基于超级SIM的5G端云安全体系架构与关键技术

Security Architecture and Key Technologies for Super SIM-Based 5G End-Cloud System

李佩源/LI Peiyuan，刘建伟/LIU Jianwei
（北京航空航天大学，中国 北京 100191）
(Beihang University, Beijing 100191, China)

DOI：10.12142/ZTETJ.202301004
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20230224.1443.002.html
网络出版日期：2023-02-24
收稿日期：2022-12-24

摘要：基于超级用户身份识别模块（SIM）卡的增强型安全功能，以及终端、云、端云协同3个方面的安全需求，结合区块链、雾计算、轻量认证等技术，设计了适配于5G大规模物联网场景下的安全高效且去中心化的端云鉴权认证机制。该机制以端云联动、主动立体防御为核心实现了终端应用全生命周期的安全防护，构建起云、端、卡协同运作的安全体系，为5G+业务安全赋能。

关键词：端云安全；超级SIM；访问控制；隐私保护；终端安全

Abstract: Based on the enhanced security function of the super subscriber identity module (SIM) card, and the security requirements of terminal, cloud, and terminal cloud collaboration, combined with technologies such as blockchain technology, fog computing, and lightweight authentication, a secure, efficient, and decentralized end cloud authentication mechanism suitable for 5G large-scale Internet of Things scenarios is designed. The mechanism takes end-cloud linkage and active three-dimensional defense as the core to realize the security protection of the whole life cycle of the terminal application, and builds a security system of collaborative operation of cloud, end, and card, which prompts the security of 5G business.

Keywords: end-cloud security; super SIM; access control; privacy protection; terminal security

随着物联网和云计算技术的发展，各类小型化智能终端能够通过“云”进行大容量数据存储和高速复杂计算，并将所需结果下载至终端本地。过去，由于网络带宽及可靠性有限，端云协同难以在实际应用中部署。5G网络因其“高带宽、高可靠、低时延、海量连接”特性，使端云协同的网络架构在实际应用部署中成为可能。在端云协同系统的运行过程中，云、终端、协同机制任一部分的安全影响的不仅是其自身，还会是整个系统。攻击者可以以任意一个模块的安全缺陷为跳板，对整个系统进行攻击。端云协同体系作为国家信息基础设施的重要底座，直接影响国家信息基础设施安全，因此亟需构建一套5G环境下安全的端云协同体系。

1 5G端云网络架构及其安全挑战

过去几年，中国云计算产业呈现出高速增长的态势。根据中国信息通信研究院（后文简称信通院）《云计算白皮书（2021）》中的相关数据，2020年中国云计算整体市场规模达2 091亿元，企业“上云用云”进程加快。同时，物联网技术的发展进入快车道。根据信通院预测，到2025年中国物联网连接数将达到80.1亿个。万物互联将进一步释放数据驱动力，推动各行业数字化转型发展。两种技术在各自快速发展的过程中又互相渗透、彼此融合，形成端云一体化协同运作的网络架构[1]。

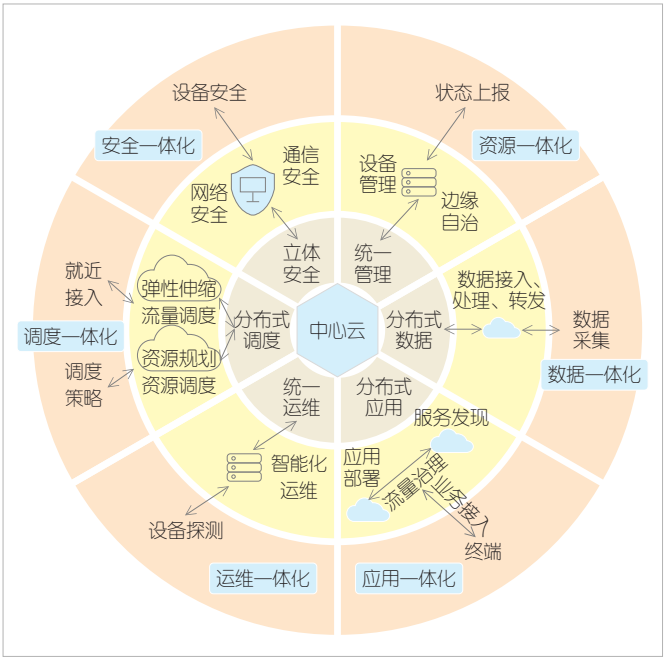
1.1 5G端云网络架构简介

5G通信技术使得海量终端和云基础设施的一体化融合成为可能。终端设备具有大量传感器，可以实时捕获大量数据，但由于其受到存储能力、计算能力、通信能力的限制，无法对海量大数据进行集中统一的整合处理。这使得数据价值得不到充分发挥，出现数据孤岛的窘境。云计算将海量物联网终端设备在感知层获取的数据信息，通过网络层传输到一个标准平台上，再利用高性能的中心云进行处理，并赋予

基金项目：国家重点研发计划（2021YFB2700200）；国家自然科学基金（U21B2021、61972018、61932014）

这些数据智能，最终转换成对终端用户有用的信息。同时，云端也可以长期存储海量数据，并统一管理广泛分布的终端，终端设备间也可以通过云端进行远距离交互和信息共享。5G通信技术的出现，极大促进了云计算和物联网技术的融合与优势互补，5G端云一体化网络架构（如图1所示）的形成有力推动了中国信息化产业的高质量发展[2]。

5G环境下的端云融合是信息技术（IT）与通信技术（CT）融合的新阶段，是新型信息基础设施的底座，是赋能数字化转型的基础，同时也是电信运营商、互联网公司和各类信息与通信技术（ICT）制造商和供应商共同追逐的目标。端云旨在屏蔽云、端分布式异构基础设施资源，提供统一视角进行资源的管理和使用，实现数据自由流通、业务应用统一运行，构建立体化安全保障能力，满足多样化、实时敏捷、安全可靠业务需求。如图2所示，端云融合可以实现资源一体化、运维一体化、数据一体化、应用一体化、调度一体化、安全一体化的目标[1]。



▲图2 端云一体化融合架构

1.2 5G端云网络架构的安全风险

现有的端云体系在终端、云、端云协同机制3个方面都存在一定的安全隐患：

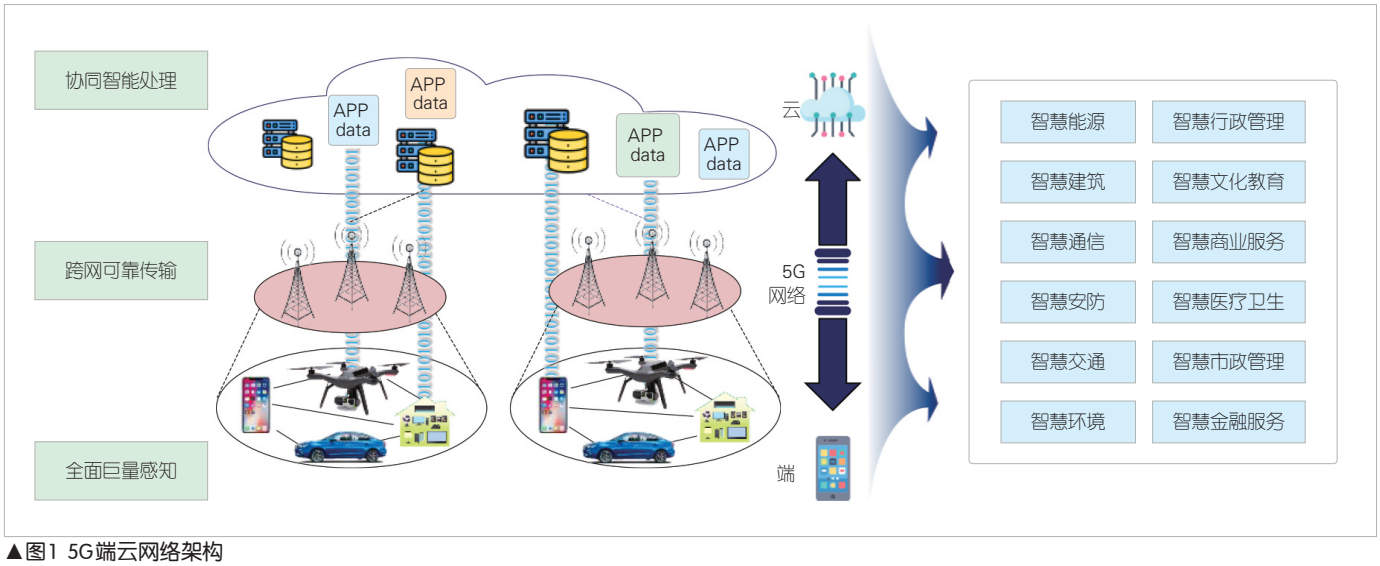
1）在终端应用安全方面，缺乏有效的应用安全检测和防御技术，并且缺少高效率的终端应用合规检查和运行质量检测系统。

2）在云端数据存储方面，主要存在隐私保护方面的问题。终端与服务器之间的通信过程存在数据窃听、数据泄露以及数据完整性破坏的风险，海量用户数据的云端存储和动态更新将会使服务器数据隐私保护面临挑战[3]。

3）在端云协同机制方面，主要存在身份认证方面的风险。现有终端认证服务吞吐量低、可扩展性较差；由于连接设备种类多样，认证面临劫持终端、冒用身份等安全接入风险。

1.3 5G端云网络架构的安全需求

在5G场景下，海量终端存在大规模的接入认证等需求。同时，用户对云计算、云存储等云服务的需求越来越广泛，而端云网络架构的安全性是确保用户能够正常使用网络服务的关键。针对上述安全威胁，我们从终端、云、端云协同机



▲图1 5G端云网络架构

制3个层面提出对应的安全需求：

1）在终端层面，存在终端应用安全防御、多应用安全隔离、应用安全评测等需求；

2）在云层面，需要有安全、层次化的密钥管理措施，高效的数据隐私保护机制和分布式、可扩展的安全服务；

3）在5G网络端云协同机制层面，网络需要满足低时延的身份认证、大规模的访问控制和高效加解密等需求。

2 超级SIM的安全优势与挑战

2.1 超级SIM简介

5G超级用户身份识别模块（SIM）的出现，能够赋能端云安全体系，如图3所示。超级SIM增强了安全能力，实现了机卡接口升级，并通过空间开放和多应用安全隔离为各行业的合作伙伴提供了多业务承载的大容量高安全等级的优质容器，是5G用户网络身份认证和应用敏感数据的安全存储空间。

超级SIM创建了安全信任根，能够提供安全可信的计算能力：在存储方面，融合了存储卡和SIM卡，支持GB级别的大容量安全可信存储。与此同时，超级SIM进行了卡机接口升级，其高开放性能够为设计和开发人员提供更便捷的应用。在超级SIM的可信存储和计算之上，能够实现增强的接入认证等功能。

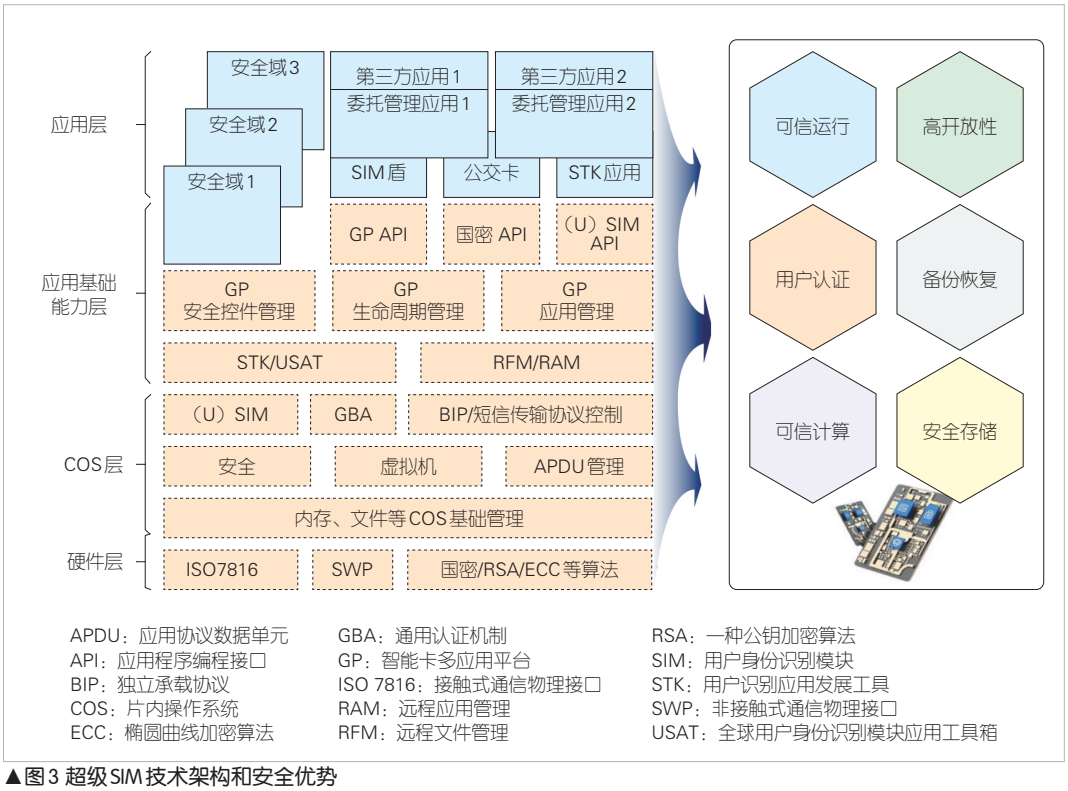
2.2 超级SIM的安全优势

SIM卡作为运营商认证用户身份的硬件载体，从2G时代就作为终端接入网络的主要凭证。在SIM卡中存储用户的证书密钥，能够实现终端与网络的双向认证接入。随着接入认证场景的安全需求越来越高，传统SIM卡用于终端与网络的认证已难以满足5G时代大连接、多应用场景需求，而超级SIM为业务合作带来无限可能，将成为承载各类业务的高安全性优质容器。基于超级SIM实现端云一体化鉴权认证是技术发展的大趋势，有助于实现真正的万物互联，构建可信的网络空间。

1）目前弱口令认证机制存在易破解、效率低的缺陷。基于超级SIM的端云一体化鉴权机制充分发挥了超级SIM具备的安全可信运行环境、安全可信存储环境、安全可信计算能力等优势，可有效弥补现有鉴权认证方式的不足，提升系统身份鉴别与登录认证能力，从技术上解决信息安全风险，提升网络安全整体水平。

2）超级SIM能为多行业大连接终端提供增强接入认证。此外，与2G/3G/4G的SIM对比，超级SIM除提供基础电信服务外，还可凭借高安全性、高开放性特点发挥更大作用，赋能千行百业。丰富的业务能力需要多层架构、多组件的支撑。一方面，超级SIM通过将加密认证机制与终端硬件层、片内操作系统（COS）层、应用层紧密耦合，保障接入终端的硬件可信；另一方面，引入统一的SIM卡鉴权认证机制，能够有效屏蔽物联网场景下多终端接入安全性差异，实现可编程、动态的授权接入，也能够基于终端位置、标识、可信根等多种维度对终端接入网络和云上应用进行鉴权认证，从而有效防范劫持终端、冒用身份等安全接入风险。

3）建设超级SIM生态能够有效提高中国相



▲图3 超级SIM技术架构和安全优势

关技术自主化可控水平。超级SIM主要依赖的网络终端访问控制机制是以美国为主导的，并不是开源的。如果出现针对超级SIM的技术限制，那么将影响中国基础电信服务的正常运作，也会影响接入5G网络使用超级SIM的各行业的正常运作。因此，我们要开展超级SIM生态的研究，构建基于SIM卡的跨终端多层接入认证和加密通信架构设计，形成具备中国自主化技术的超级SIM终端生态安全，构建基于5G超级SIM的安全端云完整体系架构。

2.3 基于5G超级SIM的端云体系的安全问题

基于5G超级SIM的端云体系尚存的安全问题具体如图4所示。在5G网络异构、终端异质、海量连接的场景下，在终端设备鉴权过程中，传统中心化身份认证、访问控制等方式存在单点故障、易遭受拒绝服务攻击等安全问题。

5G超级SIM中的信息涉及用户的隐私，具有高度敏感性。用户数据安全与隐私保护问题是制约5G超级SIM网络应用普及的重要因素。协同系统提供多种手段来支持运营商合作伙伴间的信息共享，这和云端服务器的数据安全与用户的隐私保护需求之间形成了激烈的冲突[4–5]。

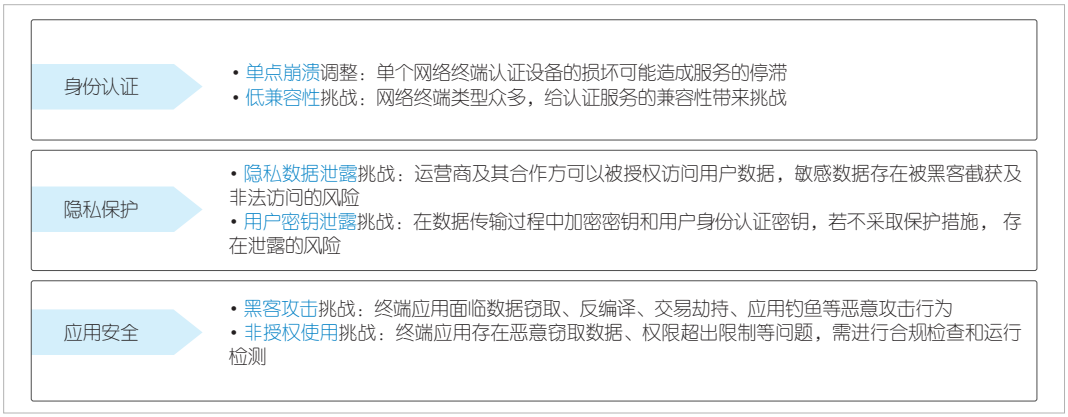
随着移动互联网场景化需求的快速发展，移动端应用的数量和业务种类呈现出爆发式增长。与此同时，移动终端面临的安全威胁种类和数量也在不断增多，例如：手机操作系统漏洞存在不可预知的业务逻辑缺陷，动态攻击、虚假设备等攻击手段和网络黑产链严重威胁用户的资金和隐私安全。现有的防御方法主要有对终端应用的静态特征检测、动态特征检测、动静结合的特征检测、基于深度学习的特征检测等，这些防御方法大都是从被动防御的角度在应用正式使用前或使用时进行测评，只考虑了在终端应用的部分生命周期，且仅局限于单个软件安全的层面。这造成了长期以来针对终端系统的恶意攻击层出不穷、“治标不治本”的后果[6–9]。

3 基于5G超级SIM端云安全体系的关键技术

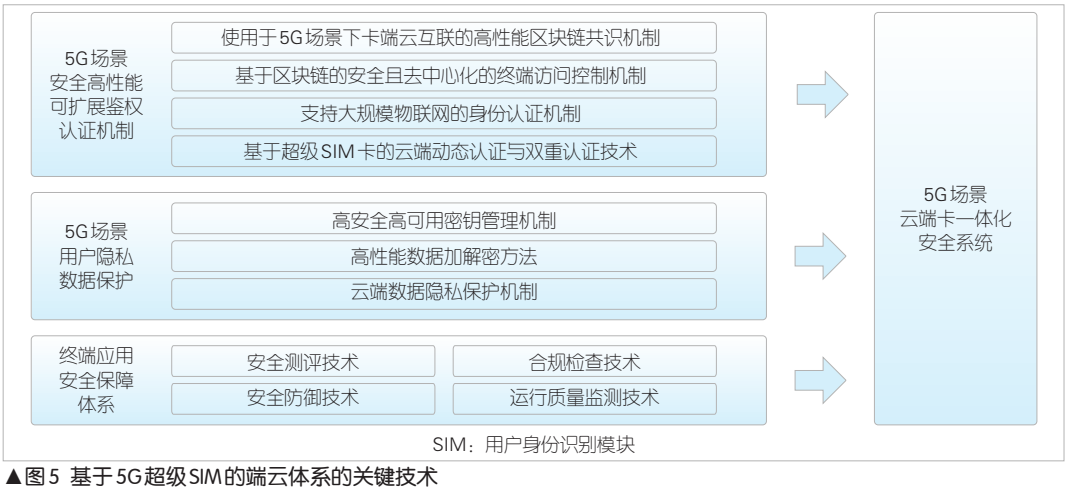
针对上述基于5G超级SIM的端云体系尚存的安全问题，结合区块链、雾计算、零信任等新兴信息技术，我们创新性地提出以下关键保障技术（如图5所示），进一步完善安全机制，构建基于5G超级SIM的安全端云体系[10]（如图6所示）。

3.1 5G场景下基于区块链的终端访问控制机制

由于5G网络规模庞大，5G终端设备从硬件类型到操作系统均有较大差异，因此如何能够在5G海量网络终端的环境下以超级SIM为核心，实现安全且去中心化的终端访问控制机制成为首要问题。这个机制能够使网络设备进行统一的鉴权验证，确保入网终端的安全可靠，并实现安全且去中心化的认证。该机制要具备如下一些特点：首先，要保证抗损



▲图4 基于5G超级用户身份识别模块(SIM)的端云体系尚存的安全问题



▲图5 基于5G超级SIM的端云体系的关键技术

毁效果好，稳定性强，单个或多个网络终端备鉴权认证设备的损坏不会造成重大影响；其次，要兼容性好，对网络终端设备的硬件类型、操作系统、业务应用有较好的兼容性；同时，还要保证维护性强，在网络终端设备出现故障时能够实现快速维修。

采用区块链技术能够实现去中心化的SIM卡终端鉴权认证和访问控制，防止鉴权服务节点发生单点故障，从而提供安全的身份认证和访问控制。5G场景下安全高效及可扩展的访问控制机制以云、端、卡互联的高性能区块链共识为基础，基于区块链构建去中心化的网络终端鉴权认证体系框架，对各终端进行安全去中心化的访问控制。

适用于5G场景下云、端、卡互联的高性能区块链共识机制，以可验证随机函数、可验证秘密分享和门限签名等重要密码工具为基础，主要包括3个模块：云端分布式随机数生成模块，用于委员会成员分配、委员会领导节点选举以及重配置过程；5G云节点重配置模块，用于筛选和替换参与共识的节点；云节点委员会内共识模块，用于处理交易并对新区块达成共识。

在5G海量终端背景下，需要以区块链为基础、超级SIM为核心，构建基于区块链的网络终端访问控制机制。区块链中的区块应包含加密后的终端详细信息及对应的访问控制权限。网络中任意一台入网终端都能够访问区块链上的信息，但只有合法终端能通过解密算法对区块链上的信息进行读取，从而判断该终端的类型及访问行为是否合法。可以采用基于区块链的访问控制模型，将权限绑定到角色，并将角色分配给5G网络终端以促进权限管理。

5G网络终端设备在注册和激活后可接入系统，设备之间、客户端和设备间进行交互前需要进行身份认证和权限验证，以确认设备或用户的身份以及对相关资源的访问权限。设备注册、设备激活、设备身份认证和设备访问权限认证以及访问控制策略管理都需要和区块链平台进行交互。使用基于区块链技术的分布式鉴权认证模式，可实现在网络状态不稳定、入网终端分散、维护力量薄弱的情况下的入网终端的鉴权工作。

3.2 支持大规模物联网场景的身份认证技术

针对大规模物联网场景，构造基于身份信息的区块链能够保证物联网设备身份的完整性和可靠性，同时可以基于端、雾、云提供不同设备的身份认证机制。为了保证物联网安全性，同时对用户敏感信息进行最大程度的保护，基于超级SIM的物联网设备的合法身份凭证只有经过加密和承诺后才能注册到区块链上，区块链平台再使用智能合约对设备进行访问权限控制。在不同的物联网设备交互前，发起设备需先向物联网平台和相应接入设备节点发送鉴权请求和接入请求，经平台调用后区块链系统对接入设备双方进行身份标识认证和管理，保证各设备在不泄露敏感信息的前提下，实现数据的安全交互。具体技术路线如下：

1）在线快速身份（FIDO）。FIDO可用于SIM卡端身份信息认证。该技术的核心是将身份认证手段与身份认证协议解耦，以密码技术为基础，采用非对称密码算法机制，以密钥作为用户凭证，通过签名验签的方法完成对用户的身份鉴别。

2）轻量级设备安全认证技术。大规模物联网中存在大量计算能力极低且存储力极低的终端设备，如电力感知层设备、车间监控设备等。NTRU（公钥密码体制名）是一种基于格理论的轻量级公钥密码算法，可根据不同的安全级别进行不同的参数集选择，具有内存和计算量少、加解密和签名/验证速度快、安全性高等优势，适用于海量终端的物联网场景下资源受限的轻

▲图6 基于5G超级用户身份识别模块(SIM)的端云体系架构

量级节点的无线通信环境。

3）融合端雾云架构与区块链技术的物联网系统。在物联网中选取满足一定计算和存储能力的设备或高性能节点作为控制中心雾节点，以其为中继进行多层次计算任务卸载和大数据处理。网络边缘的雾计算节点实时感知多个SIM卡设备终端的计算资源富余信息，雾控制节点能够以整体效率最大化的方式有效管理终端自组织微集群的构建。一方面，雾计算节点可以实时检测多终端计算卸载的任务，合并用户计算任务中的同质任务，实现多个同质任务一次卸载而多用户共享，从而减少网络通信开销和云资源占用；另一方面，雾控制中心可利用雾计算节点充当计算预处理节点，按需调配云计算资源，与公有云协同应对大型计算任务。

3.3 基于超级SIM的云端动态认证与双重认证技术

端云协作鉴权认证机制以超级SIM的安全能力为访问主体（包括用户、设备、应用等）建立可信身份标识，结合零信任安全架构，并基于终端SIM卡标识、位置、网络地址等多维度因子，构建可信应用代理、可信应用程序编程接口（API）代理、可信访问控制台、智能身份分析系统，从而实现基于会话连接粒度的动态访问控制。

在终端接入5G网络时，SIM卡网络层与应用层的双重认证可以构建“端–网–云”的可信通信。针对5G终端业务低时延、大并发、高可靠等不同场景，基于物联网轻量级认证要求、轻量级安全认证协议、轻量级网络认证机制，形成针对“终端–终端”“终端–边缘云”“终端–核心云”“终端–接入网”等多段超级SIM认证方案。

3.4 高安全高可用密钥管理机制

针对5G网络环境中大数量级终端、复杂接入场景等新情况所带来的密钥管理问题，需建立新的全套密钥管理方案，以适应云、端、卡协同体系中的密钥管理需求。

在密钥的生成、分发和认证模块中，根据用户所需的不同密钥安全等级，按照不同的密钥产生方式生成不同等级的密钥；根据不同的网络架构，利用多种密码技术，选择相应的密钥分配模式以实现密钥分发。

在密钥分发过程中，我们需要对密钥进行认证，以确保密钥被正确、完整地送达。在密钥分级保护、存储与备份模块中，根据密钥的使用场景和安全等级对密钥进行分级保护，并在密钥存储时选择合适的方法，保证密钥的机密性、可认证性和完整性，以防止密钥泄漏和被篡改。在密钥保护和存储过程中需要考虑密钥的备份问题，以避免密钥因意外而丢失而造成的损失。

在密钥更新与销毁模块中，当密钥泄漏或丢失时，设计合理的更换密钥方法，可以使损失最小化；根据密钥的作用和安全等级，设置合理的密钥使用期限，实现分级管理；对已泄漏、已过期的密钥及时进行销毁，设计安全可靠的销毁方式，以避免攻击者通过旧密钥寻找有关的秘密信息。

3.5 高性能数据加解密方法

面向5G场景下大带宽实时传输的通信需求和日益强大的攻击者，我们需设计基于超级SIM的高性能数据加解密算法，以及算法的相应逻辑电路实现方式和应用模式。

在算法层面，结合国产密码算法系统和密码评价标准，以及5G网络对密码算法轻量级、低功耗、抗侧信道攻击等要求，我们需要设计可应用于超级SIM及整个5G网络系统的密码算法系列。

在硬件层面，根据所选密码算法逻辑结构特点，结合超级SIM平台，我们要选择适宜的并行电路架构，并采用流水线技术等，缩减电路规模，提高密码算法电路的工作频率和数据吞吐率。在接口设计方面，采用容错技术、握手机制与端口数据寄存技术等，并兼顾算法自检电路设计，确保密码算法电路异常工作状态能够被实时检测，从而提升整个密码模块的工作可靠性。采用动态电压调节、门控时钟和可变频率时钟等技术，可以降低密码算法实现电路的功耗。

在应用层面，我们需要结合5G场景具体应用需求，设计密码算法的智能化调用策略；并引入多级安全、域隔离等思想，制定不同需求下的密码算法的调用规则，包括对称密码与非对称密码算法的高效运用策略、密码强度分级策略等，实现整个系统效率与安全性的统一。

3.6 云端数据隐私保护机制

为了应对5G网络下海量的个人数据与用户终端有限的存储和计算能力之间的矛盾，我们往往需要借助于云端来辅助用户数据的处理，从而带来数据所有权与管辖权的分离。在上述条件下，我们需要在保护云端数据安全的同时，保证用户对数据合法、灵活、高效的访问。

1）数据安全共享机制。该机制利用层次身份基的可撤销数据访问权限管理方案，以免交互的方式撤销无效用户的访问凭证，动态地管理用户数据的访问权限，为有效用户免去权限撤销操作中繁复的计算和通信开销。同时，考虑到超级SIM协同体系的巨大规模，基于分层的用户结构可以减轻私钥生成中心（KGC）为所有用户生成访问控制凭证的负担，提高系统的工作效能。

2）跨系统的云端隐私数据保护机制。针对计算能力较

弱的移动设备，该机制利用轻量级的基于身份的广播加密系统，根据授权用户集合对用户隐私数据实施大范围、灵活的控制。引入代理重加密机制，在身份基广播加密和身份基加密这两种系统之间搭建超级SIM数据直接共享的通道，使得不同加密系统下的超级SIM用户可以快速安全地共享个人隐私数据。

3.7 终端应用安全保障机制

基于当前应用市场的安全现状和现实需求，亟需提出一套能满足以下需求的全新终端应用安全管理方案：多平台通用、主动被动防御结合、在系统层面进行预防监测、涵盖终端应用全生命周期。具体应包括：

1）终端应用安全性检测。该方案利用了被动防御的思想。首先，检测对象覆盖范围要全面，针对终端平台上的所有应用类型，包括Android应用、iOS应用、Web应用、开发包、函数库等；其次，检测类型要全面，包括软件恶意行为检测，软件漏洞检测与修复，软件行为、权限、隐私策略等。针对上述目标，结合深度静态检测、动态监测、源代码扫描、人工智能、自然语言处理等技术，构建一套高效、自动化的测评系统。

2）终端应用安全加固。该方案利用了主动防御的思想，针对移动应用面临的反编译、二次打包、内存注入、动态调试、数据窃取、交易劫持、应用钓鱼等恶意攻击行为，将针对各种应用安全缺陷的保护技术集成到应用客户端内，构建全面保护软件安全的主动防御体系。这些技术主要包括：代码防逆向技术、应用防篡改技术、反调试技术、数据防泄漏技术、运行环境保护技术等。

3）运行时监控与态势感知。该方案利用系统防御、应急处置、恢复溯源的思想，针对某些恶意应用采用高级反检测技术逃过安全性检测的情况，或者某些恶意软件隐蔽性极高的高级可持续威胁（APT）攻击，从系统安全的角度对移动应用上线后的动态运行安全问题及运行稳定性问题进行实时监控，充分挖掘软件运行模式，识别其安全属性，同时为软件检测提供丰富的数据支持。基于上述数据，可以进一步建立企业端和用户端联动的立体化安全态势感知体系，这样既弥补了企业业务反欺诈、风控等业务系统对终端风险监测的短板，又为用户快速建立事前预警、事中处置、事后恢复的自动化安全体系。

4 结束语

本文中，我们认为需要以高性能国产密码SIM为核心，充分发挥区块链、雾计算、端云联动立体防御等新兴技术的优势，构建“云、端、卡”协同运作的完整安全体系。这一举措既可以适应5G场景下大规模物联网设备接入认证的新场景，也能覆盖芯片硬件、芯片操作系统、终端芯片、终端硬件设计、终端应用等的研发和应用，为5G+业务安全赋能，推动数字中国关键基础设施的构建。

参考文献

[1] 云边协同产业方阵. 云边端一体化发展报告(2022年) [R]. 2022
[2] 徐恩庆, 李昂, 王蕴婷. 云边端一体化创新助推算力泛在化发展 [J]. 通信世界, 2022, 4(18): 44-45. DOI: 10.13571/j.cnki.cww.2022.18.006
[3] 欧阳雪, 徐彦彦. IaaS 云安全研究综述 [J]. 信息安全学报, 2022, 7(5):39-50
[4] ZHAO H Y, YANG X, LI X L. cTrust: trust aggregation in cyclic mobile ad hoc networks [C]//Proceedings of the 16th International Euro-Par Conference on Parallel Processing: Part II. ACM, 2010: 454-465. DOI: 10.5555/1885276.1885325
[5] ZHANG C, SUN J Y, ZHU X Y, et al. Privacy and security for online social networks: challenges and opportunities [J]. IEEE network, 2010, 24(4): 13-18. DOI: 10.1109/MNET.2010.5510913
[6] LI J, SUN L C, YAN Q B, et al. Significant permission identification for machine-learning-based android malware detection [J]. IEEE transactions on industrial informatics, 2018, 14(7): 3216-3225. DOI: 10.1109/TII.2017.2789219
[7] ALZAYLAEE M K, YERIMA S Y, SEZER S. DL-droid: deep learning based android malware detection using real devices [J]. Computers & security, 2020, 89: 101663. DOI: 10.1016/j.cose.2019.101663
[8] DIMJASEVIC M, ATZENI S, RAKAMARIC Z, et al. Android malware detection based on system calls [R/OL]. [2022-12-10]. https://www-old.cs.utah.edu/docs/techreports/2015/pdf/UUCS-15-003.pdf
[9] YU L, LUO X P, QIAN C X, et al. Enhancing the description-to-behavior fidelity in android apps with privacy policy [J]. IEEE transactions on software engineering, 2018, 44(9): 834-854. DOI: 10.1109/TSE.2017.2730198
[10] 天融信：构建“云、管、边、端”协同防御的5G端到端安全闭环 [EB/OL]. [2022-07-05]. https://zhuanlan.zhihu.com/p/537693680

作　者　简　介

李佩源，北京航空航天大学在读硕士研究生；主要研究领域为网络攻防、系统安全、软件安全。

刘建伟，北京航空航天大学网络空间安全学院教授、博导、院长，享受国务院政府特殊津贴，现任国务院学位委员会第八届学科评议组成员、教育部高等学校网络空间安全专业教学指导委员会委员、中国密码学会常务理事、中国指挥与控制学会常务理事、中国电子学会网络空间安全专委会副主任委员、中国指挥与控制学会网络空间安全专委会副主任委员、中关村智能终端操作系统联盟副理事长；曾获国家技术发明一等奖、国防技术发明一等奖、中国指挥与控制学会科技进步一等奖等，所编写的教材获全国普通高校优秀教材一等奖、国家网络安全优秀教材、国家精品教材、全国优秀科普作品奖、第四届中国科普作家协会优秀科普作品金奖等；出版教材7部、专著2部、译著1部。