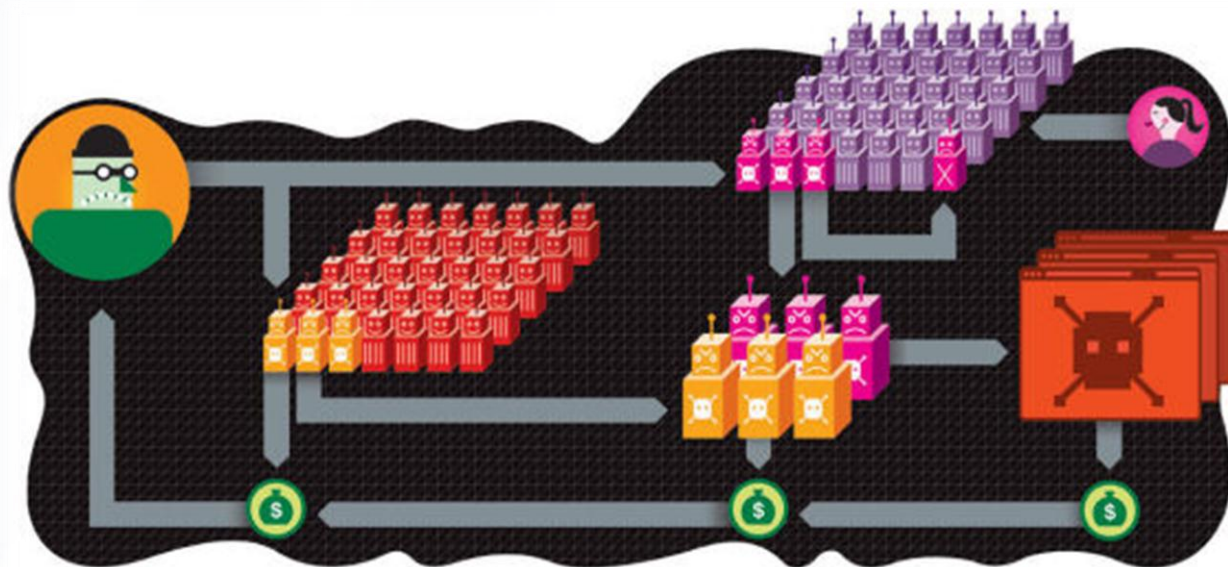


云取证技术研究

丁丽萍

中国科学院软件研究所

云环境更加脆弱



云

云环境存在的安全问题



云环境中的安全需求

执行安全需求

用户的任务能够在可信的执行环境中正确地完成

数据安全需求

用户的隐私数据不会被第三方以及恶意的云服务提供商所窃取

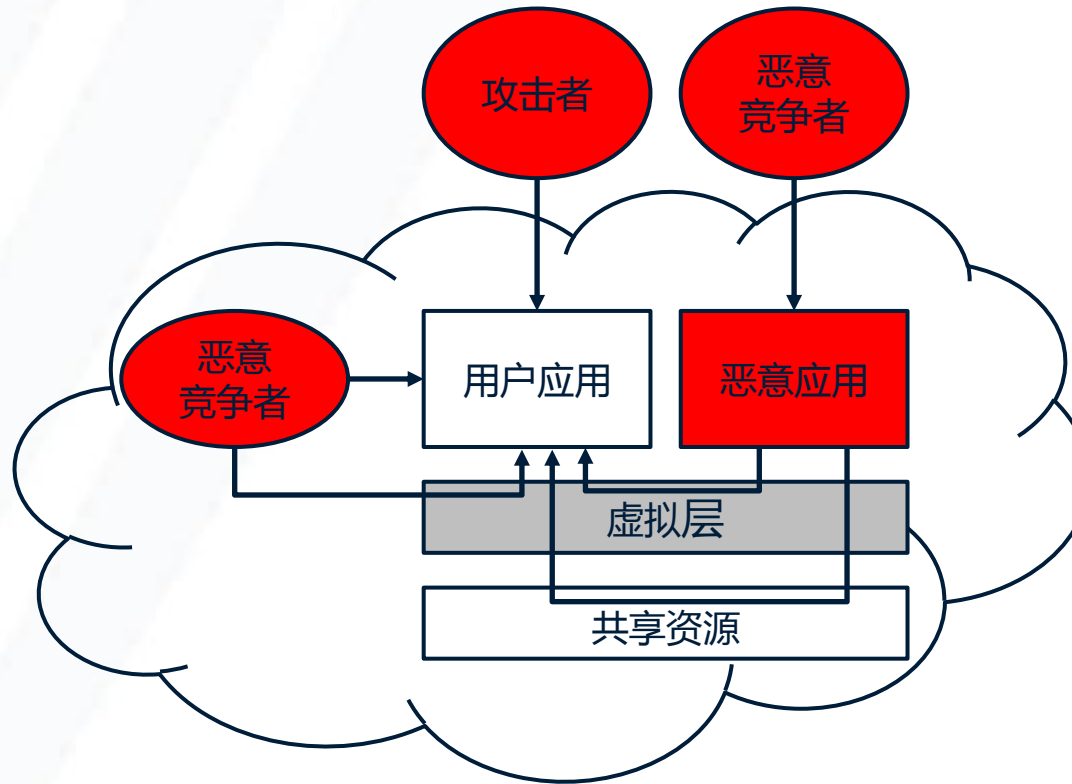
服务安全需求

用户能够在任何时间、任何地点无缝地接入云服务，并且整个接入过程是安全、可靠、可验证的

诉讼维权需求

运营商和用户在云环境遭遇了安全事件后，如何获取法庭认可的电子证据提起诉讼，维护自己的合法权益

云环境中的恶意行为定义



重要性

1

云计算环境下的恶意行为检测与取证技术研究**符合国家政策、时代发展和科技发展的必然要求**

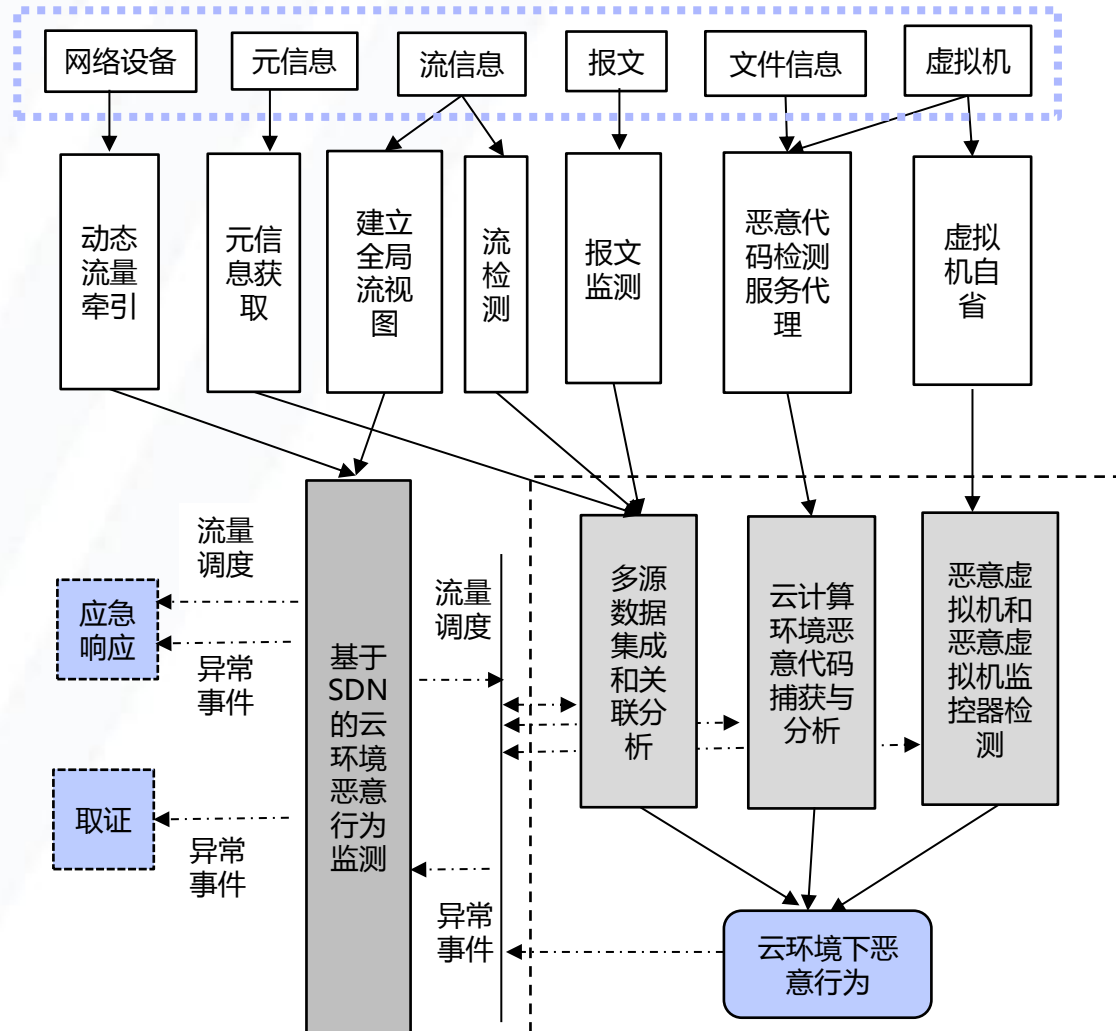
2

云计算环境下的恶意行为检测与取证技术研究是**目前云计算安全状况的迫切需求**

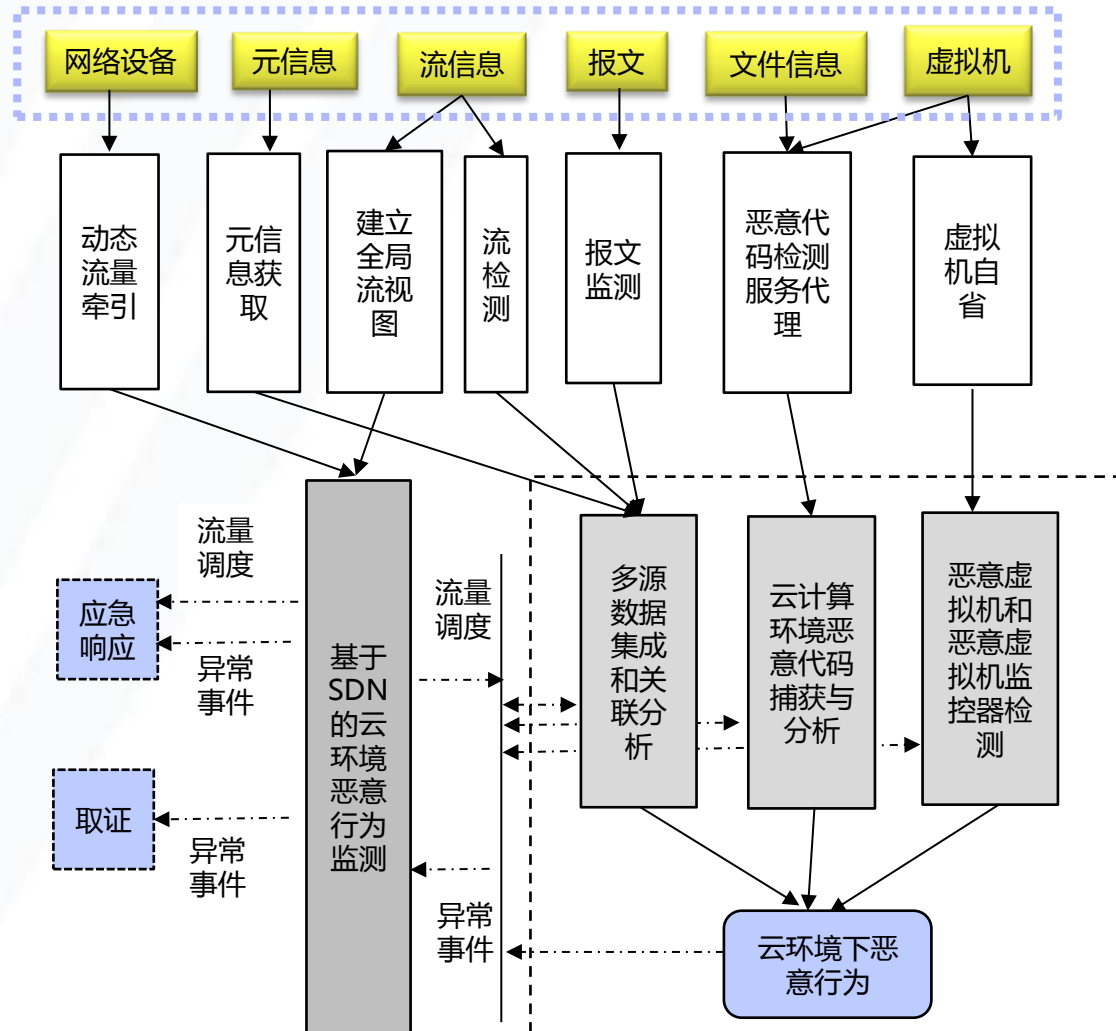
3

云计算环境下的恶意行为检测与取证技术研究是**目前云安全、云取证实践的迫切需求**

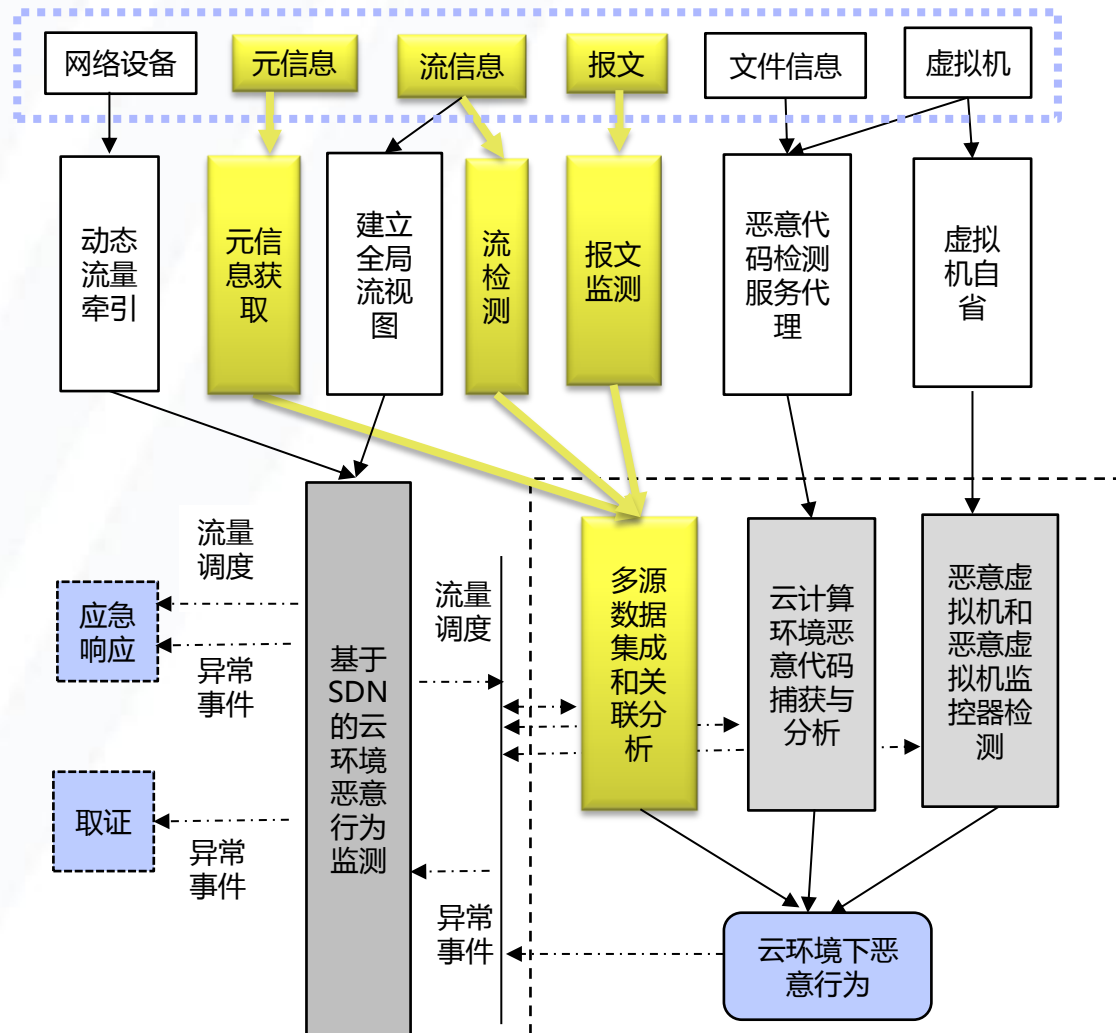
云环境下恶意行为检测系统



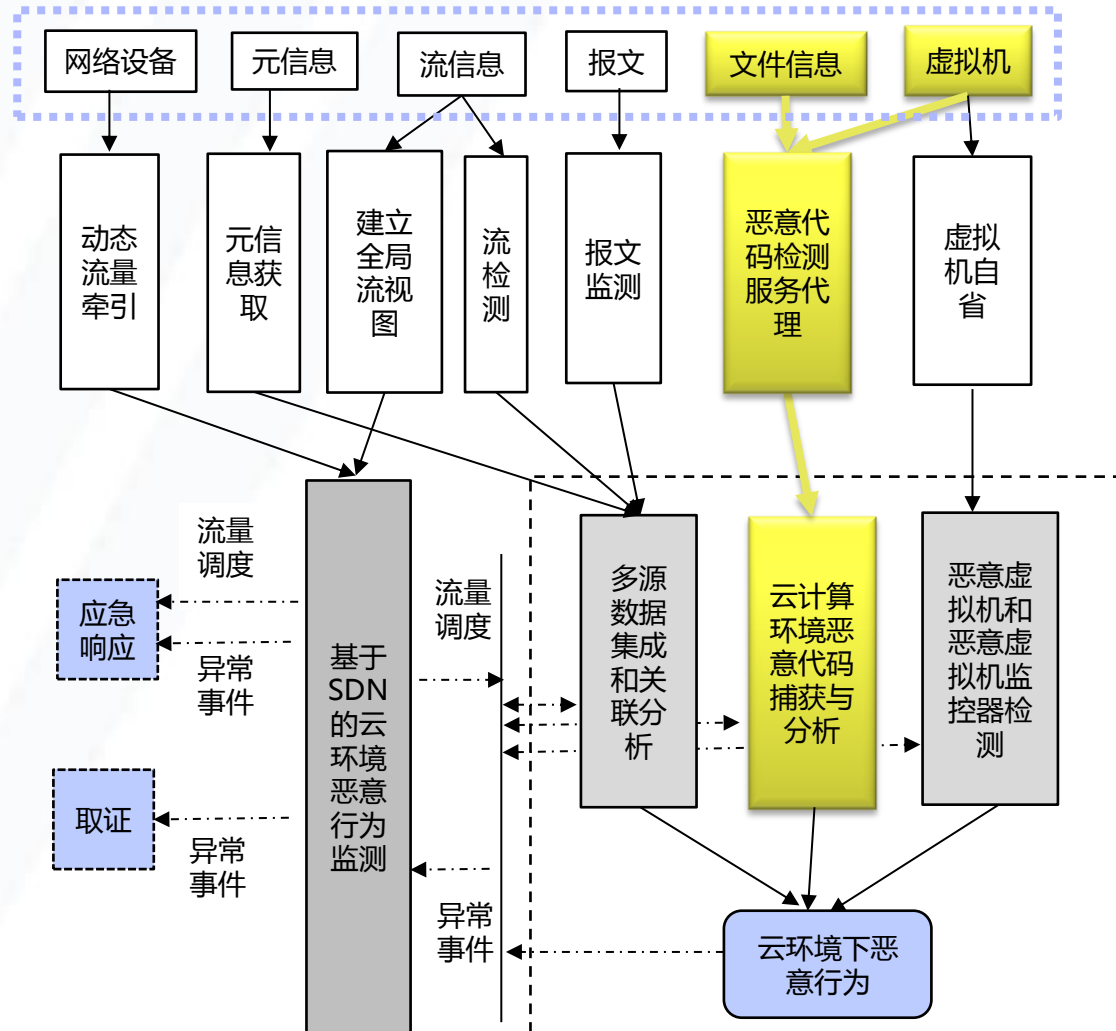
云环境下恶意行为检测系统



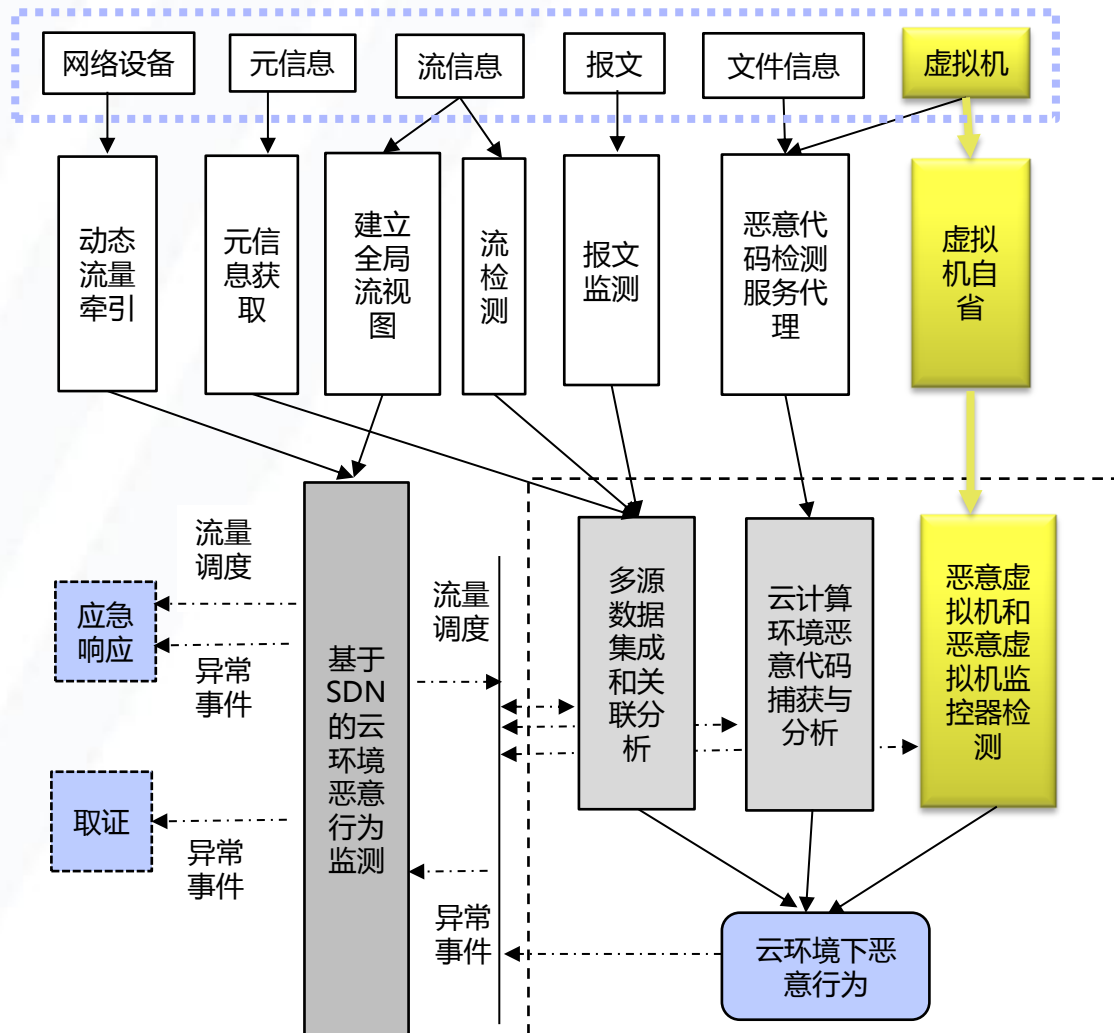
多源数据集成和关联分析



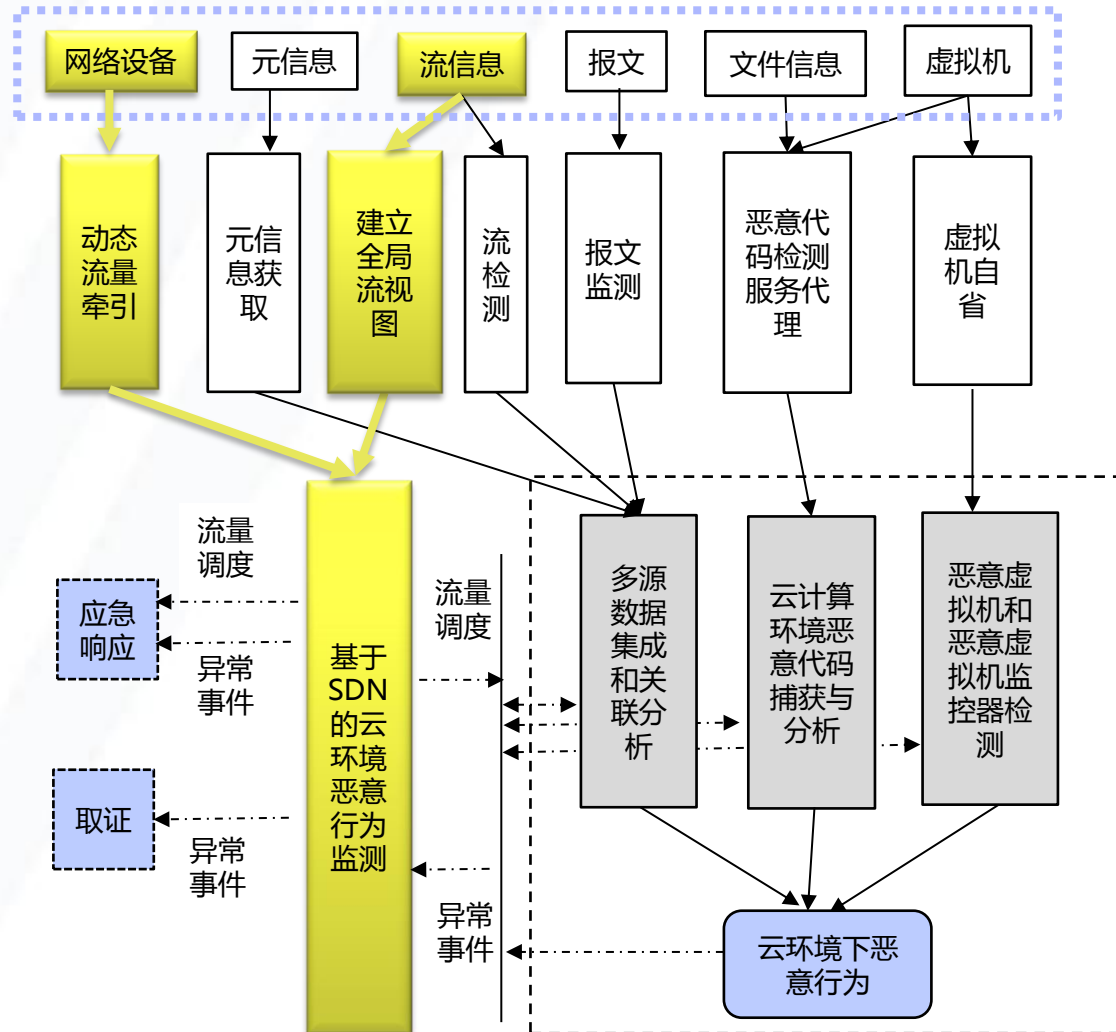
云环境下恶意代码捕获与分析



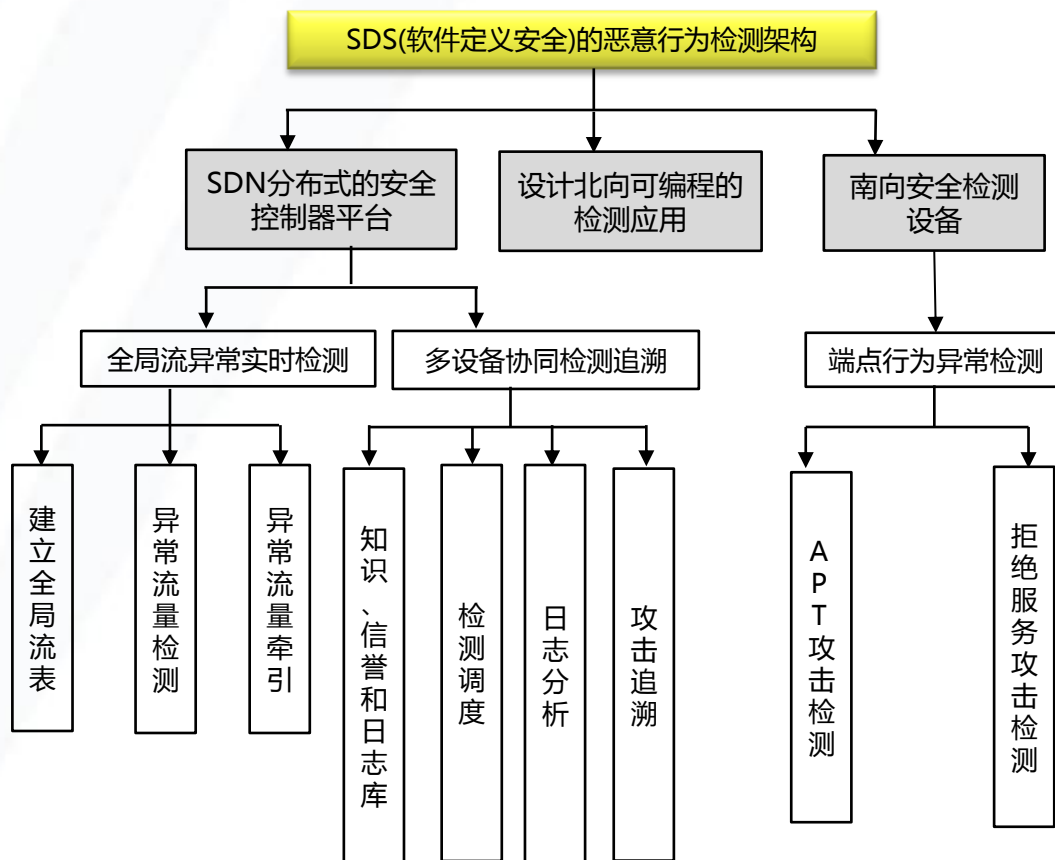
恶意虚拟机和恶意虚拟监控器检测



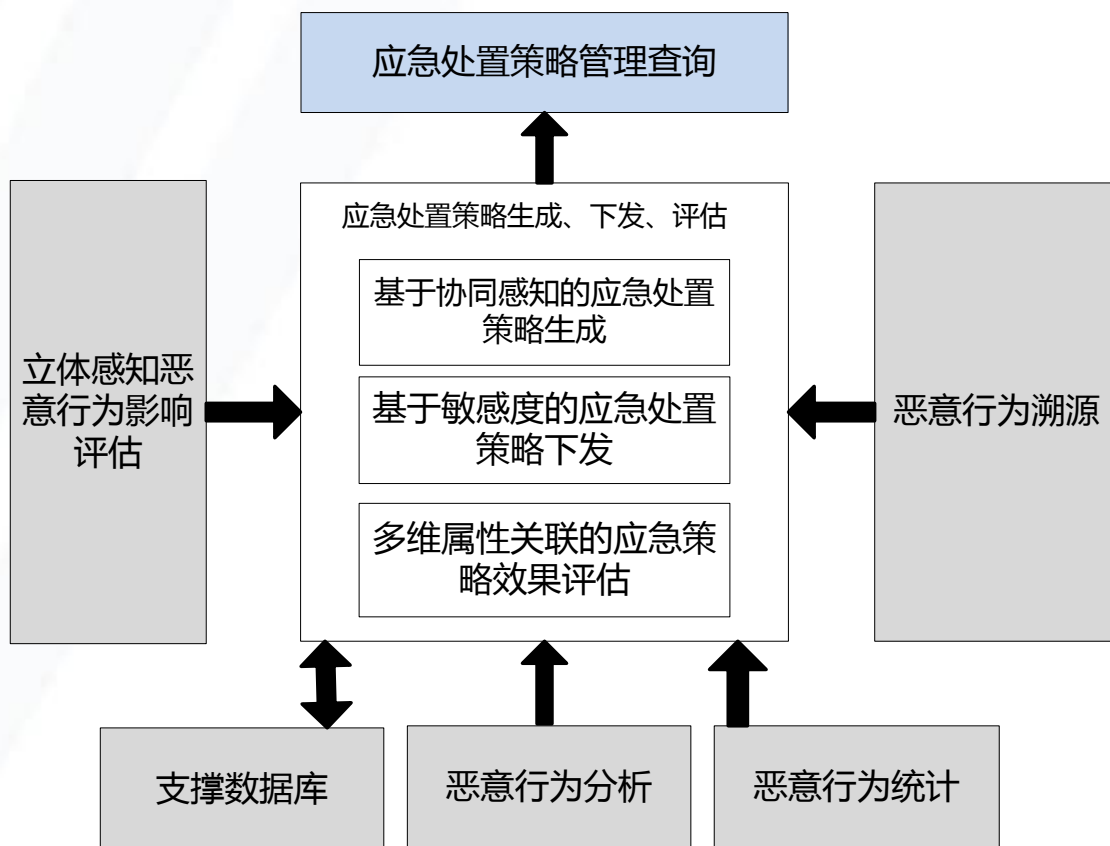
基于SDN的云环境恶意行为监测



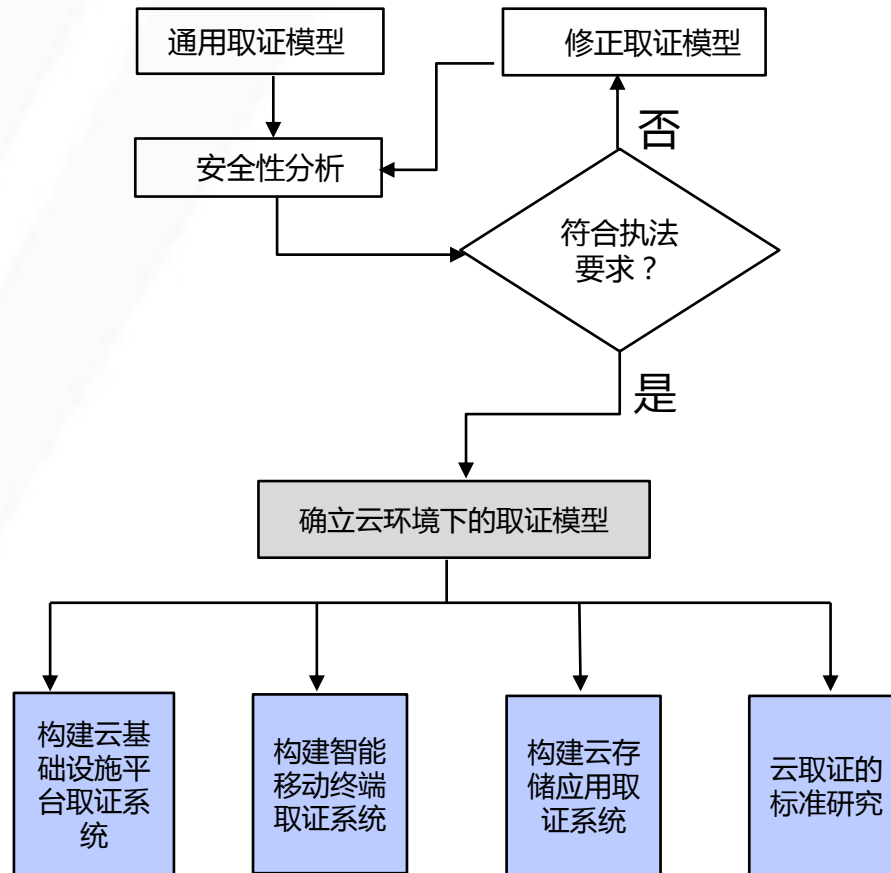
基于SDS的云环境恶意行为检测技术



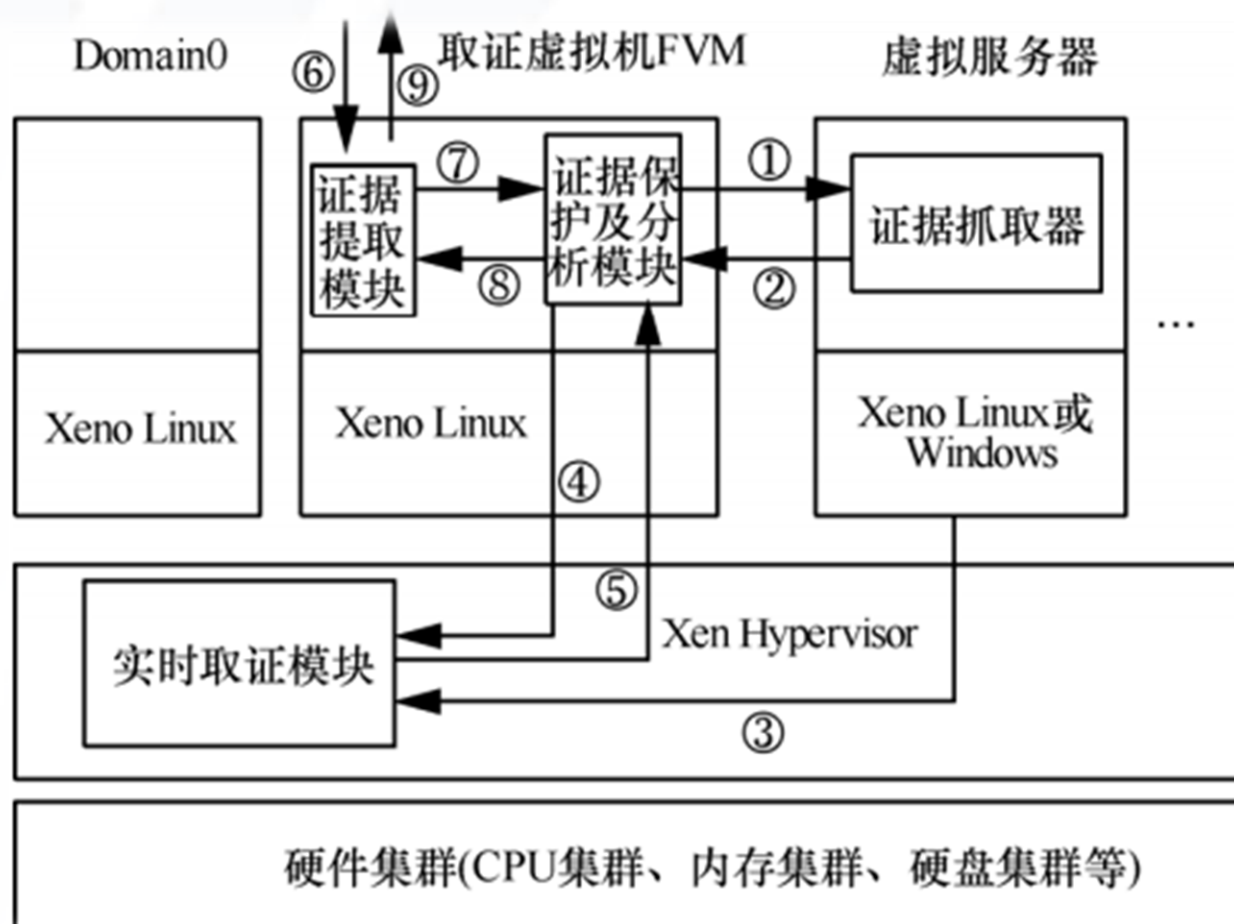
云环境下的恶意行为应急处置与溯源系统



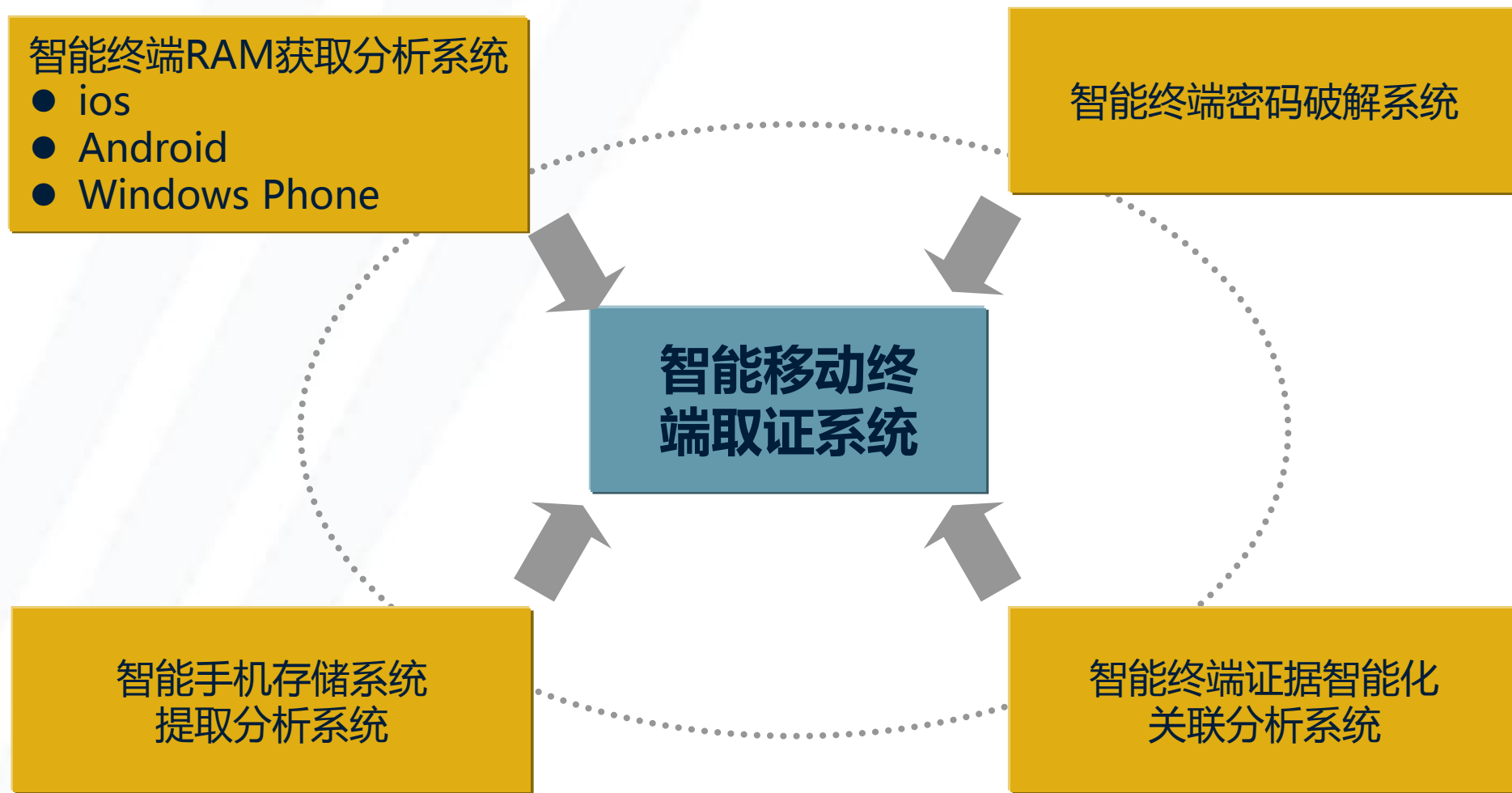
云环境下的取证系统



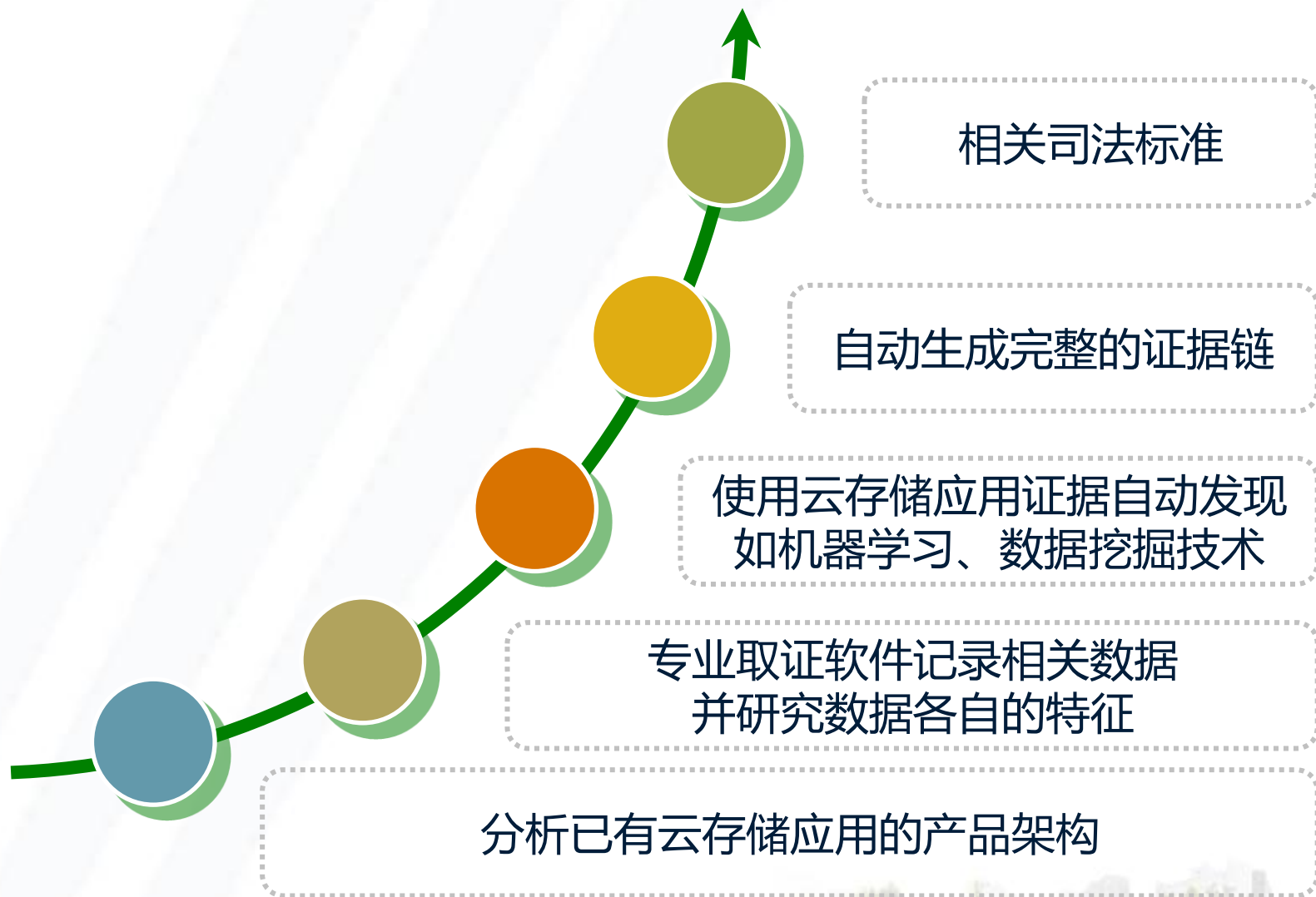
云基础设施平台取证系统



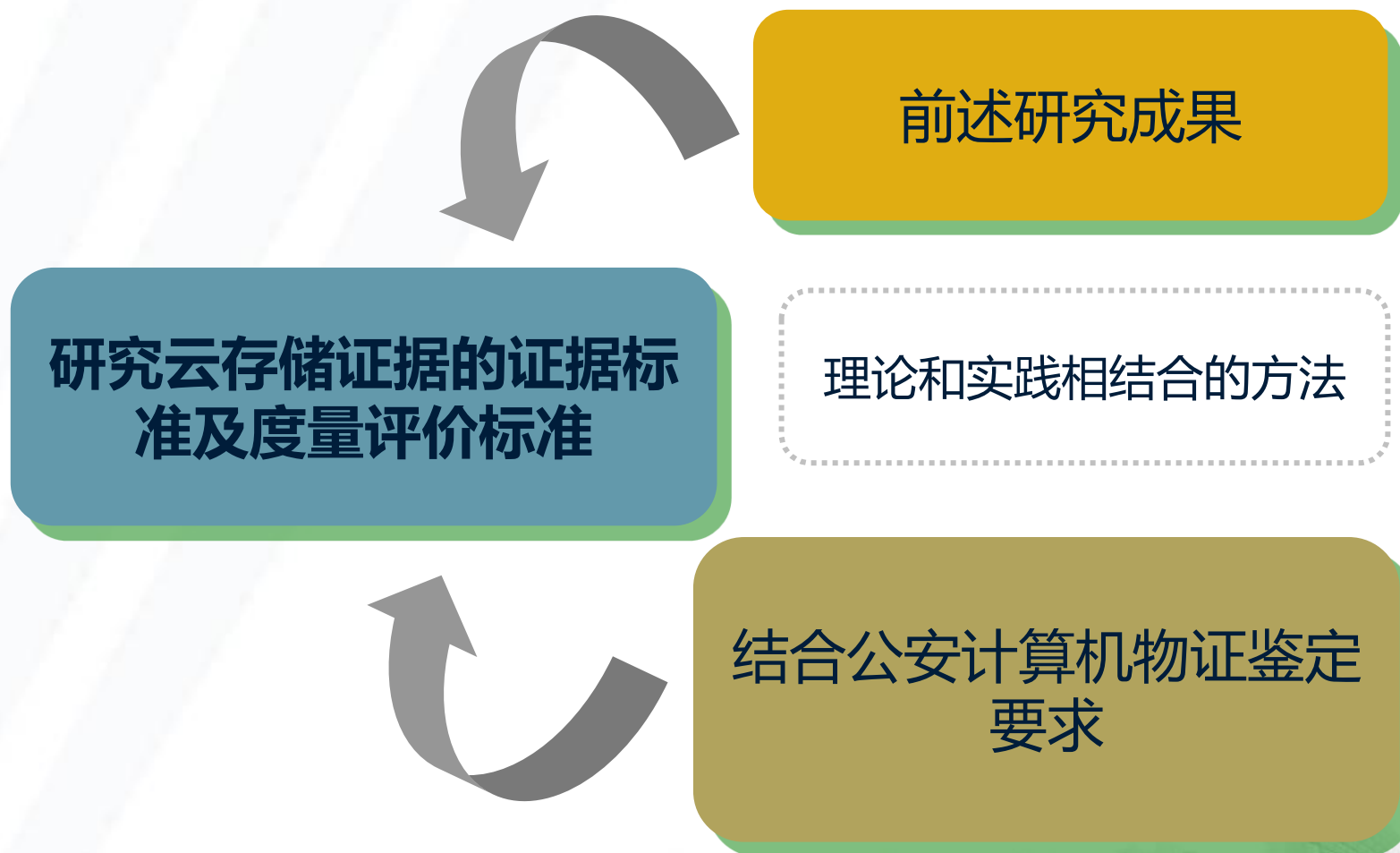
智能移动终端取证系统



云存储应用取证系统



云取证标准





**谢谢大家
请批评指正**