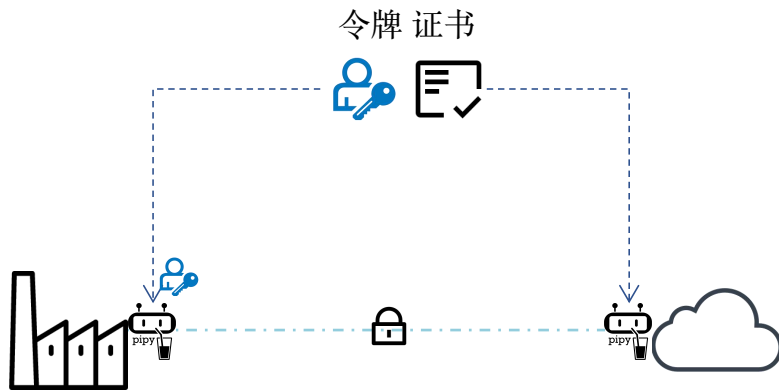




加强身份验证

技术

- 代理 Pipy
- 证书、令牌管理
- 双向认证 mTLS
- 授权



案例

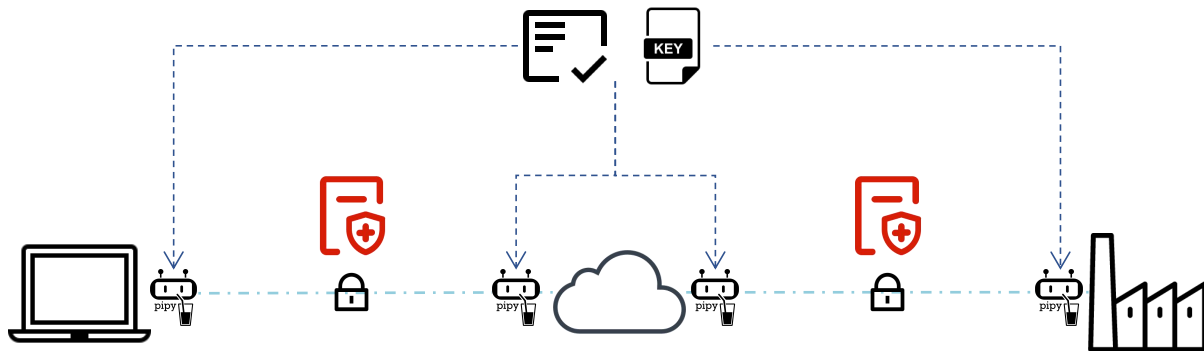
- 金融行业使用 mTLS 来增强通信安全，并符合对数据保护和隐私的严格监管要求。
- 云服务提供商提供基于角色的访问控制（RBAC），为不同用户和服务分配不同的权限。



数据加密实践 - 加密传输

技术

- 代理 Pipy
- 证书密钥管理
- 加密 TLS
- 签名



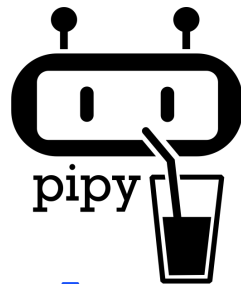
案例

- 智能家居设备使用端到端的加密，为每个设备实施唯一的身份验证机制，并使用安全的通信协议如 SSL/TLS。以此保护用户隐私数据、增强设备安全、符合法规要求。



数据加密实践 - 信创

- 自主研发的代理 Pipy
- 支持国密 sm2/3/4、zuc
- 支持铜锁 openssl



Tong 铜锁
SUO





数据加密实践 - 隧道

技术

- 代理 Pipy
- 正向隧道
- 反向隧道
- SSL/TLS/SSH



案例

- 建立从设备/边缘云到云平台的隧道，将数据安全地传输到云平台。这种隧道可以在不安全的公共网络上建立安全的“隧道”。





防御恶意流量和负载过滤

- **WAF**：在通过分析 HTTP 流量来保护网络应用程序免受各种攻击。监控、过滤和阻挡恶意流量，以防止针对Web应用程序的攻击，如跨站脚本（XSS）、SQL注入、会话劫持等。
- 使用 **Pipy** 和 **ModSecurity** 打造可编程的 WAF。
 - 可编程性
 - 完全控制
 - 平台无关
 - 实时监控
 - 威胁检测和预防
 - 自定义规则开发
 - 日志和报告



Pipy + ModSecurity





Q&A



关注我们



flomesh.io



github.com/flomesh-io



flomesh-io.slack.com



源于社区 服务社区

THANKS!

