第68卷 第1期
2022年2月

武汉大学学报(理学版)
J. Wuhan Univ. (Nat. Sci. Ed.)

Vol. 68 No. 1
Feb. 2022, 1~7

**DOI:** 10.14188/j.1671-8836.2021.2000

# 小米“手机×AIoT”安全隐私技术

崔宝秋,宋文宽,王宝林,潘双全,张晓芳,赵彤彤,吕莹楠
小米集团,北京 100085

收稿日期:2021-12-30
作者简介:崔宝秋,男,博士,现从事云计算、大数据、人工智能、信息安全和隐私保护方面的研究。E-mail:cuibaoqiu@xiaomi.com

**摘　要**:在万物互联时代,安全和隐私风险逐步扩大,越来越多的人开始担忧产品的安全和隐私问题。小米集团具有手机和物联网等多种业务形态,“手机×AIoT”也已成为小米的核心战略。围绕手机和AIoT(人工智能物联网),小米在信息安全与隐私保护方面面临着非常大的挑战,也做了大量的工作。本文基于小米的信息安全和隐私保护发展历史,介绍了在手机、IoT以及AI领域的信息安全和隐私保护技术。这些技术包括了小米可信执行环境MiTEE(Mi trusted execution environment)、差分隐私技术、MIUI隐私保护技术、AI算法隐私保护、移动端深度学习框架MACE(mobile AI compute engine)、IoT软件开发平台Xiaomi Vela,以及IoT的其他安全技术能力等。

**关　键　词**:信息安全;隐私保护;MIUI;差分隐私;MiTEE(Mi trusted execution environment);MACE(mobile AI compute engine);Xiaomi Vela

**中图分类号**:TP309　　**文献标志码**:A　　**文章编号**:1671-8836(2022)01-0001-07

# Xiaomi “Smart Phone×AIoT” Security & Privacy Technology

**CUI Baoqiu, SONG Wenkuan, WANG Baolin, PAN Shuangquan, ZHANG Xiaofang, ZHAO Tongtong, LÜ Yingnan**
Xiaomi Inc., Beijing 100085, China

**Abstract**: In the era of Internet of Things, security and privacy risks are gradually expanding. More and more people begin to worry about product security and privacy. Xiaomi has a variety of business forms such as mobile phone and Internet of Things, and “Mobile Phone × AIoT” has become Xiaomi's core strategy. Around mobile phones and AIoT, Xiaomi is facing great challenges in information security and privacy protection and has done a lot of work. Based on the development history of Xiaomi's information security and privacy protection, this paper introduces our information security and privacy protection technologies in the fields of mobile phones, IoT and AI. These technologies include Xiaomi's Trusted Execution Environment (MiTEE), differential privacy, MIUI privacy protection features, AI algorithm privacy protection, Mobile AI Compute Engine (MACE), IoT software development platform Xiaomi Vela, and other security technology capabilities related to IoT.

**Key words**: information security; privacy protection; MIUI; differential privacy; MiTEE (Mi trusted execution environment); MACE(mobile AI compute engine); Xiaomi Vela

## 0　引　言

据统计,2020年联网设备数量突破217亿[1],并预计在2025年联网设备达到412亿。随着互联设备的增加,安全和隐私风险也在不断扩大,安全事件(比如数据泄漏,服务不可用等)造成的影响也在逐年增加。2021年4月,CyberNews报道职业社交网站领英发生了5亿个人数据泄漏[2];2021年10月,Facebook又爆出了15亿个人数据泄漏的事件[3]。据卡巴斯基报告[4],仅2021年上半年,就有超过

引用格式:崔宝秋,宋文宽,王宝林,等. 小米“手机×AIoT”安全隐私技术[J]. 武汉大学学报(理学版),2022,68(1):1-7. DOI:10.14188/j.1671-8836.2021.2000.
CUI Baoqiu, SONG Wenkuan, WANG Baolin, *et al*. Xiaomi “Smart Phone×AIoT” Security & Privacy Technology [J]. *J Wuhan Univ* (*Nat Sci Ed*), 2022, 68(1): 1-7. DOI: 10.14188/j.1671-8836.2021.2000(Ch).

15.1亿IoT设备遭到网络攻击。这些安全事件的发生,对用户,对企业,甚至对国家危害都是非常巨大的。万物互联时代,用户在享用着科技带来的便捷的同时,也越来越担心科技带来的其他问题。近几年,安全和隐私问题更是成为了用户关注的热点,用户的安全隐私意识在逐步增强,全球多个国家和地区也纷纷加速对安全隐私相关立法和标准的发布,更加关注智能化、数字化可能引起的安全隐私问题。欧盟的《通用数据保护条例》(general data protection regulation,GDPR),美国加州的《加州消费者隐私保护法案》(California consumer privacy act,CCPA),以及国内2021年出台的《数据安全法》和《个人信息保护法》等法律法规和指导文件,对企业和产品提出了基本的安全隐私要求。快速扩大的安全风险,逐步增强的用户安全隐私意识,以及日趋严格的法律法规要求,使得信息安全与隐私保护成为了每个企业的生命线。

## 1 小米的安全隐私保护概述

### 1.1 小米的安全隐私保护发展历史

小米是一家以智能手机、智能硬件和IoT平台为核心的消费电子及智能制造公司,"手机×AIoT"是小米的核心战略。小米一直以来都很重视信息安全和隐私保护,早在2012年就创建了信息安全团队;2014年,随着集团国际化布局的开启,成立了安全与隐私委员会,开始与国际知名隐私认证公司TrustArc合作,整体提升集团的隐私保护水平;2016年,小米网和小米手机操作系统MIUI全面拿到了TRUSTe隐私认证;2018年,欧盟的《通用数据保护条例》(GDPR)开始生效,由于小米很早开始布局,在安全和隐私策略及技术方面的积累使得小米可以很好地应对GDPR,业务与国际化步伐未受到影响。过去几年来,围绕组织保障与隐私意识、管理体系与流程、信息安全与隐私保护权威认证,小米打造了一套比较成熟的隐私合规体系,也沉淀了小米的隐私保护五大基本原则:公开透明(transparency)、用户可控(control)、企业责任(accountability)、安全保障(secure)、合法合规(compliance)。目前小米已获得的安全与隐私认证包括TrustArc隐私认证、ISO/IEC 27001信息安全管理体系、IOSO/IEC 27018公有云个人数据保护指南、ISO/IEC 27701隐私管理体系以及中国信息通信研究院泰尔实验室颁发的手机系统隐私保护认证等。

### 1.2 小米的"手机×AIoT"安全隐私保护技术

这些年,很多人对于安全和隐私治理的看法还停留在"七分靠管理,三分靠技术",但随着互联网、云计算、大数据和人工智能的发展,当我们站在当下展望未来,安全和隐私治理应当是"三分靠管理,七分靠技术",信息安全与隐私保护技术在当下显得愈发重要。小米的"手机×AIoT"安全隐私保护技术可以分为以下三个部分:1)手机全链路安全隐私技术,2)IoT平台化安全隐私技术,以及3)AI算法应用中的安全隐私技术。

## 2 手机全链路安全隐私技术

### 2.1 MiTEE小米可信执行环境

"安全和隐私是一对双胞胎",如果数据的安全性得不到有效保护,用户隐私权益的保障也就无从谈起。Android系统是目前应用最广泛的手机操作系统,拥有非常开放的生态环境,由此它的安全性也备受大家关注。在Android系统中,Root用户对所有的应用和应用数据拥有完整访问权限。设备上某些恶意应用利用内核错误或安全漏洞获得Root权限,就可对系统和应用的安全保护带来严重的威胁。为了更好地解决这类安全问题,一种新的基于硬件隔离的解决方案——独立于Android系统之外的可信执行环境(trusted execution environment,TEE)——就应运而生了。与可信执行环境(TEE)相对应的是运行普通操作系统和应用程序的REE(rich execution environment)。相比于运行在REE的Android系统,TEE拥有更高的权限,它运行于Android无法访问的独立执行内存中,应用程序可以把关键处理和敏感数据放在TEE中执行或加密存储,这样即便是有攻击者获得了Android系统的Root权限,也无法进一步窃取或攻击TEE中的处理或数据。

芯片是手机中最核心的组成部分,通过TEE构建设备的安全能力需要从芯片出发。小米手机主要采用高通或联发科生产的ARM芯片。因此小米主要基于ARM硬件总线隔离技术(也被称为ARM TrustZone隔离技术[5])来构建小米可信执行环境,这个环境称之为MiTEE(Mi trusted execution environment)。MiTEE是小米基于开源技术打造的基于微内核的TEE(如图1)。MiTEE主要包含五个组成部分:

1)面向CA(client APP)的GP API框架接口层,主要用于和安全应用进行交互;

2)MiTEE驱动,主要用于实现Linux内核和TEE OS的直接通讯;

3) MiTEE SPD,主要用于接收和响应TEE和REE的异常命令,并实现两个环境之间的切换;

4) TEE OS ,包括可以有效减小可信基并加强权限管控的微内核和TEE框架层,TEE框架层包含安全应用管理、应用权限管理、密钥算法(基于安全硬件的真随机数)、安全存储、安全硬件驱动和时间系统(基于安全硬件的时钟),主要负责对安全应用进行管理,并为上层安全应用提供服务;

5) 运行于TEE可信应用(trusted applications, TA),主要用于提供关键服务给普通应用使用,如隐私计算、金融支付、生物识别和密钥保护等功能。

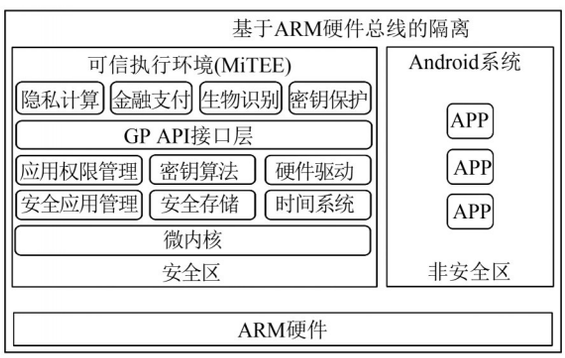


图1　MiTEE架构

Fig. 1　MiTEE architecture

MiTEE除了上面提到的隔离,即对执行环境及数据处理进行隔离保护之外,另一个重要的功能是安全数据存储,即安全文件系统。

MiTEE的安全文件系统采用“一机一密”,不同安全应用加密密钥不同。安全应用进行安全文件存储时,首先会基于硬件HUK(hardware unique key)以及安全应用信息派生出一把应用唯一密钥(该密钥不会流出于MiTEE之外),然后对数据进行加密并计算HMAC(Hash-based message authentication code)信息,最后存储到存储设备上。安全文件具有机密性、完整性的特点。同时MiTEE也有支持RPMB(replay protected memory block)存储,如果数据选择存放到RPMB,还可以防重放攻击。

MiTEE为小米手机的安全性提供了根本、坚实的保障,它不仅可以对执行环境的数据处理进行有效的隔离保护,还可以在金融支付、用户身份识别、数据安全存储等方面起到关键性作用。

### 2.2　差分隐私技术

差分隐私(differential privacy)是密码学中的一种手段,也是近些年来逐步兴起的一种新型的隐私保护技术。利用差分隐私技术,可以在保留统计学特征的前提下最大程度地避免个体特征的暴露,以达到保护用户隐私的目的。例如,当有人尝试在一个学校的数据库中查询学号排名在前9个的学生的院系分布,会得到统计结果A,第二次查询前10个学生的院系分布,会得到统计结果B。通过比对结果A和B,就可以轻易知道第10个学生的院系信息。为了在进行数据分析时尽量减少此类单个用户被识别的可能性,我们可以在每次结果输出时添加一个随机噪声,这样在两次查询后,就无法准确判断第10个学生的院系情况了。在实际应用差分隐私技术时,常向查询结果中加入服从拉普拉斯分布的噪声,这种方法也被称为“拉普拉斯机制”。

我们不仅在数据查询端广泛地使用差分隐私,在原始数据采集端也会适当地添加噪声数据。产品质量和用户体验是小米非常关注的问题,想要做好这些改进工作离不开大数据,离不开数据驱动。我们需要了解和分析终端设备上的相关性能数据,比如启动速度、元器件温度、耗电量、内存使用情况和系统崩溃情况等数据,这些数据汇总后将对小米开展质量和体验改进工作提供极大的技术支持。在这些场景下,设备或应用并不需要关心具体某一个用户的情况,因此如何在快速、高效地获取端上数据的同时,尽量降低对用户隐私数据的过度收集,就成了亟须解决的隐私问题。

差分隐私在解决这个问题上扮演了重要的角色。如图2所示,在进行手机设备的性能优化时,需要采集和分析设备上的硬件状态、存储占用和电池温度等相关信息。为了最大程度地保护用户隐私,避免识别出单个用户的原始数据,小米手机在相关数据产生后就在端侧添加了噪声数据。这些掺杂了噪声的设备性能数据在上传至小米的服务器时,便在最大程度上失去了被准确识别出单个用户的可能性。经过实际验证,这些噪声数据并不会对后续的数据分析产生实质影响。

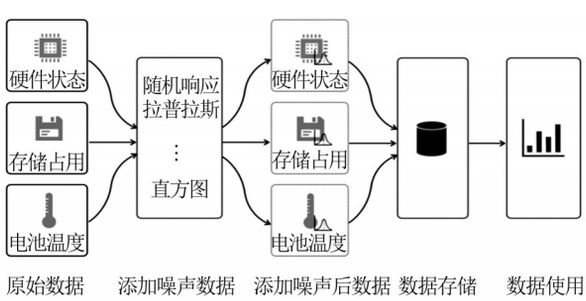


图2　差分隐私技术应用于性能数据统计

Fig. 2　Differential privacy technology apply on data statistic

### 2.3 MIUI操作系统中的安全隐私保护

MIUI是小米基于Android深度定制的移动操作系统。在操作系统层面,MIUI一直致力于用户安全与隐私保护。过去十年中,MIUI每年都会向用户提供更加领先的安全与隐私保护能力。2020年发布的MIUI12/12.5版本,就为用户提供了三大隐私保护功能:照明弹、拦截网和隐匿面具。

照明弹功能针对APP的不规范行为对用户做了各种提醒,为用户提供了应用行为记录、敏感行为提醒、剪切板隐私保护和相册图片防误删等功能。拦截网功能给用户提供了更多的控制权,使其能够禁止后台相机的唤醒和使用,而且当一个APP申请一些权限时,拦截网可以帮用户控制权限使用的范围,对没有说清权限用途的APP,将不提供"始终允许"的选项;拦截网也可以让用户在分享照片时擦除敏感信息,做到分享生活但不分享隐私。隐匿面具功能给用户提供了更加灵活的隐私保护措施,包括空白通行证、虚拟身份ID、模糊定位和上网防追踪功能,让用户在不影响使用各种APP的正常功能的同时,最大限度地保护自己的隐私。

在这三款隐私保护功能发布后,各种APP敏感权限调用次数大幅度降低,不必要的权限调用大大减少。例如,地理位置权限调用降低了98%,联系人权限调用降低了93%,本地存储权限调用降低了92%,剪切板权限调用降低了86%。这些大幅度敏感权限调用次数的降低体现了这三款隐私保护功能的威力,体现了它们对整个Android生态的安全隐私保护起到的净化作用,更体现了小米对隐私保护的极致追求。MIUI的照明弹等功能将被列入中国智能手机入网标准,这也代表了小米在行业上的贡献。

## 3 IoT平台化安全隐私技术

小米自2014年开始打造物联网生态系统,如今小米的IoT平台已成为全球最大的消费级IoT平台,截至2021年11月(Q3财报数据[6])小米物联网平台联网设备数量超过4亿,有超过800万米粉拥有5件以上的IoT设备。随着物联网生态的迅猛发展,小米的安全边界随之扩大,物联网安全存在的问题和挑战日渐凸显。以绿盟《2020物联网安全年报数据》[7]中对物联网安全事件及物联网相关漏洞利用分析为参考,物联网安全面临的问题主要体现在设备硬件层防护能力不足、软件存在安全漏洞、碎片化的物联网生态成为建立攻击链的突破口。

面对消费级物联网市场的高度碎片化和极具差异性的现状,小米IoT平台本着从设计着手的隐私保护(privacy by design)和默认安全(security by default)两大原则,构造统一的硬件架构、软件架构及安全解决方案,通过将技术实现和平台管控的能力结合,为开发者提供统一的平台化安全隐私保护能力及技术支撑。

### 3.1 统一IoT硬件架构筑牢物联网设备安全基石

小米IoT平台推出米家安全芯片,支持"一芯一密"、ECC256安全加密算法等,为产品提供硬件级的安全防护。同时平台推出了统一的通信模组(包括BLE模组、WIFI模组、Mesh模组、ZigBee3.0模组),从而统一了认证、签名、加密方案,实现了统一的安全加固能力。

### 3.2 统一IoT软件框架巩固物联网设备安全围墙

IoT与人工智能、大数据、5G、边缘计算等技术结合,开启了万物智能互联时代,也使AIoT(人工智能物联网)成了一个新的行业热词。在AIoT生态中,为了给用户提供智能服务,就不可避免地要对用户智能终端上的一些数据进行采集和使用。为最大程度降低用户信息的安全与隐私风险,小米推出了自主研制的移动端深度学习框架MACE(mobile AI compute engine),将更多的AI推理和模型训练留在智能终端上。另外,为了解决AIoT生态中的碎片化问题及对不同设备提供统一的安全和隐私保护平台,小米基于开源的RTOS系统NuttX打造了自己的IoT软件开发平台Xiaomi Vela系统。

#### 3.2.1 统一的移动端深度学习框架MACE

2017年,小米AI团队开启了MACE研发项目,并在2018年正式对外开源。MACE是一种面向手机和AIoT移动端的深度学习框架,在提高端上的AI计算能力的同时,为用户提供安全隐私保护。MACE支持TensorFlow、Caffe、Pytorch、MegEngine和ONNX等模型。同时,相较于其他移动端开源深度学习框架对异构计算支持的不足,MACE作为一个真正可用的支持异构计算的移动端深度学习框架,已实现对CPU、GPU、DSP(digital signal processor)、APU(accelerated processing unit)异构计算的支持。MACE的架构如图3。

2020年4月,MACE推出微控制器引擎MACE Micro,MACE Micro是针对微控制器推出的AI框架。全面支持手机与AIoT设备超低功耗推理场景,并在小米低功耗DSP上落地了人体行为识别应用。在国内其他开源端侧深度学习推理框架均面

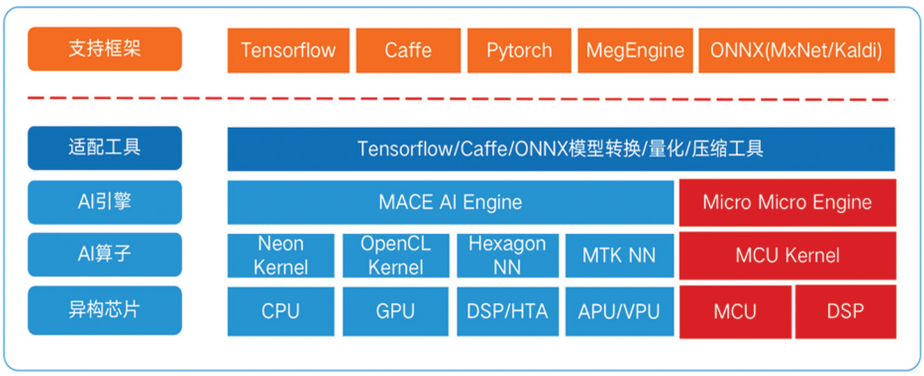


图3　MACE技术架构

Fig. 3　MACE framework

向手机芯片的情况下，MACE率先实现了面向AIoT微控制器芯片的支持。

比如，在运动健康领域，如何在超低功耗的场景下7×24小时地智能感知用户运动行为并给出合理的健康建议，是智能手机、智能手表等设备厂商一直关注的难题。而其中的关键，就是获取用户设备端的数据并评估用户状况。所以各大厂商始终从硬件、软件、算法等各个层面不断迭代优化，以获取更多、更准确的用户运动健康数据。

小米手机上的小米健康这一系统APP基于MACE Micro实现了灵弦算法——AI运动行为感知技术。用户只需要将手机携带在身上，即可自动记录一整天的步行、跑步、骑行和爬楼梯等运动行为。而该功能24小时的耗电量不超过手机电量的1%。经泰尔实验室测试认证，灵弦算法的准确率为94.3%，召回率为80.9%，均超过Google的表现。当前，国内其他开源端侧深度学习推理框架均面向手机芯片，但没有针对AIoT设备的微控制器芯片进行研发，MACE Micro的推出和开源，对开发者具有重要的意义。作为运动健康算法的核心，MACE Micro在功耗、性能、存储等方面都处于业界领先地位，表1是小米运动健康算法的核心指标。

MACE Micro具备高性能、低能耗、易移植、易使用的特点，已在小米的AIoT设备（手表、音箱、耳机等）上落地，从端侧为用户的安全隐私保驾护航。

### 3.2.2　统一开发平台Xiaomi Vela

2019年，小米与开源的RTOS系统NuttX[8]展开了战略合作，基于NuttX打造了小米的IoT软件开发平台Xiaomi Vela。Xiaomi Vela提供统一的软件平台，通过丰富的组件和标准化的软件框架，打通了碎片化的物联网应用场景，为AIoT设备提供了统一软件层安全保护措施，降低了IoT应用的安全和隐私风险。Xiaomi Vela系统架构图如4。

**表1　小米运动健康算法核心指标**

**Table 1　Core indicators of Xiaomi sports health algorithm**

| 指标 | Float32 | BFloat16 |
|---|---|---|
| Micro核心库大小/KB | 43 | 43 |
| 模块SO大小（源模型224KB）/KB | 368（包含所有内存） | 256（包含所有内存） |
| 初始化耗时/ms | 0 | 0 |
| 热启动运行性能（骁龙855 SDSP）/ms | 0.825 | 0.880 |
| 冷启动运行性能（骁龙855 SDSP）/ms | 4.60 | 2.58 |
| 精度（与源框架对比）/% | 100 | 99.98 |
| 底层功耗/mA | ＜1 | ＜1 |

Xiaomi Vela的架构主要分为三个部分：NuttX内核（NuttX kernel）、应用框架（application framework）和工具集（tools）。

1）NuttX内核

Xiaomi Vela和NuttX的内核关系可以类比为Android和Linux内核的关系，NuttX提供基础的内核功能，包括任务调度、文件系统、TCP/IP协议栈、设备驱动和电源管理等，对上提供标准的POSIX接口。

2）应用框架

为解决物联网应用碎片化问题，其中最重要的途径是让Xiaomi Vela像NuttX一样，模块化，可伸缩、可裁剪，实现支持从简单到复杂，从低端到高端的各种产品形态，让开发者可根据实际需求对系统进行定制。

Xiaomi Vela的应用框架可以看作一个软件中间件，它是各种软件库、实用程序（如cloud SDK，

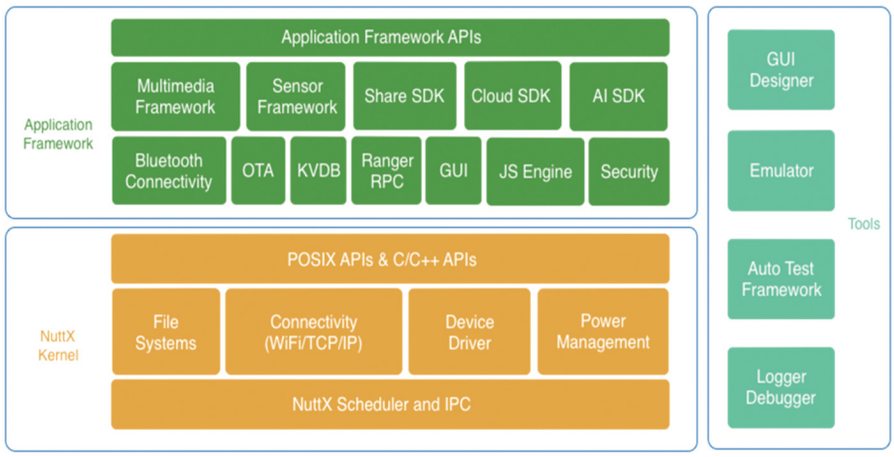


图4 Xiaomi Vela系统架构

Fig. 4 Xiaomi Vela framework

GUI等)和框架的集合,用于支持各种不同的物联网应用。针对不同的应用形态,我们开发了不同的应用框架,包括多媒体应用框架、传感器应用框架、蓝牙互联互通框架、云服务开发框架等。

3) 工具集

Xiaomi Vela的工具集除了提供嵌入式开发环境和仿真器外,还提供一套完整的自动化测试框架,以保证OS和上层应用都可以通过一套CI/CD流程确保高质量的交付。另外,我们也投入了大量的人力开发新的日志和调试工具。

### 3.3 统一IoT解决方案加固物联网设备安全纽带

小米IoT平台为开发者提供统一的安全方案(如固件云验签、传输加密、存储加密、业务逻辑等),并打造了自动化AIoT安全测试平台,平台通过手机、树莓派、电视三大安全评估引擎,与日常工作通知系统相结合,实现了自动化安全检测、漏洞告警、数据跨境检测、7×24小时安全监控等功能。在应用中能够帮助开发者快速便捷地发现问题、定位问题、持续监控、告警同步。

## 4 AI算法应用中的安全隐私技术

小米在2016年开始实施“All in AI”的长期战略。小米秉承技术为本的铁律,自主研发占据主导,全面赋能小米各业务线——从软件到硬件,从手机到生态链。几乎所有的AI技术在小米都有用武之地,而几乎所有的小米产品都需要AI来赋能。今天的AI是大数据和深度学习引领的AI,而提到大数据就避免不了信息安全和隐私保护的问题。

### 4.1 小米可信赖AI四原则

小米作为全球领先的智能手机制造商,致力于开发可信赖的人工智能技术(以下称为“可信赖AI”),造福并赋能于每一个用户。小米在AI技术的开发和应用过程中遵守国际公认的道德标准,参照欧盟关于可信赖AI的道德准则[9],并结合小米的隐私保护实践,建立了小米可信赖AI的四项基本原则:安全性(security and safety)、隐私保护(privacy)、公平性(fairness)、可解释性(explainability)。这些原则在小米人工智能技术的研究、开发和应用的整个过程中得到贯彻。

### 4.2 小米AI应用中的安全隐私保护实践

技术措施层面,小米通过建立安全架构保护算法操作环境和用户信息的安全。AI模型被深度集成到设备中且只在本地运行,通过AI算法处理的数据不会备份或传输到任何其他地方。端侧的AI算法只有在用户授权的情况下才会被调用,并且根据数据最小化的原则,仅处理服务运行所必需的数据。

非技术层面,小米建立了包括AI伦理委员会和安全与隐私委员会在内的完整管理体系,监督小米的AI处理流程并实现最佳实践。其中,小米人工智能伦理委员会承担以下工作:

- 统一职责,制定和监督落地企业内AI标准及规范;
- 支撑业务,探索行业内最佳AI技术实践;
- 风险掌控,识别AI面临的伦理风险、安全与隐私风险,通过风险评估模型降低风险的发生;
- 引导标准,推动AI伦理标准规范、法律法规。

2021年5月,小米对外发布了《小米可信AI白皮书》[10],白皮书中对小米可信AI治理进行了介绍,并结合小米在人脸识别、通信降噪等领域的AI方面研究,描述了通话降噪、图像优化、人脸解锁和指纹

解锁四个重要的AI应用在安全隐私保护的具体实践。

## 5　结　语

小米安全隐私体系由小米安全隐私组织架构保证,以手机、IoT、AI算法的技术能力为支撑。手机和IoT从芯片等硬件到操作系统再到上层应用甚至最后的产品层面、人机交互,需要大量的技术投入,在未来这也是小米重点的投入领域。

小米的使命是:要坚持做感动人心、价格厚道的好产品,让全球每一个人都能享受科技带来的美好生活。“科技”更多的是人工智能技术和未来的手机×AIoT技术,作为安全和隐私技术的引领者,小米希望安全和隐私技术能为人们美好生活保驾护航,这也是小米一直以来努力的方向——构建一个保护用户隐私的强大生态。

## 参考文献:


[1] LUETH K L. State of the IoT 2020 [EB/OL]. [2020-11-19]. *https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time*.

[2] Cybernews Team. Scraped Data of 500 Million Linkedin Users Being Sold Online, 2 Million Records Leaked as Proof [EB/OL]. [2021-04-06]. *https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2*.

[3] ZOLTAN M. Web Scrapers Claim to Possess and Sell Personal Data on 1.5 Billion Facebook Users on a Hacker Forum [EB/OL]. [2021-11-21]. *https://www.privacyaffairs.com/facebook-data-sold-on-hacker-forum*.

[4] CYRUS C. IoT Cyberattacks Escalate in 2021, According to Kaspersky [EB/OL]. [2021-09-17]. *https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky*.

[5] ARM.Learn the Architecture: AArch64 Exception Model [EB/OL]. [2021-09-17]. *https://developer.arm.com/documentation/102412/0100*.

[6] 小米集团. 2021年第三季度业绩发布 Third Quarter 2021 Financial Results [EB/OL]. [2021-11-23]. *https://company.mi.com/zh-cn/ir/indexContent/index.html*.
Xiaomi Inc. Third Quarter 2021 Financial Results [EB/OL]. [2021-11-23]. *https://company.mi.com/zh-cn/ir/indexContent/index.html*.

[7] 绿盟科技. 2020物联网安全年报 2020 IoT Security Annual Report [EB/OL]. [2021-01-18]. *https://www.nsfocus.com.cn/html/2021/92_0118/147.html*.
NSFocus. 2020 IoT Security Annual Report [EB/OL]. [2021-01-18]. *https://www.nsfocus.com.cn/html/2021/92_0118/147.html*.

[8] NuttX. NuttX Documentation [EB/OL]. [2021-12-19]. *https://nuttx.apache.org/docs/latest/index.html*.

[9] European Commission. Ethics Guidelines for Trustworthy AI [EB/OL]. [2019-04-18]. *https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf*.

[10] Xiaomi Inc. Xiaomi Trust Worthy AI White Paper [EB/OL]. [2021-09-17]. *https://trust.mi.com/en*.


□