擦系数降低 30% 以上，从而改善位移协调能力。对于钢制支座的防腐与加固，则采用超高压水射流除锈技术结合环氧富锌底漆与聚氨酯面漆形成多层防护体系。对于应力集中区域，可加装不锈钢衬板或外包防护罩以延缓二次腐蚀，显著提高支座的服役寿命与可靠性。

4.3 新型材料与复合工艺的应用

近年来，新型高分子材料与复合修复工艺的推广显著提升了支座修复的效率与质量。碳纤维增强聚合物（CFRP）在支座底板及受拉部位的加固中表现出优异的强度重量比与抗疲劳性能，其粘贴层可有效分散局部应力集中，提升整体承载能力。纳米改性橡胶材料通过分子级填充与交联技术，增强了橡胶的抗紫外、抗氧化与耐磨特性，使其在高温与潮湿环境下保持稳定性能。同时，具有自愈合功能的聚合物材料开始应用于微裂纹修复中，其内部微胶囊在受力破裂后释放修复剂，可自动填充细微裂隙，恢复原有力学性能。复合工艺方面，采用真空注胶与热压结合的工艺路径，不仅提升了材料致密度，还减少了施工误差。上述新技术的集成应用，使支座修复由传统的“事后修补”转向“功能再造”，标志着桥梁养护向长寿命、高可靠与低维护方向的转型发展。

5 支座长期服役性能监测与数据分析

5.1 监测系统构建与布设方案

为实现桥梁支座性能的长期健康监测与精细化管理，构建了一套集传感检测、数据采集、无线传输与云端分析于一体的综合监测系统。系统监测指标涵盖竖向位移、水平滑移、转角变形、温度应力及结构应变等关键参数，全面反映支座的工作状态与性能演化特征。传感器布设采用光纤光栅（FBG）与微机电系统（MEMS）复合监测技术，兼具高灵敏度、抗干扰性与长期稳定性，可实现微米级变形量的精确测量。各监测节点分布于主梁与支座连接区域，通过 LoRa 低功耗广域通信与 4G 无线网络实现实时数据回传，极大提升了数据传输的可靠性与时效性。监测数据经边缘计算终端初步处理后上传至云端数据库，云平台对采集信息进行集中存储、动态展示与异常可视化分析，为桥梁支座性能评估提供连续、可靠的数据支撑。

5.2 长期数据分析与健康评估

长期监测数据的分析是实现支座健康状态量化评估的核心。通过时间序列分析与多维特征融合建模，对支座位移、温度、应变等多参数数据进行趋势识别与异常诊断。利用主成分分析（PCA）方法提取关键特征，去除冗余噪声数据，提升模型计算效率；结合神经网络与深度学习算法，建立支座性能退化识别模型，能够动态识别出由老化、疲劳或环境变化引起的非线性响应特征。系统自动生成健康指数（HI）变化曲线，通过与历史监测数据及气候、荷载等环境因素的耦合分析，实现对支座性能变化的定量追踪与预测。

5.3 预警机制与智能运维模式

在健康评估基础上，构建了基于人工智能与大数据技术的支座性能预警与智能运维体系。系统通过异常检测算法对实时监测数据进行多维特征比对，当监测参数出现突变或偏离阈值时，自动触发预警信号并生成事件报告。结合贝叶斯推断与模糊逻辑模型，可判断异常的性质与严重程度，并依据历史数据分析提供针对性的运维建议。管理人员可通过移动终端或控制中心界面实时查看支座运行状态，实现远程化、可视化的决策支持。系统预警响应时间不超过 5 秒，可实现“数据采集—异常识别—预警提示—维修决策”的闭环管理流程。智能运维模式的引入，不仅提升了桥梁支座维护的主动性和科学性，还显著降低了人工巡检频率与维护成本，推动桥梁结构安全管理向数字化、智能化与预防性维护方向转型。

6 结语

公路桥梁支座的健康状态直接关系到结构安全与行车稳定性。本文以支座病害为研究对象，系统分析了其成因机理、修复性养护技术与长期监测方法，构建了集评估、修复、监测与预警为一体的综合技术体系。研究表明，通过科学的技术选型与信息化监测手段，可显著延缓支座老化进程，降低病害发生率，提升桥梁全寿命周期的服役性能。未来，支座养护应向数字化、智能化与可持续方向发展，充分利用物联网、人工智能与数字孪生技术，实现桥梁支座的精准诊断与自适应维护，推动公路基础设施管理水平迈向新阶段。

参考文献

[1] 张晓东.高速公路桥梁伸缩缝病害修复技术研究[J].汽车周刊,2025,(11):95-97.

[2] 杨红海.高速公路桥梁路面养护与维修技术探究[J].建材发展导向,2025,23(11):58-60.

[3] 刘金乾,张萌,赵华.公路桥梁养护中桥面病害诊断与修复技术研究[J].运输经理世界,2025,(16):139-141.

[4] 朱峰,毕超.基于传感器数据的高速公路桥梁支座位移检测方法[J].装备制造技术,2023,(11):202-204.

[5] 戴鹏飞.寒冷地区公路混凝土桥梁病害养护及修复技术研究[J].北方交通,2022,(12):17-20.

Research on the Application of Commercial Cryptography in Cloud Environments

Yu Liu[1] Jun Dong[2] Peng Zhang[3] Xiaoning Hu[3] Zhe Hao[4]

1.China Railway Information Technology Group Co., Ltd., Beijing, 100044, China
2.China Railway Express Co., Ltd., Beijing, 100000, China
3.China Railway Information Engineering Group Co., Ltd., Beijing, 100844, China
4. Beijing Institute of Computer Technology and Applications, Beijing, 100854, China

Abstract

Cryptography is the core technology and fundamental support for safeguarding network and information security, as well as the most effective, reliable, and economical core technical means to maintain network and information security. Therefore, aiming at the characteristics of scenario applications in cloud environments (abbreviated as: on the cloud), how to correctly and effectively apply commercial cryptography technology to solve network and information security problems is the key focus of this research. In view of this, this paper elaborates on the application characteristics and facing problems of commercial cryptography on the cloud, clarifies the universal needs of commercial cryptography application in on-cloud scenarios, constructs a commercial cryptography application service support system on the cloud, and demonstrates its exemplary value combined with application practices. The research results can provide theoretical guidance and practical reference for the systematic promotion of the implementation and application of commercial cryptography in the railway industry .

Keywords

Cloud-based; Cloud Password; Commercial Cryptography; Password Resource Pool; Application Service Support Platform.

云环境下商用密码应用研究

刘宇[1] 董军[2] 张鹏[3] 胡小宁[3] 郝哲[4]

1. 中国铁路信息科技集团有限公司，中国·北京 100044
2. 中铁快运股份有限公司，中国·北京 100000
3. 中铁信息工程集团有限公司，中国·北京 100844
4. 北京计算机技术及应用研究所，中国·北京 100854

摘 要

密码是保障网络与信息安全的核心技术和基础支撑，也是维护网络与信息安全最有效、最可靠、最经济的核心技术手段。因此，针对云环境（简称：云上）的场景应用特点，如何正确有效应用商用密码技术解决网络和信息安全问题，是本文的研究关键所在。鉴于此，本文详细剖析了商用密码在云上的应用特点与面临问题，明确了云上场景商用密码应用的普适性需求，构建了云上密码应用服务支撑体系，并结合应用实践体现其示范价值。本研究成果可为铁路行业体系化推进商用密码落地应用提供理论指导与实践参考。

关键词

云上；云密码；商用密码；密码资源池；应用服务支撑平台

1 引言

随着各行业数字化转型全面提速，企业业务系统向云上迁移已成为主流趋势。基于云上虚拟化、资源共享、分布式架构的特性，在其带来弹性伸缩、降本增效的同时，也催生了新型安全风险；叠加相关法律法规要求、密码应用安全性评估及网络安全等级保护的合规约束，传统密码技术的物理部署模式已难以适配云端动态化、分布式的应用场景[1-2]。综上，推动商用密码技术向云上转型应用，构建体系化的云上密码应用服务支撑，已成为保障云上安全与合规落地的核心路径。本文重点聚焦云上商用密码应用服务支撑体系的构建及关键技术研究，旨在破解技术瓶颈、强化安全防护能力，

【基金项目】“铁路商用密码体系架构及应用研究”；子课题 2“铁路商用密码技术体系及关键技术研究”（项目编号：WJZG-CKY-2024041（2024P02））。

【作者简介】刘宇（1993—），男，蒙古族，中国内蒙古赤峰人，硕士，工程师，从事铁路网络安全和信息化研究。

为云上业务稳健运行筑牢密码安全根基。

2 研究现状

2.1 云上密码应用现状分析

云上商用密码应用现状分析从密码应用合规、密码应用形态、密码应用覆盖、密码应用交付等四方面展开分析。

1）密码应用合规方面。云上商用密码应用合规性测评以《中华人民共和国密码法》《商用密码管理条例》《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）等要求为参考依据，技术层面主要围绕国密算法与合规产品使用、密钥全生命周期安全、场景化应用有效性及云架构适配性展开；管理层面聚焦制度建设、运维规范与密评闭环管理推进落实 [7]。

2）密码应用形态方面。云上商用密码应用的核心形态是“云密码服务资源池化”，该形态主要针对云计算虚拟化、分布式、多租户的架构特性，基于云上业务动态弹性、资源共享的核心需求，构建系统化密码服务模式。其以云上分散密码资源整合为基础，依托云服务器密码机等专用硬件设备提供底层算力支撑，通过多租户隔离机制保障不同用户密码资源的安全隔离，封装形成密钥全生命周期管理、数据传输与存储加解密、身份安全认证等标准化核心服务能力，最终实现密码资源的弹性调度、按需分配与规模化应用，既满足云上业务动态安全防护需求，又契合密评、等保等合规要求，成为云上安全保障与合规落地的核心支撑。

3）密码应用覆盖方面。商用密码在云上的应用已深度贯穿数据存储、传输、运行全生命周期，形成全链路云上密码应用安全服务能力，可全面满足云上多场景、多维度的安全需求。

4）密码应用交付方面。“密码即服务”已成为云上商用密码应用的主流应用模式。该模式摆脱了传统硬件设备的物理部署限制，企业可通过标准化 API 接口快速接入云上密码服务，获取密钥管理、加解密等核心服务能力，大幅降低业务系统改造门槛与建设成本。

综上所述，云上密码应用以合规测评要求为核心原则，以“云密码服务资源池化”为核心应用形态，深度贯穿云环境中数据存储、传输、运行全生命周期，以“密码即服务”为核心交付模式，全面支撑云上密码应用与企业业务高效、安全开展。

2.2 云上密码应用面临挑战分析

1）安全合规与风险防控。云上密码应用要满足密评、等保等合规要求，但云环境多租户隔离特性、数据流转动态性加大了密评合规落地难度，同时也会面临密钥泄露、非法调用等安全风险。

2）技术适配与性能优化要求高。云端分布式架构与动态调度特性，对密码技术的场景适配性提出更高要求。部分传统密码算法在虚拟化环境下存在性能损耗，大规模并发访问场景下易出现响应延迟；同时，密钥同步与信任机制的协同难度较大。这些问题均会影响云上密码应用的稳定性与效果 [1-2]。

3）密码管理及运维复杂度增加。云上密码的集约建设模式，加大了密码监控覆盖范围、实时预警与动态扩展的管理难度，直接导致密码管理及运维复杂度显著上升。如何对多租户环境下密码资源的全生命周期管控，对云上密码资源的集中统一监控、实时预警及动态扩展，以成为云上密码管理方面的核心难题。

综上所述，云上密码应用面临安全合规与风险防控、技术适配与性能优化、密码管理及运维复杂度增加三大核心挑战，涵盖合规落地、技术适配、日常运维等关键环节，需针对性形成有效解决路径。

3 应用需求

云环境下商用密码的应用应着重考虑以下合规、技术、管理等三点核心需求。

合规需求。需依据《国家密码法》、《商用密码管理条例》等相关规定，定期开展商用密码应用安全性评估，确保云上商用密码应用全流程合法合规、安全有效 [4-6]。

2）技术需求。一方面，传统信息系统架构中，密码技术多以软件、硬件产品形态独立提供服务，而云上密码技术核心强调资源共享与按需使用，通过虚拟化、分布式等技术实现密码资源池化与动态弹性分配，二者架构特性存在显著差异。因此，需将传统密码服务技术转型升级为云原生密码服务技术，并建设适配云架构的密码服务支撑平台，才能符合云上密码应用的需求。另一方面，云上在身份鉴别、数据传输加密、数据存储加密、操作抗抵赖等多个环节均有密码应用需求 [2]，因此密码服务需具备多样化、全场景覆盖的服务能力，进而需要构建起闭环可控的云上密码应用安全防护体系。

3）管理需求。云上密码管理需具备三大核心能力：一是统一管理能力，可对密码服务接口、服务订购、应用调用、应用认证及平台运行状态进行全流程管控；二是多租户管理能力，需具备租户间安全隔离与独立自治管理，满足多租户差异化需求；三是核心运营管理能力，涵盖密码资源统筹调度、密钥全生命周期追溯、密码资源状态监控等功能，保障云上密码管理规范、高效、合规。

4 应用研究

4.1 总体框架设计

依据现有商用密码管理标准及规范，结合云环境场景基本特性与密码应用需求，本文从四个方面来阐述云上商用密码服务支撑体系框架及其业务内容。该框架设计是将密码软硬件资源以云密码资源池化的方式融入云环境，并依托云上密码应用服务支撑平台将多类商用密码能力通过统一接口以服务的方式动态灵活的提供服务，实现“密码即服务”，为云租户的云上应用系统提供合规、安全、便捷的商用密码

服务支撑，满足云上应用系统的密码应用需求。总体框架设计见图 1。

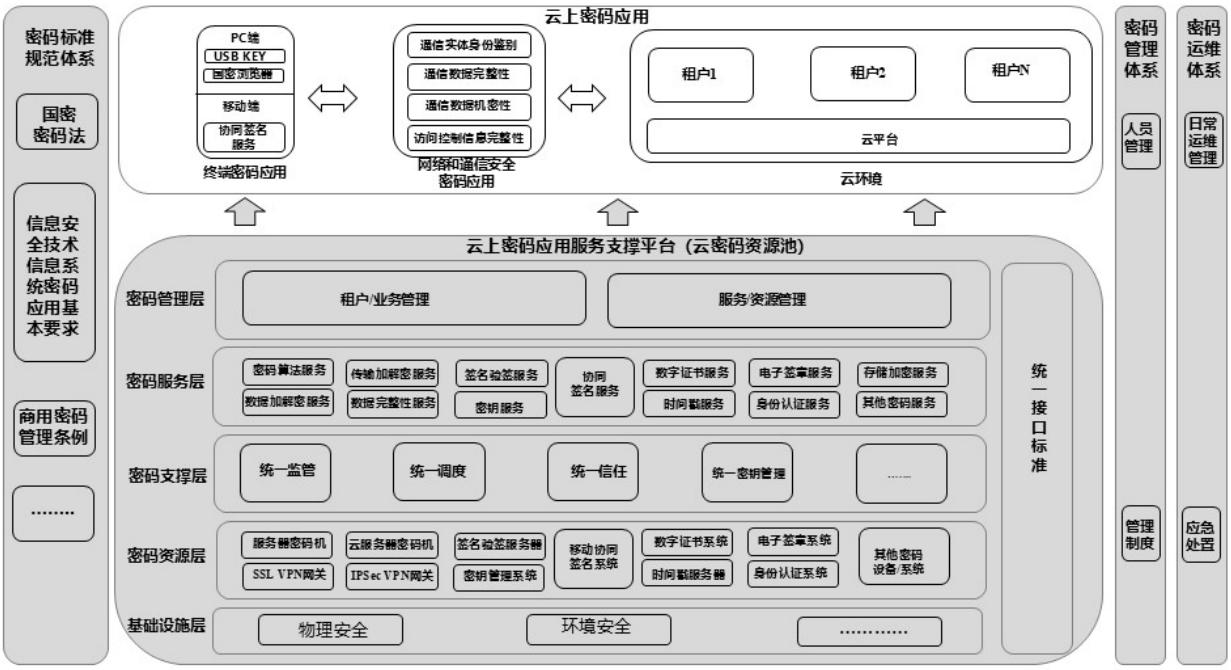

图 1 云上商用密码服务支撑体系总体框架图

其中，云上密码应用服务支撑平台是整个体系框架的服务能力中心，密码管理标准规范则是整个体系框架的标准规范中心，密码管理体系是整个体系框架的管理中心，密码运维体系是整个体系框架的运维中心 [3]。上述四大能力中心既各司其职，又相互依赖，共同构筑完善的云上商用密码应用服务支撑体系。

1）云上密码应用服务支撑平台采用层次化、结构化设计思路，为云上业务系统提供密码服务能力。自下而上分为基础设施层、密码资源层、密码支撑层、密码服务层、密码管理层，低层级为上一层级提供资源支撑。

基础设施层。基础设施层涵盖物理安全、环境安全等，为上层密码资源提供基础运行环境。

密码资源层。密码资源层是所有服务的基础，为云上各类密码服务提供产品和技术支撑，包括服务器密码机、云服务器密码机、签名验签服务器、SSL VPN 网关、IPSec 网关、签名验签服务器、移动协同签名系统、数字证书系统、时间戳服务器、电子签章系统、身份认证系统、服务器密码机、其他密码设备及系统等。密码设备中，VPN 安全网关将支持 SSL VPN 及 IPSec VPN 等通信链路传输加密服务，云服务器密码机支持将授权开通服务器密码机或签名验签服务器功能，同时支持虚拟出多个虚拟机；移动协同签名系统为云上业务系统和密码资源调度中心提供移动签名验签服务。时间戳服务器为云上业务系统中安全服务统一提供的可信时间服务。

密码支撑层。位于密码服务层与密码资源层之间，它按照云上不同的密码应用场景、不同的密码应用诉求等，基于底层密码资源协同纳管、调度运行能力，为密码服务层提供同类型的密码服务支撑，主要提供统一监管、统一调度、统一信任、统一密钥管理支撑等。如密码监管平台作为密码设备的统一监控、管理平台，可提供资源管理、密码安全监察等功能；密码调度平台支持对密码设备的集中管理，包括虚拟化的云密码机和传统的密码设备；统一信任服务为云上业务系统提供统一网络信任支撑；统一密钥管理提供密钥全生命周期统一管控支撑。

密码服务层。以国产密码技术为基础，为云管理平台及云上业务系统提供相应的密码安全服务能力，包括密码算法服务、数据加解密服务、数据完整性服务、传输加密服务、签名验签服务、密钥服务、数字证书服务、电子签章服务、存储加密服务、时间戳服务、身份认证服务、其他密码服务等。如密码算法服务：采用加解密算法和认证算法对云上业务系统中的敏感数据进行加解密，同时能为云上业务系统和密码资源调度中心自身提供密码算法、信息鉴别、数据完整性及抗抵赖服务，保证信息安全；传输加解密服务：可为云上业务系统和密码资源调度中心自身提供敏感信息传输加解密服务，通过对称加密、非对称加密和数字签名等方法保证用户与密码传输链路之间的安全性，确保身份可信、服务可信、信息可信。

密码管理层。用于对云密码资源及服务的统一标准化管理，是用户层面使用云上各类商用密码服务以及内部密码管理和运维人员用于密码管理和运维的交互界面，根据用户

身份的不同，可提供租户业务管理、服务资源管理两大类管理能力。其中租户业务管理主要为云租户使用，云租户可实现对云上商用密码服务的订购和使用；服务资源管理主要为云上密码应用服务支撑平台的管理及运维人员提供的服务，如租户管理、订单管理、许可管理、密码服务接口、调度管理、平台运行监控告警等，帮助管理及运维人员掌握云上商用密码应用及平台运行情况，实现对云上密码应用服务支撑平台进行统一便捷化的管理。

统一接口标准：云上密码应用服务支撑平台与外部平台以统一的 Web 接口标准进行对接，包括资源管理接口标准、接入认证接口标准等多个方面规范平台的接入与开发标准，以标准化要求提高服务质量与服务效率，支撑实现密码服务使用的统一、便捷、高效、安全。

2）密码标准规范体系。标准规范是云上密码规范化应用和管理的重要依据，更是云上密码应用服务支撑平台规范化建设、运行、管理的指导依据，其构建以《中华人民共和国密码法》为根本遵循，以《商用密码管理条例》为重要监管准则，同时严格遵循《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）等国家强制性标准 [1]，确保云上密码应用全流程合法合规、规范有序。

3）密码管理体系。包括人员管理及制度管理两方面，为云上密码应用服务支撑平台的建设、使用、运维提供管理保障。其中人员管理：包括密码岗位组织架构及人员设置情况、培训等，如密码操作员、密码安全审计员、密钥管理员等具体岗位设置情况、岗位职责设定等；制度管理：包括密码人员管理、密钥管理、建设运行、应急处置、密码设施管理等制度规范，以及日常密码应用管理相关的操作规程、操作执行记录、业务处理流程等内容。

4）密码运维体系。包括日常运维管理和应急处置两方面，为云上密码应用服务支撑平台提供运维管理保障。其中日常运维管理：包括对云上密码服务支撑平台的运维人员、日常运维策略以及日常运维流程的制定与管理；应急处置：包括对云上密码应用应急策略制定、应急组织管理和事件应急处置流程的制定等。

4.2 关键核心技术

密码资源虚拟化技术。

该技术是平台适配云环境弹性特性的核心基础，核心目标是打破传统密码硬件“物理绑定、刚性分配”的局限。一方面，通过采用支持硬件虚拟化隔离技术的密码产品，实现单个租户独享专属密码芯片的隔离效果，既保障租户密码运算的独立性，又从底层规避租户间的安全干扰风险。另一方面，结合云环境的虚拟化能力，将密码资源层的各类软硬件密码资源进行统一虚拟化处理，整合为可弹性调度的密码资源池。资源池支持密码资源按需分配给不同租户，不仅解决了传统密码设备采购周期长、扩展灵活度低的痛点，还能实现毫秒级响应，轻松承载云上高并发业务场景的密码运算需求。

2）国密算法适配与标准化封装技术

该技术是平台构建合规密码服务能力的核心支撑，既保障密码应用符合监管要求，又降低云租户接入难度。平台以国密算法为能力底座，全面集成 SM2（非对称加密）、SM3（哈希运算）、SM4（对称加密）、SM9（标识加密）等标准国密算法，所有密码运算操作均严格按照《密码法》及商用密码应用安全性评估（密评）相关规范，从算法层面筑牢合规底线 [5]。同时，通过对底层不同厂商的加密卡、密码机等硬件设备的运算能力进行抽象封装，屏蔽硬件型号、技术架构的差异，对外提供统一、标准化的密码服务接口。在此基础上，可将数据加解密、签名验签、密钥协商等核心功能封装为模块化、可复用的标准化服务，并搭配轻量级 SDK，兼容主流开发框架，云租户无需关注底层硬件适配细节，通过简单调用接口即可快速集成密码服务，大幅降低云上密码应用的接入门槛与开发成本。

密钥全生命周期管控技术。

密钥作为密码服务的核心，其安全管理依赖全流程管控技术。平台搭建集中式密钥管理系统，实现密钥从生成、分发、存储到销毁的全生命周期可控。在生成环节，采用随机数生成算法保障密钥的唯一性和随机性；分发环节通过密钥云安全分发技术，结合加密通道完成密钥的安全传输，避免传输过程中泄露；存储环节则借助云原生数据库等自主可控存储产品，对密钥片段、租户密码服务规则等数据加密存储，并搭配 CRedis 缓存处理高频访问的密钥相关数据，兼顾安全性与访问效率；销毁环节则通过不可逆的密钥清除机制，确保废弃密钥无法被恢复。

多场景协同签名与安全传输技术。

该技术聚焦解决移动端与云平台的密码协同难题，同时保障数据传输全链路安全。针对移动端协同签名需求，移动端密码模块与云平台采用挑战应答机制完成双向身份验证与协同运算，既确保移动端身份的真实性与合法性，又保障签名数据的机密性、完整性与不可否认性，充分满足移动多终端的协同签名需求。在数据传输层面，平台集成 SSL 安全网关等专用模块，提供零侵入式通信加密服务，通过 TCP、HTTP/HTTPS 等标准化协议构建端到端加密传输通道，全程保障云上应用系统间、租户与平台间的数据传输安全，确保通信实体身份可信、传输数据不被篡改、窃取或伪造。

多租户隔离与动态调度技术。

面对多租户共享平台资源的场景，该技术是保障租户数据安全的核心。平台从资源分配、权限管理、数据存储多维度实现隔离，比如通过租户 ID 标识对密码资源、密钥数据进行逻辑隔离，每个租户仅能访问自身授权的资源；在权限管理上，划分平台管理员（包括运维人员）与租户两类角色，细化操作权限，避免越权访问。同时，依托云计算调度技术实现资源动态伸缩，当租户面临业务高峰时，平台可自

动扩容密码运算资源，应对高并发访问；业务低谷时则回收资源，降低运维成本。

监控与审计技术。

该技术为平台稳定运行和合规追溯提供支撑。平台集成日志分析、告警预警等功能，并采用 Elasticsearch 等工具处理密码服务中的海量日志，对密钥操作、密码服务调用、租户访问行为等进行全面记录。同时通过平台可视化界面，可实时展示资源状态、服务响应速度等信息，一旦出现密钥泄露、服务中断等异常，可快速告警并定位故障。此外，审计日志会留存完整的操作轨迹，涵盖操作人、操作时间、操作内容等关键信息，既满足等保、密评等合规要求，更为安全事件的追溯提供可靠依据。

5 应用实践

为满足云租户对云上应用系统的数据签名验证、数据加解密、移动端协同签名等多样化商用密码应用需求，某行业结合云环境弹性伸缩、多租户隔离等特性与商用密码合规要求，创新提出云上密码服务支撑体系的整体构建方案。该行业通过整合云上商用密码基础设施资源、规范密码服务接口标准、优化密钥全生命周期管理流程，成功搭建功能完备、安全可控的云上密码应用服务支撑平台，形成了云密码服务资源池。基于该平台提供的标准化、集约化云密码资源服务能力，有效解决了该行业商用密码应用合规性不足、移动端签名安全性保障弱等多项核心难题，推动了该行业数字化转型等场景的商用密码应用落地。这一实践不仅为该行业云上商用密码应用的标准化推广、体系化建设提供了可复制的实施路径，更积累了丰富的技术与管理经验，为后续全行业商用密码规模化应用推广，奠定了坚实基础。应用场景如下图 2 某行业商用密码应用拓扑图所示。

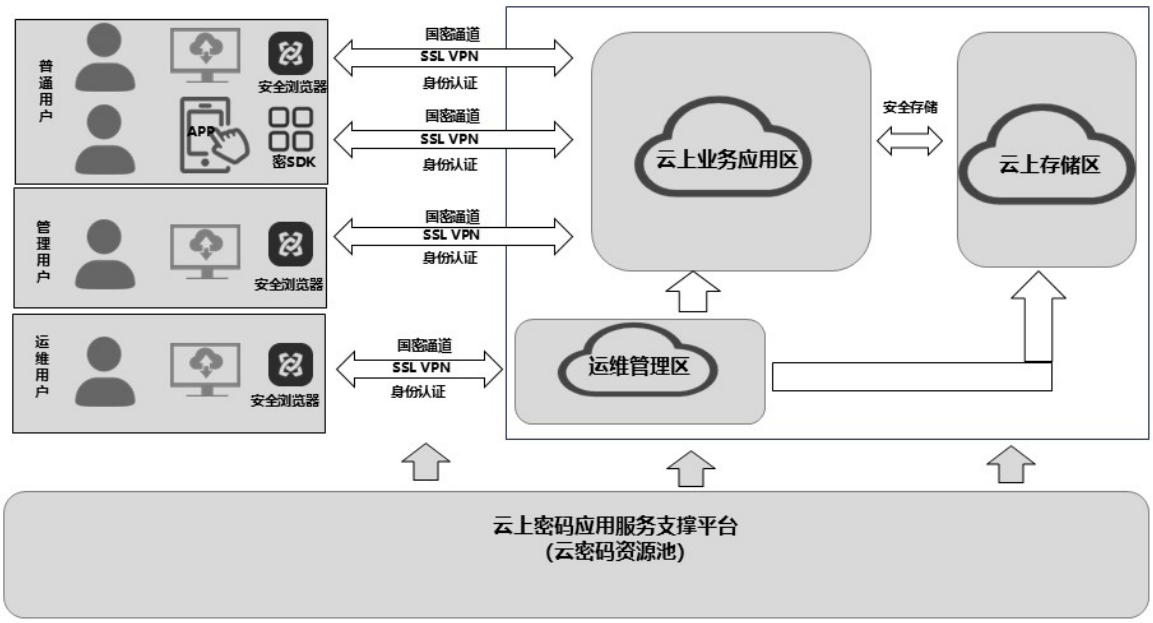

图 2 某行业商用密码应用拓扑图

云上密码服务支撑平台为某行业业务应用提供 PC 终端及移动端密码服务能力（支持移动终端本地数据加密保护）、身份认证、传输加密保护、重要业务数据保护、文件存储加密等安全防护。

移动办公系统密码应用。将密码服务 SDK 套件嵌入手机端移动办公 APP，通过商用密码算法实现对办公人员移动终端的认证与鉴权、移动办公业务应用的加解密服务。

备份容灾密码应用。在两地三中心备份架构中，采用商用密码算法对云平台数据进行加密存储，保障存储系统内部数据安全，同时提供用户身份认证、权限管理等多类保护措施，形成了可靠的数据存储系统和数据保护体系。

6 结语

当前，云计算的普及推动各行业业务系统加速向云端迁移，云上业务的规模化部署使商用密码应用需求愈发迫切。然而，云上商用密码应用尚未形成体系化、规范化、标准化的可落地指导性建设路径，制约了商用密码安全能力与云上业务的深度融合。针对这一核心痛点，本文开展系统性研究与实践，一方面通过构建云上密码应用服务支撑体系，明确云上密码服务支撑平台的核心功能与关键技术路径；另一方面通过应用落地与实践验证，形成可复用、可推广的实施范式。

本研究成果与实践案例，不仅为铁路行业体系化推进商用密码服务建设提供切实可行的实践借鉴，具备较强示范