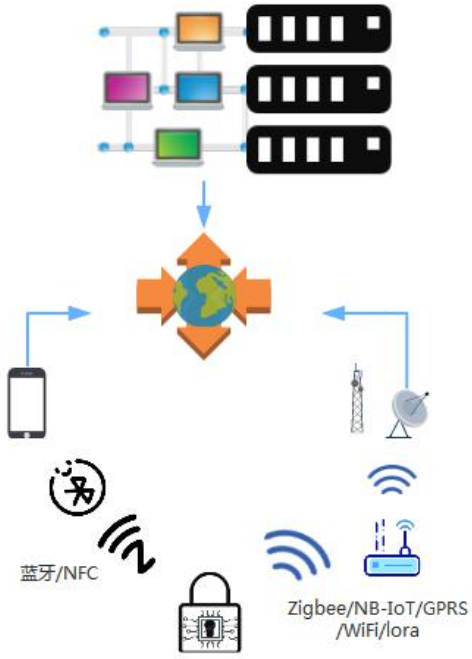
1.智能锁典型应用结构



终端、智能锁电子部分以单片机开发为主，往往由主控芯片，通信模块，GPS 以及其他传感器等组成。部分简单的智能锁应用则只需要通信模块二次开发，而无需另外的主控芯片。终端往往集成了多种通信方式，按联网方式分类，主要包括通过手机与外部网络连接和通过网关与外部网络相连。通过手机的方式主要是 NFC，蓝牙。通过网关与外部网络相连的方式则至少包括如 Zigbee 网关接入 Zigbee 子网网络，Lora 网关接入 Lora 子网网络，NB-IoT 和 GPRS 基站接入运营商网络，433 私有协议网关接入路由然后接入互联网，WiFi 路由或以太网路由接入家庭网络。终端传感器可能包括生物特征识别传感器，陀螺仪，重力传感器，温度传感器，3D 传感器等。

Zigbee 等方式还可能与自组网等其他智能设备进行联动。应用层往往使用标准机制互联互通，比如 Zigbee 应用层协议或者 OCF 协议。

服务端应用，则可能基于公有云开发，也可能基于混合云模式开发，或者独立机房自行维护软硬件开发智能锁平台应用。服务端平台应用往往包括与智能锁交互的服务和与手机远程控制端 web 服务，服务端往往通过适配物联网的协议来与智能锁交互，比如 mqtt，xmpp,coap,jt808 等，而 与手机交互往往沿用传统的 web 技术。

2.解决方案

我们推出了适合智能锁业务的轻量级安全解决方案，从攻击者角度出发，方案能有效提高攻击者的技术门槛。主要包括：

- 通信安全增强。端到端的轻量级应用层安全协议，ISO 标准化机制，适合智能锁单片机环境集成。基于应用层且跟业务分层，适合多种终端通信方式，一致性的安全建设。
- 传感器安全增强。通过 TEE 技术或安全芯片 SE 技术，对传感器存储和比对过程进行隔离。与终端方案企业合作集成高可靠生物特征传感器。
- 应用层安全增强。终端和平台业务层身份密钥的安全分发，存储，计算。通过安全激活过程把业务终端识别号与身份密钥绑定，配合业务通信安全协议，使得业务的访问控制机制具有强身份认证基础。
- 本地终端系统安全增强。实现安全升级功能。与合作企业合作开发使用安全启动，软件沙盒，代码安全等保护机制。
- 锁芯和结构安全增强。与合作终端企业合作开发 C 级锁芯和 B 级智能锁。
- 自组网安全增强。通过非对称密钥分发实现无需在线第三方的身份认证和通信安全。
- 供应链安全。不绑定某一家云平台或者安全芯片厂商，防止密钥泄露和供应保障。

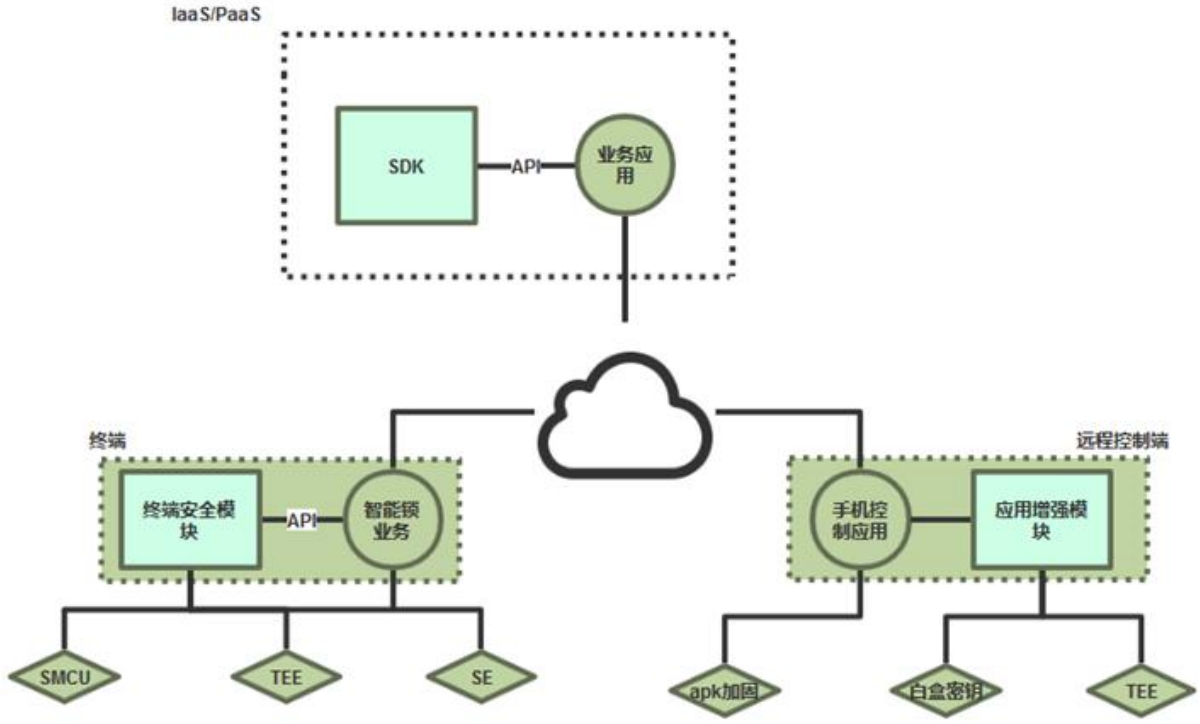
方案包括三个部分，智能锁安全组件，移动端增强安全组件和服务端组件。

智能锁安全组件，根据业务选择的开发平台和安全需求适配 SMCU，TEE 或 SE 平台，包括安全密钥烧录和管理，安全对时，安全激活管理，安全通信，安全存储和认证等功能。安全组件是可移植的。

移动端增强安全组件，包括 app 加固以及基于白盒密钥或 TEE 的应用增强安全方案，应用增强方案针对认证身份和 https/蓝牙通信进行了安全加固。

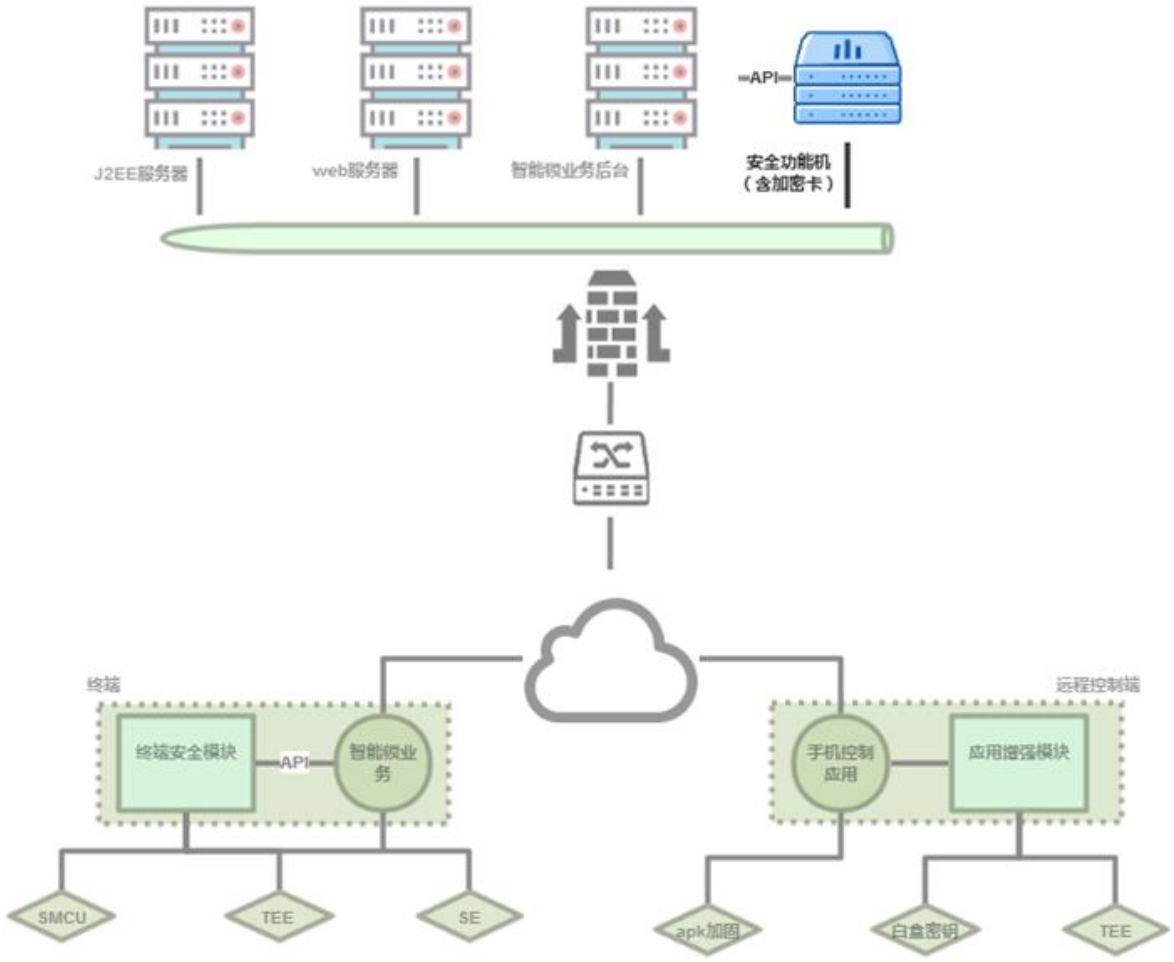
服务端组件，包括基于公有云的 SDK 部署以及基于私有云或服务器的单独安全功能机部署。单独安全功能机本身除了集成了公有云模式下平台 SDK 的所有安全功能之外，还集成了我司自主研发的高性能加密卡，能有效保障业务密钥安全和计算安全。【详细的集成可参考开发中心】

2.1 基于公有云业务应用部署



如果业务完全托管在公有云，如阿里云 ECS 上，则需要业务服务端集成安全 SDK。因为安全 SDK 处于应用层 ,且与业务层分层 ,所以您的业务框架无需任何改变。目前 SDK 基于 java JDK1.7+. 更多平台支持请联系我们。

2.2 基于混合云或业务机房应用部署



如果业务运行在您自己的机房，或者使用混合云模式模式开发，我们支持独立安全功能机部署。把安全功能机部署在业务服务可访问的网络段即可。安全功能机拥有所有的安全功能 ,并部署我们量产的 PCIE 加密卡 ,保证服务端侧密钥存储和计算的高安全。我们的 PCIE 加密卡参数参考本网站的安全产品页内容。