海云安全体系架构

章睿*, 薛锐, 林东岱

中国科学院信息工程研究所信息安全国家重点实验室, 北京 100093

* 通信作者. E-mail: zhangrui@iie.ac.cn

收稿日期: 2014-10-31; 接受日期: 2014-12-03; 网络出版日期: 2015-04-20

国家自然科学基金 (批准号: 61402471, 61472414, 61170280) 和中国科学院战略性先导科技专项 (批准号: XDA06010701) 资助

摘要 21 世纪的信息化进程, 正以“彻头彻尾彻里彻外”的形式, 以前所未有的速度、深度和广度, 走向人类社会 (人) 与信息网络 (机)、物理世界 (物) 彻底融合, 并带来感知终端与人机交互终端 (海)、新型网络技术 (网)、云计算 (云) 的新型组合模式和使用模式趋势. 把握“人、机、物”三元融合的发展趋势和机遇, 创建和发展海云协同计算的新一代信息技术体系, 最终实现“感知中国”的目标, 已成为新一代信息技术发展的迫切需求. 然而, 任何信息系统的稳定运行, 都离不开信息安全体系结构的构建. 信息系统的安全体系结构直接关系信息系统安全策略的实现效果, 它的合理与否直接影响信息系统的功能和运行. 因此, 构建基于海云三元融合复杂环境的安全体系架构, 是保障海云创新试验环境稳定运行的首要前提和基础. 本文从海云的概念入手, 在提出海云信息体系结构的基础上, 分析海云各层面临的安全挑战和安全需求, 最终提出海云安全体系架构, 为构建海云创新试验环境提供重要的理论依据和技术支撑.

关键词 海云 信息安全体系架构 “人、机、物”三元融合 异构网融合 安全技术

1 引言

“感知中国”是我国应对世界信息化变革浪潮的重大抉择, 是中国信息化的新阶段. 海云创新试验环境 (以下简称为“海云”) 是面向感知中国的新一代信息技术体系和先导技术研究的试验平台, 是三元融合应用与业务模式创新研究的资源池和开发环境. 通过海云的实施, 将促进新一代信息技术的跨越式发展, 推动新兴的信息通信技术战略性新兴产业的形成, 引领中国新一代信息技术创新进入国际领先行列.

信息系统的安全体系结构是系统安全功能定义、设计、实施和验证的基础. 该体系结构应该在反映整个信息系统安全策略的基础上, 描述该系统安全组件及其相关组件相互间的逻辑关系与功能分配. 这种描述的合理性和准确性将直接关系信息系统安全策略的实现, 确保其可用性、完整性、机密性、可认证性、不可否认性等安全特性^[1].

海云网络中的三元世界信息融合、海量终端规模等特性, 带来了多元身份标识与管理、隐私保护与监管能力的均衡、多源安全信息融合处理、可控可测的安全防护等新的安全问题, 对信任体系、隐私保护、安全防护、监控监管等安全机制提出了新的挑战. 因此, 需要构建面向海云的可溯源、可控

引用格式: 章睿, 薛锐, 林东岱. 海云安全体系架构. 中国科学: 信息科学, 2015, 45: 796–816, doi: 10.1360/N112014-00332

制、可验证的信息安全体系,从云端、海端、云海交互 3 个层面上保障云端数据安全、云端应用安全防护、海端可信终端构建、海端感知安全防护、海云交互安全等核心要素安全,并对海云信息安全体系进行整体的安全性分析与验证.

2 海云体系架构

海云是一种是由感知节点和智能终端(海)、新型网络技术(网)、云计算平台(云)组成的超大规模分布式网络形式.它将无处不在的末端设备和设施,包括具备“内在智能”的传感器、移动终端、工业系统、楼控系统、家庭智能设施、视频监控系统等,和“外在使能”的,如贴上 RFID 的各种资产、携带无线终端的个人与车辆等等“智能化物件或动物”或“智能尘埃”,通过各种无线或有线的长距离或短距离通讯网络实现互联互通、应用大集成、以及基于云计算的 SaaS 营运等模式,在内网、专网或互联网环境下,采用适当的信息安全保障机制,提供安全可控乃至个性化的实时在线监测、定位追溯、报警联动、调度指挥、预案管理、远程控制、安全防范、远程维保、在线升级、统计报表、决策支持等管理和服务功能,实现对“万物”的“高效、节能、安全、环保”的“管、控、营”一体化服务.

2.1 海云的定义

海云是基于个人、组织机构和社会的需求,实现“人、机、物”之间按需进行信息获取、传递、存储、认知、决策、使用等服务,网络具有超强的环境感知、内容感知及智能性,为个人、组织结构和社會提供无所不在的、无所不含的信息服务和应用.简言之,即人或设备能够不受时间、地域和技术限制地通信和获得服务.

从字面上分析,“海”指的是大量终端设备以及由这些设备产生或收集的海量数据;“云”指的是用于处理海量数据和为不同应用提供服务的各种云计算平台.

从网络技术上看,海云是通信网、互联网、物联网高度融合的目标,它将实现多网络、多行业、多应用、多异构技术的融合和协同.如果说通信网、互联网发展到今天解决了人与人信息通信的问题,物联网则实现网络连接、接入、延伸到物理世界的泛在物联阶段,解决人与物、物与物的通信.通信网、互联网、物联网各自发展为海云的搭建奠定了坚实的基础,海云的最终目标将是通信网、互联网、物联网高度融合和协同.

2.2 海云的组成部分

海云由“海、网、云”3 个主要部分组成.海端的感知节点和智能终端是实现“人、机、物”通信的基础设施,也是海量数据的来源和收集者;传感网和互联网以及新型网络组成中间的网络层,负责海端和云端之间的数据和信息的传输;云端的云计算平台是实现海量数据处理的计算平台,并为大量终端提供各种云服务.

2.2.1 海

“海”包括感知设备和所有的智能终端.感知设备是指射频识别(RFID)、红外感应器、全球定位系统、激光扫描器等信息传感设备,它们按约定的协议,把任何物品与互联网相连接,进行信息交换和通信,以实现对物品的智能化识别、定位、跟踪、监控和管理.智能终端设备是指那些具有多媒体功能

的智能设备, 这些设备支持音频、视频、数据等方面的功能. 如: 可视电话、会议终端、内置多媒体功能的 PC/PDA/手机等.

海端设备具有种类繁多、数量庞大 (数量达数百万、数千万) 的特点, 并且运行于海端设备上的系统、软件以及数据的类型多种多样、设备的接入方式和信息的传输方式也各不相同.

2.2.2 网

“网”包括传统的传感网和互联网以及多种新型网络, 它们将各种终端设备以无线/有线方式连接在一起, 将终端的数据传输到云端处理或为终端提供服务或数据传输功能.

因为“海”的所有权特性, 海云应用在相当一段时间内都将主要在内网和专网中运行, 形成分散的众多“物—物连接的网络”, 最终走向互联网, 形成真正的“海—云互联的网络”. 海—云互联的网络由 4 大支撑网络组成. (1) 短距离无线通讯网: 包括 10 多种已存在的短距离无线通讯 (如 Zigbee、蓝牙、RFID 等) 标准网络以及组合形成的无线网状网 (mesh networks). (2) 长距离无线通讯网: 包括 GPRS/CDMA, 3G, 4G, 5G 等蜂窝 (伪长距离通讯) 网以及真正的长距离 GPS 卫星移动通信网. (3) 短距离有线通讯网: 主要依赖 10 多种现场总线 (如 ModBus, DeviceNet 等) 标准, 以及 PLC 电力线载波等网络. (4) 长距离有线通讯网: 支持 IP 协议的网络, 包括计算机网、广电网和电信网 (三网融合) 以及国家电网等通讯网.

2.2.3 云

“云”包含为海端提供服务和资源的各种云计算平台. 云计算是一种新兴的基于互联网的计算方式, 是网络计算、分布式计算、并行计算、网络存储、虚拟化、负载均衡等传统计算机技术和网络技术发展融合的产物. 它是一种可以方便的、按需从网络中获取共享池中可配置计算资源的模型. 这些计算资源可以是网络、服务器、存储、应用及服务, 可以通过最少的管理工作及最少的与平台提供商的交互在网络中快速提供与发布资源. 和电网、自来水管网的形式类似, 接入互联网的计算机终端可以按需使用来自云计算平台提供商的软硬件资源, 而不用关心“云”的细节, 例如这些资源具体存放在什么地方, 或者怎样提供. 通过部署和使用云计算, 可以减少企业和单位的使用成本, 节约耗损开销, 同时减少了数据由于没有备份而损坏或丢失的风险 [2].

2.3 海云的特点

海云的目的是构建更智能的无处不在的信息社会, 包括新型终端网络、异构服务网络融合、可信与管理. 海云的构建依赖于 3 个实体层的存在和互动. 一是无所不在的终端单元; 二是无所不在的基础网络; 三是无所不在的网络应用.

相对于现有的网络, 海云要求实现更透彻的感知, 更可靠、更广泛的网络传送, 和更智能的分析和处理. 通过底层的全连通的、可靠的、智能的网络, 以及融合的内容技术、纳米技术和生物技术, 将通信服务扩展到教育、智能建筑、供应链、健康医疗、日常生活、灾害管理、安全服务、运输等行业, 并为人们提供更好的服务, 让人们享受信息通信的便利, 让信息通信改变人们的生活, 更好地服务于人们的生活.

(1) 更透彻的感知. 意味着部署更多类型的传感、识别和感知设备, 未来这些无处不在的传感器、RFID、摄像头、二维码等是实现人与物、物与物“交流”、“对话”的基础.

图 1 海云技术体系架构

Figure 1 The technical architecture of sea-cloud

(2) 更广泛的网络传送. 意味着海云网络的传送技术将包含各种有线、无线网络技术, 并且 IP 网络将成为传送的核心网络, 通过充分利用各种有线和无线网络技术, 将可以实现更广泛的互联互通以及更广地域的感知信息传送. 同时引入 IPv6^[3] 是实现更广泛互联互通的基础, 因为在海云网络环境下, 将有海量的“物—物”接入, 现有 IP 地址明显不足, IPv6 的引入一方面可以解决地址空间不足的问题, 另外通过 IPv6 的永远在线、移动性和安全性等新功能的支持, 还将有利于创造更多的新应用. 此外, 将感知信息进行网络传送时, 还需要同步考虑实现“人、机、物”之间通信的融合, 实现“三网”融合的发展目标.

(3) 更智能的分析和应用, 也就是需要考虑采用云计算等分布式处理技术, 对数据进行智能地分析和处理. 对于海云网络应用, 由于需要处理的数据可能跨各个行业领域, 而且同时又考虑到各个行业应用的个性需求有所不同, 因此可以引入“通用平台 + 子应用”或者“中间件”的概念. 通过通用平台或者中间件实现公共信息的交换以及公共管理功能, 各个行业的个性化应用将可以通过子应用的方式来呈现.

2.4 海云参考模型

海云体系架构可以粗略地划分为 3 层, 包括感知延伸层、网络传输层、以及业务应用层, 其中的每一层又涉及诸多关键技术, 如图 1 所示.

2.4.1 感知延伸层

终端节点不仅能够提供事物本身的信息, 而且能够探测、存储、处理乃至整合各种与事物相关的

信息, 从而向全网络提供各种关联信息. 随着微电子技术、嵌入式技术、短距离通信技术、传感器技术、智能标签等技术的发展与成熟, 现实世界中越来越多的物理实体需要自组织来实现智能环境感知并对其进行自动控制, 并具备通信和信息处理的能力. 网络的触觉不断得到延伸, 越来越多的“物品”进入信息网络内部进行通信, 接入信息通信网络的物理实体数量和范围可无限扩展, 由传统的人与人的信息通信网络向人与物、物与物的信息通信网络拓展.

2.4.2 网络传输层

任何终端节点在网络中都能实现互联. 由终端节点组成的网络, 如传感器网、RFID、家庭网、个域网、身体域网、车载网等, 架构在基础通信网络上, 形成一个广泛互联的网络. 随着移动宽带化和宽带移动化的趋势, 融合网络是网络基础设施的未来发展方向. 海云网络要满足未来不同的信息化应用, 要求基础网络具有不同安全可信等级和不同服务质量的网络能力. 海云环境的使用者, 可以在任何时间任何地方无障碍地使用信息通信网络. 在这个网络中, 通信不仅是人与人, 其业务流还可能来自人与能感知客观环境的设备之间, 以及设备和设备之间.

2.4.3 业务应用层

海云将对信息进行综合分析并提供更智能的服务, 推动人的智能、社会物质和能源资源潜力充分发挥, 使社会经济运行向高效、优质的合理化方向发展. 海云网络的智能业务为各种行业具体应用提供公共服务支撑环境. 由于海云环境中的数据量巨大, 各种业务用户的分布广泛, 决定了海云中大部分的业务信息处理和服务由云计算平台来完成. 云计算平台将分散的资源集中, 并按需分配给各个用户. 同时, 云计算平台通过虚拟化技术将相同的资源提供给多个用户同时使用. 但是云计算平台的海量信息、资源聚合和按需服务的特点, 也使云平台的安全性和用户的隐私性成为目前主要关注的重点.

3 海云面临新的安全挑战

安全是基于网络的各个系统运行的重要基础, 海云环境的开放性、高度融合性也使它面临更多的安全隐患. 海云的推广和应用需要在海云环境基本特征的基础上深入研究其安全问题.

海云是一个庞大复杂的分布式系统, 它的“人、机、物”三元融合和网络的异构融合的特点使得海云面临的安全问题既包括互联网、物联网和云计算中同样的安全问题, 也有它自身特有的安全问题, 如异构网络的认证与访问控制问题、信任域管理问题、信息隐私问题以及网络的稳定和可靠性问题、如何实现上下联动和横向联动的安全协同等, 主要体现在以下 6 点:

(1) 异构网络间的认证问题. 在海云环境中, 不同网络间的业务使用非常频繁, 这就要求海云环境除了网络与用户之间的相互认证之外, 还必须要进行异构网络间的相互认证以及用户与为其服务的终端之间的相互认证, 这样才能保证一个让用户放心使用且安全的网络环境.

(2) 建立以用户为中心的信任域. 在海云环境中, 作为服务提供者 (服务通常以云服务的形式提供) 需要构建整合各种网络资源、信息装置、基础平台、应用内容及解决方案; 而对于服务使用者, 必须有一个让使用者放心且安全的环境, 使其能随时随地、方便地建立以自己为中心的信任域来处理任何事情. 其终端节点具有动态性、智能性, 且多种接入方式和多种承载方式融合在一起以实现无缝接入. 它要求任何对象 (人或设备等) 无论何时何地都能够通过合适的方式获得永久在线的宽带服务, 随时随地存取所需信息. 海云的这些特点, 为我们提出了一个移动安全机制方面新的问题, 即如何高效、便捷

地建立以用户为中心的信任域。

(3) 信任域的动态管理问题. 海云网络的动态性是指以用户为中心的信任域中, 终端会随时加入或退出, 此时为有效地保障用户隐私, 一般要求终端退出后不知道信任域中的信息交流和业务来往, 而新加入的终端不知道进入信任域之前的任何信息, 即保证前向安全性和后向安全性。

(4) 信息隐私问题. 信息隐私是海云信息机密性的直接体现, 如感知终端的位置信息、基于数据挖掘的用户行为分析等. 因此, 要在海云的各个部分建立访问控制机制, 控制信息采集、传递和查询等操作. 信息的加密是实现信息机密性的重要手段, 但是海云的多源异构性, 使密钥管理成为一个较困难的问题, 特别是对感知网络的密钥管理是制约海云保持信息机密性的瓶颈。

(5) 网络的稳定性和可靠性问题. 海云的感知互联过程要求网络具有高度的稳定性和可靠性. 海云是与许多应用领域的物理设备相关连的, 要保证“人、机、物”之间任何通信的稳定性和可靠性是一个需要重点关注的问题。

(6) 多层联动协同安全问题. 海云计算是一个庞大的分布式结构, 对于它的安全防护所采用的技术是现有安全技术的松散耦合, 如何实现上下联动和横向联动的协同安全, 是实现海云安全体系架构的关键问题。

海云环境面临的安全问题可主要分为以下几个部分:

(1) 感知延伸层的信息安全问题. 海端的感知节点和智能终端具有多源异构的特点. 感知节点通常情况下功能简单、携带能量少 (使用电池), 使得它们无法拥有复杂的安全保护功能. 而感知网络多种多样, 它们的数据传输和消息也没有特定的标准, 所以没有办法提供统一的安全保护体系。

(2) 网络传输层的信息安全问题. 海云的核心网络具有相对完整的安全保护能力, 但是由于海端节点的数量庞大, 且以集群方式存在, 因此会导致在数据传播时, 由于大量设备的数据发送使网络拥塞, 产生拒绝服务攻击. 此外, 现有通信网络的安全架构都是从“机—机”的角度设计的, 对“人、机、物”三元融合的海云环境, 需要建立适合于感知信息在“人、机、物”之间传输与应用的安全架构。

(3) 业务应用层的信息安全问题. 支撑海云业务的平台有着不同的安全策略, 如云计算、分布式系统等, 这些支撑平台要为上层服务管理和大规模行业应用建立起一个高效、可靠和可信的系统, 而大规模、多平台、多业务类型使海云业务层次的安全面临新的挑战。

综上所述, 海云环境中感知信息、网络环境 and 应用需求的多样性, 呈现出网络规模大、数据处理繁琐、决策控制复杂的特点, 给海云安全体系的研究提出了新的挑战. 这要求对海云环境各个部分的安全问题和特点进行具体分析, 进而提出合适的安全体系结构。

4 海云信息安全体系架构

对于海云的各个层次, 我们将分别从安全挑战入手, 分析其安全需求, 给出合理的安全架构, 最终提出海云安全体系参考模型。

4.1 海云感知延伸层信息安全体系架构

海云感知延伸层的任务是感知外界信息, 或者说是原始信息的收集器. 该层的典型设备包括 RFID 装置、各类传感器 (如红外、超声、温度、湿度、速度等)、图像捕捉装置 (摄像头)、全球定位系统 (GPS)、激光扫描仪、手机、各类 PC 等. 这些设备收集的信息通常具有明确的应用目的, 因此传统上这些信息直接被处理并应用. 但是在海云环境中, 多种类型的感知信息可能被同时处理、综合应用, 甚至不同

的感知信息的处理结果将影响其他控制调节行为。同时, 海云感知延伸层自身的特点, 也带来了新的挑战。

4.1.1 感知延伸层的安全挑战

感知延伸层中各级节点可能会遇到的安全挑战大致分为下列几种情况^[4,5]:

(1) 有限的存储空间和计算能力。海云感知延伸层资源有限的特性导致很多复杂、有效、成熟的安全协议和算法不能直接使用, 特别是公钥密码体系。从存储空间上看, 一对公钥的长度就达到几百个字节, 还不包括各种中间计算所需要的空间; 从时间复杂度上看, 公钥密码算法所需的计算量大, 这对内存和计算能力都非常有限的感知节点来说是无法完成的。

(2) 缺乏后期节点布置的先验知识。在使用海云节点进行实际组网时, 节点往往是被随机散布在一个目标区域中, 任何两个节点之间是否存在直接连接在布置之前是未知的。

(3) 布置区域的物理安全无法保证。海云的感知节点通常散布在无人监控的区域, 使得其很可能遭到物理上或逻辑上的破坏或者俘获, 所以感知延伸层安全设计中必须考虑及时撤除网络中恶意或被俘获节点的问题, 以及因为恶意节点而导致的安全隐患问题, 即敌手可能通过恶意节点俘获能与之通信的邻居节点, 最终导致整个网络被攻破或失效。

(4) 有限的带宽和通信能量。由于目前感知延伸层主要采用低速、低功耗的通信技术, 这就要求使用的安全算法和安全协议所带来的通信开销不能太大。

(5) 网络信息安全形式多样。海云环境中每个节点的功能具有多样性, 节点不但具有检测和判断功能, 而且又担负着路由转发功能。每个节点与其他节点通信时都存在信任度和信息保密的问题。除了点到点的安全通信外, 还存在信任广播问题。基站向全网发布消息时, 每个节点都要能够有效判定消息确实来自于有广播权限的基站。

(6) 异构网络节点的标识、识别、认证和访问控制问题。感知延伸层节点之间的识别、认证和访问控制问题也是保障感知延伸层安全需要考虑的主要问题。由于感知延伸层的节点大多数都布控在无人监控的环境, 且这些节点很容易被伪造和复制, 敌手可能通过自己复制或伪造的节点向其他节点发送恶意消息。因此, 感知延伸层的节点通信之前应该有识别、认证机制, 同时在访问节点信息时也需要控制机制来保障节点上信息的机密性。但是在异构网络之间进行节点的互认证和访问控制需要考虑认证协议和访问控制策略的兼容性问题。

(7) 应用相关性。海云应用的领域非常广泛, 不同的应用对安全性的要求也不同。许多商用系统更关注信息的保密性和完整性; 对于军事领域, 除了信息的可靠性外, 还必须考虑抵抗恶意节点、异构节点入侵的能力。这就要求根据具体应用采用多样性、灵活的方式解决安全问题。

4.1.2 感知延伸层的安全需求

针对上述安全挑战和安全问题, 感知延伸层的安全需求可以总结为以下几点:

(1) 机密性。典型的海云应用网络不应该泄露数据给邻居网络。在许多应用中, 通信节点可能传递高敏感数据, 因此必须使用加密机制对这些信息进行加密传输。同时, 应该考虑因密钥泄露造成的影响, 将损失尽可能控制在一个很小的范围内。此外, 感知延伸层节点或设备的其他信息也会泄露设备持有者或拥有者的部分隐私信息, 例如, 设备的位置信息等, 因此同样应该采取措施防止这些信息的泄露。

(2) 真实性。感知延伸层节点的身份认证或数据源认证在海云的许多应用中是非常重要的。海云

环境中, 接收者只有通过数据源认证才能确信消息是从正确的节点发出的. 由于感知节点的计算能力、存储空间和通信带宽的限制, 通常使用共享的对称密钥来进行数据源的认证.

(3) 完整性. 在通信过程中, 数据完整性能够确保接收者收到的数据在传输过程中未被篡改或替换. 在感知延伸层网络中, 通常使用消息认证码来保证数据完整性.

(4) 新鲜性. 在感知延伸层网络中, 基站和簇头需要处理大量节点发来的信息, 为防止攻击者进行任何形式的重放攻击, 必须保证每条消息的新鲜性. 此外, 新鲜性还体现在密钥建立的过程中, 即通信双方所共享的密钥是最新的.

(5) 扩展性. 感知延伸层的感知节点数量巨大, 分布广泛, 环境条件、恶意攻击或任务的变化都可能影响感知延伸层网络的结构. 同时, 节点的加入或失效也会使网络的拓扑结构发生变化. 感知延伸层网络的可扩展性表现在感知节点数量、网络覆盖区域、生命周期、时间延迟、感知精度等方面的可扩展极限. 因此, 给定感知延伸层网络的可扩展级别, 安全解决方案必须提供支持该可扩展级别的安全机制和算法.

(6) 可用性. 感知延伸层的安全解决方案所提供的各种服务能够被授权用户使用, 并能够有效防止恶意攻击. 一个合理的安全解决方案应当具有节能的特点, 各种安全算法和协议的设计不应过于复杂, 计算开销、存储容量和通信能力也应当充分考虑网络资源有限的特点. 同时, 安全方案在有效防止网络攻击的同时不应限制网络的可用性.

(7) 自组织性. 由于感知延伸层网络大部分是由传感器节点以 Ad-hoc 方式构成的无线网络, 它是以自组织方式进行组网的, 这就决定了相应的安全方案也应当是自组织的, 即在感知节点配置之前无法假定节点的任何位置信息和网络的拓扑结构.

(8) 鲁棒性. 感知节点的动态性和移动性, 决定了安全解决方案应该具有健壮性和自适应性, 能够随着应用的变化而灵活拓展. 此外, 当某些节点被俘获后, 安全方案应当限制其影响范围, 保证整个网络正常运行.

4.1.3 感知延伸层的安全架构

基于以上对海云感知延伸层安全挑战和安全需求的分析, 就比较容易建立合理的安全架构. 由于感知延伸层的安全是相对独立的问题, 有些已有的安全解决方案在海云环境中也同样适用. 但由于感知延伸层节点能力受限, 要保证它的安全需求所涉及的密码技术包括轻量级密码算法、轻量级密码协议、可设定安全等级的密码技术等.

海云感知延伸层的安全机制包括以下几点:

(1) 可信计算^[6]. 用于保证终端设备的操作系统和应用软件的安全, 防止可执行文件被恶意篡改, 以及将信任链向外部网络扩展, 保证感知延伸层设备和网络传输层设备的可信连接.

(2) 漏洞扫描. 对各种智能终端设备进行漏洞扫描, 及时发现和修补系统和软件漏洞.

(3) 加密算法. 用于保证数据的机密性. 可根据节点不同的计算和存储能力选择使用对称或非对称的加密算法加密要传输的数据.

(4) 消息验证机制^[7,8]. 包括消息的完整性验证和消息源的验证, 即发送方在发送消息前采用合适的密码技术对消息产生校验和或者签名, 使得消息的接收方能有效验证消息的完整性和来源.

(5) 认证机制¹⁾. 用于内部节点或内部节点与外部设备之间的相互认证. 可根据节点能力选择对称密码或非对称密码方案解决.

1) Multi-factor authentication. http://en.wikipedia.org/wiki/Multi-factor_authentication.

图 2 感知延伸层的安全架构
Figure 2 The security architecture of perceptual layer

- (6) 密钥管理^[9]. 用于保障通信的安全. 在认证的基础上完成密钥协商是建立会话密钥的必要步骤.
- (7) 访问控制^[10]. 用于防止各级节点设备上信息被未授权用户访问, 以及控制用户对信息的读、写操作.
- (8) 入侵检测^[11]. 通过收集和分析网络行为、安全日志、审计数据、以及其他网络上可以获得的信息, 检查感知延伸层网络中是否存在违反安全策略的行为和被攻击的迹象, 用于主动防范感知延伸层网络中可能的攻击.
- (9) 安全路由^[12]. 采用 IPSec 协议、路由技术、VPN 技术、防火墙技术等, 达到任意两个节点之间安全通信的目的. 它的功能包含带有包过滤和代理协议的防火墙功能; 能够隐藏内部网络拓扑结构; 支持路由信息与 IP 数据包加密; 能够实现身份鉴别、数据签名和数据完整性验证; 具有灵活的密钥配置、支持集中式密钥与分布式密钥管理; 可有效防止虚假路由信息的接收与路由器的非法接入; 能够阻止非授权用户的访问等.
- (10) 数据归档与自毁^[13]. 定期对感知延伸层设备中的数据进行灾备, 并对不再使用或报废设备中的数据进行销毁, 防止敌手窃取信息.

综上所述, 感知延伸层的安全架构如图 2 所示.

4.2 海云网络传输层信息安全体系架构

海云网络传输层主要用于把感知延伸层收集到的信息安全可靠地传输到业务应用层, 然后根据不同的应用需求进行信息处理, 即网络传输层主要是网络基础设施, 包括互联网、移动通信网和一些专业网 (如国家电力专用网、广播电视网) 等. 在信息传输过程中, 可能经过一个或多个不同架构的网络进行信息交换, 由于每个网络架构的设施 and 标准不同, 这就增加了异构网之间信息传输的安全隐患.

4.2.1 网络传输层的安全挑战

对于海云网络传输层的安全挑战,除了存在传统网络攻击外,由于不同架构的网络需要相互连通,因此在跨网络架构的安全认证方面会面临更大的挑战.因此,除了信道窃听、数据流信息、密钥和隐私信息泄露等安全问题,海云网络传输层的安全挑战大致分为 3 类: DoS 攻击、DDoS 攻击等拒绝服务攻击;假冒攻击、中间人攻击等网络攻击;跨异构网络的攻击.

目前的互联网或下一代互联网将是海云网络传输层的核心载体,多数信息要经过互联网传输,因此互联网中的各种网络攻击威胁仍然存在,特别是 DoS 攻击和 DDoS 攻击,需要采用更好的防范措施和灾难恢复机制,减小网络攻击造成的损失.考虑到海云连接的终端设备性能和对网络需求的巨大差异,对网络攻击的防护能力也有很大差别,因此很难设计通用的安全方案,应针对不同网络性能和网络需求采取不同的防范措施.

4.2.2 网络传输层的安全需求

网络传输层中,异构网络的信息交互将成为安全性的脆弱点,特别是在网络认证方面,难免存在中间人攻击和其他类型的攻击(如异步攻击、合谋攻击等).这些攻击都需要有更高的安全防护措施.海云网络传输层的安全需求可概括为以下几个方面:

- (1) 数据的机密性.即保证数据在传输过程中不泄露其内容.
- (2) 数据的完整性.即保证数据在传输过程中不被非法篡改,或非法篡改的数据容易被检测出.
- (3) 数据流的机密性.某些应用场景需要对数据流量信息进行保密,防止敌手从中推测出有用信息,目前只能提供有限的数据流机密性.
- (4) 隐私信息的机密性.对于某些特殊应用需要考虑隐私泄露问题,特别是与个人绑定的手持终端或者用于军事、电力系统的感知设备和智能终端,在接入互联网时需要保持设备标识和用户身份的匿名性;传输路径和平台配置信息的机密性等.
- (5) 网络和节点的可用性. DDoS 攻击是网络中最常见的攻击现象,在海云网络环境中将更为突出.因此,需要对脆弱节点的 DDoS 攻击进行防护,保证节点和网络的可可用性.
- (6) 移动网中认证与密钥协商机制的一致性 or 兼容性.是指通信双方在完成相互认证的同时也完成了会话密钥的协商,这样可以提高通信效率,降低通信量和计算量.
- (7) 域内、网内节点的可认证性.是指同一安全域或者网络架构内部的节点通信之前需要进行相互认证,确定通信对方的身份,阻止非法节点接入.
- (8) 域间可认证性和异构网间可认证性.是指存在于两个不同安全域或网络架构的通信双方可以相互认证,这需要考虑不同域或网络架构中安全机制和策略的融合问题.

4.2.3 网络传输层的安全架构

网络传输层的安全机制可分为端到端的安全机制和节点到节点的安全机制.对于端到端的安全机制,需要建立端到端的认证机制、密钥协商机制、密钥管理机制和数据验证服务.对于节点到节点的安全机制,需要节点间的认证和密钥协商协议,这类协议需要重点考虑效率因素.对于跨网络架构的安全需求,需要建立不同网络环境的认证衔接机制.另外,根据业务应用层的不同需求,网络传输模式可能区分为单播通信、组播通信和广播通信,针对不同类型的通信模式也应该有相应的认证机制和机密性保护机制.简言之,网络传输层的安全机制主要包括以下几个方面:

(1) 可信接入^[14,15]与平台的远程证明^[16]. 无论是海端的感知设备或智能终端接入网络, 还是云端的计算平台接入网络都需要进行可信的远程证明过程. 通信双方的终端平台通过远程证明向对方平台证明自己拥有的属性, 使得平台的可信向网络进一步延伸, 从而防止运行恶意程序的终端接入网络窃取信息.

(2) 加密算法. 用于防止传输过程中数据被攻击者窃听和篡改, 保证数据传输 (无线/有线) 过程中的机密性.

(3) 消息验证. 包括消息的完整性验证和消息源的验证, 即发送方在发送消息前采用合适的密码技术对消息产生校验和或者签名, 使得消息的接收方能有效验证消息的完整性和来源. 对于节点到节点的情况, 消息验证应根据实际需要选择.

(4) 隐私保护. 对于隐私信息的保护需要针对保护内容的不同采用不同的安全技术, 例如对于设备标识信息的保护, 应采用匿名认证的方式; 对路由信息的保护, 应采用安全的、隐私保护的路由方式^[17]; 对平台属性配置信息的保护, 应采用的远程匿名证明^[16]的方式等.

(5) 网络攻击检测与防护. 采取相应的网络攻击检测方法对网络进行实时监控, 防止各种网络攻击, 包括各种 DOS 攻击, 确保网络中各级设备的可用性和数据的可达性.

(6) 密钥管理. 在认证的基础上完成密钥协商是建立会话密钥的必要步骤. 此外, 还需要保证密钥在产生、分发、存储、更新、销毁过程中的安全性.

(7) 域内节点认证和访问控制. 传输节点之间要进行身份认证和访问控制, 阻止非法用户和设备的接入和访问, 同时对各个设备进行读取控制, 限制它们的访问权限, 防止网络中的数据被未授权的用户访问.

(8) 跨域节点认证和访问控制^[18]. 需要考虑认证机制、访问控制策略和所采用的密码算法的融合或兼容的问题.

(9) 安全路由. 与感知延伸层类似. 采用 IPSec 协议、路由技术、VPN 技术、防火墙技术等, 达到任意两个节点之间安全通信的目的. 它的功能包含带有包过滤和代理协议的防火墙功能; 能够隐藏内部网络拓扑结构; 支持路由信息与 IP 数据包加密; 能够实现身份鉴别、数据签名和数据完整性验证; 具有灵活的密钥配置、支持集中式密钥与分布式密钥管理; 可有效防止虚假路由信息的接收与路由器的非法接入; 能够阻止非授权用户的访问等.

综上所述, 网络传输层的安全架构如图 3 所示.

4.3 海云业务应用层信息安全体系架构

海云业务应用层是对信息到达处理平台后, 根据不同的业务应用, 对信息进行处理, 然后为平台用户提供各种应用. 云计算平台是海云业务应用层的主要信息处理和提供应用服务的平台, 因此云计算的安全挑战也是海云业务应用层面临的主要安全挑战.

传统的访问控制、数据传输和存储加密、身份认证、系统安全加固、漏洞扫描、安全配置管理等机制都可以在一定程度上解决计算机和网络存在的安全问题, 但是云计算自身的特点为这些安全机制带来了新的挑战^[19~21].

(1) 庞大的用户群和海量的数据. 和传统的网络服务相比, 云计算服务的用户群非常庞大, 而且需要存储海量的数据. 这就为用户的身份认证、密钥管理、并发处理等方面带来了很大的挑战. 如何在大量并发的数据处理中还能够高效地完成数据的加解密、访问控制, 特别是用户的隔离、数据的隔离等等, 都是需要解决的问题.

图 3 网络传输层的安全架构

Figure 3 The security architecture of network layer

(2) 高性能和可靠的计算服务. 云计算环境中资源高度集中和多租户共享的特点, 导致资源的使用者和所有者分离, 为有效地控制资源的授权使用、确保云服务的可用性、可靠性提出了严峻的挑战, 亟需建立云服务可用性保障机理和可验证的安全机制.

(3) 可信保证. 云计算中的虚拟化技术对可信验证带来挑战. 可信计算技术可以保证用户身份的真实, 也可以保护数据的完整性. 但是在虚拟化环境中, 一些物理设备中不可变的属性会因为虚拟化的出现而变得容易修改. 例如在数据版权和保护的验证中, 有些数字内容的版权是通过传统计算机中的固定的硬件特征 (如 MAC 地址等) 进行保护. 如果这些特征发生变化, 受保护的数字内容将无法继续使用. 但是在虚拟化服务器中, 多个虚拟机共享一个实体机器, 每个虚拟机被分配到虚拟的硬件特征, 此特征是容易更动或是伪造的, 数字版权的保护将成为一大问题.

(4) 云的多种部署模式. 云服务有公有云、私有云、社区云和混合云等多种部署模式. 和私有云、社区云相比, 所有用户都可以使用公有云提供的服务. 因此一旦发生信息泄漏, 将会带来很严重的影响. 然而, 混合云面临的安全威胁更为严峻. 在混合云中, 私有云和公有云会通过某些机制联系在一起. 由于私有云服务于组织内部, 里面通常会保存组织内部的敏感数据. 私有云和公有云的结合, 不仅可能会使私有云中的敏感数据泄漏到公有云中, 还可能会导致公有云中的应用破坏私有云中数据的完整性. 这些现实问题都给云计算中的数据安全带来了挑战.

4.3.1 业务应用层的安全挑战

针对以上云计算模式下新的安全挑战, 以下列举了基于云计算的海云业务应用层可能遇到的安全问题 [22~24].

(1) 虚拟机自身的安全问题 [25]. 虚拟机技术将计算机物理资源表示成若干个虚拟域, 每个虚拟域

都可以运行独立的操作系统作为一台独立的计算机进行工作和对外提供服务. 虚拟机的体系结构本身可以增强虚拟域操作系统的安全性, 因为它对虚拟域中的应用是透明的, 这些运行在虚拟域中的应用程序通常无法发现自己运行在虚拟域环境中. 根据虚拟机的隔离机制, 一个虚拟域中的恶意程序不会影响到其他虚拟域, 也很难影响到虚拟机监控器和真实的硬件设备. 而且通过虚拟机架构中用于管理功能的特权域, 可以对其他虚拟域中的操作系统和应用程序进行监控和扫描. 这些都增强了虚拟域的安全性. 但是, 这种对安全增强的前提是虚拟机具有严格的隔离机制. BlackHat 在近几年提出了多种攻击 Xen 虚拟机监控器的方法^[26], 这些攻击都展示出虚拟机监控器的脆弱性和其安全系统的复杂性. 而事实上, 几乎所有的主流虚拟机都存在安全漏洞. 这就使得虚拟机安全和云计算安全成为空谈. 虚拟机体系结构带来的主要安全问题有: 虚拟机逃逸、特权域安全、虚拟机监控器安全、虚拟域的安全迁移、拒绝服务等.

(2) 操作系统安全漏洞^[27]. 用户接入云计算服务获得计算资源时, 会获得一个虚拟域的使用权限. 运行在虚拟域中的操作系统和真实的操作系统一样会存在自身的安全漏洞. 目前的云平台提供商提供的常见的虚拟域操作系统有包括 Windows, Linux 等在内的多个版本, 但是这些操作系统都存在安全漏洞. Microsoft 每个月都会为 Windows 发布多个安全补丁, 而 Linux 的内核也经常被报告存在安全漏洞. 在发布补丁或提出解决方案之后, 管理员需要及时修复系统漏洞. 而在补丁或解决方案在发布之前, 操作系统将处于危险状态.

(3) 共享虚拟化资源池安全问题^[28]. 云计算环境是多用户环境, 所有用户的数据都在云中存储和处理. 如果数据不能有效地隔离将会导致用户私人数据被其他用户盗取、篡改、破坏. 这就要求不同用户的数据必须做到严格的隔离, 防止用户读写他人的文件. 用户提交的计算作业首先被分配在共享虚拟化资源池中. 如果不能保证这些计算作业是由可信的用户提交到资源池, 将会导致资源池中的所有共享资源被盗取、篡改以及破坏的危险. 动态的资源在使用完毕或失效后需要立即销毁, 否则将会造成信息泄漏的危险.

(4) 数据丢失和数据不一致性. 在普通的计算机中, 磁盘的物理损坏可能会造成用户数据的丢失, 云存储也是如此. 用户的数据最终存放在存储介质中, 如果存储介质因为供电或使用寿命等原因造成物理损坏, 也会造成数据的丢失. 冗余机制和灾难备份机制可以在很大程度上保护用户的数据不会因为存储介质的损坏而丢失.

云存储的底层使用的是存储阵列, 用户的数据会被分块存储到不同的物理设备中, 并存在冗余备份. 同时考虑到灾难备份的机制, 数据还可能同时存储在外地的数据中心中. 当用户的数据更新后, 存在不同数据中心的数据可能不能即时同步. 如果同步时间过短又可能会增加网络负载. 这就要求需要通过版本控制对数据进行标记和保护, 防止发生数据的不一致性.

(5) 网络攻击. 传统的网络安全只专注在实体网络环境的防护, 但是在云计算和虚拟化的背景下, 虚拟的网络也会带来很多的安全问题. 而传统的网络安全问题在云计算中依然存在.

虚拟网络中的攻击. 不同的虚拟机有不同的虚拟网络实现机制. 有的虚拟机中, 不同虚拟域使用各自独立的网络接口, 这就可以根据安全级的不同做到隔离. 有的虚拟机中, 多个虚拟域共享网络接口, 当数据包到达虚拟机后, 虚拟机再根据数据包的头部信息进行转发. 软件实现的虚拟交换机或集线器的设计或实现的缺陷会使数据包嗅探成为可能, 一个虚拟域将能够获取其他虚拟域的网络数据包. 传统实体主机的对外传输封包需离开主机本体, 因此可通过位于外部的网络安全设备对封包内容进行安全检查. 而虚拟化架构下的网络缺乏传统实体主机的网络安全防护机制. 在虚拟网络中, 虚拟机之间的流量并未被任何的网络安全设备检查, 而直接通过虚拟机内部的虚拟交换机、虚拟集线器进行转发或传播, 因此虚拟机间的攻击、入侵将无法通过外部的网关进行检查和拦截, 因此也很难避免虚拟机

间蠕虫的快速扩散。

拒绝服务攻击. 和虚拟机安全问题中提到的拒绝服务攻击不同, 拒绝服务攻击不仅可以攻击具体的一个虚拟机, 也可以对云计算平台提供商的网络进行攻击, 造成云计算服务的网络瘫痪. 拒绝服务攻击也可以针对一些具体的应用, 例如, 如果云计算服务的用户身份认证服务器被攻击, 虽然用户的虚拟机依然能够运行, 但是用户却因为无法通过身份认证而无法正常使用、维护和使用. 这就要求云计算服务必须能够抵御拒绝服务攻击, 维护正常的服务。

(6) 信道窃听. 云计算是面向是公众的服务, 因此很容易发生假冒、窃听等黑客攻击行为. 即使云计算平台提供商自身提供的服务是安全的, 用户使用的计算终端也是安全的, 但是由于通信的信道很容易被窃听, 传输的数据包可能会被非法篡改, 使用户和云计算平台提供商接收到的数据的机密性和完整性受到破坏. 通过建立安全信道可以避免这样的安全威胁. 在用户和云计算平台提供商建立连接的时候, 双方需要互相确认身份, 并在此基础上协商会话密钥. 之后的通讯数据将通过密钥加密, 防止窃听和篡改的发生。

(7) 密钥、密码的丢失和泄露. 用户使用云计算服务时, 需要通过身份认证才能登录到云平台中进行管理和设置. 如果用户的密码被攻击者获取, 那么攻击者就可以登录进入云平台获取用户的敏感信息和破坏用户的数据. 而如果系统管理员的密码被泄露, 则可能会影响到云计算平台中所有用户的数据. 如果密钥被泄露, 那么通过密钥加密的数据也会被泄露. 虽然目前的动态口令、证书等机制能够在一定程度上保证用户的安全登录, 但是现在依然有很多钓鱼网站能够诱导一些用户泄露个人信息 (如网络银行的密码、动态口令等)。

(8) 云计算 API 的安全问题. 云计算提供的服务主要有 IaaS, PaaS 和 SaaS 等. 普通用户使用最多的是 SaaS, 而这些 SaaS 应用服务都是基于云计算平台 API 进行开发的. 而对于其他的 service 形式, 用户也需要使用云计算平台 API 进行管理和交互. 如果这些 API 存在漏洞, 或者使用这些 API 进行开发的软件存在漏洞, 同样会导致数据的泄露或者破坏. 因此, 这些 API 接口的设计必须能够防御意外和恶意企图的政策规避行为, 以确保强用户认证、加密和访问控制的有效。

(9) 云服务的可靠性问题. 云计算环境下, 各种软、硬件资源以服务的形式提供给用户, 这种资源的所有权和控制权分离的特点, 导致云服务提供商对资源的控制和管理更加困难, 租户的隐私信息更容易泄露. 因此, 需要有效地控制租户对资源的使用、保证云服务的可用性、可靠性的机制, 同时保护服务过程中用户隐私信息。

(10) 云计算安全中的其他问题. 除了前面提到的技术类问题之外, 还有一些云计算安全涉及的非技术类问题, 例如云计算的标准、平台的监管等等。

云计算领域发展速度非常迅猛, 但是相关的测评体系、技术标准却并不完善, 这就给云计算服务的统一带来很大的困难. 要实现云安全软硬件的标准化, 就必须建立相关的质量体系、测评指标和标准规范. 我国已经启动了关于云计算的一些标准 (如: 《云计算参考架构》^[29]、《云计算数据中心参考架构》^[30] 等) 的起草工作, 但是关于云计算安全方面的标准依然空缺。

云计算的模式使得平台提供商的权利巨大, 用户很难进行监督, 这就导致用户的权利难以得到保证. 确保和维护两者之间平衡, 不仅需要技术手段, 还需要有国家级的监管和第三方审计. 当缺乏对云供应商程序和流程认识的时候, 恶意内部人员的风险就会加剧. 企业应该了解供应商的信息安全和管理政策, 强迫其使用严格的供应链管理以及加强与供应商的紧密合作. 同时, 还应在法律合同中对工作要求有明确的指定说明, 以规范云计算运营商处理用户数据等这些隐蔽的过程。

4.3.2 业务应用层的安全需求

基于云计算的海云业务应用层的安全需求可主要归纳为以下几点:

(1) 云平台的可靠性. 可靠性是指系统能够安全可靠运行的一种特性, 即系统在接收、处理、存储和使用信息的过程中, 当受到自然和人为危害时所受到的影响. 系统的高可靠性是云计算系统设计的基本要求. Google 电子邮件服务中断、微软云计算平台 Windows Azure 运行中断、亚马逊的“简单存储服务”(simple storage service, S3) 中断等问题都可以归结为是云计算系统可靠性设计的不足造成的.

(2) 云服务的可用性. 可用性指授权个体可访问并使用其有权使用的信息的特性. 安全的云计算系统应允许授权用户使用云计算服务, 并在系统部分受损或需要降级使用时, 仍能为授权用户提供有效的服务. 为保证云计算平台可用性的需求, 涉及的安全机制包括标识与认证、访问控制、数据流控制和审计等.

(3) 云服务的可靠性. 服务的可靠性是指, 云计算平台忠实地执行租户的计算指令, 以及返回正确的计算结果. 云服务提供商应该有充足的证据让租户确信云端提供或使用的软件正确可靠的得到了运行, 租户的要求被正确执行. 云服务的可靠性问题可以使用审计、可信计算和可验证计算等技术来保证.

(4) 数据的机密性. 机密性要求信息不被泄露给非授权的用户、实体或供其利用. 为保证云计算平台中数据的机密性, 首先要加强对相关人员的管理. 其次, 利用密码技术对数据进行处理. 此外, 云平台设施要能够防侦听、防辐射, 并要利用限制、隔离、掩蔽、控制等措施保护数据不被泄露.

(5) 数据的完整性. 完整性是指系统内信息在传输过程中不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等以造成破坏和丢失的特性. 为保证存储、传输、处理数据的完整性, 可采用分级存储、密码校验、纠错编码、安全协议等方法.

(6) 不可抵赖性. 不可抵赖性也可称作不可否认性, 指在信息交互过程中, 明确厂商及用户的真实同一性, 任何人都不能否认或抵赖曾经完成的操作和承诺. 由于云计算制度的不完善, 云提供厂商和用户之间可能会在非技术层面产生各种纠纷, 对此, 云计算平台可以通过可信第三方机构来协调供应商和用户之间的业务, 并可利用密码技术来防止发送方和接收方事后否认已发送或接收的信息.

(7) 可控性. 可控性指系统对其数据应具有控制能力. 云计算平台应对服务或数据传播的内容、速度、范围、方式等进行有效控制, 以增加系统的扩展性、有效性和容错能力.

4.3.3 业务应用层的安全架构

基于云计算的海云应用面临的信息安全问题主要包括两个方面, 一是云计算服务自身存在的安全隐患; 二是通过云计算为客户及其具体应用提供服务时的安全隐患, 涉及访问控制、权限管理、数据隔离、数据恢复、计算可靠性验证以及第三方审计、法律法规等各方面. 因此, 必须针对云计算平台提出科学的安全策略, 保证云计算安全和服务应用安全.

(1) 通过风险评估建立公有云和私有云. 云端的安全防护不同于一般系统的防护, 海云用户在使用云计算中的服务之前应该对海云数据和应用服务风险进行评估分析, 根据评估结果划分出公有云和私有云, 并根据服务的重要性划分安全等级.

(2) 建立可信云^[31,32]. 使用可信计算技术建立企业可信云. 可信计算是由可信模块到操作系统内核层, 再到应用层依次建立信任关系, 并在此基础上, 扩展到网络中建立信任链. 通过对系统启动过程中可执行文件的验证, 来阻止病毒和木马的入侵. 在云计算平台中同样可以通过可信模块建立从硬件到软件, 再到云应用的可信链, 从而建立可信的云计算平台.

图 4 基于云计算平台的业务应用层安全架构
Figure 4 The security architecture of cloud-based application layer

- (3) 安全认证. 安全认证可采用单点登录认证 [33]、强制用户认证、代理、协同认证、资源认证、不同安全域之间的认证或者不同认证方式相结合的方式. 对于用户的认证应采用强制用户认证和单点用户认证相结合的方式允许用户进入云应用的, 这样可以防止用户在使用自己的服务时将密码泄露给第三方.
- (4) 数据加密及相应的密码机制. 数据的机密性是云计算安全的基本要素之一. 而数据的机密性主要通过加密的方式来保证. 无论是用户还是存储服务提供商, 都要对文件数据进行加密, 这样既保证文件的隐私性, 又可以进行数据隔离. 但是, 在确保了用户数据安全的同时, 还需要提供其他的密码机制以保证密文数据的可用性. 涉及的密码技术包括: 可搜索加密 [34,35]、同态加密 [36]、属性加密 [37,38]、谓词加密 [39] 等.
- (5) 建立云服务可用性保障机理和可验证的安全机制. 可靠性和可用性是云计算平台高质量服务的基础. 云服务提供商应该有充足的证据让租户确信所要求的服务和计算被正确执行. 此外, 还要保证服务随时随地在线, 业务连续运行和随租随用的便利. 这方面需要的安全技术包括: 计算可靠性验证 [40,41]、分析检测方法 [42]、系统分析恢复方法 [43] 和系统安全加固 [44] 等.
- (6) 访问权限控制 [45,46]. 云计算服务提供商应该对不同级别的用户提供不同的访问权限, 以防止高安全级别的数据被低安全级别的用户访问.

综上所述, 基于云计算平台的海云业务应用层的安全架构如图 4 所示.

4.4 海云安全体系参考模型

综合以上对海云三层体系结构的分析, 海云安全体系参考模型如图 5 所示. 感知延伸层的安全机制需要针对海端节点和网络设备的多样性和移动性, 及其计算和存储能力的限制采用合理的安全技术. 网络传输层的安全机制需要区分不同的网络架构, 针对不同的传输方式提出防范网络攻击特别是 DoS 攻击的方法. 此外, 异构网络之间的互认证和安全机制的融合也是考虑的重点. 业务应用层的安全机制应主要针对云计算的特点带来的安全问题, 提出相应的安全机制和解决方案.

图 5 海云安全体系参考模型
Figure 5 The reference model of sea-cloud security architecture

密码技术是保证系统机密性、完整性和可用性的基本安全技术, 包括密码算法、密码协议和其他密码机制. 但是密码技术的使用会增加系统的计算量和存储量, 因此在提出安全策略时, 需要根据系统设备的特点, 权衡安全技术和系统效率之间的关系. 由于海端大多数设备都使用电池供电, 且计算、存储和通信能力有限, 因此对于海端设备和网络应采用轻量级的密码算法和密码协议, 例如, 对称加密算法、消息验证码等, 来保护其安全性. 而对于云端的设备具有较高的计算性能、存储能力和通信带

宽, 因此可采用较复杂的密码算法和密码协议, 例如, 公钥加密算法、基于证书的远程证明协议等, 来保障云端数据和服务的安全性.

海云信息安全体系结构是一个“三纵五横”的结构, “三纵”分别是海、网、云 3 部分基础架构; “五横”从底至上分别是物理安全、系统安全、网络安全、应用安全和数据安全. 此外, 为了保证海云环境的安全运行, 除了提出这 5 层安全体系外, 还需要对海云制定安全管理标准, 并按照制定的标准建立、运行和维护海云环境.

5 总结

本文首先对海云的定义、组成部分、特点以及参考模型等方面作了详细的介绍, 然后深入分析了在新的网络环境下海云面临的安全挑战, 最后给出了每一层的安全体系架构和海云总体安全体系架构, 以期能为海云创新试验环境的构建提供安全参考.

由于篇幅限制, 这里并未对构建海云安全体系架构所涉及的各种安全技术做详细介绍, 有兴趣的读者可以参考文后列出的相关参考文献.

参考文献

- 1 Feng D G, Sun R, Zhang Y. Information Security Architecture. Beijing: Tsinghua University Press, 2008. 1–9 [冯登国, 孙锐, 张阳. 信息安全体系结构. 北京: 清华大学出版社, 2008. 1–9]
- 2 Mell P, Grance T. The NIST definition of cloud computing. 2011
- 3 Deering S, Hinden R. Internet protocol, Version 6 (IPv6) specification. RFC 2460, 1998
- 4 Pathan A, Lee H, Hong C. Security in wireless sensor networks: issues and challenges. In: Proceedings of the 8th International Conference of Advanced Communication Technology, Phoenix Park, 2006. 1043–1048
- 5 Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks. Commun ACM Wirel Sens Netw, 2004, 47: 53–57
- 6 Feng D G. Trusted Computing: Theory and Practice. Beijing: Tsinghua University Press, 2013 [冯登国. 可信计算——理论与实践. 北京: 清华大学出版社, 2013]
- 7 ISO/IEC. Information Technology-Security Techniques-Message Authentication Codes (MACs)-Part 1: Mechanisms Using a Block Cipher. ISO/IEC 9797-1, 2011
- 8 ISO/IEC. Information Technology-Security Techniques-Message Authentication Codes (MACs)-Part 2: Mechanisms Using a Dedicated Hash-Function. ISO/IEC 9797-2, 2011
- 9 Barker E, Smid M, Branstad D, et al. A framework for designing cryptographic key management systems. NIST Spec Publ, 2013, 800: 130
- 10 Shen C X. Introduction to Information Security. Beijing: Publishing House of Electronics Industry, 2009. 124–129 [沈昌祥. 信息安全导论. 北京: 电子工业出版社, 2009. 124–129]
- 11 Qing S H, Jiang J C, Ma H T, et al. Research on intrusion detection techniques: a survey. J China Inst Commun, 2004, 25: 19–29 [卿斯汉, 蒋建春, 马恒太, 等. 入侵检测技术研究综述. 通信学报, 2004, 25: 19–29]
- 12 Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Netw, 2003, 1: 293–315
- 13 Geambasu R, Kohno T, Levy A, et al. Vanish: increasing data privacy with self-destructing data. In: Proceedings of the 18th Conference on USENIX Security Symposium, Montreal, 2009. 299–316
- 14 TCG. Trusted network connect TNC architecture for interoperability. Specification Version 1.5 Revision 3. 2012
- 15 The State Standard of the People's Republic of China: Information security technology—trusted computing specification—trusted connect architecture. GB/T 29828-2013, 2013 [中华人民共和国国家标准: 信息安全技术·可信计算规范·可信连接架构. GB/T 29828-2013, 2013]
- 16 Brickell E, Camenisch J, Chen L. Direct anonymous attestation. In: Proceedings of ACM Conference on Computer and Communications Security, Washington, 2004. 132–145

- 17 Al-Muhtadi J, Campbell R, Kapadia A, et al. Routing through the mist: privacy preserving communication in ubiquitous computing environments. In: Proceedings of 22nd International Conference on Distributed Computing Systems, Vienna, 2002. 74–83
- 18 Chen Y, Yang S B, Guo L T, et al. A dynamic access control scheme across multi-domains in grid environment. *J Comput Res Dev*, 2006, 11: 1863–1869 [陈颖, 杨寿保, 郭磊涛, 等. 网格环境下的一种动态跨域访问控制策略. *计算机研究与发展*, 2006, 11: 1863–1869]
- 19 Armbrust M, Fox A, Griffith R, et al. A view of cloud computing. *Commun ACM*, 2010, 53: 50–58
- 20 Chen Y, Paxson V, Katz R H. What's New About Cloud Computing Security? Technical Report No. UCB/EECS-2010-5, 2010
- 21 Takabi H, Joshi J, Gail-Joon A. Security and privacy challenges in cloud computing environments. *IEEE Secur Priv*, 2010, 8: 24–31
- 22 Feng D G, Zhang M, Zhang Y, et al. Study on cloud computing security. *J Softw*, 2011, 22: 71–83 [冯登国, 张敏, 张妍, 等. 云计算安全研究. *软件学报*, 2011, 22: 71–83]
- 23 Lin Z Y, Lai Y X, Lin C, et al. Research on cloud databases. *J Softw*, 2012, 23: 1148–1166 [林子雨, 赖永炫, 林琛, 等. 云数据库研究. *软件学报*, 2012, 23: 1148–1166]
- 24 Hwang K, Fox G, Dongarra J, Wu Y W, Qin Z Y, Li Z Y, et al. Translate. Distributed and Cloud Computing: From Parallel Processing to the Internet of Things. Beijing: China Machine Press, 2013. 88–123 [Hwang K, Fox G, Dongarra J. 武永卫, 秦中元, 李振宇, 等译. 云计算与分布式系统 —— 从并行处理到物联网. 北京: 机械工业出版社, 2013. 88–123]
- 25 Pearce M, Zeadally S, Hunt R. Virtualization: issues, security threats, and solutions. *J ACM Comput Surv*, 2013, 45: 17
- 26 Wojtczuk R. Subverting the Xen hypervisor. Black Hat USA, 2008
- 27 Silberschatz A, Galvin P B, Gagne G. Operating System Concepts. 9th ed. Chapter 15 Security. Hoboken: Wiley, 2012. 657–704
- 28 Scarfone K, Souppaya M, Hoffman P. Guide to security for full virtualization technologies. NIST Spec Publ, 2011, 800–125
- 29 Cloud Computing Standards Working Group. Information Technology-Cloud Computing-Reference Architecture. No. 20121421-T-469, 2012 [云计算标准工作组. 云计算参考架构. 计划号: 20121421-T-469, 2012]
- 30 Cloud Computing Standards Working Group. Information Technology-Cloud Computing-Data Center-Reference Architecture. No. 20120571-T-469, 2012 [云计算标准工作组. 云计算数据中心参考架构. 计划号: 20120571-T-469, 2012]
- 31 Santos N, Gummadi K, Rodrigues R. Towards trusted cloud computing. In: Proceedings of HotCloud'09, San Diego, 2009
- 32 Hwang K, Li D. Trusted cloud computing with secure resources and data coloring. *IEEE Internet Comput*, 2010, 14: 14–22
- 33 Wang R, Chen S, Wang X. Signing me onto your accounts through facebook and google: a traffic-guided security study of commercially deployed single-sign-on web services. In: Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, 2012. 365–379
- 34 Song D, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proceedings of IEEE Symposium on Security and Privacy, Berkeley, 2000. 44–55
- 35 Boneh D, Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search. *Adv Cryptol Eurocrypt*, 2004, 3027: 506–522
- 36 Gentry C. Fully homomorphic encryption using ideal lattices. In: Proceedings of STOC'09, Bethesda, 2009. 169–178
- 37 Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of ACM CCS 2006, Alexandria, 2006. 89–98
- 38 Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: Proceedings of IEEE SP'07, Oakland, 2007. 321–334
- 39 Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Proceedings of EUROCRYPT'08, Istanbul, 2008. 146–162
- 40 Goldwasser S, Kalai Y, Rothblum G. Delegating computation: interactive proofs for muggles. In: Proceedings of the

- ACM Symposium on the Theory of Computing (STOC'08), Victoria, 2008. 113–122
- 41 Gennaro R, Gentry C, Parno B. Non-interactive verifiable computation: outsourcing computation to untrusted workers. In: Proceedings of CRYPTO, Santa Barbara, 2010. 465–482
  - 42 Payne B, Carbone M, Sharif M, et al. Lares: an architecture for secure active monitoring using virtualization. In: Proceedings of IEEE Symposium on Security and Privacy (Oakland'08), Oakland, 2008. 233–247
  - 43 Prabhakaran V, Arpaci-Dusseau A, Arpaci-Dusseau R. Analysis and evolution of journaling file systems. In: Proceedings of the Annual Conference on USENIX Annual Technical Conference (USENIX'05), Anaheim, 2005. 8
  - 44 Sharif M, Lee W, Cui W, et al. Secure in-VM monitoring using hardware virtualization. In: Proceedings of ACM CCS 2009, Chicago, 2009. 477–487
  - 45 Zhu Y, Hu H, Ahn G, et al. Towards temporal access control in cloud computing. In: Proceedings of IEEE INFOCOM'12, Orlando, 2012. 2576–2580
  - 46 Younis Y, Kifayat K, Merabti M. An access control model for cloud computing. J Inform Secur Appl, 2014, 19: 45–60

Security architecture of sea-cloud

ZHANG Rui*, XUE Rui & LIN DongDai

State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

*E-mail: zhangrui@iie.ac.cn

Abstract The processing of information in the 21st century is moving towards a consolidation of human society (human), information networks (cyber), and the physical world (physical) completely fused with total and absolute form and unprecedented speed, depth, and breadth. This supports the trend towards a novel combination and the usage patterns of sensing and human-computer interaction terminals (sea), new network technology (network), and cloud computing (cloud). Seizing the trend and opportunity of the ternary integration of human-cyber-physical, establishing and developing the new generation of information technology architecture of sea-cloud collaborative computing, and ultimately realizing the goal of sensing China, has become an urgent demand for the new generation of IT development. However, the stable operation of any information system requires the establishment of an information security architecture. The security architecture of an information system is directly related to the influence of a security policy and affects the function and operation of the systems. Therefore, building the security architecture of sea-cloud based on the complex environments of the ternary integration of human-cyber-physical is a critical prerequisite and foundation for guaranteeing stable operation of a sea-cloud innovative experimental environment. This paper first introduces the concept of sea-cloud and then analyzes the security challenges and requirements that each layer of sea-cloud faces based on the proposed information architecture. Finally, we build a security architecture for sea-cloud to provide an important theoretical basis and technical support for establishing a sea-cloud innovative experimental environment.

Keywords sea-cloud, information security architecture, ternary integration of human-cyber-physical, convergence of heterogeneous network, security technology

ZHANG Rui was born in 1981. She received a Ph.D. degree in Information Security from Beijing Jiaotong University, Beijing in 2011. She is now an assistant researcher at the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences. Her research interests include cloud data security, privacy preservation, and security protocols

XUE Rui was born in 1963. He received a Ph.D. degree in Mathematics from Beijing Normal University, Beijing in 1999. Currently, he is a senior researcher at the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences. His research interests include information security, cryptography, and security protocols. He has published more than a hundred papers. Dr. Xue is a member of IEEE, ACM, CACR, and CCF. He is currently serving as the Vice Chairman of the Security Protocols branch of CACR.

LIN DongDai received his M.S. and Ph.D. degrees in fundamental mathematics from the Institute of Systems Science, Chinese Academy of Sciences in 1987 and 1990, respectively. He was an associate professor from 1993 to 1998 and a professor from 1998 to 2001 at the Institute of Systems Science. He was also a professor from 2001 to 2011 at the Institute of Software, Chinese Academy of Sciences. He is currently a professor at the Institute of Information Engineering of the Chinese Academy of Sciences and the Director of the State Key Laboratory of Information Security. His research interests include cryptology, security protocols, symbolic computation, and software development. He is currently working on multivariate public key cryptography, sequences and stream cipher, zero knowledge proof, and network-based cryptographic computation.