智能音箱酒店行业安全白皮书

百度在线网络技术（北京）有限公司　华住酒店集团

目录

前言

当前，智能物联网（AIoT）正在推动酒店行业走上智能化的道路。以智能家居为代表的智能终端是推动智慧酒店发展的重要力量。其中，智能音箱作为对话式的人工智能交互平台，以便利的交互方式、丰富的互联网内容、强大的扩展性，受到众多消费者的喜爱，也成为酒店中的智能“管家”。

但是，层出不穷的设备漏洞、设备入侵、用户数据窃取等事件表明智能音箱的安全问题不容忽视。尤其是酒店场景下，对安全问题应该给予更大的重视，并要求设备具有更高的安全性。为研究智能音箱酒店行业的安全风险现状以及应对措施，百度与华住基于调研分析和自身实践，制定了《智能音箱酒店行业安全白皮书》。本白皮书阐述了智能音箱酒店行业的安全现状和典型安全风险，提出了相应的安全架构设计与安全防护方案建议，展示了百度与华住在智能音箱酒店行业的安全实践。希望能够为智能音箱在酒店行业应用涉及的各个参与方提供参考，共同构建安全的智能音箱酒店行业生态体系。

编写团队：百度安全、华住集团

编写人员：林道正、焦龙龙、曲乐炜、马如彬、沈林

1 智能音箱酒店行业安全现状

1.1 安全问题

随着智能音箱的快速发展，智能音箱逐渐占据了智能家居的入口地位，集成的功能也越来越多种多样，包括语音交互、IoT 控制、支付等功能。随之而来的是其安全性也备受关注，尤其是对用户敏感信息（如语音、视频）的处理及分发等方面，引发用户对于个人隐私问题的担忧。近来，国内外的各大破解赛事，也将智能音箱作为破解对象，各种破解技术的“show”也在打击用户对智能音箱安全性的信心。

随着智慧酒店概念的兴起，智能音箱作为核心入口也被引入了酒店场景，使酒店客人能够体验到人工智能带来的便利。然而在兴奋之余，公开暴露的智能音箱也为黑客接触设备提供了便利通道，并且使分析利用智能音箱漏洞的门槛进一步降低。对于酒店这样一个敏感使用场景，智能音箱的麦克风、用户隐私数据是否处于监控之中，交互语音是否存在泄漏，设备是否足够安全，成为人们关注的焦点。因此，智能音箱在酒店行业将迎来更大的安全挑战，如何保障酒店场景下设备、交互的安全也成为智能音箱 toB 场景拓展的瓶颈。

1.2 安全事件

酒店场景的智能音箱，可定义为公共场景下的智能设备，近来智能设备的安全隐私问题层出不穷。

2017 年 8 月，英国安全研究人员 Mark Barnes 通过物理接触亚马逊 Echo 设备，将 Echo 的底座去掉，利用暴露的金属垫片对 Echo 进行改造，关闭了 Echo 的安全机制，并安装了间谍软件，监控用户录音。在 2018 年的 DefCon 上，研究人员通过破解 Echo 智能

音箱，不仅能够远程控制设备进行录音，还能将设备的录音发送到攻击者的服务器上，做到了远程窃取用户隐私。Echo 在美国的市场占有率达 70%，亚马逊为该音箱设置了非常高的安全等级，但如此高安全等级的设备也难以抵挡攻击者的破解行为。如果在酒店场景中，上一位房客对智能音箱进行了破解，并监听该房间中后续房客的音频，后果将不堪设想。

2019 年 1 月，在某连锁火锅品牌门店，一位顾客通过破解门店 Wi-Fi，使用智能电视开放的 DLNA 投屏服务，将手机上的黄色视频投放到电视上，影响极其恶劣，这是典型的公众场合设备被攻击的案例。

2019 年 11 月，安全研究人员 Takeshi Suguwara、Kevin Fu 和一组密歇根大学的研究人员一起将一种神奇的现象——麦克风能够将照射其上并以正弦波的形式随时间改变强度的高功率激光转换成电信号——变成了某种更令人不安的事情，他们可以使用激光以静默方式向任何接受语音命令的设备发送信息，包括智能手机、Amazon Echo 音箱、Google Home 和 Facebook 的 Portal 视频聊天设备。这种技巧使他们可从数百英尺远的地方发送控制指令，比如打开车库门、在线购买商品或者做出各种恶作剧或恶意行为。当设备的所有者不在家里时，攻击者可以轻松地通过窗户，让目标设备进行响应。

2020 年 1 月，小米智能摄像头再被曝出隐私安全隐患，用户在将设备中的内容传输到谷歌 Nest Hub 时，看到了非该用户的影像，造成严重用户隐私泄漏。谷歌随即禁用了小米智能摄像头的访问权限，并与小米一同针对漏洞进行修复。

由此可见，智能音箱无论是本身的安全性，还是在处理用户隐私信息的安全性方面均受到了严重挑战。而酒店场景中，由于涉及到与酒店云端的联动，参与模块众多，更容易暴露安全问题。以往黑客只是将目标锁定在智能音箱上，现在整个酒店云端、客房 RCU 均可成为黑客攻击的对象，一处失守就可导致远程任意控制或用户敏感信息泄漏。

黑客攻击的目的，一方面是窃取用户隐私，获取用户敏感数据；一方面是远程控制，包

括控制音箱和控制客房的 IoT 设备。

1) 窃取用户隐私

黑客在智能音箱通信的各个路径中进行监听和嗅探，可获取用户敏感信息；或对酒店云平台、客房 RCU 展开攻击，获取用户发往 IoT 设备的控制指令，进行用户习惯分析；或攻击设备固话服务，嗅探用户的通话语音，达到语音钓鱼的目的等。

2) 远程控制

黑客会对从智能音箱发送请求到最终客房 RCU 控制设备的各个阶段展开分析，利用音箱本身存在的脆弱点，或交互控制中的未授权访问接口，达到远程控制的目的。

1.3 安全威胁发展趋势

依据智能音箱在酒店行业固有的特征，目前针对酒店行业的智能音箱攻击呈现出几大威胁趋势：

首先，针对数据的攻击会尤为严重。攻击者的目的是窃取用户敏感数据，因此攻击者除了直接攻击音箱之外，也会对酒店云平台、客房 RCU、音箱云端同步展开攻击。此外，用户数据在进行训练或标记时，脱敏不完全或违规采集用户数据，也会存在用户隐私泄漏的风险。

其次，针对开放接口的攻击会成为入口点。智能音箱往往具备较多功能的开放服务，如 DLNA 投屏、蓝牙连接。若权限校验不当，则会出现未授权的连接，给用户造成恐慌；若存在安全漏洞，便可让攻击者在不接触设备的情况下，获得设备的权限，进而在设备中植入后门，监听用户数据。

最后，硬件攻击会变得尤为方便。在 toC 家庭场景下，物理接触设备成本较高，但在酒店场景下，若房客是恶意攻击者，便可自由接触设备。通过拆机等方式，利用硬件的调试接口或漏洞直接对设备进行刷机或后门植入，会直接威胁后续入住房客的隐私安全。

另外，酒店的智能音箱可能会成为跳板。智能音箱往往会跟酒店的客房 RCU 进行内网互通，并与用户 Wi-Fi 网络进行隔离。若设备被攻破，则攻击者会以智能音箱为跳板进行后续攻击，绕过访问控制策略，进而威胁整个酒店的用户及数据安全。

2 智能音箱酒店行业典型安全风险

智能音箱存在典型的十大安全风险（参考中国通信研究院中国泰尔实验室的《互联网设备智能音箱安全白皮书》），其在酒店场景下，会延伸出如下安全风险：

1) 个人信息明文存储及传输，造成用户信息泄漏

智能音箱在采集到个人信息后，以明文或弱加密方式存储，导致极易发生个人信息泄露问题；传输个人信息时，采用明文或弱加密方式传输，黑客在同一局域网或网关处进行嗅探即可获得用户信息，如语音、身份认证 token 等。

2) 个人信息收集处理规则模糊，存在过度收集及使用风险

智能音箱在处理用户敏感数据时，存在过度收集使用，尤其是在酒店场景下：

a) 智能音箱作为整个智慧酒店房间的中控，其本身会采集用户的音视频等信息，并传输云端进行解析与训练，音视频中往往包含用户行为习惯、声纹等敏感信息，其在隐私政策中并未提及，而在以上数据的收集、转移、存储、处理中，一旦被泄漏，将对用户造成非常恶劣的影响。

b) 智能音箱会集成较多第三方 APP 或 SDK，但第三方引入代码由于其不开源性，智能音箱无法掌控其行为，通常只能通过协议来进行约束，其中一些敏感权限如：摄像头、麦克风、通讯录等权限，是默认授予的，因此若第三方代码存在窃取用户隐私问题，或在处理用户数据时发生隐私泄漏，将对用户造成非常恶劣的影响。

c) 大部分酒店版本的智能音箱，其隐私协议并未进行专门定制，如在酒店场景下，音箱应对用户的数据采取“阅后即焚”策略，但隐私协议仍然使用 toC 场景下的内容，相关内容并不符合酒店 toB 场景的设备实际情况与用户需求，用户阅读完隐私协议之后可能会产生恐慌与误解。

3) 身份认证机制缺陷，存在会话劫持伪造风险

a) 设备与云端

酒店场景的设备通常是预置登陆态或无登陆态，在接受用户语音并将其传输到云端进行指令解析的过程中，若采用 CUID、SN 号等作为身份凭证，与云端进行交互，则存在极大风险。黑客可模拟使用 CUID 和 SN 作为凭证参数，向云端接口发送交互指令，并远程控制客房中的 IoT 设备。

b) 云云对接

音箱云端在完成指令解析后，通常会将解析的指令发送到酒店的云端服务器，完成云云对接。该过程中，如未使用身份验证或使用弱身份凭证，则会导致黑客直接向酒店云端发送控制指令，远程控制客房中的 IoT 设备。

c) 酒店云端与客房 RCU

酒店云端通常会解析音箱云端的指令，并转发到客房 RCU 控制中心。该过程中，如未进行身份认证或采用身份弱认证，黑客可直接构造请求向 RCU 发送命令，远程控制客房中的 IoT 设备。

d) 客房 RCU 与 IoT 设备

客房 RCU 通常会解析酒店云端发送的客控指令，并通过 Wi-Fi 或射频协议，进行 IoT 设备的直接控制。该过程中，IoT 设备若不对客房 RCU 进行认证或进行弱认证，黑客可直接发送控制命令，远程控制客房中的 IoT 设备。

4) 未授权接口对外暴露，存在任意控制风险

在酒店公共场景中，未授权接口对外暴露引发的问题尤为严重。若房客未明确授权连接蓝牙、远程 DLNA 投屏等的情况下，黑客通过暴露的接口远程控制设备，则会为房客带来恐慌，从而对智慧酒店产生质疑。

5) 硬件安全防护不当，存在硬件破解后门植入风险

在酒店公共场景中，用户可物理接触设备，若设备存在物理调试接口或可连接进行任意刷机，黑客可植入后门，并持续获取后续入住同一客房的房客的敏感信息。

6) 设备系统更新不及时，存在高危漏洞利用风险

在酒店场景中，智能音箱设备更新迭代速度较 toC 场景慢，因此在智能音箱出现通用安全问题时，酒店中的设备可能未同步对齐更新，存在高危漏洞被利用风险。

7) 重置处理不当，存在用户信息泄漏风险

在酒店场景中涉及到典型的问题就是房客退房，相应信息的抹除，如用户的账号、蓝牙配置、视频及图像。若未做到完全清除，则后续房客可轻易获取前房客的隐私数据。或前房客可通过蓝牙、DLNA 等继续保留对设备的控制权，造成远程控制或用户信息泄漏。

8) 网络隔离不当，存在设备对用户网络暴露风险

在酒店场景中，由于不存在用户配网授权过程，因此不需用户与设备存在同一局域网中。若仍保持用户和设备存在同一局域网中，则增加设备被入侵的风险，黑客可对音箱进行扫描，DDoS 攻击等，增加设备被入侵的安全风险。

9) 缺乏应急响应流程及措施，存在威胁扩大化的风险

在酒店场景中，音箱是与酒店紧密耦合的共同体，二者合力为用户提供良好的科技感入住体验。无论是酒店还是音箱本身出现安全问题，都会对整个智慧酒店行业产生严重影

响。当问题发生时，目前多数厂商并没有一套完整的应急响应流程，也不存在有效的手段弥补漏洞并及时止损，这可导致房客对智慧酒店形象产生怀疑，甚至丧失信心，进而影响整个行业的发展。

10) 集成固话服务存在安全问题，造成用户通话语音泄漏

在酒店场景中，往往涉及客房服务，需要通过酒店集成的固话服务来进行通话。若固话中存在安全漏洞或采用明文传输用户语音，黑客则可进行语音钓鱼、用户通话语音窃听等攻击，造成用户隐私泄漏。

3 总体安全框架

智能音箱安全性与设备本身、网络传输过程、数据处理过程等方面的安全性密切相关。为了实现酒店场景下的高安全性要求，需要智能音箱厂商、酒店以及各个服务提供商，在设计、使用、运维等各个阶段满足相关的安全业务要求。

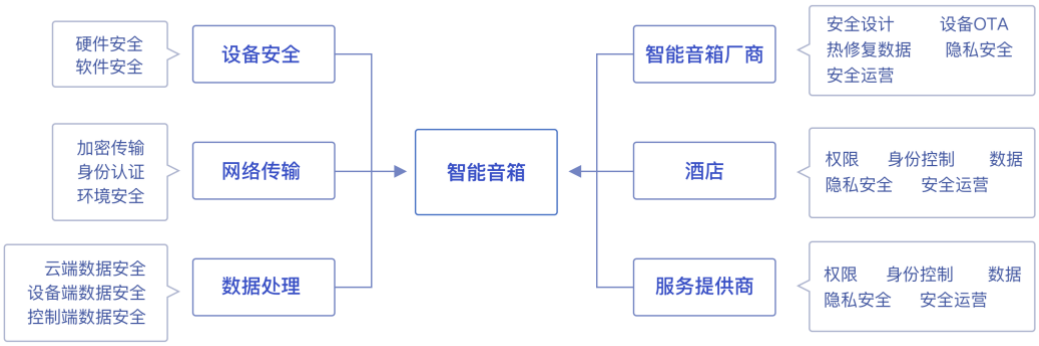

图 1 安全需求

智能音箱在酒店场景下的安全业务逻辑可抽象为六层，如图 2 所示，主要包含：应用设备层、网络传输层、数据处理层、数据安全与隐私层、人工智能服务层、安全运营层。

- 应用设备层安全需求：保障硬件、固件、操作系统以及应用软件安全，对系统、软件进

行安全配置，保护智能音箱业务、权限，保证应用软件的合法性；

- 网络传输层安全需求：保障智能音箱数据传输过程的安全性；
- 数据处理层安全需求：保障云端、设备控制终端、网关等数据处理端的安全性；
- 数据安全与隐私层安全需求：保障敏感、隐私数据在流通、存储过程中的安全性；
- 人工智能服务层安全需求：保障人工智能算法、模型在使用过程中的安全性；
- 安全运营层安全需求：对智能音箱行为进行审计，建立应急响应机制，保证能够及时发现、处理安全威胁。

图 2 安全业务框架

4 智能音箱酒店行业安全规范

4.1 应用设备层安全规范

4.1.1 硬件安全规范

4.1.1.1 物理接口

类型	级别	定义
最小化原则	强制	应遵循最小化原则，移除显式调试接口等非必需的物理接口
隐式调试接口	强制	应去除隐式调试接口或去除隐式接口的部分器件、添加接口验证

4.1.1.2 可信执行环境

类型	级别	定义
安全启动	强制	应使用硬件级安全启动，从不可变代码开始启动，仅能加载校验通过的安全固件。
数据存储	强制	应将安全启动校验密钥等关键证书密钥存储在不可改写的存储区域； 应对系统、用户的关键数据进行加密存储。
密钥策略	强制	安全启动校验密钥应至少采用一型一密、一批一密、一机一密中的一种。
TEE	推荐	应使用支持 TEE 的硬件平台； 应在 TEE 中执行关键数据的加解密、验证、加密存储等敏感操作；

4.1.1.3 硬件设计

类型	级别	定义
存储芯片	强制	应使用具有数据保护电路的存储芯片
摄像头、麦克风	强制	应移除摄像头部件或添加用户可控的摄像头物理遮挡措施； 应具备状态指示器用于展示摄像头、麦克风的工作状态；
物理按键	强制	应具备关机、关闭麦克风、关闭摄像头等功能明确的物理按键； 应通过硬件电路的方式实现物理按键的功能；
电路板	强制	应抹除电路板中管脚的标注
外壳	推荐	应采用防拆设计

4.1.2 软件安全规范

4.1.2.1 通用安全

类型	级别	定义
加密	强制	应使用强加密算法，加密强度不低于 AES 128、ECC 163、RSA 2048、SM2/4/9、ZUC
密码	强制	密码长度应大于 8 位且至少由大写字母、小写字母、数字、特殊符号 4 类中的 3 类组成； 不应与 10 个历史密码相同或包含用户名中的连续多个字符； 应使用强加密保护密码或者对密码进行散列加密；
更新	强制	应支持 OTA 更新与热修复； 应使用加密信道传输更新包文件并对更新包文件进行强校验；

		应仅能通过指定平台进行应用安装、更新； 智能音箱自带应用的添加与更新应经过安全审计，服务商不应通过其他方式远程安装任意应用； 应关注 CVE、CNVD、CNNVD 等漏洞平台以及官方发布的重大安全补丁，及时通过 OTA 更新、热修复打安全补丁，不应存在 6 个月前的高危问题；
回滚	强制	应支持回滚功能并对回滚包文件进行强校验，保证回滚至稳定安全的版本
重置	强制	应支持重置功能，保证将用户数据完全删除
版本	强制	应使用主流系统、开源库/第三方组件，并在保证稳定的情况下采用最新版本
编译	强制	应开启地址随机化、堆栈不可执行等保护措施，并去除符号表信息
加固	推荐	应使用代码混淆、数据加密、加壳、校验、反调试等保护措施进行加固

4.1.2.2 系统安全

类型	级别	定义
安全配置	强制	应开启地址随机化、堆栈不可执行等保护措施； 应开启 SELinux 或其他类似的强制访问控制策略，按组为系统进程配置不同的访问权限； 应启用分区加密，并为关键区域设置正确的权限； 应隐藏开发者选项入口，关闭未知来源安装，禁止通过浏览器安装应用；
网络服务	强制	应去除 SSH、Telnet、adb 等非必需服务； 应修改常用服务的端口，并对开放端口应进行访问控制；
更新	强制	应支持内核热修复、系统 OTA 更新、工厂包更新；

		不应在更新失败时出现系统不可用的情况； 在线更新时，应不支持从高版本降级到低版本； 应及时将工厂包更新至最新稳定安全的版本；
密码	推荐	应使用强密码或动态密码保护系统登录、系统设置等功能

4.1.2.3 应用安全

类型	级别	定义
安全配置	强制	应默认禁止任何进程或应用获取系统的超级用户权限； 应不存在后门隐藏接口；
最小化原则	推荐	应去除不需要的应用，保持应用数量最小化
白名单	强制	应使用白名单机制管理应用，禁止安装非白名单应用
回滚	强制	应仅能由指定服务平台启动回滚，不应支持设备本地发起回滚； 应在回滚时，验证服务器签名，并且仅在验证通过后执行；

4.1.2.4 第三方安全

类型	级别	定义
准入	强制	应有第三方应用、SDK、技能准入规范，对数据存储、对外接口、更新、通信、隐私等制定安全基线，并仅在符合准入规范的情况引入
SLA	强制	第三方提供者应具备对安全问题修复和紧急安全事件响应的能力； 第三方提供的应用、SDK、技能不应存在后门隐藏接口；
白名单	强制	应使用白名单机制管理第三方应用，禁止安装非白名单应用，不安装未签名应用或者非可信代码；

回滚	强制	应仅能由指定服务平台启动回滚，不应支持设备本地发起回滚； 应在回滚时，验证服务器签名，并且仅在验证通过后执行；

4.2 网络传输层安全规范

4.2.1 协议规范

类型	级别	定义
协议选择	强制	应选择支持设备授权认证、加密传输等安全扩展功能的通信协议
协议安全	强制	应与 GB/T 38648-2020、GB/T 35290-2017、GB/T 22239-2019 等信息安全技术相关国家标准一致
协议实现	强制	应遵循相关标准，并预防因编程语言的固有缺陷而可能造成的安全问题

4.2.2 网络通信规范

4.2.2.1 通用安全

类型	级别	定义
加密	强制	应使用带有 TLS 的通信协议传输敏感数据，避免混合内容； 应使用强加密算法，加密强度不低于 AES 128、ECC 163、RSA 2048、SM2/4/9、ZUC； 应在 SSL/TLS 密钥协商的过程中，对公钥进行校验； 无法使用 TLS 的场景下，应采用安全的密码算法，并且必须通过安全评估； 使用对称加密算法过程中，应对通信密钥做好保护；
证书	强制	应选择强算法签名的证书，并确保证书的覆盖范围，避免无效证书警告，

		同时避免使用通配符证书； 应加强证书管理，每年更新证书，同时更新私钥，并且在发现系统被攻陷后，及时吊销旧证书，生成新的密钥和证书；
签名	推荐	应使用包含时间戳在内的数据签名
认证	推荐	应在敏感数据传输过程中采用双向身份认证

4.2.2.2 固话协议

类型	级别	定义
协议实现	推荐	应基于 SIP 协议实现固话服务； 应兼容酒店门店 PSTN 接入； 应采用加密方式传输通话数据；
云端部署	推荐	固话服务应统一部署在的云端服务器； 应保证固话服务的通畅与数据安全； 应保证服务系统的管理便捷性、系统稳定性； 应提供可靠的灾难恢复，并使用云端平台管理固化服务相关账号；

4.2.3 网络环境规范

类型	级别	定义
网络隔离	推荐	智能音箱连接的无线网络应与酒店客户使用的网络处于隔离状态
DNS	推荐	应具备检测 DNS 劫持、修复 DNS 劫持的能力
Wi-Fi	推荐	应具备防范伪 Wi-Fi 热点的能力
运营商网络	推荐	应具备防范伪基站攻击，防范已知的运营商劫持方式；

		应避免使用存在已知漏洞的运营商网络协议；

4.2.4 短距离通信规范

类型	级别	定义
蓝牙	推荐	应在不使用时关闭蓝牙模块； 应使用最新版本的蓝牙技术，并使用蓝牙协议提供的安全加密机制，通过 BLE 提供的加密方式传输数据； 应使用数字比较或者配对码模式，禁止使用 Just Works 模式； 应遵循标准蓝牙 Mesh 协议规范，开启其安全特性，保护数据的完整性、机密性和可用性；
ZigBee	推荐	应使用 Z-Stack 协议栈编程，并使用最新版本的 ZigBee 技术； 应采用高级安全模式，并使用其提供的安全加密机制；
Z-Wave	推荐	应使用最新版本的 Z-Wave 技术； 应遵循 Z-Wave Security 2 安全架构，并使用其提供的安全加密机制；
NFC	推荐	应使用最新版本的 NFC 技术； 应禁用非加密的 IC 卡，并正确使用 NFC 技术提供的安全加密机制；
红外	推荐	应对红外控制请求进行严格过滤，不响应非法来源的控制请求

4.3 数据处理层安全规范

4.3.1 云端安全规范

类型	级别	定义

云端服务器	推荐	应遵循云安全联盟的《云计算关键领域安全指南 v4.0》，选择安全服务提供商，具备抗攻击能力，正确处理网络请求及参数，通过权限隔离、身份授权与管理、安全检测等方式提升安全性
云端对接	强制	云端之间通信应使用双向身份验证、包含时间戳在内的数据签名； 应采用白名单机制，禁止白名单之外的访问请求；
设备管理	强制	云端应向其他云端提供其管理的智能设备身份、权限等的验证

4.3.2 移动控制端安全规范

类型	级别	定义
外发版本	强制	应关闭 Log 输出，并且任意情况下不发布 debug 版
安全补丁	强制	应具备安全问题响应与修复能力，能够短时间内修复安全问题并更新
加固	推荐	应进行加固，并使用安全厂商提供的安全服务加强安全性
证书验证	强制	应对服务端证书、重要数据进行校验，并确保校验逻辑无法被绕过
外部数据	强制	应对 UIWebView、WebView、URLScheme 等不可信来源的数据进行充分校验、过滤，Android 端不对外提供 ContentProvider
更新	强制	Android 端更新应使用 HTTPS； 应至少校验更新包的大小、哈希值、签名、版本号等；
模块组件	强制	应对加载的模块进行合法性校验，并储存在私有目录； 应关闭无用的系统组件，不开启调试、备份功能； 应避免开放端口提供服务，对开放端口进行访问控制以及身份认证；
文件权限	强制	应在创建文件时，做好文件权限控制

4.3.3 设备交互控制规范

类型	级别	定义
注册	强制	智能音箱应在酒店云端注册后，才能够使用客房控制、客需服务等涉及与酒店内其他设备、服务人员交互的功能； 智能音箱应是酒店专用设备，仅在可信的酒店网络环境下正常工作；
认证	强制	交互控制数据应包含足够的信息，以确认智能音箱的身份； 应在处理交互控制数据前对设备身份以及请求的有效性、合法性进行充分校验；
加密	强制	应使用强加密算法进行交互控制数据加密 加密强度不低于 AES 128、ECC 163、RSA 2048、SM2/4/9、ZUC
签名	推荐	应对交互控制数据进行签名，签名应包含时间戳

4.4 数据安全与隐私层安全规范

4.4.1 数据安全规范

类型	级别	定义
信息采集	强制	应在隐私协议中对所有敏感信息的采集行为进行说明； 不应在未经用户允许的情况下采集任何隐私相关信息；
信息存储	强制	不应在本地或云端存储姓名、手机号、邮箱、身份证号、银行卡号等用户个人敏感信息； 应在存储账号、密钥、身份凭证等敏感信息时使用加密存储； 应使用二进制程序实现加密，或对加密代码进行混淆；

		不应在代码中硬编码加密密钥；
信息使用	强制	密钥、身份凭证等认证信息应具有时效性并限定作用域； 认证信息超时或超出作用域后应重新分配；
权限管理	强制	应以最小化原则设置敏感数据访问权限，仅限特定用户/应用访问
信息传输	强制	传输敏感信息应使用非对称加密处理； 传输正常数据信息应至少采用对称加密处理； 任何用户相关数据不应明文传输；
云端数据安全	强制	应启动云提供商的数据安全性措施，利用架构提高数据安全性； 不应完全依赖访问控制与加密； 应利用现有标准，正确使用、管理加密及密钥；

4.4.2 隐私规范

类型	级别	定义
数据采集	强制	智能音箱、APP、云端，不应采集用户个人信息
数据存储	强制	智能音箱采集的音频、视频等隐私数据，应采取“阅后即焚”策略，不在任何地方落地存储； 涉及用户隐私的数据应在确实需要存储时进行脱敏、加密处理；
数据流通	强制	数据因业务需要在内部流通时，应有相应的管理委员会进行管理，并经法务部门进行评估； 智能音箱相关的任何数据不应向第三方提供；
隐私协议	强制	应根据酒店行业的特殊情况单独制定隐私协议，并在合适的地方展示给用户，并且可通过简单步骤重复查看；

		智能音箱的行为应符合隐私协议中的规定；

4.4.3 用户数据生命周期规范

类型	级别	定义
初始化	强制	应在酒店客户入住时，进行数据初始化，并且数据与用户个人无关； 应在第一时间通过隐私协议等方式展示需要采集的数据，以及这些采集的数据是否会用于后续的服务优化等其他任务； 所有的用户数据采集、使用行为，均应仅在用户同意的情况下执行，并且默认用户不同意执行相关行为； 不应以不提供某项功能/服务等方式要挟用户同意某些用户数据采集、使用行为，除非该功能/服务必须以真实用户数据为基础；
处理	强制	用户数据的处理应采用匿名化处理； 一般情况下，应采用不落盘的方式处理用户数据，当确实需要落盘储存用户数据时，应进行匿名化处理并加密储存；
销毁	强制	酒店客户退房、用户调用销毁功能或其他需要的时候，应对使用记录、个人信息等用户数据进行销毁，范围包括智能设备以及云端； 智能音箱应提供远程数据销毁与设备禁用功能，用于在丢失、挪用等场景下销毁用户数据； 若初始化时用户同意数据可在匿名化后用于服务优化，应在数据销毁时再次确认用户是否继续同意此行为；

4.5 人工智能服务安全规范

类型	级别	定义
身份验证	推荐	应支持对用户进行基于个人生物信息的身份验证，并且仅在身份验证通过的情况下响应用户的请求
数据采集	推荐	应采取硬件、软件措施对摄像头、麦克风等传感器采集的数据进行过滤，抛弃异常的、正常范围外的数据
数据传输	推荐	应确保设备与人工智能服务之间的交互数据传输安全可靠
对抗攻击	推荐	人工智能服务使用的机器学习算法应具备对抗攻击防护能力
模型保护	推荐	人工智能服务应具备对其使用的机器学习模型进行保护的能力

4.6 安全运营规范

4.6.1 日志审计规范

类型	级别	定义
数据记录	强制	应保留充分的数据记录用于检测分析； 涉及用户敏感数据的应进行脱敏处理；
监控	推荐	酒店或服务提供商对智能音箱的状态进行实时监控，监控范围包括但不限于：音箱工作状态是否正常、音箱是否被挪用或盗用
设备端	推荐	智能音箱应具备在线/离线检测设备入侵情况的能力
云服务	推荐	应对云服务进行在线/离线审计，检查范围包括但不限于：是否使用带有 TLS 的通信协议、是否启用证书校验、是否使用弱身份凭证、是否进行身份验证、是否进行权限验证、服务代码是否有已知安全问题

服务提供商	推荐	厂商、酒店以及其他服务提供商应对涉及智能音箱的业务进行在线/离线审计，检查范围包括但不限于：数据来源检查、使用过期身份凭证、以错误方式使用身份凭证、身份凭证滥用、超作用域使用身份凭证、身份凭证泄露

4.6.2 内容审查规范

类型	级别	定义
内容审查	推荐	应对云端、移动端展示的内容进行审查与过滤，防止出现违反国家法律法规、扰乱社会秩序、危害公共安全、侵犯公民权利以及其他危害社会的内容

4.6.3 应急响应规范

类型	级别	定义
应急响应规范	强制	应制定合理的应急响应流程，涵盖事件处理过程的每个阶段：准备、检测、遏制、根除、恢复、跟踪
应急响应准备	推荐	应制定完善的事件应急响应流程，确定相关的处理人员、处理方式；应进行应急响应的相关培训； 应确保各服务提供商能够主动评估安全风险；
事件检测与分析	推荐	应从智能音箱提供商、服务提供商、酒店、国家应急中心、安全团队以及其他威胁情报来源获取、发现安全事件； 应利用流量、日志、安全产品等多维度数据分析安全事件的原因，确定安全事件的威胁程度；

事件遏制	推荐	应及时采取行动，防止进一步的损失，采取的抑制手段包括但不限于：断开网络连接、关闭特定服务、禁用特定软件/应用、关闭系统
事件根除与恢复	推荐	在确定安全事件的原因之后，应进行安全事件根除与业务恢复，具体的工作包括但不限于：清除系统中的异常服务/进程/程序/代码；消除安全事件原因；增强安全策略；问题消除后，协助恢复正常业务；持续监控；
设备端安全事件响应时间	推荐	高危问题应在 7 个自然日内完成修复开发或合入修复 Patch，并通过更新渠道进行升级修复； 严重问题应在 15 个自然日内完成修复开发或合入修复 Patch，并通过更新渠道进行升级修复； 普通问题应在 30 个自然日内完成修复开发或合入修复 Patch，并通过更新渠道进行升级修复；
云端安全事件响应时间	推荐	应在检测到云端安全事件 20 分钟响应； 安全事件涉及的云服务器不大于 5 台时应在 3 个自然日内处理完成，超出 5 台时，每 5 台增加 1 个自然日；
事件报告与持续跟踪	推荐	应在安全事件处理完毕后对事件进行复盘研究，分析安全事件的现象、原因、处理过程、处理结果，给出相应的安全建议，并撰写安全事件应急响应报告，对涉及的服务提供商提出反馈/投诉； 应对安全事件的处理结果进行持续跟踪，对进入司法程序的安全事件进行进一步调查；

5 小度-华住智慧酒店最佳实践

百度与华住在智慧酒店的实践中，针对酒店行业这个特定场景，以小度系列智能音箱为基础，应用多种安全隐私保障措施，开发了酒店行业定制版小度智能音箱及其关联系统，用于确保智能音箱在酒店行业各个场景下的安全管理以及隐私保护。以小度在家智能屏 X8 酒店版（以下简称酒店版小度音箱）为例，其整体安全隐私保护框架如图 3 所示。

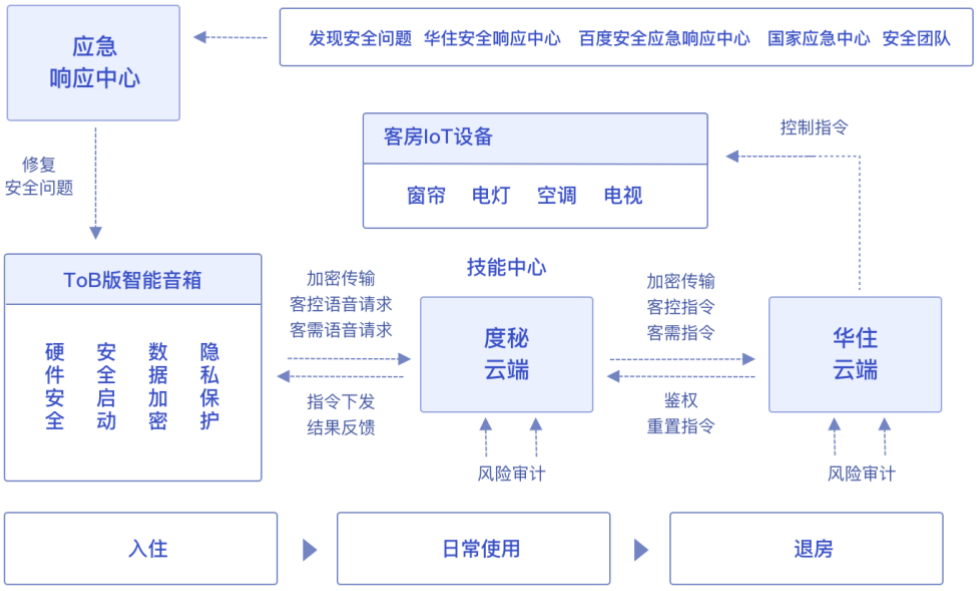

图 3 酒店版小度音箱安全隐私保护框架

酒店客户入住时，通过设备的安全设计、安全启动等措施保障酒店客户使用的是未被篡改的设备和系统，同时以加密、强认证、可关闭的传感器等保护用户隐私。

酒店客户日常使用智能音箱的过程中，以加密的方式传输语音请求、控制指令等敏感数据，并且通过鉴权防范数据伪造、越权控制等行为。

酒店客户退房时，使用重置的方式清理设备、云端的用户数据，降低数据泄露的可能性。

在日常的维护中，通过风险审计机制检测服务过程是否存在异常，同时高度关注各个途

径发现的安全问题，以高效的应急响应及时修复这些安全问题，保障整体的安全性。

5.1 入住

酒店客户入住时，首先接触到的是酒店版小度音箱硬件设备。为了满足酒店行业的高安全性需求，酒店版小度音箱采用了更加安全的方案。

5.1.1 硬件安全设计

酒店版小度音箱无摄像头，因此不存在任何非法视频监控用户的行为。设备表面无外露螺丝，除充电口外无外露的物理端口，并且移除 OTG 接口，使用安全 ADB 方案，提高了从外部直接进行破解的难度。

酒店版小度音箱提供明确的物理按键，用于关机、关闭麦克风。酒店客户能够在有需求的情况下，通过物理按键直接关机或者关闭麦克风，使设备上包括语音唤醒在内，任何可能的语音数据获取行为失效。

酒店版小度音箱使用硬件级的安全启动执行启动操作，保证音箱启动的系统是可信的，防止恶意刷机操作。在此基础上，实现了对可信执行环境的支持，能够在外部无法影响的可信执行环境中执行安全存储、加解密等敏感操作。

5.1.2 数据加密

一、加密存储

酒店版小度音箱使用了分区加密技术，酒店客户在日常使用中产生的用户数据，将以加密的形式进行存储，能够有效防止攻击者通过固件提取的方式搜集相关数据。为进一步保护用户数据，酒店版小度音箱设备中的核心应用经过了安全加固，支持防逆向、防调试等安全

功能，能够有效防范可能的数据窃取行为。

二、加密传输

酒店版小度音箱在传输敏感信息时，全程使用 HTTPS 加密传输，并进行证书强校验，防范可能的数据窃取、证书伪造等攻击行为。

三、密钥/证书更新

酒店版小度音箱密钥/证书由百度内统一的证书托管服务进行管理，保证密钥/证书的安全性。

设备芯片 efuse 区域中的密钥，因该区域不可更改的硬件特性而无法更新。当发生相关的密钥泄露事件时，将弃用使用同样密钥的硬件设备，并对泄露事件进行排查与修复，防止再次发生类似事件。

设备固件中使用的其他密钥/证书将定期通过 OTA 进行更新。当发生相关的密钥泄露事件时，将弃用相关的密钥，为固件更新密钥/证书，并对泄露事件进行排查与修复，防止再次发生类似事件。

云端使用的密钥/证书采取定期更新的策略。当发生相关的密钥泄露事件时，将弃用相关的密钥，在安全加固的物理设备上生成新的密钥/证书，并对泄露事件进行排查与修复，防止再次发生类似事件。

5.1.3 隐私保护

为保护酒店客户使用智能音箱时的个人隐私，酒店版小度音箱采取了多种隐私保护措施：

1) 采用与用户无关的策略，酒店客户无需绑定个人账号，即可正常使用；

2) 在对外网络连接时，采用 HTTPDNS 方案，有效防止 DNS 劫持问题；

3) 无摄像头，不存在任何视频监控行为，同时针对用户语音请求数据，采用“阅后即

焚”策略，仅保存语音解析出的控制指令供安全审计，不会落地存储任何语音数据；

4) 安装的应用通过百度史宾格系统的 APP 隐私合规检测；

5) 处理涉及用户的数据时，采取脱敏处理，无法通过脱敏后的数据对应到具体的用户；

6) 数据内部流通均在百度的数据资产管理委员会与数据流通小组报备，并经百度的法务评估和数据资产管理委员会审批；同时百度与华住不会将设备相关信息与第三方分享；

7) 百度法务部门针对 toB 酒店版设备制定酒店版隐私协议，阐述 toB 设备在隐私数据采集、流通上的合规性，并保证设备行为符合协议规定。

5.2 日常使用

在入住期间，酒店客户除了能够使用一般智能音箱所具有的闹钟、天气、新闻、音视频播放、互动问答等服务，还可以使用酒店版小度音箱进行控制客房 IoT 设备、呼叫客需服务等酒店场景特色服务。

目前，酒店版小度音箱控制客房 IoT 设备，采用的控制协议均为统一的酒店客控技能标准，详细接入文档请参见《酒店客控技能介绍》；酒店版小度音箱使用的客需服务为统一的酒店客需服务技能标准，详细接入文档请参见《酒店客需服务介绍》。客房控制、客需服务的通信数据流通过程如图 4 所示。

度秘云端在将用户的语音指令识别成文本，并进行语义理解获得实际的客房控制意图、者客需服务意图后，调用客控技能或者客需技能，由华住云端处理客控/客需意图。

在此过程中，华住云端与度秘云端在使用 HTTPS 传输数据并进行证书强校验的基础上，基于 OAuth 2.0、白名单、签名等安全机制，保证华住云端接收到的客控/客需意图是由度秘云端发出的，并防止攻击者通过重放攻击、中间人攻击、伪造请求数据等方式恶意控制客

房 IoT 设备或呼叫客需服务。

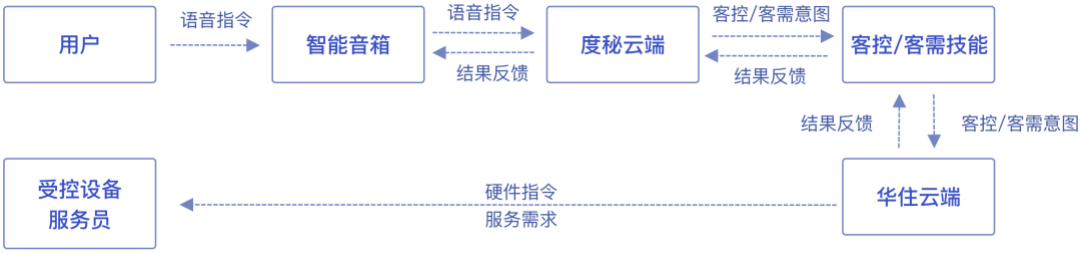

图 4 客控/客需通信数据流图

5.3 退房

酒店客户退房时，酒店版小度音箱将通过重置功能进行设备重置，清除设备、云端的用户数据，包括：

1) 清除设备端使用记录：闹钟/计时器，视频播放记录，音频播放记录，应用账号信息，应用使用记录等；

2) 设备端系统还原：音量恢复默认，屏幕亮度恢复默认，关闭蓝牙，关闭麦克风，清理缓存，设备恢复系统模式；

3) 设备端技能退出：执行中的系统原生技能、客控技能、客需技能退出；

4) 清除云端使用记录：闹钟/计时器，视频播放/收藏记录，音频播放/收藏记录，技能上下文状态失效，新建一个虚拟账号。

重置完成后，酒店版小度音箱设备以及云端将不存在任何与酒店客户个人相关的数据，同时音箱设备将恢复初始设置，为下次服务做准备。

5.4 风险审计

除了上述酒店客户在入住、日常使用、退房时接触到的酒店版小度音箱安全措施外，还会持续对音箱的行为进行风险审计。

目前用户的语音请求不进行保存，只是在度秘云端将其解析成控制指令，转发到技能平台，由技能平台调用客控、客需等服务技能，将控制指令转发至华住云端，因此，针对智能音箱的风险审计可在百度侧及华住侧同步展开。风险审计的内容包括：

1) 技能安全：检查技能是否进行了充分的安全配置，如技能代码无安全漏洞、HTTPS 传输数据、强证书校验、强身份凭证等；
2) 白名单：检查白名单设置是否合适，白名单是否正常生效，分析白名单之外的访问请求；
3) 非法访问：检查访问记录，分析越权访问、使用非法 Token 等非法访问请求；
4) 异常访问：检查访问记录，分析访问请求数据中鉴权失败、接口调用失败、非正常使用凭证/Token 等异常访问请求。

5.5 应急响应

除常规的安全措施外，当发生安全事件时，百度与华住会立即启动应急响应，确保第一时间分析事件原因，提供修复方案，并通过热修复、安全 OTA 进行修复，最大程度降低事件影响。

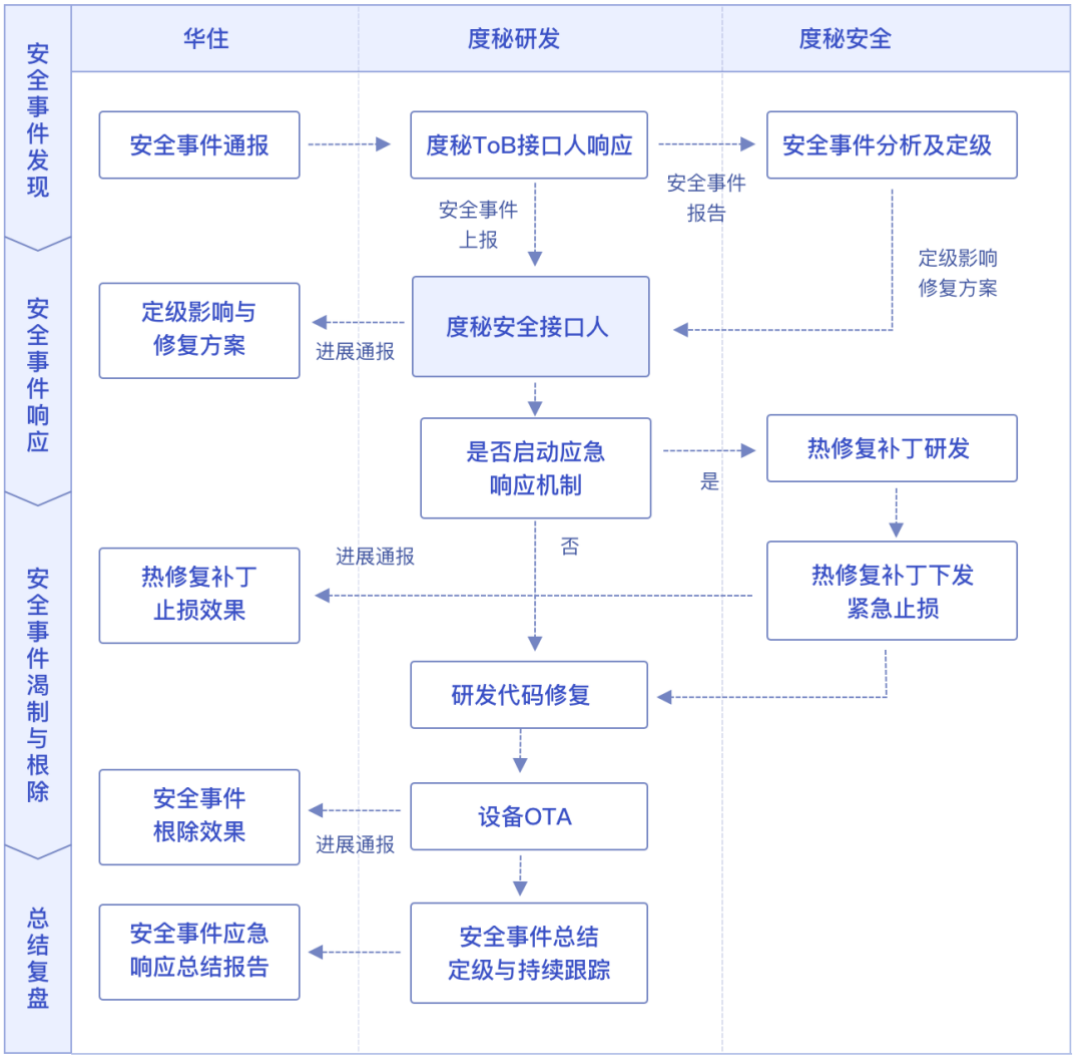

图 5 华住-度秘应急响应流程

1) 发现安全事件，途径如下：

a) 华住侧直接报告安全事件；

b) 华住安全响应中心；

c) 百度安全应急响应中心；

d) 国家应急中心；

e) 度秘安全团队安全评估；

f) 其他威胁情报；

2) 度秘 toB 接口人收到报告将细节同步度秘安全团队，同时上报度秘安全接口人；

3) 度秘安全团队对安全事件进行分析、给出定级、影响及修复方案，并将结果同步华住；

4) 度秘安全接口人根据以上信息判断决定是否启动应急响应流程；

5) 对于高危及严重安全事件，启动应急响应机制，度秘安全团队启用热修复下发补丁紧急止损；

6) 对于普通安全事件，走常规 OTA 进行修复；

7) 安全事件根除后，进行事件研究总结与持续跟踪，并对华住输出此次安全事件的应急响应总结报告。

百度内有多名安全接口人，保证任意时刻的安全事件，均有相关接口人进行响应。一旦出现安全事件，百度将首先在 3 天内完成事件的分析，并下发热补丁进行热修复，然后通过后续的 OTA 进行完全根除。

热修复采用百度全栈式自适应热修复方案，能够通过热补丁，实时修改内存中正在运行的系统或代码的逻辑流程，在短时间内以无需重启设备、打扰用户正常使用的方式实现对安全问题的修复。同时，热修复过程并不会修改任何系统及内核文件，打完热补丁的系统同样可以正常进行 OTA 升级。

OTA 采用百度安全 OTA，通过采用加密传输 OTA 升级包，对升级数据进行有效性、完整性、签名等验证，确保来源合法性，有效杜绝网络重放、DNS 劫持、数据内容劫持，升级包伪造等攻击行为。同时，OTA 升级由百度和华住共同进行监管，并且仅在双方均审核通过的情况下生效。

5.6 Q&A

1) 最佳实践中安全措施是否已应用到设备？

最佳实践是以小度在家智能屏 X8 酒店版为基础进行阐述，所有的安全措施均已在该型号上应用。

2) 智能音箱是否会通过摄像头监控或者记录住客行为？

酒店版小度音箱无摄像头部件，不会在任何时刻进行视频、图像监控。

3) 智能音箱什么时候会录音？住客如何知道智能音箱会不会录音？

语音数据是语音交互控制的基础，小度音箱会一直等待获取用户的语音数据，以便随时提供服务，但语音数据采取阅后即焚策略，不会进行存储。

非唤醒状态下，小度音箱仅判断获取到的语音数据是否是唤醒指令，不会进行传输、存储等其他处理；唤醒状态下，获取到的所有语音数据仅作指令解析，不会在设备端或云端落地存储。

如需要禁止音箱获取语音数据，可通过小度音箱上的开关机键关闭音箱，或者通过麦克风静音键关闭麦克风。

4) 智能音箱是否会收集/传输/存储住客的隐私数据？

酒店版小度音箱本身在使用过程中无需用户个人信息，百度与华住也不会在任何情况下搜集用户的隐私数据。同时，针对语音请求数据，采取阅后即焚策略，不进行存储；针对非语音数据采取脱敏处理，并进行必要的安全合规检查。

5) 住客的隐私数据是否会被泄露及公开？

小度音箱使用强加密传输所有的敏感数据，可以有效防止数据在传输过程中的泄露问题。同时，数据在处理时进行了脱敏，抹除用户相关的敏感数据，无法通过脱敏后的数据获取用

户的个人信息。

百度与华住之间的数据交互，仅与智能音箱设备相关，不涉及用户的个人信息，不存在个人隐私数据的泄露风险。同时，百度与华住不会将设备相关信息向第三方公开，能够防止通过其他途径发现设备与用户的关联。

6) 住客在智能音箱上使用 APP 时的账号及其相关信息是否会被窃取？

APP 的账号及其相关信息通常储存在 APP 的私有目录下，不会被其他 APP 窃取。同时，小度音箱使用分区加密技术，以加密的形式存储此类私有数据，能够防止通过固件提取的方式窃取这些数据。

7) 住客在智能音箱上设置的闹钟、个人事项等隐私数据是否会被下一个住客获取？是否可以手动清除？

酒店版小度音箱会在住客退房时执行重置操作，清除设备与云端的缓存数据、个性化配置、使用记录等用户相关信息，保证这些数据无法被下一个住客获取。

如需要手动清除这些数据，可以在音箱上使用重置功能执行清除操作。

8) 操作智能音箱的语音信息都会被谁获取到？

用户操作涉及语音指令时，语音数据将被百度获取，用于进行指令解析，并根据指令内容调用对应的服务（如相关技能）；在此过程中，用户的语音数据仅会在百度单独设立的度秘云端解析成指令信息，不会在任何地方存储，并且后续相关服务将仅能获取到解析出的指令信息，无法获取语音数据。

当操作控制客房 IoT 设备、呼叫客需服务等酒店场景专有功能时，操作行为及其相关信息将会被华住酒店获取，用于提供对应的服务。

9) 是否可以使用智能音箱控制其他房间的智能设备？

酒店版音箱以及其他智能设备均会与其所在的酒店客房绑定，音箱的设备控制权限仅限

于绑定到同一酒店客房下的智能设备。用户通过音箱发出的所有设备控制指令，在真正实施之前，都会进行权限校验，并且仅在权限校验通过后，才会实际执行。因此，用户仅可以使用音箱控制同一客房内的各个智能设备，无法控制其他客房的智能设备。

10) 用户是否可以在智能音箱上安装其他应用？

小度音箱提供官方应用市场，用户仅可从该应用市场下载安装应用，无法通过其他途径安装应用。

11) 用户是否可以在智能音箱上刷入其他固件？

酒店版小度音箱使用了安全启动技术，仅支持百度与华住提供的专用固件，用户无法刷入其他固件。

12) 房间内的智能音箱会不会自己发出声音？

当您设置的闹钟、提醒、习惯等定时任务触发时，智能音箱会播放相应的声音；

当使用投屏、蓝牙播放等远程播放功能时，智能音箱会播放相应的声音；

当智能音箱开机、接收到唤醒词时，会发出声音进行响应；

在其他未唤醒、未使用的状态下，智能音箱不会发出声音。

6 结束语

智能音箱携带语音交互的天然优势，在经过几年的发展后，已成为现阶段的智能 IoT 设备控制中心。受制于中国庞大的人口数量，国内的智能音箱市场在 toC 和 toB 领域都还处于早期采用者阶段。智能音箱酒店行业作为一个典型的 toB 场景，虽然在使用场景上与 toC 家庭场景类似，但是对安全性明显具有更高的要求。然而各个智能音箱厂商虽然在不断地推出新技术、新产品，但大多数情况下与安全的关系并不大。未来一旦在酒店行业中爆发智能

音箱安全问题，将极大影响智能音箱的发展进程。

无论智能音箱的使用场景如何变化，“用户——智能音箱——云端”都是主要的服务形式之一。因此，智能音箱酒店行业的安全防护可紧扣提高服务的安全性，保护好物理设备、系统软件、传输链路、云端服务以及数据的采集、传输、处理、储存、销毁等环节，并借助日常安全运维、应急安全响应，将安全能力扩展到智能音箱服务过程中涉及的方方面面，建立联合安全防护体系，最大化提高智能音箱酒店行业的安全性。

参考文献

[1] 艾瑞.中国智能物联网（AIoT）白皮书（2020 年）, 2020.

[2] 中国泰尔实验室. 互联网设备智能音箱安全白皮书（2019 年）, 2019.

[3] 大数据安全标准特别工作组. 人工智能安全标准化白皮书（2019 年）, 2019.

[4] 百度安全事业部. 人工智能硬件安全白皮书（2018 年）, 2018.

[5] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing v4.0, 2017.

[6] 全国信息安全标准化技术委员会. GB/T 38648-2020 信息安全技术 蓝牙安全指南, 2020.

[7] 全国信息安全标准化技术委员会. GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求, 2019.

[8] 全国信息安全标准化技术委员会. GB/T 35290-2017 信息安全技术 射频识别（RFID）系统通用安全技术要求, 2017.

附录 I 术语与定义

应用设备层：由各种有线/无线传感器、智能硬件设备等组成，本文也包括运行于其上的系统软件；

网络传输层：通过各种有线/无线的方式，与设备进行实时通信；

数据处理层：对收集的信息进行处理，实现智能化识别、管理等应用；

可信执行环境(Trusted Execution Environment ,TEE):设备主处理器上的一个安全区域，保证加载到该环境下的代码、数据的完整性、机密性、可用性；

安全启动 :在启动过程中对后续即将执行的程序进行验证，确保只有通过验证的程序才能在设备上运行；

HTTPDNS：使用 HTTP 协议向 HTTPDNS 服务器请求域名解析，代替基于 UDP 的 DNS 协议，能够避免本地 DNS 的域名劫持、不准确等问题；

热修复：在系统正常运行情况下，应用补丁，修复系统问题；

空中下载技术（Over-The-Air，OTA）: 终端通过无线网络下载远程服务器上的升级包，对系统或应用进行升级；

阅后即焚 :在本文中用于描述一种数据处理策略，在数据处理完成后立即删除相关数据，不在任何地方落地存储；

固件：嵌入硬件中的软件，一般担任着系统最底层的工作；

efuse :一次性可编程熔丝技术 ,是一种 OTP(One-Time Programmable ,一次性可编程）存储器，其内部数据只能写入一次。

附录 II 缩略语

下列缩略语适用于本文：

AES	高级加密标准	Advanced Encryption Standard
AI	人工智能	Artificial Intelligence
AIoT	智能物联网	AI + IoT
API	应用程序接口	Application Programming Interface
APP	应用	Application
BLE	蓝牙低功耗	Bluetooth Low Energy
CA	数字证书认证机构	Certification Authority
CNNVD	中国国家信息安全漏洞库	China National Vulnerability Database of Information Security
CNVD	中国国家信息安全漏洞共享平台	China National Vulnerability Database
CSRF	跨站请求伪造	Cross-site request forgery
CVE	通用漏洞披露	Common Vulnerabilities and Exposures
DDoS	分布式拒绝服务攻击	Distributed Denial-of-Service attack
DLNA	数字生活网络联盟	Digital Living Network Alliance
DNS	域名系统	Domain Name System
ECC	椭圆加密算法	Elliptic curve cryptography
ECDSA	椭圆曲线数字签名算法	Elliptic Curve Digital Signature Algorithm
HTTP	超文本传输协议	Hyper Text Transfer Protocol

HTTPS	超文本传输安全协议	Hyper Text Transfer Protocol Secure
IoT	物联网	Internet of things
PSTN	公共交换电话网	Public Switched Telephone Network
RCU	客房控制器	Room Control Unit
rootfs	根文件系统	root file system
RSA	RSA 加密算法	RSA algorithm
SDN	软件定义网络	Software-Defined Networking
SQL	结构化查询语言	Structured Query Language
SLA	服务水平协议	Service-Level Agreement
SIP	会话发起协议	Session Initiation Protocol
SSH	安全外壳协议	Secure Shell
SSL	安全套接层	Secure Socket Layer
TEE	可信执行环境	Trusted Execution Environment
TLS	安全传输协议	Transport Layer Security
toB	面向企业、机构	To Business
toC	面向消费者	To Customer
XSS	跨站脚本	Cross-site scripting