青莲云安全白皮书

[20200102]

V2.0

北京市朝阳区祁家豁子 8 号健翔大厦 5 层 502
商务合作：biz@qinglianyun.com

【版权声明】

【商标声明】

【服务声明】

本文档意在向客户介绍青莲云全部或部分产品、服务在当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的青莲云产品、服务的种类、服务标准等应由您与青莲云之间的商业合同约定，除非双方另有约定，否则，青莲云对本文档内容不做任何明示或模式的承诺或保证。

目 录

北京市朝阳区祁家豁子 8 号健翔大厦 5 层 502
商务合作：biz@qinglianyun.com

1 白皮书介绍

物联网云平台是物联网产业链中不可或缺的一环，青莲云作为安全的物联网云平台提供商，竭诚为客户提供安全、可信、合规的云服务，帮助客户实现其硬件产品安全快速联网需求的同时，保证客户系统及数据的保密性、可用性和完整性。

本白皮书介绍了青莲云云安全体系，内容包括：

- 青莲云介绍
- 安全责任共担
- 合规性
- 青莲云安全

2 青莲云介绍

青莲云是国内首家安全可信的物联网云平台，为企业客户提供智能硬件安全联网解决方案，保证硬件产品的安全性，保证用户隐私不被泄露，帮助企业树立安全、可信、智能的品牌形象。同时提供一站式的智能硬件研发服务，结合青莲云 MCU SDK 和青莲智能 APP 助力企业快速实现智能升级，加速硬件智能化。

青莲云一直专注于物联网安全领域和高性能云平台的前沿技术研究，基于自主研发的物联网安全网关实现对设备的身份鉴权、密钥保护、会话管理、行为监控等安全策略的整合，结合后端稳定的分布式高性能物联网云计算平台，为企业客户提供诸如消息推送、告警管理、安全 OTA 升级、设备联动、应用授权、数据分析、自动化运维等功能，实现安全快速的产品接入和持续稳定的业务平台支撑。在帮助企业快速实现智能化转型升级的同时，提供持续的物联网安全防御能力，实现产品的安全研发和设备集中管理的统一。

3 安全责任共担

基于青莲云的服务模式，其安全责任需要三方共同承担：青莲云负责在基础云服务（阿里云）之上的所有云服务、API 服务、SDK 服务和数据交互的安全管理和运营，同时在云上和规范使用青莲云解决方案接入方式的数据交互的安全性负责；阿里云确保基础云服务平台的安全性；客户负责自身业务安全，包括硬件的业务逻辑安全和 APP 的业务逻辑安全。

安全责任共担模式之下，青莲云在阿里云提供的安全基础云服务上，为客户提供降低 IoT PaaS 服务的风险，使客户安心使用 IoT BaaS 服务，更专注于核心业务的发展。

3.1 青莲云的安全责任

青莲云覆盖数据安全和云服务安全，青莲云承诺利用其安全团队以及全球范围内知名的安全服务厂商的攻击防护技术方面的专业经验，提供云平台的安全运维和运营服务，切实保护青莲云的安全运营，以及保障客户、终端用户隐私和数据的安全。青莲云应保护客户的阿里云账户，合作关系解除后，青莲云应主动删除客户的账户信息，除非客户请求，否则不再用客户的账号进行任何操作。

主要覆盖但不限于如下：

- 数据安全：指客户在云计算环境中的业务数据自身的安全管理，包括数据收集与识别、权限与加密等方面。
- 访问控制管理：对资源和数据的访问权限管理，包括用户管理、产品管理、设备管理、应用管理、授权管理等。

- 云服务安全：青莲云提供的云平台系统安全、硬件 SDK、APP SDK、API 接口等安全。
- 通信链路安全：青莲云的通信全部采用 AES 或 SSL 进行加密传输和算法签名，保障了数据传输的安全性，能够有效的防重放攻击、防数据篡改。

3.2 客户的安全责任

物联网企业客户基于青莲云公有云或私有云服务，开发自己的智能硬件和 APP/小程序，综合运用青莲云产品的安全功能，客户应负责自身硬件和 APP 的业务本身的安全。

客户应保护自身的账户安全，包括青莲云账户、第三方账号。在客户不再需要青莲云进行技术支持的情况下，请务必要求青莲云删除客户的相关账号密码的存储，或自行修改原有密码，以保障账户安全。

3.3 供应商的安全责任

青莲云选择了全球知名的云主机服务商阿里云作为公有云服务的供应商，阿里云负责基础设施、物理设备、分布式云操作系统及云服务产品安全，并为客户提供保护云端应用及数据的技术手段。

- 阿里云保障云平台自身安全:
- 保障云数据中心物理安全;
- 保障云平台硬件、软件和网络安全，如操作系统及数据库的补丁管理、网络访问控制、DDoS 防护、灾难恢复等;
- 及时发现云平台的安全漏洞并修复，修复漏洞过程不影响客户业务可用性;
- 通过与外部第三方独立安全监管与审计机构合作，对阿里云进行安全合规与审计评估。
- 阿里云为客户提供保护云端信息系统的技术手段:
- 为客户提供多地域、多可用区分布的云数据中心以及多线 BGP 接入网络，使得客户可利用阿里云基础设施构建跨机房高可用的云端应用;
- 云账户支持主子账号、多因素认证、分组授权、细粒度授权、临时授权;
- 为客户提供安全审计手段;
- 为客户提供数据加密手段;
- 为客户提供云盾安全服务;
- 引入第三方安全厂商，为客户提供个性化的行业安全解决方案。

4 合规性

青莲云遵守国际权威机构的安全标准和行业要求，将团队多年的企业级安全产品和大规模云计算平台研发及服务经验，融入到云平台的安全防护中，将众多的安全合规标准融入到青莲云安全产品中。到目前为止，青莲云拿到多家机构的认证，是一家拥有多个认证的 IoT 解决方案提供商。

4.1 合规性

4.1.1 ISO 27001

ISO 27001 是信息安全领域的国际管理体系标准，从数据安全、网络安全、通信安全、操作安全等各个方面证明青莲云平台履行的安全职责，保障企业信息的完整性、可用性、保密性。青莲云正积极准备通过第三方机构的 ISO 27001 的认证审核，以满足国际管理体系的标准来为客户提供更安全的服务，使客户的信息安全得到国际认可的安全合规保障。

4.1.2 ISO 27017

ISO 27017 是云安全管理体系认证，为适用于提供和使用云服务的信息安全控制提供指导，推荐实施专门针对云的信息安全控制。此实施规程针对云服务提供商提供了更多信息安全控制实施指导。青莲云正积极准备通过第三方机构的 ISO 27017 的认证审核，以符合 ISO 云安全管理体系标准的云服务，为客户的云平台提供更安全合规的云端功能。

4.1.3 ISO 27018

ISO 27018 是公有云中作为个人可识别信息（PII）处理器的个人身份信息保护实用规则，针对保护云中个人数据安全的国际实施规程。青莲云正积极准备通过第三方机构的 ISO 27018 的认证审核，以验证平台对个人数据的保护实施，为企业对终端客户的数据保障提供标准支持。

4.1.4 工信部“智能硬件（IOT）开放平台”的测试评估

青莲物联网云平台软件在 2017 年智能硬件（IOT）可信评估（第二批）中，通过了移动智能终端技术创新与产业联盟“智能硬件（IOT）开放平台”的测试评估。青莲云在功能完备性、性能指标、安全可靠性、资源调配能力、故障恢复能力、数据安全保护能力等多方面均受到了认可。

4.2 隐私保护

青莲云深知用户信息安全的重要性，我们将按照法律法规要求，采取安全保护措施，对用户个人信息进行保护。青莲云将严格执行公开发布的《青莲云隐私权政策》，切实保护用户隐私。

基本原则：收集最小化数据原则，不收集和提供的服务无关的信息。

4.2.1 企业客户与云平台开发者的隐私数据收集和使用

（1）充分的用户知情权

- 隐私条款必须包含收集的所有用户数据及这些数据用来提供的服务。
- 隐私条款必须在涉及注册、更新等重要时机通过邮件等方式告知用户。
- 隐私条款必须包含数据收集、删除、保存、用户选择权等。

（2）网站 Cookie 声明

Cookie 的作用及用户选择权。

（3）用户权限

- 访问权：用户可通过 web 平台访问青莲云收集的个人数据、无需另外技术支持。
- 被遗忘权：用户拥有账户注销权限。
- 纠正权：对于用户主动提供的个人信息，如果存在不准确的情况，可在 web 上手动修改。

（4）隐私数据传输

- 内容脱敏或加密：使用 AES/SSL 加密数据内容，在不影响业务使用的情况下，数据脱敏后传输。
- 传输通道加密：证书双向认证。
- 密钥管理：安全可靠的秘钥管理，完整的密钥全生命周期的管理，包括创建、激活、禁用、转换、分发、备份、销毁等，同时基于密钥的数据加密存储。

（5）隐私数据使用

- 精细粒度的云存储访问权限控制，用户的数据存储在青莲云上，我们会为每个人分

配最小/仅必要的权限，确保不能访问到不该被访问的数据。

- 登录限制，所有内部系统只允许在公司内网访问。且有严格的账户权限级别，只有管理员才有数据访问权限。

（6）隐私数据保存

- 对敏感数据进行集中地分布式存储，统一监控管理，通过 VPC 隔离。
- 所有 APP/硬件的 API 做数据权限隔离，确保不同用户，不同设备之间不能不经授权的互相访问。
- 文件数据加密，云存储在 AWS/阿里云上，使用 AES256 加密。
- 数据库加密，对所有隐私信息进行加密或 hash。

（7）隐私数据删除

敏感数据的归属方有权限对数据进行删除操作，用户可以通过云平台上的账号注销功能或提交反馈/联系官网客服的方式对数据做完全的删除。

4.2.2 Demo APP 开发者的隐私数据收集和使用

（1）充分的用户知情权

- 隐私条款必须包含收集的所有用户数据及这些数据用来提供的服务。
- 隐私条款必须在涉及注册、更新等重要时机通过邮件、APP 弹窗等方式告知用户。
- 隐私条款必须包含数据收集、删除、保存、用户选择权等。

（2）用户权限

- 访问权：用户可通过手机 APP 访问青莲云收集的个人数据、无需另外技术支持。
- 被遗忘权：用户拥有 APP 账户注销权限。
- 纠正权：对于用户主动提供的个人信息，如果存在不准确的情况，可在 APP 上手动修改。

（3）隐私数据传输：

- 内容脱敏或加密：使用 AES/SSL 加密数据内容，在不影响业务使用的情况下，数据脱敏后传输。
- 传输通道加密：证书双向认证。
- 密钥管理：安全可靠的秘钥管理，完整的密钥全生命周期的管理，包括创建、激活、禁用、转换、分发、备份、销毁等，同时基于密钥的数据加密存储。

（4）隐私数据使用

- 精细粒度的云存储访问权限控制，用户的数据存储在青莲云上，我们会为每个人分配最小/仅必要的权限，确保不能访问到不该被访问的数据。
- 登录限制，所有内部系统只允许在公司内网访问。且有严格的账户权限级别，只有管理员才有数据访问权限。

（5）隐私数据保存

- 对敏感数据进行集中地分布式存储，统一监控管理，通过 VPC 隔离。
- 所有 APP/硬件的 API 做数据权限隔离，确保不同用户，不同设备之间不能不经授权的互相访问。
- 文件数据加密，云存储在 AWS/阿里云上，使用 AES256 加密。
- 数据库加密，对所有隐私信息进行加密或 hash。

（6）隐私数据删除

敏感数据的归属方有权限对数据进行删除操作，用户可以通过 app 上的账号注销功能或提交反馈/联系官网客服的方式对数据做完全的删除。

4.3 数据存储区域

公有云数据存储：中国，数据保存在中国华北 2 和华东 1，由阿里云提供基础云计算支持。阿里云的数据库备份 DBS 提供数据库异地备份能力，满足企业数据异地容灾需求。

私有云数据存储：由客户提供服务器，数据保存在客户提供的服务器上。

5 青莲云安全

5.1 云平台安全基础架构

图 5-1 青莲云安全体系架构

青莲云对安全问题尤为重视，采用分层部署、纵深防御的方式，分别从设备安全、云端安全、数据安全、传输安全、应用安全等多层次进行安全部署，并采用多端协同防御的方式，行成一个安全闭环，不断持续迭代，以保障用户及硬件设备的信息安全。

5.2 云平台系统安全

5.2.1 物理安全

青莲云作为物联网云计算服务提供商，青莲云平台着力为每一个公有云客户提供安全、稳定、持续、可靠的物理设施基础。青莲云公有云服务器部署在阿里云机房，数据中心建设满足 GB 50174《电子信息机房设计规范》A 类和 TIA 942《数据中心机房通信基础设施标准》中 T3+标准。

技术部支持人员、安全管理员、IT 运维部以及其他人员可能因工作需要访问信息资源物理设施。对信息资源设施物理访问的批准、控制以及监控对于全局的安全是极其重要的。青莲云中负责信息资源安装和支持的所有人员，负责信息资源安全的人员以及数据的所有者，都应遵守 IT 运维部发布的《青莲云物理访问策略》，以保障青莲云物理安全。

5.2.2 人员管理

青莲云数据库和云平台各部分代码均对各开发中心人员开放对应访问权限，若人员转岗或离职，权限立即收回。

青莲云基于员工工作岗位和角色，遵循最小权限和职责分离原则，授予员工有限的资源访问权限。公司为根据员工工作需要，为每个员工设置不同的 SVN 访问权限，若人员转岗或离职，权限立即收回。青莲云员工在未经授权或获得明确同意的情况下，不可以尝试访问公司内部系统中包含的任何数据或程序。

青莲云不定期展开针对业务、代码、产品的安全技术培训，以提高青莲云员工技术能力和安全意识，每个员工直接对自己的操作行为负责。

5.2.3 数据存储

接入青莲云公有云的客户，青莲云提供通用公有云服务，并按接入公有云的设备数量收费，设备一旦接入青莲云公有云，即将设备和用户数据存储到青莲云公有云，数据将永久存储。

接入青莲云私有云的客户，由客户提供私有云服务器，青莲云提供私有云部署和技术支持服务，设备与用户等数据存储到客户的服务器，数据保存期限由客户购买服务器的期限决定。

5.3 网络通信安全

青莲云平台上的通信都收到了 HTTPS 安全协议的加密保护，提供的 API 接口也具有完善的 HTTPS 加密等安全能力，能够对客户提供端口级别的安全保障。设备端和云平台之间也是通过 SSL 或者 AES 进行通道加密和数据加密进行传输。

5.4 网络隔离和访问控制

青莲云平台上的通信都收到了 HTTPS 安全协议的加密保护，提供的 API 接口也具有完善的 HTTPS 加密等安全能力，能够对客户提供端口级别的安全保障。设备端和云平台之间也是通过 SSL 或者 AES 进行通道加密和数据加密进行传输。

青莲云制定了严格的内部网络隔离规则，通过物理和逻辑隔离方式实现内部的办公网络、开发网络、测试网络、生产网络等的访问控制和边界防护；青莲云确保非授权人员禁止访问任何内部网络资源；以及所有员工如需从公司网络前往生产网络开展日常运维时，都必须经过严格的审批和权限控制，才能登录生产系统。同时，针对云端用户层面的网络访问隔离，青莲云提供虚拟化控制层资源访问控制策略、云平台内部私有网络间隔离策略、 Web 控制台权限分配与身份验证、接口会话 ID 与访问密钥等安全机制，确保客户只能访问其用户产生的相关数据，有效实现多客户之间的访问隔离。

5.5 网络冗余

青莲云数据服务云主机遍布全球多个区域，构建了网络跨地域的灾备能力，能够最大化的减小非人为因素导致的网络故障的业务影响。同时，采用冗余的网络建设方式，同时同城也采用多物理机房部署，能够实现网络的便捷性和流量附和的工程调度，确保网络服务不会因为单点故障而中断，实现同城和跨城容灾。同城多机房网络冗余部署如下图：

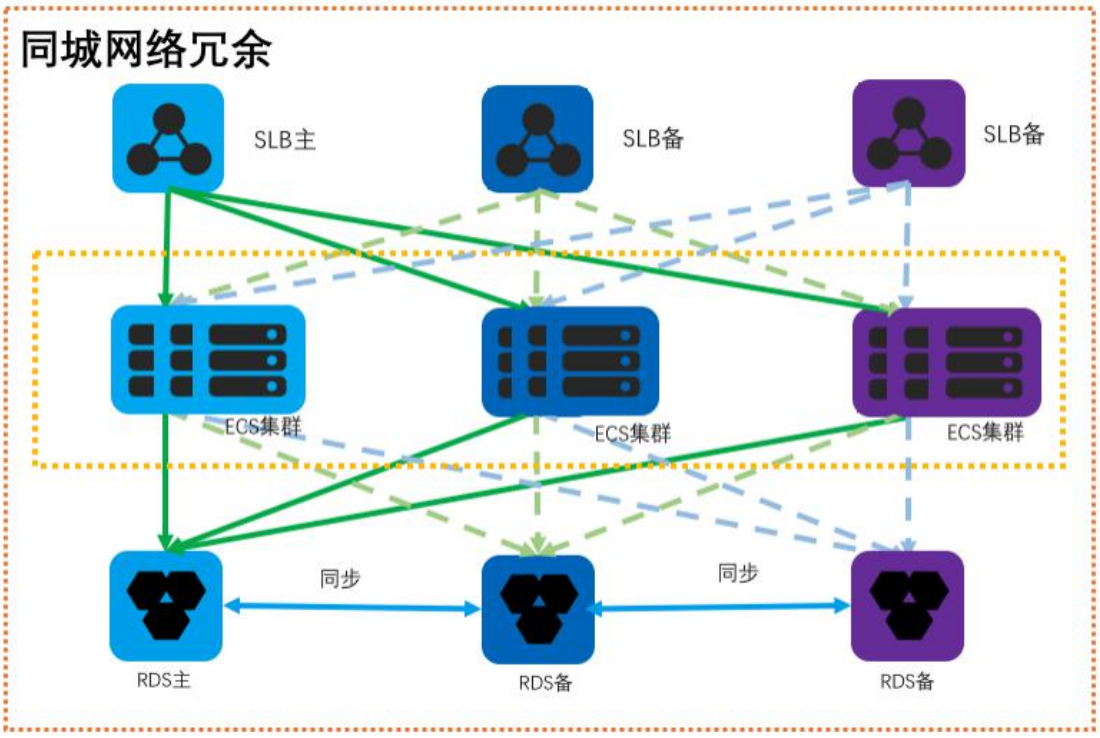

图 5-2 青莲云同城多机房网络冗余部署

5.6 云服务器供应商要求

青莲云选用的云服务商，提供的基础云服务满足的服务可用性应为：

（1）服务器可用性：①对于单实例维度，承诺一个服务周期内 ECS 的服务可用性不低于 99.95%；②对于单地域多可用区维度，承诺一个服务周期内 ECS 的服务可用性不低于 99.99%；

（2）负载均衡可用性：多可用区实例服务可用性不低于 99.95%，单可用区实例可用性不低于 99%；

（3）RDS（即数据库）服务可用性不低于 99.95%；

（4）CDN 服务可用性不低于 99.9%。

5.7 硬件 SDK 安全

5.7.1 安全双向身份验证机制

青莲云采用的强安全身份验证机制，需要接入设备和云端进行多次认证交互。

5.7.2 基于会话管理的安全机制

设备接入物联网，在安全连接的基础上需要加入会话的机制，保证连接的安全生命周期非永久。当设备的安全连接会话超时，设备被强制断开连接，重新进行安全连接。安全的会话管理机制保证设备通信逻辑隔离。不同设备直接的通信从逻辑上进行区分，确保会话的唯一性和安全性。即使同一台设备上运行多个连接实例，连接通信完全没有关系，各自不会相互影响。

5.7.3 OTA 机制

- 高度集成到 SDK，采用闭合的 OTA 升级逻辑
- 采用基于有限状态机的方式维持 OTA 升级的状态

- 可自动从升级异常状态恢复正常状态
- OTA 升级源可性验证
- 严格的 OTA 数据块签名验证
- 严格的 OTA 数据确认逻辑

5.8 APP SDK 安全

SDK 的所有 API 接口都是通过 HTTPS 安全协议的加密保护，而且涉及到的隐私数据通过加密之后进行传输。所有发布出去的 SDK 都进行严格代码安全扫描，对扫描发现的漏洞或者隐患进行修复，确保通过代码安全扫描之后才能正式发布使用。

5.9 数据库安全

青莲云对数据库的权限进行严格的统一管理和限制，并且对所有数据库的增删改查都进行完备的日志审计。

5.10 运维安全

通过青莲云的安全运维平台进行统一的管理，采取严格的访问控制、监控审计来确保运维安全。

5.10.1 账号管理

使用统一的账号管理审核模式，所有青莲云官网产品注册的账号都是运维平台统一审核。

5.10.2 授权管理

运维平台统一对用户进行授权，包括用户的下的产品 license、设备的解绑和绑定操作等。

5.10.3 监控管理

各业务平台的日志数据定期自动化分析，将各平台各模块存在的问题，自动通知相关管理人员。自动化监控系统对云平台网络设备、服务器、数据库、应用集群以及核心业务进行全面实时监控。监控系统广泛使用仪表盘展示青莲云关键运营指标，并可配置告警阈值，当关键运营指标超过设置的告警阈值时，自动通知运维和管理人员。

5.10.4 审计

对员工对生产系统的所有运维操作必须且只能通过跳板机进行。所有操作过程完整记录下来实时传输到集中日志平台。

对违规事项定义审计规则，发现违规行为并通知安全人员跟进。

5.11 账户安全

账号安全是青莲云服务体系的基础，所以针对账号的注册、登录、忘记密码、注销、修改账号资料、多设备登录、单点登录等都进行了严格的安全建设和日志审计。客户的数据之间通过账号进行访问隔离，客户自主保存自己的青莲云账号。

同时，针对账号体系的数据存储、查询和修改都进行了严格的保护。针对常见账号风险来源进行严格的策略保护。

青莲云平台完善的运营安全能力能够为客户提供云服务的全天候技术支持。